Allegato n. 1 alla deliberazione della Giunta Comunale n. ….. del ../../2018 (proposta n. 329/2018)

avente per oggetto: REGOLAMENTO (UE) 2016/679 DEL 27/04/2016 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E LORO LIBERA CIRCOLAZIONE – DISPOSIZIONI OPERATIVE IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONI DEI DATI PERSONALI ED ADOZIONE DEL REGISTRO DEGLI INCIDENTI DI SICUREZZA E DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH – PAR. N. 5 ART. 33 GDPR).

DISPOSIZIONI OPERATIVE IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Aggiornamento: GIUGNO 2018

1. CRONOLOGIA REVISIONI E SINTESI MODIFICHE

Cronologia revisioni:

Data	Versione	Provvedimento di Approvazione	Descrizione

Sintesi delle modifiche rispetto alla precedente versione:

2. FONTI

Nella redazione del presente documento, oltre che dalla lettura del Regolamento UE 2016/679 del 27/04/2016, sono state tratte notizie e/o incorporati documenti redatti da:

- guida all'applicazione del GDPR resa disponibile dall'autorità nazionale Garante per la protezione dei dati personali;
- linee guida del gruppo di lavoro istituito in virtù dell'art. n. 29 della direttiva 95/45/CE (gruppo di lavoro indipendente con funzioni consultive dell'UE nell'ambito dalla protezione dei dati personali e della vita privata);
- linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali adottate dall'Autorità Garante per la protezione dei dati personali con provvedimento n. 221 del 26/07/2012 (G.U. n. 183 del 07/08/2012 – doc. web n. 1915485);
- provvedimento del Garante nazionale per la protezione dei dati personali in materia della disciplina sulla comunicazione dei dati personali (s.d. "*data breach*") del 04/04/2013 (G.U. n. 97 del 26/04/2013 – doc. web 2388260);
- interventi e materiale resi disponibili dalla Regione Piemonte in collaborazione con il CSI Piemonte, l'ANCI, l'UNCEM ed alcuni Enti Piemontesi.

3. GLOSSARIO

Ai fini del provvedimento di cui il presente documento costituisce l'allegato n. 1 si intende per:

- **GDPR o RGPD** - Regolamento Europeo in materia di protezione dei dati personali nonché della libera circolazione di tali dati che abroga la direttiva 95/46/CE sulla stessa materia. Pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04/05/2016, entrato in vigore il 24/05/2016 e diventerà definitivamente applicabile in via diretta in tutti i paesi UE a partire dal 25/05/2018. L'acronimo GDPR si riferisce al termine anglosassone "*General Data Protection Regulation*" mentre l'acronimo RGPD si riferisce alla definizione nazionale "Regolamento Generale sulla Protezione dei Dati".

- **Codice** - Codice nazionale in materia di protezione dei dati personali (D.Lgs 30 giugno 2003, n. 196) attualmente in corso di adeguamento al GDPR.

- **Garante** - Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente, il GDPR identifica questa figura denominandola "Autorità di controllo" (vedasi art.li n. 51 e successivi del GDPR).

- **Titolare** – Titolare del trattamento - l'autorità (nel ns. caso l'Amministrazione Comunale) che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali.

- **Responsabile** – Responsabile del trattamento - soggetto pubblico o privato, che tratta dati personali per conto del Titolare del trattamento.

- **Data Breach** – evento in conseguenza del quale si verifica una "**violazione dei dati personali**". Con il termine "data breach" si intende un incidente di sicurezza in cui dati: personali, sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. La casistica è molto estesa, un "data breach" si può anche verificare a seguito di un problema hardware o software o con una divulgazione di dati riservati o confidenziali all'interno di

un ambiente privo di misure di sicurezze (da esempio, su web) in maniera involontaria o volontaria o con il furto di dati ecc.…

- **accountability** - principio per cui il titolare dovrà dimostrare l'adozione di politiche privacy e misure adeguate in conformità al GDPR.
- **privacy by design** – principio dal quale discende l'attuazione di adeguate misure tecniche e organizzative sia all'atto della progettazione che dell'esecuzione del trattamento.
- **privacy by default** – principio dal quale discende l'attuazione di adeguate misure tecniche e organizzative volte a tutelare la vita privata per "impostazione predefinita".
- **RACI** – standard di matrice per la definizione di ruoli e responsabilità per l'esecuzione di una determinata attività dove vengono poste in relazione le risorse con le attività che esse devono svolgere.
- **WP29** – gruppo di lavoro istituito in virtù dell'art. n. 29 della direttiva 95/45/CE (gruppo di lavoro indipendente con funzioni consultive dell'UE nell'ambito dalla protezione dei dati personali e della vita privata).

4. INTRODUZIONE

Per "***Data Breach*"** si intende un evento in conseguenza del quale si verifica una "**violazione dei dati personali**". Con questo termine ci si riferisce ad un incidente di sicurezza in cui dati: personali, sensibili, protetti o riservati vengono: distrutti, consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato.

L'art. 33 del GDPR impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali entro settantadue ore dal momento in cui il titolare ne viene a conoscenza.

Il termine delle settantadue ore non è perentorio, tuttavia nel caso in cui questo termine sia superato, unitamente alla notifica occorre giustificare i motivi del ritardo (art. 33 paragrafo n. 1 del GDPR).

Secondo il sopracitato articolo 33 del GDPR la notifica al garante non è necessaria quando sia improbabile che la violazione dei dati personali presenti un rischi per i diritti e le libertà delle persone fisiche (paragrafo n. 1).

Il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati) e la imposizione di sanzioni amministrative (secondo l'art. 83 GDPR, l'importo può arrivare a 10.000.000 di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore).

La mancata notifica può inoltre dare luogo ad ulteriori accertamenti da parte del Garante in quanto può rappresentare un indizio di carenze più profonde e strutturali che se accertate possono dar luogo ad ulteriore irrogazione di sanzioni.

Inoltre quando la violazione dei dati è suscettibile di presentare rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve comunicare la violazione all'interessato senza ingiustificato ritardo (art. 33 paragrafo n. 1 del GDPR).

Tutti gli eventi di "data breach", compresi quelli per cui non sono necessarie le notifiche, devono essere documentati dal Titolare ivi incluse le circostanze, le conseguenze e i provvedimenti adottati (art. 33 par. 5 del GDPR) su un registro tenuto, per estensione, secondo le indicazioni fornite dal Garante con il provvedimento n. 393 del 02/07/2015 (GU n. 179 del 04/08/2015 - doc. web n. 4129029). Tuttavia essendo in corso le opportune modifiche per l'adeguamento al GDPR della normativa nazionale è possibile che i tipi di dati e notizie che devono comparire nel registro subiscano variazioni.

E' importante tenere presente che, ai sensi dell'art. 24 paragrafo n. 1 del GDPR, il titolare deve mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato in conformità del regolamento europeo.

Prima dell'emissione del GDPR, a livello nazionale già sussisteva l'obbligo di notifica da parte delle PA di un incidente informatico, tali disposizioni, introdotte con le modifiche al D.lgs. 133/2003 dal Dl. 28/05/2012 n 69, inizialmente limitate ad alcuni settori (fornitori di servizi di comunicazione elettronica accessibili al pubblico) sono state, di fatto, estese a tutta la PA con la circolare AgID n. 2/2017 in quanto impone alle PA di comunicare gli incidenti informatici a CERT-PA ed al garante se l'incidente riguardi dati personali.

