COMUNE DI
SAN BENEDETTO VAL DI SAMBRO

CITTA' METROPOLITANA DI BOLOGNA

DELIBERAZIONE **N. 70**

O R I G I N A L E

VERBALE DI DELIBERAZIONE DELLA
GIUNTA COMUNALE

Oggetto: **REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI - APPROVAZIONE MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E MODELLO GESTIONE INCIDENTI DI SICUREZZA (DATA BREACH).**

Addì **VENTINOVE GIUGNO DUEMILADICIOTTO,** alle ore **18:00** nella Casa Comunale.

Previa l'osservanza di tutte le formalità prescritte dalla vigente legislazione, vennero oggi convocati i componenti la Giunta Comunale.

All'appello risultano:

1)	***SANTONI ALESSANDRO***	***- Sindaco***	***Assente***
2)	***STEFANINI PAOLA***	***- Vicesindaco***	***Presente***
3)	***MONCIATTI GABRIELE***	***- Assessore***	***Presente***
4)	***BORELLI PIERLUIGI***	***- Assessore***	***Presente***
5)	***NIVAZZI FRANCESCA***	***- Assessore***	***Assente***

Partecipa il SEGRETARIO COMUNALE, **BONANNI MARCELLA,** il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti, **RAG. STEFANINI PAOLA - VICESINDACO,** assume la Presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato.

OGGETTO:
Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - Approvazione modello organizzativo in materia di protezione dei dati personali e modello gestione incidenti di sicurezza (data breach).

LA GIUNTA COMUNALE

PREMESSO:

- che il 25 maggio 2018 è entrato in vigore 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 (di seguito Regolamento) il quale ha abrogato la direttiva 95/46/CE (di seguito "RGPD");
- che il RGPD detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni;
- che le disposizioni del D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali", nonché i provvedimenti di carattere generale emanati dal Garante per la protezione dei dati personali (di seguito "Garante"), continuano a trovare applicazione nella misura in cui non siano in contrasto con la normativa succitata, ed è previsto comunque l'adeguamento della normativa nazionale alle disposizioni del Regolamento;

CONSIDERATO:

- che per dare attuazione ai suddetti obblighi ed adempimenti, occorre rivedere l'assetto delle responsabilità tenuto conto della specifica organizzazione dell'Ente;
- che il RGPD individua diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:
  1. il Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
  2. i Soggetti Delegati attuatori: attuatori degli adempimenti necessari per la conformità dei trattamenti dei dati effettuati dall'Ente in esecuzione del Regolamento;
  3. il Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
  4. il Responsabile della protezione dei dati (di seguito anche Data Protection Officer o DPO): figura prevista dagli artt. 37 e ss. del regolamento, che ne disciplinano compiti, funzioni e responsabilità;
  5. l'Incaricato autorizzato al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile: figura che si desume implicitamente dalla definizione di "terzo" di cui al n. 10 del comma 1 art. 4 del Regolamento.

RICORDATO che con propria precedente deliberazione n. 54 del 25.05.2018 si stabiliva:

- di avvalersi della facoltà, prevista dall'art. 37, paragrafo 3, del Regolamento e di procedere alla nomina condivisa di uno stesso RPD (DPO) con l'Unione dei Comuni dell'Appennino Bolognese ed i Comuni aderenti;
- che l'Unione avrebbe provveduto alla designazione del RDP nell'ambito dei servizi GDPR conferiti a LEPIDA S. p.A.;

RICHIAMATO il Decreto Sindacale n. 3/2018 (agli atti con il prot. n. 3923/2018), con il quale, in esecuzione della sopra citata deliberazione, la società Lepida S.p.A. veniva designata Responsabile della Protezione dei dati personali (RPD) per il Comune di San Benedetto Val di Sambro;

RITENUTO, pertanto, necessario definire l'assetto organizzativo interno, per consentire l'attuazione degli obblighi derivanti dalla normativa in oggetto, approvando i seguenti documenti:

1. Modello organizzativo in materia di protezione dei dati personali;
2. Informativa per il trattamento dei dati personali, ai sensi dell'art 13 del RGPD;
3. Modello di gestione incidenti di sicurezza (data breach);

ACQUISITO il parere favorevole in ordine alla regolarità tecnica del Segretario Comunale, ai sensi degli artt. 49 co.1 e 147-bis del D.Lgs. n. 267/2000);

VERIFICATO che il presente provvedimento non comporta effetti diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'Ente, e dunque non necessita di parere di regolarità contabile;

Con voti favorevoli unanimi, resi ed accertati nelle forme di legge,

DELIBERA

per quanto indicato in premessa, che qui si intende recepito e confermato:

1) **DI APPROVARE**, in attuazione degli obblighi e degli adempimenti di cui al RGPD, entrato in vigore il 25 maggio u.s., i seguenti documenti:

- Modello organizzativo in materia di protezione dei dati personali;
- Informativa per il trattamento dei dati personali ai sensi dell'art 13 del RGPD;
- Modello di gestione incidenti di sicurezza (data breach);

nei testi che si allegano alla presente deliberazione, per farne parte integrante e sostanziale;

2) **DI PUBBLICARE** i documenti sul sito istituzionale, alla Sezione: Amministrazione Trasparente/Altri contenuti/Trattamento dei dati personali;

3) **DI DICHIARARE**, con separata votazione unanime, resa ed accertata nelle forme di legge, la presente deliberazione **IMMEDIATAMENTE ESEGUIBILE**, stante l'urgenza di provvedere, ai sensi dell'art. 134 - 4° co. del d.lgs. n. 267/2000.

COMUNE DI SAN BENEDETTO VAL DI SAMBRO

(Città metropolitana di Bologna)

Via Roma, n. 39 - 40048 San Benedetto Val di Sambro (BO)
Tel: 0534/95026 → int. 117 - C.F. 80014530374
PEC:comune.sanbenedettovaldisambro@cert.provincia.bo.it
e-mail: segretario@comune.sanbenedettovaldisambro.bo.it

MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Indice generale

Indirizzi generali 2

Il titolare 2
I responsabili del trattamento 4
Responsabile competente in materia di sistemi informativi 4
I responsabili del trattamento esterni 5
Gli incaricati .....

Il Responsabile della Protezione dei dati (DPO) 6
Pareri del DPO 6
Pareri obbligatori 6
Pareri facoltativi 7
Il Servizio ICT competente 7
Il Gruppo dei referenti privacy 8
Accesso civico generalizzato e ruolo DPO 9

Indirizzi generali

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 anche solo "Regolamento") detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni.
Le disposizioni del D.lgs. n. 196/2003 "Codice in materia di protezione dei dati personali", nonché i Provvedimenti di carattere generale emanati dal Garante per la protezione dei dati personali (di seguito anche solo "Garante"), continuano a trovare applicazione nella misura in cui non siano in contrasto con la normativa succitata. Si evidenzia che è previsto comunque l'adeguamento della normativa nazionale alle disposizioni del Regolamento.

Per dare attuazione ai suddetti obblighi ed adempimenti, occorre rivedere l'assetto delle responsabilità tenuto conto della specifica organizzazione dell'Ente Unione dei Comuni dell'appennino bolognese.

Il regolamento europeo individua diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:
il titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

il responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

il Responsabile della protezione dei dati (di seguito anche Data Protection Officer o DPO): figura prevista dagli artt. 37 e ss. del regolamento, che ne disciplinano compiti, funzioni e responsabilità;

persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile: figura che si desume implicitamente dalla definizione di "terzo" di cui al n. 10 del comma 1 art. 4 del Regolamento.

Con il presente documento l'Ente definisce il proprio ambito di titolarità, definisce i criteri generali da rispettare nell'individuazione dei soggetti autorizzati a compiere le operazioni di trattamento, delineando il complessivo ambito delle responsabilità, come sintetizzato nello schema di seguito riportato.

Il titolare

Titolare dei trattamenti di dati personali, ai sensi dell'art. 4 n. 7 e art. 24 del Regolamento, è l'Ente cui spetta l'adozione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento. Spetta pertanto in particolare all'Ente:
adottare, nelle forme previste dal proprio ordinamento, gli interventi normativi necessari, anche con riferimento alle disposizioni del Codice per la protezione dei dati personali oggetto di prossimo adeguamento al Regolamento;

- designare il Responsabile della protezione dei dati;
- designare eventualmente i soggetti delegati all'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;
- effettuare, a mezzo della struttura competente, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il DPO designato;
- verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;
- disporre, in conseguenza alla verifica di cui alla lett. a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
- adottare soluzioni di privacy by design e by default;
- tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza;
- predisporre le informative relative al trattamento dei dati personali nel rispetto dell'art.13 del Regolamento;
- individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "incaricati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento ed, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;
- predisporre ogni adempimento organizzativo necessario per garantire agli interessati

l'esercizio dei diritti previsti dalla normativa;

- provvedere, anche tramite gli incaricati, a dare riscontro alle istanze degli interessati inerenti l'esercizio dei diritti previsti dalla normativa;
- disporre l'adozione dei provvedimenti imposti dal Garante;
- collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
- adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri Soggetti delegati all'attuazione, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla propria area di competenza;
- individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
- garantire al Responsabile del Servizio competente in materia di sistemi informativi e al DPO i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
- designare gli amministratori di sistema in aderenza alle norme vigenti in materia;
- effettuare preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- consultare il Garante, in aderenza all'art. 36 del Regolamento e nelle modalità previste dal par. 3.1 lett b), nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenta un rischio residuale elevato;
- richiamare obbligatoriamente nei contratti di sviluppo di software e piattaforme, la policy in materia di sviluppo delle applicazioni, disponendo che il mancato rispetto dei requisiti ivi previsti equivale a grave inadempimento, con facoltà per l'Ente di risoluzione del contratto;
- designare i Responsabili del trattamento.