Secondo il provvedimento m. 393/2015 sopracitato il Garante ha stabilito in quarantotto ore dalla conoscenza del fatto le violazioni dei dati o gli incidenti informatici che possano avere impatto significativo sui dati personali contenuti nelle proprie banche dati utilizzando per la comunicazione lo schema costituente l'allegato 1 allo stesso provvedimento. Tale termine pare ora superato dalle disposizioni contenute nell'art. 33 del GDPR.

5. DEFINIZIONE DI VIOLAZIONE DEI DATI ("*DATA BREACH*")

Come in precedenza accennato, per **"Violazione di dati**" o "***data breach***" si intende una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 par. 12 GDPR).

In particolare si intende un evento in grado di provocare danni fisici, materiali o immateriali alle persone fisiche (perdita di controllo dei dati personali, limitazioni nei diritti discriminazione, furto, usurpazione di identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione perdita di riservatezza di dati protetti da segreto professionale, danni economici o sociali ecc..). Per una migliore definizione di violazione vedasi quanto riportato: al paragrafo n. 12 dell'art. 4, agli articoli 33 e 34 ed al considerato n. 85 del DGPR.

Per data breach si intende dunque il verificarsi di eventi quali: la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica, o l'accesso non autorizzato ai dati.

Non è corretta quindi l'associazione tra data breach e attacco o problema informatico poiché tale violazione può avvenire anche (ad esempio) a causa di un dipendente infedele che sottrae della documentazione cartacea.

All'art. 4 punto 12) del Regolamento Europeo 679/2016 (GDPR) la "violazione dei dati personali" ("*data breach*") è così definita: "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";

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

Il WP29 riporta nelle sue linee guida esempi che chiariscono la differenza tra un incidente di sicurezza e un "*data breach*". In particolare sottolinea che il GDPR si applica solo in caso di violazione di dati personali.

Il WP29 chiarisce che la conseguenza di una violazione è la perdita della capacità di garantire che il trattamento dei dati sia effettuato in conformità con i principi indicati nell'articolo n. 5 del GDPR. Questo evidenzia la differenza tra un incidente di sicurezza e una violazione dei dati personali - in sostanza, mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

6. VINCOLO DI OSSERVARE LE PRESENTI INDICAZIONI

Poiché il processo di gestione del "*data Breach*" può avere diverse varianti ed aspetti non definibili a priori, non si fa vincolo di seguire scrupolosamente le indicazioni procedurali contenute nel presente documento, esse sono fornite al solo scopo di indicare una possibile metodologia per affrontare al meglio ed assolvere i compiti che scaturiscono dalle norme in materia di "violazione dei dati" sotto la responsabilità dell'Amministrazione Comunale.

Allo stesso modo non si fa obbligo di utilizzare i moduli qui riportati a solo scopo indicativo delle informazioni da raccogliere e trasmettere soprattutto nella loro veste grafica in quanto potrebbero rilevarsi inadeguati per la rilevazione e gestione di casi particolari.

Inoltre potrebbe verificarsi il caso in cui l'evoluzione normativa o di pensiero espressa da organi superiori in materia di sicurezza o di gestione degli incidenti renda per un certo periodo di tempo superate le indicazioni contenute in questo documento. In tale caso, ovviamente, si dovranno osservare le disposizioni superiori dove contrastanti con le indicazioni qui contenute.

E' tuttavia fatto obbligo ad ogni soggetto sotto la responsabilità del Titolare di collaborare e seguire le istruzioni che di volta in volta gli vengono fornite dallo stesso Titolare o dai responsabili interni coinvolti nella gestione di un processo di "*data breach*".

L'esecuzione dei compiti e delle azioni che vengono poste in capo a qualsiasi soggetto devono essere esperite con precedenza assoluta e senza indugio. Questo per permettere il rispetto delle stringenti tempistiche fissate dalla normativa.

7. FASI DEL PROCESSO DI "*DATA BREACH*"

Il Titolare, venuto a conoscenza dell'incidente lo deve poter identificare, stabilire se l'incidente incide sui dati personali ed in che modo, se l'incidente ha coinvolto archivi o strutture digitali o analogiche quindi provvedere alle eventuali comunicazioni: al garante, a CERT-PA ed agli interessati. Il tutto in tempo utile per eseguire le comunicazione entro i termini prescritti.

Per la gestione del processo di "*data breach*" il Titolare deve avvalersi delle strutture comunali ed eventualmente dei soggetti incaricati come responsabili esterni; quindi è necessario stabilire a priori modalità di gestione dei vari sotto processi (fasi):

- **acquisizione**, rilevazione, comunicazione evento al Titolare - (Fase n. 1);
- **gestione tecnica** (analisi; raccolta informazioni; definizione dei soggetti coinvolti; accertamento dell'effettiva sussistenza del "*data breach*") - (Fase n. 2);
- **valutazione** (occorre valutare se l'incidente riguarda o meno un evento che non presenti rischi per i diritti delle persone fisiche se deve essere notificato al Garante, comunicato agli interessati a CERT-PA e/o alle forze dell'ordine) - (Fase n. 3);
- **notifica al garante** - (Fase n. 4);
- **segnalazioni** agli organi di polizia e, nel caso di incidente informatico, a CERT-PA - (Fase n. 5);
- **comunicazione agli interessati** e raccolta riscontri dell'avvenuta comunicazione - (Fase n. 6);
- **registrazione della violazione** oppure degli eventi che non necessitano di notifica - (Fase n. 7).

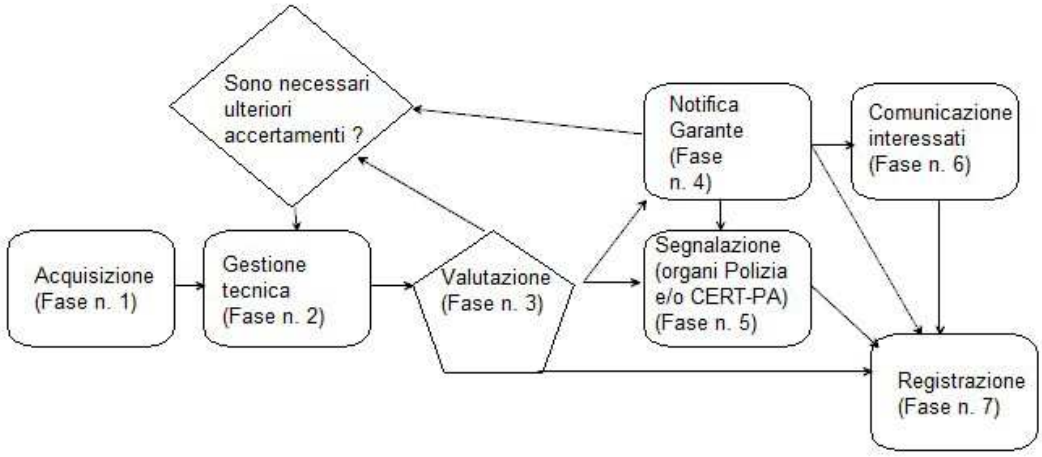
Non necessariamente le fasi devono seguire l'ordine qui riportato, infatti è nella fase di valutazione che il Titolare dovrà stabilire le azioni da intraprendere ed il loro ordine di importanza (ad es. può essere valutata l'opportunità di comunicare una violazione agli interessati contestualmente o prima di eseguire la notifica al Garante).

L'attribuzione di incarichi da parte del titolare ad eseguire, coordinare o gestire una o più delle fasi del processo ed effettuare notifica e comunicazioni non necessariamente devono essere preventivamente formulati per iscritto.

E' importante che sia dimostrabile ogni riferimento temporale sull'incidente e la sua gestione, in particolare sul momento in cui il Titolare viene a conoscenza dell'evento poiché da questo momento decorrono le 72 ore per la notifica al Garante.

La definizione dei ruoli e delle responsabilità che spettano ad ogni interessato per l'esecuzione delle attività relative alle varie fasi è espressa più avanti in questo documento sotto forma di matrice "raci".

L'intero processo può essere a livello generale essere così schematizzato:



8. FASE N. 1 – ACQUISIZIONE

La prima fase nella gestione del "*data breach*" è quella che porta a conoscenza della violazione o presunta violazione di sicurezza e della sua comunicazione al Titolare.

Le modalità con cui un si viene a conoscenza del verificarsi di un "*data breach*" sono molteplici e non enumerabili in modo esuasivo; a puro titolo di esempio una segnalazione può pervenire:

- dagli addetti all'amministrazione dei sistemi informativi;
- da personale interno all'ente;
- da parte di organi pubblici (altri enti, Polizia, Carabinieri, Magistratura ecc..);
- da parte dei soggetti esterni incaricati all'esecuzione di trattamenti (o parti di essi) per conto del comune;
- da parte di Cittadini o comunque di soggetti privati esterni all'ente.

<u>Raccolta della segnalazione</u>

E' importante che la raccolta della segnalazione o l'esecuzione della segnalazione da parte degli uffici avvenga raccogliendo quante più informazioni possibili (identificazione dei segnalatori, data ed ora in cui la segnalazione è avvenuta, dati descrittivi sulla violazione segnalata ecc..).

Nel caso in cui la segnalazione sia raccolta da persone fisiche è opportuno che chi riceve la segnalazione provveda anche a raccogliere informazioni di contatto sul/i segnalatori (indirizzo di reperibilità, numeri telefonici, indirizzo di posta elettronica).

Gli ulteriori elementi da raccogliere potranno, nel caso, essere utili durante la fase di gestione tecnica per reperire maggiori informazioni circa la violazione segnalata.

Se la segnalazione è raccolta direttamente dall'interessato per la redazione dell'informativa dovrà essere osservato quanto disposto all'art n. 13 del GDPR mentre se i dati non siano ottenuti direttamente dall'interessato si dovrà seguire quanto previsto al successivo art. n. 14 del GDPR.

In ogni caso, in questa fase è opportuno non raccogliere dati appartenenti alle categoria particolari di cui al paragrafo n. 1 dell'art. 9 del GDPR (dati sensibili) se non strettamente necessari.

Ove possibile è anche opportuno invitare l'interessato a rendere la propria dichiarazione per iscritto.

Anche le segnalazioni anonime e/o verbali devono essere raccolte ed inviate al titolare per consentire a quest'ultimo di accertare la reale sussistenza della violazione, disporre l'eventuale notifica o le comunicazioni ed assumere i provvedimenti atti ad evitare l'aggravamento della situazione.

Per la raccolta delle segnalazioni verbali è consigliato seguire la traccia del modello di segnalazione al titolare per desumere quali sono le notizie da reperire.

Se la segnalazione perviene da un responsabile esterno incaricato ad eseguire un trattamento o parte di esso per conto dell'ente (obbligato in tal senso da quanto disposto dall'art. 33 paragrafo n. 2 del GDPR), da un altro organismo pubblico o da un servizio interno occorre darne immediata comunicazione al titolare seguendo le istruzioni di seguito riportate.

Modello di informativa da rendere al segnalatore

Chi raccoglie la segnalazione dovrà inoltre fornire al segnalante un'informativa circa le modalità e finalità con cui i dati conferiti saranno trattati. E' opportuno che l'informativa sia resa per iscritto.

L'informativa da rendere deve essere redatta in osservanza:

- dell'art. n. 13 del GDPR se i dati sono forniti e raccolti direttamente dall'interessato, in questo caso l'informativa deve essere resa al momento in cui sono ricevuti i dati personali:
- dell'art. n. 14 del GDPR se i dati non sono raccolti direttamente dall'interessato, in questo caso la norma prevede che l'informativa vada resa entro un termine ragionevole ma al più tardi entro un mese dall'ottenimento dei dati; nel caso i dati siano destinati alla comunicazione con l'interessato, l'informativa deve essere resa al più tardi al momento della prima comunicazione oppure, nel caso sia prevista la comunicazione ad altro destinatario non oltre la prima comunicazione dei dati personali.

Nell'allegato n. 5 al provvedimento con cui si approva il presente documento è riportato un modello utilizzabile per rendere tale informativa a chi segnala un "*data breach*" (presunto o effettivo).

Comunicazione al Titolare

Immediatamente dopo aver raccolto la segnalazione è necessario inoltrare all'amministrazione Comunale la segnalazione raccolta. La segnalazione deve essere eseguita in forma scritta anche utilizzando mezzi elettronici (es. posta elettronica) e deve almeno:

- contenere i riferimenti temporali del momento in cui si è raccolta, acquisita ed inoltrata la segnalazione;
- essere più completa e dettagliata possibile (ivi comprese le modalità in cui si è venuti a conoscenza della presunta violazione).

Chi esegue la segnalazione deve ritenersi a completa disposizione del Titolare per consentire l'eventuale integrazione delle informazioni trasmesse con la segnalazione.

La segnalazione deve essere comunque inoltrata, anche in caso di presunta violazione, sarà poi il Titolare, eseguita la valutazione sulla base di quanto emerso nella successiva fase n. 2 a stabilire se ci si trova o meno davanti ad un caso di violazione di diritti.

Qualora la segnalazione pervenisse per posta elettronica certificata o ordinaria su una casella qualsiasi (istituzionale o meno) non è sufficiente il solo inoltro del messaggio al Titolare ma occorre comunque seguire le modalità di seguito riportate. Allo stesso modo se la segnalazione perviene su supporto cartaceo non è sufficiente la sua registrazione al protocollo e conseguente assegnazione al titolare ma occorre comunque seguire le indicazioni sotto descritte. Questo per accertarsi che la segnalazione non passi inosservata.

Poiché il Titolare potrebbe non essere reperibile o non poter prendere in carico la comunicazione, questa deve essere inoltrata anche al sostituto del rappresentante dell'Amministrazione ed agli organi apicali dell'ente che possono essere coinvolti nel processo (Segretario Comunale, Dirigenti).

In caso di assenza di uno dei soggetti di cui sopra, si dovrà inoltrare la comunicazione a coloro che ne fanno le veci operano secondo i criteri di sostituzione del Titolare e delle le figure apicali; tali criteri o sono previsti dalla normativa o negli appositi provvedimenti in materia emessi periodicamente dall'Amministrazione (Il Sindaco è sostituito da: Vicesindaco, Presidente del Consiglio, Consigliere anziano o altro membro delegato - il Segretario Comunale è sostituito dal Vicesegretario o altro soggetto delegato – per la sostituzione dei dirigenti vedasi i provvedimenti emessi periodicamente dall'Amministrazione).

Contestualmente alla comunicazione scritta della segnalazione è necessario avvertire il Titolare e gli organi apicali dell'ente (o loro sostituti) anche in modo verbale allo scopo di assicurarsi che quanto comunicato non passi inosservato.