Nello svolgimento dei predetti compiti il Titolare del trattamento è coadiuvato dal Segretario/Direttore generale.
Relativamente ai trattamenti di dati personali trasversali a più strutture si applica il criterio della prevalenza.

I responsabili del trattamento

Ai fini dell'effettuazione del trattamento, in qualità di soggetti che presentano le garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate sono individuati responsabili del trattamento i titolari di posizione organizzativa dell'Ente quali responsabili delle strutture apicali dello stesso. I trattamenti da parte del Responsabile del trattamento sono autorizzati e disciplinati dall'atto di incarico, in relazione ai profili funzionali di competenza di ciascuna articolazione organizzativa dell'Ente, come individuati nel registro dei trattamenti consultabile all'indirizzo *https://recorder.lepida.it,* in corso di implementazione.
Sono delegati ai titolari di posizione organizzativa in qualità di Responsabili del trattamento i compiti di cui alle lettere: E F G H J K L O P Q S U
Nell'attuazione dei compiti sopraindicati i soggetti delegati possono acquisire il parere del DPO nei casi e con le modalità specificate nel seguito.

Responsabile competente in materia di sistemi informativi

Al Responsabile competente in materia di sistemi informativi spetta, inoltre:
l'adozione di policy in materia di privacy e sicurezza informatica, con particolare riferimento all'utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario;

- la sottoscrizione degli atti di notifica e di consultazione preventiva al Garante;
- la notifica e la comunicazione delle violazioni dei dati personali all'autorità di controllo ai sensi degli artt. 33 e 34 del Regolamento.

I responsabili del trattamento esterni

Sono designati responsabili del trattamento di dati personali anche i soggetti esterni all'amministrazione che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, o altro atto comunque denominato, ad effettuare trattamenti di dati personali per conto del titolare.
Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.
Attesa la natura negoziale delle designazioni dei responsabili del trattamento, questa deve essere effettuata all'interno di contratti o convenzioni e, in ogni caso, in costanza di formazione del rapporto contrattuale, in aderenza ai fac-simili messi a disposizione dalla struttura competente in materia di privacy.

Gli incaricati

Sono autorizzati al compimento alle operazioni di trattamento dei dati i soggetti delegati attuatori di cui al precedente paragrafo ed i soggetti da loro delegati ai sensi della presente disciplina, che conformano i loro trattamenti alle policy in materia di protezione dei dati personali e alle istruzioni di seguito riportate:
sono trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- sono verificati legittimità e correttezza dei trattamenti, verificando, in particolare, i rischi che gli stessi presentano e la natura dei dati personali da proteggere.

Sono, altresì, autorizzati tutti i soggetti che effettuino operazioni di trattamento, dipendenti e collaboratori a qualsiasi titolo e che operano sotto la diretta autorità del Titolare o dei Responsabili.
Tali soggetti sono da questi formalmente autorizzati e designati:
tramite individuazione nominativa (nome e cognome) delle persone fisiche. In questo caso occorre specificare, per ciascun nominativo, i trattamenti che lo stesso è autorizzato ad effettuare;
- tramite assegnazione funzionale della persona fisica alla unità organizzativa, qualora la persona fisica effettui tutti i trattamenti individuati puntualmente per tale unità. In questo caso l'assegnazione tramite il PEG delle risorse umane alle singole articolazioni organizzative dell'ente equivale a formale designazione e autorizzazione al compimento delle operazioni di trattamento di competenza della singola articolazione organizzativa, salvo ove diversamente espressamente indicato.

Le istruzioni impartite agli incaricati del trattamento, formulate per iscritto, oltre a riguardare eventuali aspetti di dettaglio da diversificare in relazione alle specificità dei singoli trattamenti, devono quanto meno contenere un espresso richiamo alle policy dell'Ente in materia di sicurezza informatica e protezione dei dati personali.

Il Responsabile della Protezione dei dati (DPO)

Il "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 prevede l'obbligo per gli Enti pubblici di designare il Responsabile della protezione dei dati (Data Protection Officer, di seguito DPO).
Specificatamente, sono di seguito indicati i compiti del DPO in aderenza agli 37 e ss del suddetto regolamento, conformati alla precipua organizzazione dell'Ente:
informa e fornisce consulenza all'Ente in merito agli obblighi derivanti dalla normativa in materia

di protezione dei dati personali, con il supporto del gruppo dei referenti designati dalle strutture;

- sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche dell'Ente in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- coopera con il Garante per la protezione dei dati personali;
- funge da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;
- partecipa allo svolgimento delle verifiche di sicurezza svolte dal Responsabile del servizio ICT competente o ne richiede di specifiche;
- promuove la formazione di tutto il personale dell'Ente in materia di protezione dei dati personali e sicurezza informatica;
- partecipa alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy dell'Ente;
- formula gli indirizzi per realizzazione del Registro delle attività di trattamento di cui all'art. 30 del Regolamento.
- fornisce i pareri obbligatori e facoltativi richiesti dalle strutture secondo quanto specificato di seguito.

Pareri del DPO

Il DPO fornisce il proprio parere in ordine alla legittimità e alla correttezza dei trattamenti di dati personali sulle istanze che le strutture dell'Ente presentano nei casi di seguito indicati.

Pareri obbligatori

Devono essere obbligatoriamente richiesti pareri in ordine a:
individuazione delle misure che abbiano un significativo impatto sulla protezione dei dati personali che l'Ente intende adottare ai fini della tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente, anche a seguito di incidenti di sicurezza o analisi dei rischi;

- adozione di policy e disciplinari in materia di protezione dei dati personali e sicurezza delle informazioni, redazione e aggiornamento dei disciplinari tecnici con impatto sulla sicurezza delle informazioni;
- individuazione di misure poste a mitigazione del rischio delle criticità emerse dall'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali;
- incidenti sicurezza.

Pareri facoltativi

Possono essere inoltre richiesti, se ritenuti utili, pareri in ordine a:
progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza al principio della privacy by design e by default;

- valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento 2016/679;
- valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE n. 679/2016;
- opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

Le richieste di parere devono essere inviate all'indirizzo di posta elettronica **dpo-team@lepida.it** nelle modalità che saranno stabilite dall'Ente.

Possono presentare le richieste di parere i soggetti delegati attuatori o i soggetti delegati in base ai principi generali relativi all'istituto della delega.
I pareri sono espressi nel rispetto delle seguenti codifiche:
NC: acronimo di "non conformità", nei casi in cui siano rilevati elementi di non conformità alla normativa e alle policy in materia di protezione dei dati personali;

- OS: acronimo di "osservazione", nei casi in cui vi siano elementi di miglioramento che garantiscono una maggiore aderenza alla normativa e alle policy in materia di protezione dei dati personali, non costituendo vincolo di attuazione;
- PO: acronimo di "positivo", nei casi in cui siano prospettati elementi valutati come conformi alla normativa e alle policy regionali in materia di protezione dei dati personali.

Nei casi in cui il DPO esprima pareri "NC" e "OS" il soggetto delegato attuatore deve formalizzare, nelle medesime forme utilizzate dal DPO per l'espressione del parere, le motivazioni che giustificano l'esecuzione dell'attività o l'implementazione della soluzione tecnologica, in contrasto alle indicazioni fornite dal DPO.
I pareri espressi dal DPO sono conservati agli atti del soggetto delegato.

Il Servizio ICT competente

Il Servizio competente in materia di sistemi informativi ,ovvero di sicurezza informatica, svolge un ruolo di supporto al DPO in tema di risorse strumentali e di competenze.
Al fine di adeguare le funzioni assegnate con la designazione della nuova figura del DPO è necessario prevedere per il Servizio i compiti di seguito meglio specificati:
individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente. Tutte le soluzioni che abbiano un significativo impatto sulla protezione dei dati personali sono sottoposte a parere preventivo obbligatorio del DPO, come ad esempio per la redazione delle linee guida in materia di sicurezza delle informazioni e protezione dei dati personali e per la redazione ed aggiornamento dei disciplinari tecnici trasversali;

- condivide le evidenze dell'analisi dei rischi con il DPO, il quale fornisce parere obbligatorio sulle misure poste a mitigazione del rischio che abbiano un significativo impatto sulla protezione dei dati personali;
- provvede, ogni qualvolta venga avvertito un problema di sicurezza a:
  - attivare la struttura cui sono demandati compiti relativi alla gestione degli incidenti di sicurezza, assicurando la partecipazione del DPO;
  - individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del DPO;
  - segnalare al Responsabile competente in materia di sistemi informativi le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali;
- svolge verifiche sulla puntuale osservanza della normativa e delle policy dell'Ente in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del DPO e realizza le verifiche specifiche richieste dello stesso;
- promuove la formazione di tutto il personale dell'Ente in materia di sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione all'interno della Ente, coordinandosi con le azioni promosse dal DPO.