E' importante che i riferimenti temporali della comunicazione (data ed ora) coincidano il più possibile con il momento in cui il Titolare viene a conoscenza della violazione (reale o presunta) poiché da tale momento decorrono le 72 ore per la notifica al Garante.

Qualora l'incidente di violazione si verificasse presso strutture esternalizzate (trattamenti o parti di trattamento eseguiti da terzi) il GDPR, all'art. 33 paragrafo n. 2, prevede espressamente che il responsabile esterno, quando viene a conoscenza di una violazione, deve informarne, senza ingiustificato ritardo, il Titolare.

Diventa molto importate quindi l'inserimento nei contratti di fornitura di clausole appropriate che rendano evidente tale obbligo.

Schema tipo di comunicazione al Titolare

A puro titolo illustrativo si riporta, nell'allegato n. 1 al provvedimento di approvazione del presente documento, uno schema che può essere utilizzato per la comunicazione al Titolare di una violazione (reale o presunta):

9. FASE N. 2 – GESTIONE TECNICA

Si intende per gestione tecnica l'esecuzione di tutte quelle operazioni, accertamenti e verifiche tese a supportare la fase di valutazione.

La responsabilità del processo di valutazione e notifica è in capo al Titolare che, allo scopo, deve essere supportato dai servizi interni all'ente ed eventualmente dai responsabili esterni esecutori di trattamenti per conto del comune.

E' importante che questa fase, nella sua prima esecuzione, si concluda nel più breve tempo possibile, circa dieci ore, per consentire il primo processo decisionale di valutazione del Titolare e permettergli di eseguire le eventuali notifiche e comunicazioni entro i termini previsti.

Come più avanti meglio definito in questo paragrafo è possibile che in questa fase non si identifichino tutti gli elementi del "*data breach*" o che sia necessario un ulteriore approfondimento di alcuni aspetti e quindi sia necessario eseguire una o più ulteriori verifiche tecniche.

All'esecuzione di questa fase debbono partecipare tutti i settori dell'ente interessati al trattamento di dati coinvolto nella violazione eventualmente coordinati dal vertice dell'Amministrazione comunale da o suo incaricato.

Nella successiva fase di valutazione, il titolare dovrà stabilire quali azioni devono essere intraprese (semplice registrazione, notifica al garante, comunicazione agli interessati, segnalazione agli organi di polizia e/o a CERT-PA ed altre azioni mirate al contenimento della violazione) ed è pertanto che in questa fase di gestione tecnica emergano tutti gli elementi ad essa necessari. Devono inoltre essere individuate le notizie da riportare sulle varie notifiche o comunicazioni come meglio evidenziato in altre parti di questo documento.

Infatti scoprire l'incidente non è sufficiente, il titolare deve essere in grado di valutare la portata di questo in termini di impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati, dunque le attività svolte in questa fase devono essere documentate, adeguate (devono riportare le violazioni, le circostanze, le conseguenze i rimedi, ed eventualmente quanto posto preventivamente in essere per evitare il verificarsi della violazione), tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti.

Il DGPR impone poi al Titolare di mettere in atto misure tecniche ed organizzative adeguate per garantire i diritti degli interessati, ed essere in grado di dimostrare, che il trattamento è effettuato in conformità delle disposizioni in esso contenute (art. 24 paragrafo n. 1). E' opportuno che al termine di questa fase il titolare sia informato dell'esistenza delle misure poste in essere per mitigare il rischio e di quelle che potrebbero essere utili per ridurre i danni prodotti dalla violazione. Di queste misure il titolare potrà darne eventuale comunicazione al Garante allo scopo di ridurre il rischio e mitigare eventuali sanzioni.

L'art. 33 paragrafo n. 4 del DGPR recita: "Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo".

Il WP29 nelle sue linee guida chiarisce che il GDPR riconosce che i Titolari possono non aver sempre a disposizione tutte le informazioni relative ad una violazione entro il termine delle settantadue ore in quanto i dettagli dell'incidente potrebbero non essere completamente disponibili in questo periodo e possono essere necessarie ulteriori indagini ed approfondimenti.

Dunque questa fase deve terminare in più presto possibile anche se non si riescono a determinare tutti gli elementi utili ad eccezione della determinazione della sussistenza della violazione. Le verifiche potranno eventualmente proseguire dopo le valutazioni del titolare.

Inoltre il Garante o gli alti organi nazionali (polizia, magistratura, CERT-PA ecc…) o lo stesso Titolare potrebbero richiedere o ritenere necessari approfondimenti.

Dunque, l'incompletezza delle informazioni, così come la necessità di approfondimenti potrebbero rendere necessario ripetere la fase anche più volte.

Di conseguenza, la prima esecuzione di questa fase può terminare anche se non è stato possibile rilevare tutti gli elementi pertanto è necessario che la fase, per la sola prima esecuzione, sia conclusa comunque in tempi molto brevi.

A puro titolo esemplificativo la fase si può articolare in:

a) Attivazione:
Il titolare (o suo sostituto o delegato), venuto a conoscenza della violazione incarica gli organi apicali dell'ente (Segretario Generale, Dirigenti o loro sostituti) ed eventualmente il/i Responsabile/i Esterno/i di eseguire la fase di valutazione tecnica. I soggetti incaricati si avvalgono a tale scopo del personale loro assegnato per eseguire le attività.

Il Titolare o i soggetti incaricati si avvalgono dei Responsabili Esterni qualora la violazione si sia verificata, in tutto od in parte, in operazioni di trattamento svolte da questi ultimi per conto dell'ente. I Responsabili Esterni possono essere coinvolti anche quando viene ritenuto utile il loro contributo all'esecuzione della fase (ad es. i fornitori di servizi di connettività).

Le attività relative alla prima esecuzione di questa fase, eseguite per ogni violazione (è possibile che la fase si debba ripetere), devono essere concluse al più presto possibile (indicativamente entro dieci ore dall'attivazione) per permettere al Titolare di eseguire le successive fasi di valutazione, notifica e comunicazioni (anche parziali) entro i termini stabiliti dalla normativa.

Nel caso di attivazioni successive della fase, è possibile che il Titolare ritenga necessaria anche o solo la collaborazione di responsabili (interni od esterni) che non sono stati coinvolti nella prima attivazione.

b) Analisi preliminare
Per prima cosa occorre appurare se la violazione segnalata è considerabile o meno un "*data breach*" (soprattutto se perviene da soggetti privati estranei all'ente).

Per esempio, se l'ente ha esternalizzato un servizio di riscossione responsabilizzando il fornitore ed un cittadino, ignaro del fatto, segnala una violazione dei propri dati personali dopo aver ricevuto un avviso di pagamento da parte del fornitore (e non direttamente dall'ente) è palese che la violazione non sussiste, in casi simili è possibile terminare il processo dandone comunicazione al Titolare affinché concluda l'intero processo con la registrazione della segnalazione e dei motivi che hanno determinato la chiusura del processo di gestione delle violazioni.

Nessuna segnalazione deve concludersi in questo processo unicamente sulla base di un giudizio di inaffidabilità del segnalante perché occorrerà appurare comunque se la violazione si è effettivamente verificata.

Allo stesso modo nessuna segnalazione che sia relativa ad operazioni svolte con strumenti informatici deve concludersi durante l'analisi preliminare poiché anche se non sussiste una violazione di dati personali potrebbe essere necessario informare le autorità competenti (CERT-PA).

E' da tenere presente che ogni segnalazione, comprese quelle non veritiere, devono essere soggette di registrazione nel registro degli incidenti pertanto anche quando si verifica la chiusura anticipata della fase di gestione tecnica si dovrà dare comunicazione al Titolare affinché concluda l'intero processo con la registrazione.

c) Analisi approfondita

Occorre ora identificare la violazione e individuare a quale categoria può appartenere (la violazione può appartenere anche a più categorie) fra quelle identificate dal WP29:

- di riservatezza, quando si verifica una divulgazione o un accesso ai dati non autorizzato o accidentale;
- di integrità, quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata.

Quando, in qualsiasi momento dell'analisi si rilevi una problematica che faccia presupporre un incidente informatico è necessario darne comunicazione immediata al titolare ed al responsabile dell'area informatica affinché possano essere avviate le procedure per la sua comunicazione a CERTPA come prescritto nella circolare AgID n. 2/2017,

Si dovrà appurare se la violazione determina o meno l'obbligo di notifica e/o comunicazione (interessati – forze di polizia). Vi è obbligo di notifica al Garante quando la violazione così come definita all'art. 4 punto 12) del GDPR comporta un rischio, anche presunto, per i diritti e le libertà delle persone.

L'art. 33 del GDPR al paragrafo n. 3 descrive i dati minimi che deve contenere la notifica di violazione al Garante, essa, tra l'altro, deve contenere:

- la descrizione della natura della violazione dei dati personali e, ove possibile, le categorie ed il numero approssimativo di interessati in questione nonché le categorie ed il numero approssimativo di registrazioni dei dati personali in questione;
- descrivere le probabili conseguenza della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nel modello di segnalazione reso disponibile dal garante in allegato al provvedimento del 22 luglio 2015 sono indicate come "da fornire" le seguenti informazioni:

- denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati;
- indicazioni temporali sulla violazione (quando si è verificata);
- indicazioni su dove è avvenuta la violazione;
- tipo di violazione, dispositivo oggetto della violazione;
- descrizione sintetica dei sistemi di elaborazione/memorizzazione coinvolti e loro ubicazione;

- numero degli interessati, anche indicativo, colpiti;
- tipologia dei dati oggetto di violazione;
- livello di gravità attribuito alla violazione;
- misure tecniche e organizzative applicate ai dati oggetto di violazione;
- se gli interessati hanno ricevuto comunicazione della violazione ed il contenuto della comunicazione resa;
- indicazioni sulle misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future.

Il modello fornito dal Garante è riportato più avanti in questa sezione, tale modello potrebbe essere presto adeguato o sostituito.

E' opportuno che dalla verifica emerga se sono coinvolte categorie di persone (colpite o potenzialmente a rischio) a cui appartengano soggetti meritevoli di particolare tutele (minori, anziani, soggetti con disabilità ecc..).

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

Si dovranno altresì identificare eventuali falle dei sistemi di sicurezza, raccogliere tutti gli elementi necessari per la valutazione ed i dati indispensabili che dovranno essere inseriti nella notifica al garante, nella comunicazione a CERT-PA e nel registro degli incidenti, o dovranno essere citati nella comunicazione agli interessati e/o alle forze dell'ordine.

Per la completa definizione degli elementi che devono obbligatoriamente essere inseriti nella notifica o nelle comunicazioni vedasi apposite sezioni in questo documento.

Come in precedenza meglio evidenziato, la prima esecuzione di questa fase può terminare anche se non è stato possibile rilevare tutti gli elementi; pertanto è necessario che la fase, per la sola prima esecuzione, sia conclusa comunque in tempi molto brevi allo scopo di consentire al titolare di inoltrare le eventuali notifiche, comunicazioni e le segnalazioni previste dalla norma o ritenute opportune.

Poiché la casistica che si può verificare è molto amplia non si possono descrivere che sommariamente ed indicativamente i dati e le attività necessarie. E' possibile reperire questi esempi più avanti in questo documento o nelle linee guida rese disponibili dal WP29 a cui si rimanda.

d) Analisi approfondita e/o supplementare

L'analisi supplementare viene attivata se sono necessarie informazioni aggiuntive ad un'analisi già eseguita, quando ad esempio:

- il Titolare ritiene necessario un approfondimento finalizzato ad es. all'integrazione di una notifica al Garante;
- l'Autorità Garante, gli organi di polizia o la magistratura ritengono necessarie informazioni aggiuntive o approfondimenti di informazioni fornite;
- durante una delle fasi del processo di gestione del "*data breach*" sono emerse situazioni non approfondibili o non è stato possibile coinvolgere pienamente responsabili esterni o questi non hanno comunicato in tempo utile i risultati delle loro analisi.

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

10. FASE N. 3 - VALUTAZIONE

La responsabilità di questa fase è in capo al Titolare, esso può avvalersi delle strutture comunali ed eventualmente dei soggetti incaricati come responsabili esterni.

Se durante la fase di valutazione sono emersi elementi che qualificano la violazione come incidente informatico occorre dare comunicazione dell'incidente a CERT-PA.

Per le modalità di esecuzione della notifica o delle comunicazioni vedere le relative sezioni di questo documento.

Al termine della fase di "gestione tecnica" sopra descritta il titolare dovrebbe avere tutti gli elementi per poter identificare l'incidente di sicurezza, quindi, comprendere in che modo l'incidente ha impatto sui dati, se tra le informazioni coinvolte dall'incidente vi sono semplici dati personali o se sono coinvolte anche le categorie particolari di dati come quelle definite all'art. 9 del GDPR (dati sensibili), quante persone possono essere coinvolte, se fra queste vi sono soggetti appartenuti a particolati categorie (es. minori) e quali rischi o danni per le libertà ed i diritti delle persone ha causato o potrebbe causare la violazione.

Quindi il titolare può stabilire se è necessario od opportuno:

- notificare la violazione al garante, in che modo eseguire la notifica (ad es. in più fasi), in particolare dovrà essere stabilito (motivandolo) se si ritiene probabile o improbabile che la violazione comporti rischi per i diritti e le libertà delle persone;
- comunicare la violazione agli interessati ed in che modo è possibile eseguire la comunicazione (art. 34 GDPR);
- comunicare la violazione agli organi di polizia;
- richiedere ulteriori verifiche tecniche necessarie per un'ulteriore comunicazione.

L'esecuzione delle attività di notifica o comunicazione sono successivamente descritte.

In ogni caso (siano necessarie o meno notifica e comunicazioni) occorre registrare l'evento analizzato documentando la violazione dei dati personali, le circostanze ad essa relative, le sue conseguenze e le valutazioni eseguite. Questo per consentire al Garante di verificare il rispetto della normativa (art. 33 par. 5 del GDPR).