Il Gruppo dei referenti privacy

Costituisce attuazione dei principi di informazione e sensibilizzazione del Regolamento europeo n. 679/2016 la costituzione di un gruppo permanente di referenti privacy formato dal Segretario e Direttore generale dell'Ente, dal Responsabile del Servizio informatico associato e dai soggetti attuatori dei Comuni che fanno parte dell'Unione, che assicuri un presidio per le strutture dell'Ente per quel che concernono gli adempimenti continuativi, lo studio e l'approfondimento degli aspetti normativi, organizzativi e procedurali, derivanti anche delle nuove disposizioni normative.

Il Gruppo di referenti ha i seguenti compiti:
attuare, per le strutture di appartenenza, le misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo come individuate dall'Ente, anche a seguito di analisi ed approfondimenti in seno al Gruppo dei referenti privacy;

- coordinare il puntuale aggiornamento delle designazioni degli amministratori di sistema all'interno delle strutture di appartenenza e la costante verifica dei privilegi assegnati agli amministratori già designati;
- effettuare la ricognizione costante, a mezzo del Registro, dei trattamenti di dati personali effettuati dalle strutture di appartenenza, servendosi di risorse e competenze messe all'uopo a disposizione dal soggetto delegato attuatore o dal dirigente dallo stesso delegato;
- fornire supporto alle verifiche di sicurezza svolte dal Servizio ICT e/o dal DPO;
- provvedere alla revisione e all'aggiornamento dei Disciplinari Tecnici;
- coordinare le richieste di parere al DPO dei soggetti delegati attuatori di propria afferenza nei casi e con le modalità previsti dal presente documento.

Accesso civico generalizzato e ruolo DPO

Con specifico riferimento alla normativa in materia di trasparenza, si ritiene opportuno disciplinare la necessaria interazione tra il DPO, le strutture dell'Ente, e il Responsabile per la prevenzione della corruzione e trasparenza (R.P.C.T.).
Il D.L. 97/2016, di modifica del D.lgs. 33/2013 ha introdotto l'istituto dell'accesso civico "generalizzato", che attribuisce a "chiunque" il "diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione.
L'esercizio di tale diritto soggiace ai limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis" del d.lgs. n. 33/2013).
L'art. 5, c. 5, d.lgs. n. 33/2013 prevede che, per ciascuna domanda di accesso generalizzato, l'amministrazione debba verificare l'eventuale esistenza di controinteressati, eccetto i casi in cui la richiesta di accesso civico abbia ad oggetto dati la cui pubblicazione è prevista dalla legge come obbligatoria.
Il DPO funge da supporto alle strutture competenti sulle singole richieste di accesso nella fase di individuazione dei soggetti da ritenersi controinteressati e comunque per tutti gli aspetti relativi alla protezione dei dati personali inerenti le richieste di accesso civico generalizzato.
Il DPO funge altresì da supporto al R.P.C.T. nei casi di riesame di istanze di accesso negato o differito a tutela dell'interesse alla protezione dei dati personali.
Il DPO, inoltre, su richiesta delle strutture, esprime proprio parere in ordine alla valutazione dell'eventuale pregiudizio che l'accesso potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE n. 679/2016.
Il DPO, su richiesta delle strutture, formula il proprio parere, entro tre giorni, in ordine all'opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.
Sulla scorta di tale parere le strutture competenti sulle singole richieste di accesso effettueranno il bilanciamento tra gli interessi lesi e la rilevanza dell'interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare.

COMUNE DI SAN BENEDETTO VAL DI SAMBRO

(Città metropolitana di Bologna)

Via Roma, n. 39 - 40048 San Benedetto Val di Sambro (BO)
Tel: 0534/95026 → int. 117 - C.F. 80014530374
PEC:comune.sanbenedettovaldisambro@cert.provincia.bo.it
e-mail: segretario@comune.sanbenedettovaldisambro.bo.it

INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART 13 DEL REGOLAMENTO EUROPEO N. 679/2016

1. Premessa

Ai sensi dell'art. 13 del Regolamento europeo n. 679/2016, l'Ente Locale Comune di San Benedetto Val di Sambro, in qualità di "Titolare" del trattamento, è tenuto a fornirle informazioni in merito all'utilizzo dei suoi dati personali.

2. Identità e i dati di contatto del titolare del trattamento

Il Titolare del trattamento dei dati personali di cui alla presente Informativa è il Comune di San Benedetto Val di Sambro, con sede in via Roma, 39.
Al fine di semplificare le modalità di inoltro e ridurre i tempi per il riscontro si invita a presentare le richieste di cui al paragrafo n. 10, al Comune di san Benedetto Val di Sambro, via e-mail, tramite la casella PEC istituzionale

3. Il Responsabile della protezione dei dati personali

Il Comune di San Benedetto Val di Sambro ha designato quale Responsabile della protezione dei dati la società Lepida SpA, (dpo-team@lepida.it).

4. Responsabili del trattamento

L'Ente può avvalersi di soggetti terzi per l'espletamento di attività e relativi trattamenti di dati personali di cui l'Ente la titolarità. Conformemente a quanto stabilito dalla normativa, tali soggetti assicurano livelli di esperienza, capacità e affidabilità tali da garantire il rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza dei dati.
Vengono formalizzate da parte dell'Ente istruzioni, compiti ed oneri in capo a tali soggetti terzi con la designazione degli stessi a "Responsabili del trattamento". Vengono sottoposti tali soggetti a verifiche periodiche al fine di constatare il mantenimento dei livelli di garanzia registrati in occasione dell'affidamento dell'incarico iniziale.

5. Soggetti autorizzati al trattamento

I Suoi dati personali sono trattati da personale interno previamente autorizzato e designato quale incaricato del trattamento, a cui sono impartite idonee istruzioni in ordine a misure, accorgimenti, modus operandi, tutti volti alla concreta tutela dei tuoi dati personali.

6. Finalità e base giuridica del trattamento

Il trattamento dei suoi dati personali viene effettuato dal Comune di San Benedetto Val di Sambro per lo svolgimento di funzioni istituzionali e, pertanto, ai sensi dell'art. 6 comma 1 lett. e) non necessita del suo consenso. I dati personali sono trattati per le finalità descritte nell'elenco dei trattamenti, reperibile nella sezione Privacy e nella sezione Amministrazione trasparente del sito istituzionale.

7. Destinatari dei dati personali

I suoi dati personali non sono oggetto di comunicazione o diffusione, a meno di esigenze particolari del singolo trattamento, descritte nell'elenco dei trattamenti, reperibile nella sezione Privacy e nella sezione Amministrazione trasparente del sito istituzionale.

8. Trasferimento dei dati personali a Paesi extra UE

I suoi dati personali non sono trasferiti al di fuori dell'Unione europea.

9. Periodo di conservazione

I suoi dati sono conservati per un periodo non superiore a quello necessario per il perseguimento delle finalità sopra menzionate. A tal fine, anche mediante controlli periodici, viene verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che Lei fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non sono utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

10. I suoi diritti

Nella sua qualità di interessato, Lei ha diritto:

- di accesso ai dati personali;
- di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano;
- di opporsi al trattamento;
- di proporre reclamo al Garante per la protezione dei dati personali.

11. Conferimento dei dati

Il conferimento dei Suoi dati è facoltativo, ma necessario per le finalità sopra indicate. Il mancato conferimento comporterà le conseguenze dipendenti dal trattamento in questione, indicate nell'elenco dei trattamenti, reperibile nella sezione Privacy e nella sezione Amministrazione trasparente del sito istituzionale.

COMUNE DI SAN BENEDETTO VAL DI SAMBRO
(Città metropolitana di Bologna)

Via Roma, n. 39 - 40048 San Benedetto Val di Sambro (BO)
Tel: 0534/95026 → int. 117 - C.F. 80014530374
PEC:comune.sanbenedettovaldisambro@cert.provincia.bo.it
e-mail: segretario@comune.sanbenedettovaldisambro.bo.it

MODELLO DI GESTIONE INCIDENTI DI SICUREZZA

Premessa

Il presente documento rappresenta il riferimento per l'Ente Unione dei Comuni dell'Appennino bolognese e per tutti i Comuni che ne fanno parte per la regolamentazione della gestione degli incidenti di sicurezza informatica che possono occorrere ai servizi ed ai dati gestiti.
La corretta gestione degli incidenti di sicurezza permette di evitare o minimizzare la compromissione dei dati dell'organizzazione in caso di incidente; permette inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, di migliorare continuamente la capacità di risposta agli incidenti.
Inoltre, con specifico riferimento all'obbligo di cui all'art. 33 del GDPR n. 679/2016, il presente documento individua quali siano le violazioni che ricadono nell'ambito della suddetta normativa, i casi in cui l'Ente deve notificare i data breach all'Autorità Garante ed agli interessati, le misure atte a trattare il rischio e la documentazione da produrre.
Si rappresenta che l'art. 32 del Regolamento dispone che devono essere approntate misure tecniche e organizzative adeguate per garantire un livello adeguato di sicurezza dei dati personali. Individuare, indirizzare e segnalare tempestivamente un incidente di sicurezza, come una violazione di dati, è espressione dell'adeguatezza delle misure implementate dall'Ente.
L'ambito di applicazione è rappresentato da sistemi ICT dell'Ente e vengono presi in considerazione incidenti che possono scaturire sia attraverso l'azione di un attacco informatico portato da elementi esterni all'organizzazione sia generati da un eventuale comportamento negligente o scorretto, di natura ostile con obiettivi frodatori da parte di un collaboratore dell'Ente.
Tutte le violazioni dei dati personali sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.
L'obbligo di cui agli artt. 33 e 34 del Regolamento trova applicazione nei soli casi in cui la violazione riguardi dati personali, come definiti dall'art. 4 n. 1).
Il presente documento è applicabile alle risorse ed ai servizi di tipo informatico gestiti in modo diretto oppure esternalizzato da parte degli Enti.