Durante la valutazione occorre tenere presente che:

- vi è obbligo di notifica al Garante quando la violazione così come definita all'art. 4 punto 12) del GDPR comporta un rischio, anche presunto, per i diritti e le libertà delle persone fisiche. Cioè quando si è verificata una violazione di sicurezza che ha comportato, accidentalmente o in modo illecito, la: distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati sia che questi dati siano trattati all'interno che all'esterno dell'ente;
- la notifica deve essere eseguita entro il termine, non tassativo, di settantadue ore dal momento in cui il Titolare è venuto a conoscenza della violazione (cioè al termine della fase n. 1 sopra

descritta). Se non si osserva il termine delle settantadue ore il Titolare deve corredare la comunicazione con la giustificazione del ritardo (par. 1 Art. 33 GDPR). Il ritardo nella comunicazione potrebbe causare ulteriori controlli da parte del Garante con le conseguenti possibili sanzioni;

- il WP29 nelle sue linee guida precisa che la mancata comunicazione può essere sanzionata ma che nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria;

- Il WP29 raccomanda che il Titolare informi comunque l'autorità di vigilanza (notifica al Garante) il più presto possibile anche se non ha tutte le informazioni richieste e provvedere in un momento successivo all'integrazione della notifica, infatti nelle linee guida del WP29 ha altresì precisato che per soddisfare l'obbligo di notifica è possibile eseguire una comunicazione in più fasi. Questo può essere necessario quando è stata accertata una violazione ma non è ancora nota la sua portata. In proposito si esprime il GDPR che al paragrafo n. 4 dell'art. 33 riporta: "Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo";

- l'art. 33 paragrafo n. 1 chiarisce che non vi è obbligo di notifica della violazione quando è "improbabile" che comporti un rischio per i diritti e le libertà delle persone fisiche, ovviamente il giudizio che determina l'improbabilità del rischio deve essere riportato nel registro delle violazioni;

- Il WP29 chiarisce che l'obiettivo dell'obbligo di notifica è quello di incoraggiare i Titolari ad agire prontamente in caso di violazione, contenendo i possibili danni, recuperare, se possibile, i dati personali compromessi e chiedere il parere all'autorità di controllo. Inoltre, la notifica all'autorità di vigilanza entro le prime 72 ore può consentire al Titolare di assicurarsi che le decisioni in merito alla comunicazione o meno della violazione alle persone siano corrette.

- Anche nel caso in cui venga accertato in un momento successivo alla notifica che la violazione segnalata non imponga tale obbligo, il WP29 chiarisce ancora che "Non vi è alcuna penalità per segnalare un incidente che alla fine risulta non essere una violazione".

- la comunicazione agli interessati non è sempre necessaria (ma può essere opportuna), al paragrafo n. 3 dell'art. 34 del GDPR indica la comunicazione non necessaria quando:

  a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

  b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1 dello stesso art. 34;

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

- l'art. 34 del GDPR stabilisce inoltre che la comunicazione agli interessati deve essere eseguita "senza ingiustificato ritardo", ne consegue che tale comunicazione può essere eseguita anche

prima o contestualmente alla notifica al Garante senza cioè attendere una sua imposizione (anche questo potrebbe contribuire a mitigare eventuali sanzioni);

- il WP29 nelle sue linee guida evidenzia che lo scopo della notifica al Garante non è solo quello di ottenere indicazioni su se notificare o meno la violazione alle persone colpite. In alcuni casi sarà ovvio che, a causa della natura della violazione e della gravità del rischio, la notifica alle persone interessate dovrà essere effettuata senza indugio;
- il considerato n. 88 del GDPR inoltre puntualizza che: "Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.
- la comunicazione agli organi di polizia è necessaria quando è accertato che violazione sia da attribuirsi ad un comportamento illecito o fraudolento.

Più avanti nel documento un diagramma, tratto dalle linee guida del WP29 che sintetizza i requisiti necessari per la notifica al Garante o per la comunicazione agli interessati di una violazione di dati personali.

11. FASE N. 4 – NOTIFICA AL GARANTE

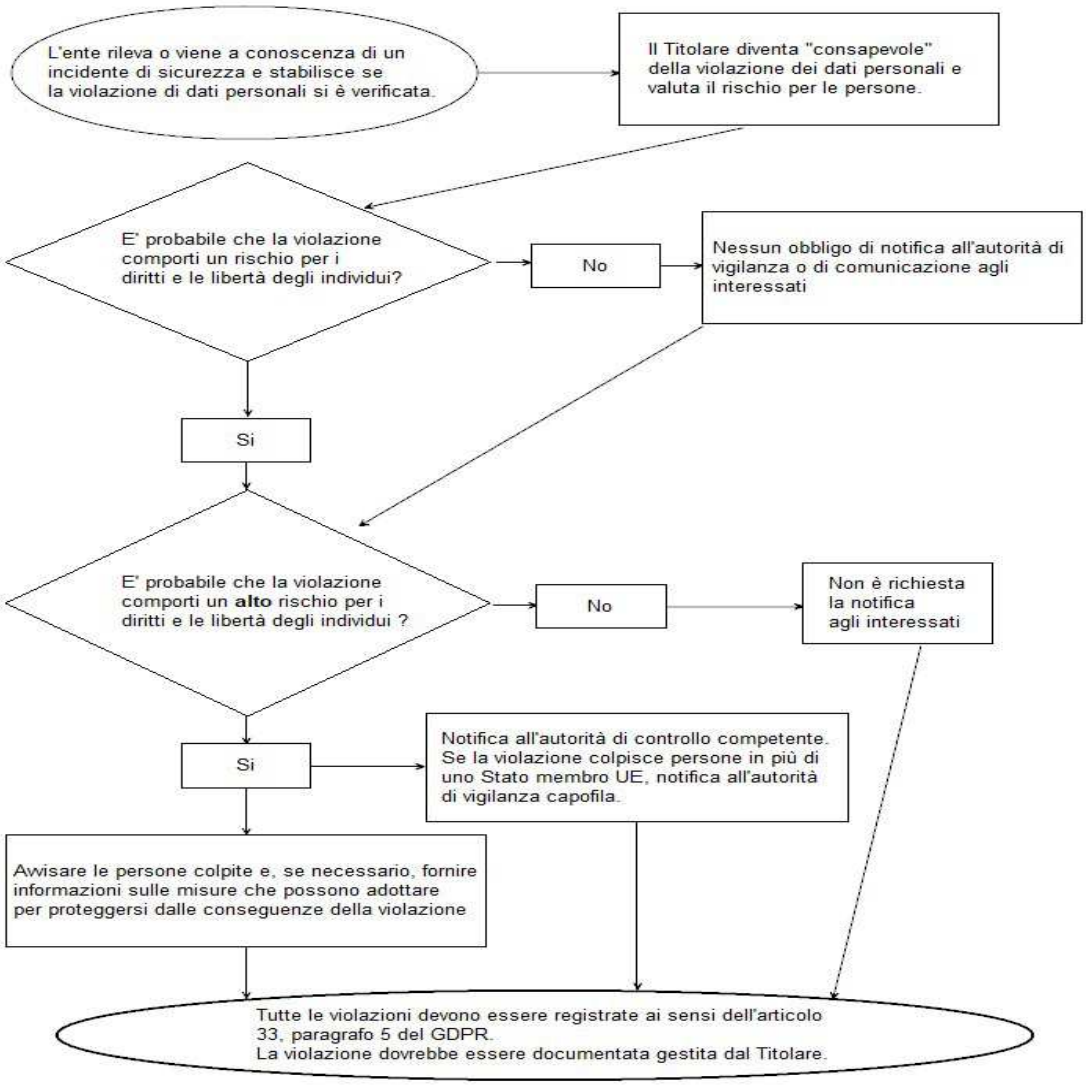
La notifica di una violazione al Garante è resa obbligatoria dall'art. 33 del GDPR nei casi in cui si verifichi una violazione dei dati personali a meno che sia improbabile che tale violazione presenti un rischi per i diritti e le libertà delle persone fisiche.

La definizione di violazione è invece riportata al punto 12) dell'art. 4 del GDPR (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 definizioni delle tipologie dei dati personali sono riportate ai punti 1), 13), 14) e 15) dello stesso art. 4 sopracitato e non differiscono sostanzialmente da quelle già in uso in Italia (D.Lgs n. 196/2003 smi e vari provvedimenti del Garante).