Incidente di sicurezza

Ai sensi del presente documento, per incidente di sicurezza deve intendersi *"la violazione, la minaccia imminente di violazione di una politica di sicurezza informatica, di politiche di utilizzo accettabili o di prassi standard di sicurezza, correlato ad una violazione di dati o informazioni"*. Esempi di incidenti sono:

un utente malintenzionato esegue operazioni al fine di inviare un numero elevato di richieste di connessione ad un server web, provocando l'arresto anomalo del servizio;
gli utenti sono indotti ad aprire un file allegato alla mail che in realtà è un malware;
l'esecuzione del tool che comporta l'infezione del dispositivo stabilendo connessioni con un host esterno;
Un utente malintenzionato ottiene dati sensibili e minaccia l'organizzazione di diffonderli se non viene pagato un riscatto in denaro

Data breach ai sensi del GDPR

Il regolamento definisce la violazione dei dati personali 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"*.
Le violazioni declinate dalla norma sono sintetizzabili come
Violazione della riservatezza, che si ha in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.
Violazione dell'integrità, che si ha in caso di alterazione non autorizzata o accidentale dei dati personali
Violazione della disponibilità, che si ha in caso di perdita o distruzioni di dati personali o di impossibilità di accesso ai dati personali da parte di soggetti autorizzati

Va sottolineato che una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione di queste.
Gli effetti di una violazione possono causare danni fisici, materiali o immateriali, ovverosia la perdita del controllo sui propri dati personali, la limitazione dei loro diritti, discriminazione, furto d'identità o frode, perdita finanziaria, inversione non autorizzata di pseudonimizzazione, danno alla reputazione e perdita di riservatezza dei dati personali protetti dal segreto professionale . Può anche includere qualsiasi altro significativo svantaggio economico o sociale per tali individui.

Notifica al Garante e agli interessati

In caso di data breach l'Ente deve valutare i rischi per i diritti e le libertà delle persone fisiche, registrando le evidenze di tale analisi.
Nell'eventualità che tale valutazione rappresenti elementi di rischio per i diritti e le libertà delle persone fisiche l'Ente effettua la notifica al Garante delle violazioni di dati personali.
Quando le violazioni di dati comportano un rischio che viene valutato come elevato per i diritti e le libertà delle persone fisiche, le stesse devono essere comunicate agli interessati senza ingiustificato ritardo, fornendo loro specifiche informazioni in ordine alle salvaguardie che devono adottare per proteggere loro stessi dalle conseguenze della violazione.
Questo rischio esiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone i cui dati sono stati violati. Tale rischio è presunto quando il data breach riguarda le categorie particolari di dati di cui all'art. 9 del GDPR.
I criteri che devono guidare la valutazione del suddetto rischio sono i seguenti:
la tipologia di violazione
la natura dei dati violati
il volume dei dati violati
il numero di individui cui si riferiscono i dati violati
caratteristiche speciali degli individui cui si riferiscono i dati violati
il grado di identificabilità delle persone
la gravità delle conseguenze per gli individui

La valutazione deve essere condotta secondo una metodologia operativa adeguata che viene di dettagliata nel seguito.
L'Ente notifica la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è stata rilevata. Oltre tale termine, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni sono fornite in fasi successive senza ulteriore ingiustificato ritardo.
Il termine principia dal momento in cui l'Ente ha consapevolezza della violazione di dati, ovverosia quando si raggiunge un ragionevole grado di certezza che si è verificato un incidente di sicurezza che ha compromesso i dati personali.
L'Ente può tardare la notifica all'Autorità Garante, nei casi in cui tale notifica possa produrre effetti negativi sugli individui.
Nei casi in cui l'Ente disponga di informazioni solo parziali della violazione, viene, comunque, effettuata la notifica al Garante.
Il Garante per la protezione dei dati personali può richiedere, in ogni caso, la notifica della violazione agli interessati.
La comunicazione della violazione agli interessati può essere ritardata nei casi in cui tale comunicazione possa pregiudicare le indagini su cause, natura e conseguenze della violazione, anche su indicazione delle varie Autorità di controllo.

L'Ente utilizza lo strumento più efficace affinché tale notifica sortisca il maggiore effetto possibile.

Ruoli e responsabilità

La criticità del processo di gestione degli incidenti di sicurezza informatica e del data breach deve essere opportunamente affrontata da una struttura operativa competente, in possesso di adeguata formazione ed in grado di prendere rapidamente le decisioni imposte dalla delicatezza del compito assegnato.
L'Ente istituisce il Gruppo per la Gestione della Sicurezza ICT, composto, come membri fissi, dal responsabile del Servizio informatico associato e dal coordinatore del Servizio di assistenza informatica. Il gruppo ha le seguenti competenze:

- rappresentare il punto di riferimento univoco a cui il personale dell'organizzazione deve rivolgersi per segnalare un potenziale incidente oppure un comportamento sospetto;
- gestire tutte le attività inerenti l'analisi e la gestione di un incidente di sicurezza, ivi comprese quelle relative alla sua notifica e documentazione;
- garantire la disponibilità delle liste di contatti (es.: personale dipendente, collaboratori, fornitori), necessarie per la gestione di un incidente di sicurezza;
- garantire che il processo di gestione incidenti sia sempre adeguato alle esigenze dell'ente, provvedendo che sia sempre aggiornato.

I riferimenti del gruppo (nominativi, indirizzo e-mail, numero di telefono ecc.) sono riportati nell'allegato STRUTTURE, tempestivamente aggiornato, e sono diffusi a tutti gli utenti tramite una specifica comunicazione e la pubblicazione sul sito istituzionale degli enti ad ogni suo aggiornamento.
Il gruppo è coordinato dal Responsabile del servizio informatico associato che sarà la figura che avrà in carico la gestione degli incidenti.
Nel corso del processo di gestione di un incidente di sicurezza informatico e, eventualmente, di un data breach, il coordinatore del gruppo potrà richiedere di volta in volta l'inclusione nel gruppo stesso dei Responsabili dei trattamenti coinvolti i cui dati sono stati oggetto di data breach, dei segretari degli Enti interessati, dei fornitori dei sistemi informatici, e di tutti coloro che il gruppo riterrà necessario coinvolgere a seconda della tipologia di incidente e della tipologia di dati coinvolti, compreso il Servizio Comunicazione Istituzionale dell'Unione.
Nelle attività del gruppo deve essere coinvolto il Data Protection Officer (DPO) designato, il quale esercita le proprie funzioni di monitoraggio della conformità in caso di data breach, fornendo il proprio parere in ordine alla necessità di effettuare la notifica e, quindi, sulle valutazioni precedentemente descritte.

In caso di data breach il punto di contatto con il Garante per la protezione dei dati personali è costituito dal Data protection officer.

Vi sono comportamenti, attività e regolamenti che ogni organizzazione deve necessariamente attivare per cercare di prevenire gli incidenti di sicurezza, riducendo il livello di rischio e l'esposizione a possibili attacchi informatici. Tali contromisure, che possono essere di natura sia tecnologica che organizzativa, devono essere descritte e adottate dall'Ente per mettere in sicurezza i sistemi ICT.

Procedura di gestione degli incidenti di sicurezza

Deve essere sviluppata, documentata e tenuta aggiornata una procedura per la gestione degli incidenti di sicurezza. Tale procedura ha i seguenti obiettivi:

- preparare il personale;
- identificare un incidente in corso;
- minimizzare i danni relativi all'incidente ed impedirne la propagazione;
- gestire correttamente il processo di ripristino dei sistemi e delle applicazioni;
- acquisire nel modo appropriato le eventuali evidenze digitali di reato;
- riconoscere gli errori commessi, assumerne le responsabilità e formulare proposte volte a migliorare la procedura stessa.

La decisione su quali soluzioni adottare è demandata al gruppo di gestione sicurezza con l'eventuale supporto delle figure ritenute necessarie tenendo conto della complessità e variabilità dell'argomento trattato.
Per facilitare la gestione degli incidenti di sicurezza occorre mantenere operativo un workflow che automatizzi le varie fasi, in particolare il flusso delle comunicazioni fra i vari attori. Tale misura ha anche lo scopo di facilitare la produzione del report relativo all'incidente e di tenere aggiornate le statistiche sugli incidenti di sicurezza.

Oltre ai requisiti di riservatezza ed integrità, occorre considerare anche le esigenze di disponibilità dei dati e dell'infrastruttura ICT preposta all'erogazione dei servizi informatici. Nel caso si verifichi di incidente di sicurezza che possa pregiudicare per un periodo sufficientemente lungo la disponibilità delle informazioni occorre intraprendere tutte le operazioni necessarie a garantire la continuità operativa dell'Ente.
Qualora, a seguito di un incidente relativo alla sicurezza delle informazioni, risulti necessario per l'Ente intraprendere un'azione legale (civile o penale) contro una persona fisica o giuridica, oppure nel caso in cui ci siano le premesse affinché l'Ente possa essere oggetto di azione legale (civile o penale), le evidenze oggettive devono essere raccolte e conservate e presentate al fine di conformarsi ai requisiti di legge applicabili nelle sedi giurisdizionali competenti. Tutta la fase di raccolta delle evidenze deve essere fatta in modo che le evidenze siano utilizzabili in un processo giuridico. La raccolta delle evidenze può avvenire anche qualora si voglia semplicemente procedere con indagini più approfondite, non necessariamente legate ad un proseguo forense.
La documentazione relativa agli incidenti di sicurezza, comprensiva delle evidenze e delle valutazioni effettuate, viene elaborata in maniera tale da non indicare dati personali. Il tempo di conservazione di tale documentazione è stabilito in 24 mesi nel caso in cui siano presenti dati personali, allo spirare del quale i dati devono essere cancellati e senza limiti di tempo nel caso non siano presenti dati personali.
Tutti i dipendenti e collaboratori dell'Ente che accedono alle risorse del Sistema Informatico Informativo dell'Ente sono tenuti ad osservare i principi contenuti nel presente documento ed a segnalare in modo tempestivo la presenza di condizioni che possano indurre a valutare delle anomalie riconducibili ad attacchi informatici oppure a comportamenti scorretti.
Gli utilizzatori dei sistemi informatici, che a causa del loro comportamento gravemente negligente o in palese contrasto con le politiche di sicurezza dell'Ente, fossero causa diretta o indiretta di incidente di sicurezza, potranno essere soggetti ad un accertamento di eventuali responsabilità e violazione delle politiche di sicurezza ICT dell'Ente.

Dettagli della procedura di gestione degli incidenti di sicurezza

Attivazione del Gruppo di sicurezza

La responsabilità della tempestiva attivazione del gruppo di sicurezza fa capo al Responsabile dei trattamenti coinvolti i cui dati sono stati oggetto di data breach. Poiché ciascun Ente ha individuato un Referente interno per il Servizio informatico associato, come previsto dal Progetto organizzativo-funzionale del Servizio, lo stesso rappresenta il punto di contatto naturale tra gli enti e il Gruppo di sicurezza e quindi il primo punto di raccolta dei potenziali incidenti di sicurezza. Il Responsabile del trattamento potrà pertanto farsi coadiuvare nella procedura dal Referente.
La segnalazione di incidente di sicurezza può arrivare al Responsabile del trattamento/Referente da parte di un utente dell'Ente o da un cittadino (attraverso le strutture di front-office dell'Ente), il quale può per esempio rilevare situazioni di alterazione di un sito web dell'Ente, di accesso non autorizzato a dati, di indisponibilità di una risorsa ICT per un tempo prolungato etc.
Il Responsabile del trattamento/Referente ha il compito di attivare il Gruppo in caso di incidenti di sicurezza e di collaborare con questo per la gestione di tutte le fasi successive. La lista dei Referenti dei vari Enti è riportata nell'Allegato STRUTTURE.
In caso di incidenti che richiedano una particolare celerità, in caso di indisponibilità del Referente, o in altri casi ritenuti opportuni, un operatore dell'Ente che venga a conoscenza di un incidente di sicurezza, potrà comunque attivare direttamente il Gruppo .
La segnalazione può pervenire in modo automatico da strumenti appositi o da un processo di analisi continuativa degli eventi di sicurezza registrati da vari dispositivi, solitamente gestiti direttamente dal Gruppo di sicurezza. Nel caso in cui venga rilevato un riscontro positivo durante l'analisi di tali eventi viene aperto un incidente di sicurezza che segue la procedura di gestione.
Nel caso di segnalazioni di incidente da parte di soggetti terzi, l'Ente avvia senza indugio un'indagine volta a verificare che sia avvenuta effettivamente la violazione di dati segnalata.

Preparazione

Si tratta di attività necessarie per consentire una adeguata gestione degli incidenti informatici di sicurezza che devono essere eseguite rigorosamente. Si tratta ad esempio di:

- definizione della struttura tecnica di supporto nella gestione degli incidenti e dei necessari interventi di formazione per le risorse potenzialmente coinvolte nella gestione degli incidenti, quindi definizione dei

membri del Gruppo che vanno ad aggiungersi ai membri fissi;

- predisposizione degli strumenti hardware e software necessari;
- definizione e distribuire le apposite procedure relative alle modalità di comunicazione verso l'esterno dell'accaduto.

Identificazione e analisi dell'incidente

Si tratta della attività che mira a valutare se un evento riscontrato sia effettivamente riconducibile ad un incidente di sicurezza oppure si tratti di un cosiddetto falso positivo. Le operazioni di identificazione (Detection and Analysis) devono permettere di verificare, per ogni caso di evento anomalo o sintomo di un incidente, se si è in presenza di un incidente reale di sicurezza.
Nel caso in cui le attività di analisi dell'incidente di sicurezza evidenzino particolari difficoltà oppure impatti che si estendono al di fuori del perimetro dell'Ente, il Gruppo valuterà l'opportunità o la necessità di coinvolgere le strutture di riferimento regionali e nazionali (ad esempio LepidaSpA considerando il proprio ruolo nell'ambito della sicurezza della Community Network, CERT-PA, …). Inoltre, il Gruppo deve prevedere il coinvolgimento dei fornitori di servizi ICT dell'Ente per il supporto all'analisi e per l'ottenimento di informazioni utili oltre alle autorità di pubblica sicurezza nel caso in cui l'incidente possa presentare risvolti dal punto di vista penale.
Il Gruppo deve inoltre coinvolgere, a seconda della gravità dell'incidente, i vertici dell'Ente per gli aspetti di comunicazione interna ed esterna e nel caso, durante la gestione dell'incidente, emergano responsabilità da parte di personale interno dell'Ente occorre coinvolgere la struttura che si occupa di gestione del personale.
Il Gruppo, si occuperà poi eventualmente di segnalare al Responsabile e al Titolare del trattamento dei dati personali, le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali.
La notifica viene effettuata al Garante, previo parere obbligatorio del DPO, qualora gli esiti della breve e spedita indagine consentano di appurare l'effettiva verificazione della violazione (quindi solo al termine dell'indagine).
Successivamente il Gruppo si occuperà di individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del DPO.

Valutazione dell'impatto dell'incidente

L'analisi degli eventi può portare all'individuazione dei possibili reali incidenti di sicurezza, che si possono classificare in diverse tipologie come segue:

Tipologia Incidente	**Descrizione**
Accesso non autorizzato	Accesso (sia logico che fisico) a reti, sistemi, applicazioni, dati o altre risorse tecnologiche di proprietà dell'Ente da parte di personale non autorizzato.
Denial of Service	Attacco informatico alla disponibilità di una rete o sistema. Qualora abbia successo, comporta la difficoltà all'accesso o la totale indisponibilità di determinati sistemi e/o servizi.
Codice malevolo	Un virus, worm, trojan, spyware, o qualsiasi altro codice malevolo che infetti un sistema.
Uso Inappropriato	Violazione delle politiche di sicurezza e delle disposizioni su corretto utilizzo.
Data leakage	Diffusione di informazioni riservate a seguito di un attacco informatico riuscito.
Alterazione delle informazioni	Modifica del contenuto di dati riservati a seguito di un attacco informatico riuscito.
Phishing	Truffa effettuata su Internet, che sfrutta tecniche di ingegneria sociale, attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso.
Furto/smarrimento totale o parziale di	l furto o smarrimento di singoli dispositivi di memorizzazione (hard disk, memorie di massa rimovibili ecc) oppure dei computer/server che li ospitano.

apparecchiature che contengono dati sensibili	Una violazione dei dati personali sensibili contenuti configura una condizione di data breach che richiede, ai sensi del GDPR, l'attivazione delle specifiche procedure di notifica verso l'autorità Garante e gli utenti coinvolti
Multiplo	Incidente di sicurezza che comprende due o più di quelli sopra elencati.
Malfunzionamento grave	Danneggiamento di un componente hardware o software, oppure degrado delle performance per cause esterne che possa arrecare impatti gravi alla disponibilità di servizio.
Disastro	Qualsiasi evento distruttivo, non provocato direttamente da azione di operatori informatici (es.: black out, incendio, allagamento, terremoto) in grado di condizionare direttamente l'operatività dei sistemi informatici.

E' di fondamentale importanza effettuare una prima valutazione sull'impatto dell'incidente ai fini di indirizzare in modo efficace le risorse necessarie alla sua gestione. Tale attività consiste in una prima classificazione della sua portata in base ad alcuni parametri di seguito elencati:

- il livello di criticità della risorsa ICT coinvolta, determinato in base alle valutazioni inerente la Business Impact Analysis (in caso di coinvolgimento di più risorse verrà assunto come tale quello a maggiore criticità);
- il numero di risorse informatiche coinvolte, inteso come numero di server/applicazioni;
- il numero di utenti o postazioni di lavoro potenzialmente impattati dalla indisponibilità del servizio informatico;
- l'eventuale coinvolgimento di risorse ICT/utenti esterni all'organizzazione;
- l'esposizione su Internet del servizio;
- il tipo di danno arrecato (economico, immagine, mancato adempimento normativo ecc.);
- gli enti o le organizzazioni coinvolte nell'incidente;
- l'eventualità di coinvolgere le forze dell'ordine a causa di possibili risvolti di natura penale.