Qualora una violazione dei dati personali coinvolga dati di persone fisiche in più Stati Membri, il titolare deve notificare la violazione all'Autorità di controllo capofila. Inoltre, l'articolo 27 del GDPR impone al titolare del trattamento (e al responsabile del trattamento) di designare un rappresentante nell'UE in caso di applicazione dell'articolo 3, comma 2, del GDPR. In tali casi, il WP29 raccomanda che la notifica sia fatta all'Autorità di controllo dello Stato membro in cui è stabilito il rappresentante del titolare del trattamento nell' UE.

Diagramma di flusso che mostra i requisiti di notifica
tratto dalle linee guida WP29



Il considerando n. 85 del GDPR spiega che lo scopo della notifica è di limitare i danni che possono derivare per effetto di una violazione a carico degli interessati e che l'efficacia di questo dovere di limitazione dipende dalla tempestività e dall'adeguatezza con cui la violazione è affrontata.

Il gruppo WP29, nelle linee guida, chiarisce ulteriormente che la responsabilità del titolare deve essere commisurata secondo la sua capacità di scoprire tempestivamente un incidente ed indagarlo al fine di valutare l'obbligatorietà della notifica.

Il paragrafo n. 3 dell'art. 33 sopracitato definisce il contenuto minimo della notifica, essa deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La normativa Italiana, antecedente al GDPR (D.lgs. 133/2003 come modificato dal Dl. 28/05/2012 n 69) prevedeva per alcune categorie di operatori (fornitori di servizi di comunicazione elettronica accessibili al pubblico) l'obbligo di notifica al Garante.

Con provvedimento n. 393/2015 il Garante nazionale ha stabilito in quarantotto ore dalla conoscenza del fatto le violazioni dei dati o gli incidenti informatici che possano avere impatto significativo sui dati personali contenuti nelle proprie banche dati utilizzando per la comunicazione lo schema costituente l'allegato 1 a tale provvedimento. Lo stesso provvedimento stabilisce poi che le comunicazioni debbono essere inviate tramite posta elettronica o posta elettronica certificata all'indirizzo: databreach.pa@pec.gpdp.it;

Il termine per eseguire la notifica fissato dal Garante in quarantotto ore pare ora superato dalle disposizioni contenute nell'art. 33 del GDPR così come pare superato il modello per la comunicazione. Modello e modalità di trasmissione potrebbero essere aggiornati, integrati o meglio illustrati dal garante in un prossimo futuro.

Inoltre, l'obbligo di notificare l'incidente informatico da parte delle PA scaturisce dalla circolare AgID n. 2/2017 in quanto impone alle PA di comunicare gli incidenti informatici a CERT-PA ed al garante se l'incidente riguardi dati personali.

Al momento, ne sul sito internet del Garante (www.garanteprivacy.it) ne su quello di CERT-PA (www.agid.gov.it/it/sicurezza/cert-pa) sono presenti indicazioni o modelli per la comunicazione al Garante di un eventuale "*data breach*". Pertanto fino a quando non saranno disponibili indicazioni più precise pare corretto utilizzare un modello che contenga: le informazioni indispensabili richieste dal GDPR (par. 3 dell'art. 33), le informazioni già richieste con il modello fornito dal Garante con il citato provvedimento n. 393/2015 e le informazioni aggiuntive che il Titolare ritiene di voler fornire a dimostrazione della conformità al GDPR del suo operato. Tali informazioni dovranno essere trasmesse via PEC algli indirizzi di posta certificata specificati: dal garante sul proprio sito internet (attualmente protocollo@pec.gpdp.it) ed all'indirizzo indicato nel provvedimento n 393/2015 (databreach.pa@pec.gpdp.it).

Di seguito si riporta a puro titolo informativo, il modello reso disponibile dal Garante con provvedimento 393/2015;

Un possibile modello di notifica è invece riportato nell'allegato n. 3 al provvedimento con cui si approva il presente documento.

La compilazione del modello reso disponibile dal garante ai fornitori di servizi di comunicazione elettronica può anche essere effettuata on-line all'indirizzo internet::

https://www.garanteprivacy.it/documents/10160/2052659/Modello+segnalazione+data+breach.pdf

Modello reso disponibile dal Garante con il provvedimento n. 393/2015

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 :

Allegato 1

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

Allegato 1

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?

12. FASE N. 5 – SEGNALAZIONI A CERT-PA ED AGLI ORGANI DI POLIZIA

La comunicazione a CERT-PA

CERT-PA opera all'interno di AgID e ha il compito di supportare le amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica.

In conformità con le regole tecniche per la sicurezza informatica delle PA, CERT-PA è in grado di fornire alle amministrazioni richiedenti:

- servizi di analisi e di indirizzo, finalizzati a supportare la definizione dei processi di gestione della sicurezza;
- servizi proattivi, relativi alla raccolta e l'elaborazione di dati significativi ai fini della sicurezza cibernetica, l'emanazione di bollettini e segnalazioni di sicurezza;
- servizi reattivi, per poter gestire gli allarmi di sicurezza;
- servizi di formazione e comunicazione per promuovere la cultura della sicurezza cibernetica.

Dal 3 marzo 2014, è operativa l'unità del CERT-PA preposta all' "*Incident response*" e pertanto le Pubbliche Amministrazioni possono contattare, per il supporto alla risoluzione di incidenti informatici, gli analisti del CERT-PA utilizzando:

- Indirizzi di posta elettronica per segnalazioni e comunicazioni cert-pa@cert-pa.it per informazioni info@cert-pa.it
- Il numero di telefono 0685264321
- Il numero di FAX 0685264326
- Il sito web www.cert-pa.it

Prima di eseguire una comunicazione è opportuno verificare che i riferimenti di contatto non siano variati.

La comunicazione a CERT-PA è divenuta obbligatoria in seguito all'emanazione da parte di AgID della circolare n. 2/2017 del 18/04/2017.

In attuazione di questa circolare le PA hanno dovuto eseguire un'operazione di autoverifica dei loro sistemi informatici secondo "*standard*" definiti all'interno della stessa circolare, dare data certa a queste verifiche e conservarle nei propri archivi.

In caso di incidente informatico, la circolare obbliga le PA a trasmettere a CERT-PA il documento di autoverifica unitamente alla segnalazione dell'incidente.

Il comune ha ottemperato a queste disposizioni ed il documento è reperibile nell'archivio informatico degli atti amministrativi in quanto allegato a presa d'atto della Giunta Comunale di esecuzione dell'adempimento. Il documento è stato inoltre inviato in conservazione sostitutiva. Eventuali modifiche o nuove versioni del documento saranno conservate con gli stessi criteri.

Occorre tenere presente che il documento di cui sopra potrebbe essere suscettibile di aggiornamento e pertanto al momento della comunicazione occorrerà accertarsi di trasmettere l'ultima versione dell'autovalutazione .

Fino ad ora non sono stati emessi altri provvedimenti che definissero quali sono le informazioni da inserire nella segnalazione e pertanto, nel caso di incidente, si ritiene opportuno contattare CERT-PA per ottenere informazioni dettagliate.

Segnalazione agli organi di polizia

Occorre sempre effettuare denuncia agli organi di polizia quando la violazione ai dati sia conseguenza di comportamenti illeciti o fraudolenti.