In questa fase il Gruppo sicurezza ICT deve anche stabilire la gravità dell'incidente di sicurezza; per fare ciò può inizialmente avvalersi della seguente matrice contraddistinta da una valutazione di tipo qualitativo, ma la classificazione della gravità dell'incidente è comunque a sua totale discrezione.

Gravità incidente di sicurezza	**Descrizione**
Alta	Il grado di compromissione di servizi e/o sistemi è elevato. Si rilevano danni consistenti sugli asset. Il ripristino è di medio o lungo periodo. L'incidente presenta una tra le seguenti condizioni: • Danni a persone e rilevanti perdite di produttività • Compromissione di sistemi o di reti in grado di permettere accessi incontrollati a informazioni confidenziali • Siti web violati o utilizzati a fini di propagazione di materiale terroristico o pornografico • Frode o attività criminale che coinvolga servizi forniti dall'ente • Impossibilità tecnica di fornire uno o più servizi critici a un elevato numero di utenti per un intervallo di tempo superiore ai 30 minuti nell'arco di una giornata • Impossibilità tecnica di fornire uno o più servizi di criticità media per un periodo di tempo superiore ai 2 giorni lavorativi • Significativa perdita economica, di immagine e/o reputazione nei confronti del pubblico o degli utenti
Media	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta". Il grado di compromissione di servizi e/o sistemi è di una certa rilevanza e possono essere rilevati danni sugli asset di una certa consistenza. Il ripristino ha tempi che non compromettono la continuità del servizio

	L'incidente presenta una tra le seguenti condizioni: • Compromissione di server • Degrado di prestazioni relativo ai servizi offerti dall'ente con conseguente perdita di produttività da parte degli utilizzatori • Attacchi che provocano il funzionamento parziale o intermittente della rete • Impossibilità tecnica di fornire uno o più servizi critici ad un elevato numero di utenti per intervalli di tempo inferiori ai 30 minuti di tempo ripetuti su più giornate • Impossibilità tecnica di fornire uno o più servizi critici ad una piccola parte di utenti per un periodo di tempo superiore ai 30 minuti di tempo nell'arco di una o più minuti ei tempo nell'arco di una o più giornate • Basso impatto in termini di perdita economica, di immagine e/o reputazione nei confronti degli utenti
Bassa	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta o media". Non vengono compromessi asset o servizi. L'incidente presenta le seguenti condizioni: • Interruzione dell'attività lavorativa di un numero ristretto di dipendenti e per un breve periodo di tempo. • Contaminazioni da virus in un medesimo sito ma • comunque identificate dai sistemi anti-malware • Nessuna o limitata perdita di operatività o di business da parte di un ridotto numero di dipendenti.

Per alcuni incidenti può risultare difficile assegnare un livello di gravità definitivo prima che l'analisi sia completa; in tal caso occorre valutarla sulla base delle evidenze note sino a quel momento, assumendo che la gravità potrebbe molto probabilmente aumentare nel caso non si effettui alcuna operazione di contenimento. In ogni caso, è opportuno verificare ciclicamente, nel periodo in cui l'incidente è in corso, la gravità assegnata allo stesso in quanto essa può variare nel tempo.
Al termine della fase di analisi, è necessario informare tempestivamente il Responsabile e il Titolare del trattamento interessati.

Valutazione dei rischi derivanti dal verificarsi del data breach

Per data breach si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
In caso di data breach l'Ente deve valutare i rischi per i diritti e le libertà delle persone fisiche, utilizzando i criteri di seguito indicati:

- la tipologia di violazione, ovverosia il tipo di violazione come declinata nel paragrafo precedente;
- la natura dei dati violati, valutando che più i dati sono "sensibili" e maggiore è il rischio di danni per le persone fisiche;
- il volume dei dati violati, considerando che la violazione di diverse tipologie di dati comporta un rischio maggiore rispetto alla violazione di una sola tipologia;
- il numero di individui cui si riferiscono i dati violati, considerando che, generalmente, maggiore è il numero di individui interessati, maggiore è l'impatto di una violazione. Tuttavia, una violazione può avere un impatto grave anche su un solo individuo, a seconda della natura dei dati personali e del contesto in cui è stato compromesso;
- caratteristiche speciali degli individui cui si riferiscono i dati violati, ad esempio minori o persone vulnerabili;
- il grado di identificabilità delle persone, considerato che l'identificazione potrebbe essere possibile direttamente dai dati personali violati senza alcuna ricerca speciale necessaria per scoprire l'identità dell'individuo, oppure potrebbe essere estremamente difficile abbinare i dati personali a un particolare individuo, ma potrebbe comunque essere possibile a determinate condizioni (sono, quindi, considerati tutti i mezzi di cui ci si possa avvalere per identificare le persone fisiche);
- la gravità delle conseguenze per gli individui: tale criterio è strettamente connesso alla tipologia di dati violati. Deve essere considerato che una violazione di riservatezza può occorrere anche nel caso in cui dei dati personali siano comunicati ad un terzo, pur non autorizzato, ma conosciuto e "fidato". In tali casi,

evidentemente la valutazione di tale criterio abbasserà il livello di gravità delle conseguenze per gli individui. Nel caso in cui i dati personali siano nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose il livello di rischio potenziale sarà più elevato.

In caso di data breach deve essere sempre coinvolto il Data Protection Officer (DPO) per la valutazione dei rischi per i diritti e le libertà delle persone fisiche, il quale esprime anche formale parere sulla necessità di effettuare la notifica.

Comunicazione degli incidenti

Tutti i potenziali incidenti dovranno essere comunicati come primo punto di contatto, al Responsabile del trattamento o, in caso di estrema urgenza, direttamente al Gruppo di sicurezza, utilizzando i contatti riportati nell'allegato STRUTTURE. L'attivazione della procedura stessa sarà quindi a carico del Gruppo per la gestione della sicurezza informatica che dovrà comunque riportare la situazione al Titolare del trattamento secondo le procedure previste.

La notifica della violazione al Garante

Nei casi in cui l'incidente consista in una violazione di dati personali, l'Ente deve notificare l'incidente al Garante per la protezione dei dati personali se, sulla scorta della valutazione approfondita, strutturata e documentata di cui al paragrafo precedente, si assuma come probabile che la violazione dei dati personali presenti effettivamente un rischio per i diritti e le libertà delle persone fisiche.
La comunicazione al Garante, da redigere in aderenza all'allegato MODELLO COMUNICAZIONE GARANTE, deve ricomprendere ogni informazione utile, oltre che la descrizione:

- della natura della violazione dei dati personali;
- delle categorie e il numero approssimativo di interessati in questione nonché le categorie (minori, persone con disabilità, dipendenti, clienti etc.) e il numero approssimativo di registrazioni (informazioni finanziarie, numeri di conti bancari, numeri di passaporto, documenti sanitari, etc.) dei dati personali in delle probabili conseguenze della violazione dei dati personali;
- delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
- i recapiti del Data Protection Officer.

La notifica della violazione agli interessati

Alcune violazioni di dati, quelle che comportano un rischio elevato per i diritti e le libertà delle persone fisiche devono essere comunicate agli interessati senza ingiustificato ritardo. Tale comunicazione, da redigere in aderenza all'art. 34 del GDPR, nonché formulata con linguaggio chiaro e comprensibile agli utenti (quindi non in gergo tecnico) deve ricomprendere:

- la descrizione della natura della violazione;
- i recapiti del Data Protection Officer;
- la descrizione delle probabili conseguenze della violazione;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nel caso in cui il numero di interessati lo consenta, la comunicazione deve essere inviata a mezzo mail (o pec, o sms) e con avviso pubblicato sul sito istituzionale. Nel caso in cui il numero di soggetti coinvolti sia particolarmente ingente, è sufficiente effettuare la comunicazione dell'avvenuta violazione di dati utilizzando il sito istituzionale.

Monitoraggio delle attività

Il Gruppo Gestione Sicurezza redige e mantiene continuamente un Rapporto dell'incidente di sicurezza. Questo è un documento dinamico da compilare in ogni fase della gestione dell'incidente, inserendo soltanto le parti che in questa fase è possibile conoscere.
Il Rapporto incidente di sicurezza sarà poi completato in tutte le sue parti in fase di chiusura dell'incidente.

Il Coordinatore del Gruppo di gestione della Sicurezza, deve conservare per la durata di cinque anni il Rapporto, in formato elettronico, in una cartella soggetta a backup periodico e ad accesso opportunamente limitato.
E' altresì fondamentale che tutte le operazioni eseguite per la gestione di un eventuale incidente siano opportunamente tracciate, permettendo in tal modo di poter identificare tutte le risorse coinvolte nelle operazioni tecniche di gestione e poterle eventualmente indicare in ambito giudiziale come testimoni. Le indagini svolte e le operazioni di gestione formeranno quindi una base dati che andrà ad incrementare la conoscenza dell'Ente in merito agli incidenti di sicurezza informatica.
Nel caso in cui l'incidente di sicurezza abbia un impatto sulla continuità operativa per un tempo di disservizio inaccettabile per il cliente (superiore all'RTO dichiarato in sede di BIA), è necessario attivare il gruppo sicurezza per tutte le operazioni di Business Continuity.

Contenimento, rimozione e ripristino

Le operazioni di contenimento hanno due importati fini:

- evitare che il danno si propaghi od almeno limitarne la diffusione;
- acquisire le eventuali evidenze digitali di reato prima che queste possano essere compromesse.

Quest'ultima attività è molto critica, infatti, è necessario:

- identificare tutti i sistemi che possono essere stati compromessi o sui cui sia possibile raccogliere eventuali evidenze digitali di reato;
- effettuare delle copie delle eventuali evidenze digitali di reato in modo valido dal punto di vista forense;
- documentare in modo dettagliato tutte le operazioni eseguite, onde evitare in un eventuale ambito giudiziale possibili contestazioni sulla correttezza delle operazioni eseguite;

le attività di contenimento dovranno essere eseguite da personale qualificato, ovvero da sistemisti o esperti applicativi appositamente addestrati per eseguire le operazioni necessarie.
Tutte le operazioni eseguite saranno comunque sotto la responsabilità del Gruppo per la sicurezza informatica il quale dovrà riportare nel Rapporto di incidente:

- data ed ora delle azioni eseguite sui sistemi, applicazioni o dati;
- le generalità delle risorse che hanno materialmente eseguito le operazioni;
- i risultati conseguiti.

Il Gruppo per la sicurezza informatica dovrà comunicare al Responsabile e al Titolare dei trattamenti interessati quanto eseguito al termine di questa fase.
Le operazioni di contenimento possono essere di due tipologie: a breve termine e a lungo termine.

Contenimento a breve termine

Le operazioni di contenimento a breve termine mirano a mettere in sicurezza gli eventuali sistemi interessati da un incidente, senza alterarne la configurazione o inquinare eventuali evidenze digitali di reato.
Come esempi di azioni di contenimento a breve termine si possono indicare:

- creazione di regole firewall atte a bloccare l'accesso ai sistemi coinvolti;
- disabilitazione di account utente sui sistemi centralizzati di autenticazione;
- cambio di configurazione sui sistemi DNS;
- disconnessione dei sistemi coinvolti dalla rete mediante riconfigurazione di apparati di rete.

Dopo aver messo in sicurezza i sistemi coinvolti nell'incidente, mediante l'operazione di contenimento a breve termine, è possibile procedere all'acquisizione di eventuali evidenze digitali (es. mediante copia forense dei dischi) oppure procedere con l'esecuzione di normali backup atti a mettere in sicurezza i dati per poterli riutilizzare nella eventuale ricostruzione del sistema colpito dall'incidente.
E' necessario procedere all'acquisizione forense delle evidenze digitali di reato in ogni caso in cui si prevede un prosieguo in ambito legale come per esempio:

- accessi abusivi a sistemi o informazioni;
- attività illecite commesse da dipendenti o comunque mediante il sistema Informativo gestito dell'Ente;
- interruzione di pubblici servizi critici;
- violazioni della privacy di utenti e cittadini;
- utilizzo illegale dei sistemi per perpetrare truffe o diffondere materiale illecito.

Quando invece l'incidente è causato da malfunzionamenti o errori umani è possibile procedere eseguendo una normale operazione di backup relativa a dati o configurazioni eventualmente presenti sul dispositivo coinvolto nell'incidente. Questa operazione potrà quindi essere eseguita utilizzando i sistemi ed i programmi utilizzati per effettuare le comuni operazioni di backup ed hanno lo scopo di mettere in sicurezza le informazioni necessarie per una eventuale reinstallazione del dispositivo.

Contenimento a lungo termine

Il contenimento a lungo termine comporta l'esecuzione di operazioni tecniche direttamente sui sistemi coinvolti nell'incidente, per questo motivo questa azione deve essere eseguita solo dopo aver messo in sicurezza le evidenze digitali di reato o i dati presenti sul sistema impattato.
Tali operazioni mirano a rendere i sistemi coinvolti più sicuri e permettono di lasciarli in attività sino al momento in cui sia possibile procedere ad operazioni più complesse di rimozione delle cause.
Come esempio di operazioni di contenimento a lungo termine si possono elencare:

- installazione di patch o aggiornamenti di sistema e/o applicativi;
- cancellazione di file o dati;
- arresto di servizi o processi malevoli;
- cambio di configurazione di programmi.

Al termine di queste operazioni i sistemi coinvolti nell'incidente non possono ancora dichiararsi sicuri, ma è possibile utilizzarli temporaneamente sino a quando non sia possibile procedere con le operazioni di rimozione definitiva di quanto ha scatenato l'incidente.
Durante questa fase, possono emergere diverse necessità, come per esempio:

- allocare risorse economiche per la fase di acquisizione forense/backup e le successive fasi di gestione;
- isolare e/o arrestare eventuali servizi o sistemi critici di produzione coinvolti;
- valutare eventuali conseguenze legali;
- relazionarsi con altri Servizi/Direzioni dell'Ente per comunicare eventuali disservizi.

In tali casi il Gruppo per la sicurezza informatica può operare le corrette scelte in autonomia, comunicando al Responsabile e al Titolare del trattamento interessato le eventuali azioni che saranno intraprese.

Rimozione

Le operazioni di rimozione sono volte all'eliminazione definitiva del problema o della vulnerabilità utilizzata per compromettere un sistema coinvolto in un incidente e riportarlo ad un livello di sicurezza elevato.
Le attività che sono solitamente eseguite in questa fase possono essere di diverso tipo, per esempio:

- aggiornamento di release dei sistemi operativi o del software presente (per rimuovere eventuali vulnerabilità di sicurezza);
- rimozione di eventuali servizi o software che, utilizzati in modo malevolo, possono compromettere il sistema stesso (hardening).

In alcuni casi, come per le infezioni da virus/malware, può essere più semplice e meno oneroso economicamente, ricostruire l'intera macchina reinstallando il software a partire dal sistema operativo.

Le operazioni di rimozione possono essere particolarmente onerose in quanto potrebbe essere necessario:

- acquisire nuovo hardware o licenze software;
- utilizzare risorse interne o esterne per l'esecuzione delle operazioni di rimozione;
- eseguire dettagliati test di funzionamento sui sistemi e sulle applicazioni interessate dall'incidente.

La valutazione dell'impatto tecnico ed economico delle operazioni di rimozione deve essere eseguita dal gruppo gestione sicurezza, eventualmente coinvolgendo tutti i soggetti interessati e fornendo al Titolare del trattamento, tramite un report di dettaglio, le indicazioni degli eventuali costi da sostenere e tempi necessari al ripristino.
I tempi necessari per poter procedere alla fase di rimozione possono essere relativamente lunghi (anche nell'ordine di 1 o 2 settimane) a causa delle necessità di approvvigionamento sopra descritte, ma non possono protrarsi all'infinito in quanto l'operazione di contenimento a lungo termine non è da considerarsi risolutiva del problema, ma solo ed esclusivamente un'azione a titolo temporaneo.

Ripristino

In questa fase le operazioni eseguite mirano principalmente a verificare che i sistemi coinvolti nell'incidente siano stati correttamente riattivati e che siano nuovamente sicuri, per considerare l'incidente effettivamente chiuso.
E' necessario ottenere un elevato grado di certezza che quanto accaduto non possa ripetersi, per questo motivo si rende necessario definire con il dovuto dettaglio tutte le fasi di riattivazione di un sistema coinvolto, sia nei modi che nei tempi attesi per il ripristino, sia nei controlli da effettuare per certificare il ritorno alla normalità.

Attività post-incidente

La decisione del momento in cui un sistema coinvolto in un incidente possa ritornare in produzione è in carico al Titolare del trattamento che, in collaborazione con il gruppo gestione sicurezza ed i gruppi di supporto tecnici coinvolti, definisce un piano di riattivazione dei diversi servizi impattati dall'incidente.
In alcuni casi specifici può essere necessario riattivare i sistemi in un periodo non lavorativo (es. nelle ore notturne oppure nei fine settimana) per dare la possibilità alle strutture che hanno in carico la gestione dei sistemi stessi di operare senza che siano presenti richieste di accesso da parte di utenti che non siano quelli deputati all'esecuzione di eventuali test di funzionamento.
Onde verificare che le operazioni di ripristino siano avvenute correttamente si rende necessario monitorare il corretto funzionamento dei sistemi per un periodo di tempo adeguato, per cui potrebbe esservi la necessità di attivare ulteriori controlli utilizzando gli strumenti di monitoraggio in uso, oppure aumentando il livello di profondità degli eventi da registrare nei file di log applicativi o dei sistemi operativi.
Sarà il Gruppo per la sicurezza informatica a richiedere la modifica o l'implementazione di nuove regole di monitoring ai soggetti preposti.
Tutti gli incidenti di sicurezza devono essere documentati. Tale documentazione, unitamente alle evidenze degli incidenti, devono essere debitamente archiviate.
Sono documentati e archiviati, in modalità distinguibile rispetto agli incidenti di sicurezza, tutti i data breach, seppure non notificati all'Autorità Garante e/o agli interessati.
Dal punto di vista tecnico le operazioni di chiusura dell'incidente, consistono nella dichiarazione della fine dello stato di incidente e nella compilazione del report relativo all'incidente stesso da parte del coordinatore del Gruppo per la sicurezza informatica.
Il report, firmato digitalmente dal Responsabile della Sicurezza tramite procedura di hashing a garanzia della sua integrità, dovrà essere conservato a cura del coordinatore del Gruppo sicurezza e dovrà essere inviato in forma riservata sotto forma di relazione sull'esito dell'incidente di sicurezza ai vertici dell'Ente e ai Responsabile e Titolari dei trattamenti coinvolti.
Il coordinatore del Gruppo della Sicurezza deve conservare il Rapporto in un repository ad accesso limitato ai membri del proprio staff, per cinque anni o per tutto il tempo ritenuto necessario (ad esempio allo svolgimento di indagini, nel caso di conseguenze penali, o perlomeno alla definitiva rimozione delle cause scatenanti l'incidente).
In seguito alla chiusura dell'incidente dovranno essere valutate tutte le operazioni eseguite per la gestione dello stesso, evidenziando sia i punti in cui queste sono state eseguite in armonia con le procedure e le aspettative, sia eventuali problemi sorti durante lo svolgimento delle operazioni.
Le informazioni raccolte durante la gestione dell'incidente dovranno essere archiviate, in forma anonimizzata nella knowledge base dell'Ente (consultabile ad accesso ristretto in base al ruolo ricoperto nel processo di gestione incidenti).
E' fondamentale che i punti critici rilevati durante l'esecuzione delle operazioni siano immediatamente condivisi con i componenti del team di gestione degli incidenti e si provveda nel più breve tempo possibile a predisporre quanto può essere necessario per eliminarli o mitigarli, migliorando quindi sia la procedura tecnica di gestione sia la capacità di operare della struttura preposta, sia agendo sulle infrastrutture e i sistemi.

Di seguito alcuni esempi di punti critici che possono essere rilevati:

- mancanza delle competenze tecniche per operare correttamente su un sistema o applicazione;
- mancanza degli opportuni strumenti tecnici;
- errori nella valutazione della gravità dell'incidente o nelle sue capacità di diffusione;
- errori o difficoltà nell'interazione con soggetti interni;
- errori nella comunicazione verso terze parti o verso dipendenti e collaboratori

In particolare può essere utile porsi le seguenti domande:

- La procedura di gestione incidenti è stata correttamente eseguita? E' risultata adeguata al contesto?
- Si sono presentati aspetti che hanno rallentato la risoluzione dell'incidente?
- Si sono presentati elementi che si ritiene siano da cambiare in modo da rendere il processo di gestione degli incidenti più efficace ed efficiente?
- E' necessario aggiornare il metodo di analisi della gravità a valle dell'incidente?
- Sono necessarie delle azioni correttive da intraprendere in fase di mitigazione dei rischi onde evitare che l'incidente possa riaccadere?
- E' necessario modificare le policy aziendali dal punto di vista tecnico (es.: aggiungere file con una determinata estensione tra quelli bloccati dal sistema antivirus)?
- E' necessario aggiornare e/o migliorare gli interventi formativi al fine di istruire il personale aziendale sulle problematiche inerenti la sicurezza e la privacy dei dati?
- Sono necessarie risorse addizionali (es.: personale, tools, strumenti hardware o software) per rendere il processo di gestione degli incidenti più efficace ed efficiente?
- Sono necessarie modifiche e/o riconfigurazioni del software (es.: aumentare frequenza di aggiornamento delle firme dei software antivirus e/o anti-intrusione e, modificare il livello di dettaglio fornito dai sistemi di difesa perimetrali)?

Questa operazione ha lo scopo di verificare che il processo di gestione incidenti sia risultato adeguato a fronteggiare la situazione e far si che le considerazioni che ne scaturiscono debbano divenire patrimonio comune all'interno del team di gestione degli incidenti.
Per questo motivo occorre che entro breve termine dalla chiusura formale di un incidente, il coordinatore del Gruppo per la sicurezza informatica convochi tutte le risorse che sono state parte attiva nella gestione, con l'obiettivo di valutare collegialmente l'efficacia della procedura di gestione degli incidenti e scrivere in un apposito verbale le considerazioni e le operazioni che possono portare a migliorare l'intera procedura.

Allegato STRUTTURE

Gruppo per la gestione della sicurezza informatica:

Membri fissi:

Eros Leoni (Responsabile del servizio informatico associato presso l'Unione dei comuni dell'Appennino bolognese) Coordinatore del gruppo

Laura Chiari (Coordinatore del servizio di Assistenza informatica)

Altri membri potranno essere coinvolti dal coordinatore in base ai particolari eventi da fronteggiare.
Contatti:
sicurezzainformatica@unioneappennino.bo.it

tel. Servizio di assistenza informatica: 053426063 – 053421683

tel. Servizio informatico associato: 051911056 (Seguire il risponditore per il servizio informatico)

cell. Responsabile del Servizio informatico associato: 3336254727

Responsabile per la Protezione dei Dati Personali (RPD) o Data protection officer (DPO)

Lepida S.p.a.
dpo-team@lepida.it
Referente: Kussai Shahin
tel: 051 633 8844 – cell. 366 66 84 754

Referenti interni agli enti del Servizio informatico associato

Ente	Referente	Telefono	e-mail
Comune di Camugnano	Eros Ferrari	0534 41710	ut@comune.camugnano.bo.it
Comune di Castel d'Aiano	Ivan Bertusi	051 6735718	info@comune.casteldaiano.bo.it
Comune di Castel di Casio	Stefano Vitali	0534 44228	Stefano.vitali@comune.casteldicasio.bo.it
Comune di Castiglione dei Pepoli	Roberta Collina	0534 801636	Roberta.collina@comune.castiglionedeipepoli.bo.it
Comune di Gaggio Montano	Maria Silvia Corsolini	0534 37439	mariasilvia.corsolini@comune.gaggio-montano.bo.it
Comune di Lizzano in Belvedere			
Comune di Marzabotto	Valentino Benini	051 6780541	valentino.benini@comune.marzabotto.bo.it

Comune di Monzuno	Carmine Caputo	051 6773343	carmine.caputo@comune.manzuno.bo.it
Comune di San Benedetto val di Sambro	Moreno Santarini	0534 95026	Moreno.santarini@comune.sanbenedettovaldisambro.bo.it
Comune di Vergato	Giampaolo Zaccanti	051 6746733	Giampaolo.zaccanti@comune.vergato.bo.it
Unione dei Comuni dell'Appennino bolognese	Eros Leoni	051 911056	Eros.leoni@unioneappennino.bo.it

Allegato 1 al Provvedimento del 2 luglio 2015

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal **Provvedimento del 2 luglio 2015**, le amministrazioni pubbliche sono tenute a comunicare al Garante all'indirizzo: **databreach.pa@pec.gpdp.it** le violazioni dei dati personali (*data breach*) che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. *p* del Codice) di cui sono titolari.

La comunicazione deve essere effettuata entro 48 ore dalla conoscenza del fatto, compilando il modulo che segue.

Amministrazione titolare del trattamento

Denominazione o ragione sociale _____

Provincia _____ **Comune** _____

Cap _____ **Indirizzo** _____

Nome persona fisica addetta alla comunicazione _____

Cognome persona fisica addetta alla comunicazione _____

Funzione rivestita _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

Eventuali Contatti (altre informazioni) _____

Allegato 1

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Il _____
- ☐ Tra il _____ e il _____
- ☐ In un tempo non ancora determinato
- ☐ E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio

Tipo di violazione

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

Dispositivo oggetto della violazione

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

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ N. _____ persone
- ☐ Circa _____ persone
- ☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- ☐ Dati anagrafici/codice fiscale
- ☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)
- ☐ Dati relativi a minori
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- ☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- ☐ Dati giudiziari
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro :

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

- ☐ Basso/trascurabile
- ☐ Medio
- ☐ Alto
- ☐ Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il

☐ No, perché _____

Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

COMUNE DI
SAN BENEDETTO VAL DI SAMBRO

CITTA' METROPOLITANA DI BOLOGNA

Proposta di deliberazione G.C. ad oggetto:

Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - Approvazione modello organizzativo in materia di protezione dei dati personali e modello gestione incidenti di sicurezza (data breach).

Parere di regolarità tecnica attestante la regolarità e la correttezza dell'azione amministrativa.

Il sottoscritto, in qualità di Segretario Comunale, ai sensi dell'art. 49,comma 1, e 147 bis, comma1 del T.U. approvato con D.Lgs. 18.08.2000, n. 267, esprime PARERE FAVOREVOLE in ordine alla regolarità tecnica e alla correttezza amministrativa della proposta di provvedimento indicato in oggetto.

Lì, 29.06.2018

SEGRETARIO COMUNALE

Marcella BONANNI

COMUNE DI
SAN BENEDETTO VAL DI SAMBRO

CITTA' METROPOLITANA DI BOLOGNA

DELIBERA GIUNTA COMUNALE
N. 70 del 29/06/2018

OGGETTO:

Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - Approvazione modello organizzativo in materia di protezione dei dati personali e modello gestione incidenti di sicurezza (data breach).

Letto, approvato e sottoscritto.

FIRMATO **IL VICESINDACO** **RAG. STEFANINI PAOLA**	**FIRMATO** **IL SEGRETARIO COMUNALE** **BONANNI MARCELLA**

Documento prodotto in originale informatico e firmato digitalmente ai sensi dell'art. 20 del "Codice dell'amministrazione digitale"(D.Leg.vo 82/2005).