Otre alle modalità conosciute per eseguire comunicazione o denuncia agli organi di polizia, per certe tipologie di "*data breach*" è possibile eseguire una comunicazione telematica, infatti da tempo è stato attivato un sito internet della Polizia Postale e delle Comunicazioni raggiungibile all'indirizzo //www.commissariatodips.it

All'interno di queste pagine è anche possibile reperire utili notizie sui tentativi di reato in corso ed eseguire denunce o segnalazioni di reati telematici previa registrazione.

Altre notizie su tentativi di frode sono ottenibili attraverso internet dal sito della struttura denominata CERT-PA (Computer Emergency Response Team Pubblica Amministrazione) operante all'interno di AgID e raggiungibile all'indirizzo //www.cert-pa.it/.

13. FASE N.6 – COMUNICAZIONE AGLI INTERESSATI

L'obbligo di dare comunicazione, senza ingiustificato ritardo, agli interessati di una violazione dei dati personali che li riguardano è previsto all'art. n. 34 del GDPR quando la violazione è suscettibile di prestare rischio elevato per i diritti e le libertà delle persone fisiche (paragrafo n. 1).

La comunicazione agli interessati, secondo quanto previsto dal paragrafo n. 3 dello stesso art. n. 34 del GDPR, non è richiesta quando:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

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

Al paragrafo n. 2 dello stesso art 34 viene precisato che la comunicazione deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e deve contenere almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del GDPR. Deve cioè contenere le seguenti informazioni:

b) il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda oppure può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta (paragrafo 4 dell'art. N . 34 del GDPR).

I considerato riportati ne GDPR collegati all'argomento sono:

- n. 75 - "I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati".

- n. 76 - "La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato".

- n. 86 - "Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione".

- n. 87 - "È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento".

- n. 88 - "Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali".

Il WP29, per consentire la valutazione dei fattori che determinano il rischio per le libertà e i diritti degli interessati, ha fissato i seguenti parametri:

- **tipo di "breach"**: il tipo di violazione è un parametro per la valutazione del rischio. La violazione dei dati sanitari di tutti i pazienti di un ospedale è ben diversa dalla perdita dei dati sanitari di un singolo paziente;

- **natura, numero e grado di sensibilità dei dati personali violati**: l'accesso al nome e all'indirizzo dei genitori di un figlio rappresenta un rischio diverso rispetto all'accesso da parte dei genitori naturali del nome e dell'indirizzo dei genitori adottivi;

- **facilità di associare i dati violati ad una persona fisica**: può accadere che i dati violati non siano facilmente riconducibili ad una determinata persona fisica;

- **gravità delle conseguenze per gli interessati**: quando il titolare del trattamento percepisce il rischio che i dati oggetto della violazione possono essere utilizzati immediatamente contro gli Interessati (es. sostituzione di persona);

- **numero di interessati esposti al rischio**: un parametro è sicuramente quello del numero degli interessati potenzialmente coinvolti;

- **caratteristiche del titolare del trattamento**: un attacco ad una struttura ospedaliera certamente è diverso dall'attacco ad una piccola azienda.

Mentre per far scattare l'obbligo di notifica è sufficiente che sussista una violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche, per la comunicazione occorre che tale rischio sia elevato.

Spetta dunque al Titolare stabilire, in fase di valutazione, se la comunicazione agli interessati è dovuta o meno oppure se opportuna, l'operazione non comporta solamente l'individuazione e qualificazione del rischio ma se tali rischi riguardano i diritti e libertà delle persone fisiche si deve anche procedere alla valutazione del livello di rischio..

La valutazione può essere molto complessa, il WP29 raccomanda al titolare, in caso di dubbio, di scegliere la strada di maggior tutela procedendo alla notifica.

14. FASE N. 7 – REGISTRAZIONE DELLE VIOLAZIONI

L'art. 33 Paragrafo n.5 del GDPR, prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

Ciò significa che le attività svolte nelle fasi precedenti (di scoperta dell'incidente, gestione tecnica, valutazione, notifica, comunicazione) come quelle successive, devono essere documentate, adeguate (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi), tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti.

Il WP29 nelle linee guida sottolinea che il titolare del trattamento dovrà documentare tutte le violazioni che si siano verificate, indipendentemente dall'obbligo di notifica, al fine di poter dimostrare la conformità al GDPR. il titolare del trattamento deve registrare i dettagli relativi alla violazione, comprese le circostanze, le sue conseguenze e i provvedimenti adottati per porvi rimedio (Art. 33 par. 5 del GDPR).

Il GDPR non specifica un periodo di conservazione per tale documentazione. Qualora tali registrazioni contengano dati personali, spetta al titolare del trattamento determinare il periodo appropriato di conservazione conformemente ai principi relativi al trattamento dei dati personali e indicare base legale per il trattamento.

La documentazione dovrà essere conservata, in conformità all'articolo 33, comma 5 del GDPR, nella misura in cui tale documentazione consenta all'Autorità di controllo di verificare il rispetto di tale articolo o, più in generale, del principio di responsabilizzazione.

Inoltre, il WP29 raccomanda di documentare la motivazione delle decisioni prese a seguito di una violazione. In particolare, se una violazione non è stata notificata, occorre documentare la motivazione circa tale decisione. Ciò dovrebbe ricomprendere i motivi per cui il titolare del trattamento ritiene improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone fisiche. In alternativa, se il titolare del trattamento ritiene che sussistano le condizioni per cui non è richiesta la comunicazione all'interessato (Art. 34 paragrafo n. 3 del GDPR), deve essere in grado di provare adeguatamente tale sussistenza.

Inoltre il GDPR non specifica quale debba essere il contenuto e la forma del "registro delle violazioni dei dati personali" ne il tipo di supporto su deve essere redatto, per estensione delle disposizioni contenute nell'art. n. 30 del GDPR (relativamente al registro delle attività di trattamento e registro delle categorie di attività di trattamento) si presume che tale registro possa anche essere di tipo elettronico.

<u>Tenuta del registro degli incidenti di sicurezza e delle violazioni dei dati personali</u>

Presso l'ente sono in corso d'acquisizione i diritti per l'utilizzo di un applicativo informatico che, come è stato richiesto in sede di affidamento, sarà anche in grado di gestire il registro di che trattasi.

Inoltre, nell'allegato n. 4 al provvedimento di approvazione del presente documento si riporta un possibile modello del "registro", è tuttavia possibile che in futuro l'evoluzione normativa o di pensiero espressa da organi superiori in materia di sicurezza o di gestione delle violazioni rendano necessarie modifiche di forma e sostanza al registro che si propone.

Il modello di registro di seguito riportato è stato realizzato come foglio di calcolo e si costituisce di due parti: una contiene i dati di sintesi sull'amministrazione titolare dei trattamenti, i riferimenti al responsabile della protezione dei dati comunali oltre ad un elenco di tutte le registrazioni eseguite con

riferimento alla relativa scheda, queste registrazioni saranno inserite inserite in singole schede con numerazione progressiva all'interno del foglio.

Fino a quando non sarà disponibile l'applicativo di cui sopra il registro degli incidenti di sicurezza e delle violazioni ai dati personali dovrà essere mantenuto su supporto informatico con l'ausilio di programmi di automazione ufficio (fogli di calcolo, editor di testi ecc..). Nel registro dovrà essere inserito in un'apposita scheda ogni evento di "data breach" anche se l'evento non ha generato violazione dei dati personali.

In attesa della sopracitata disponibilità, per garantire l'immodificabilità del registro, è necessario che ad ogni inserimento o variazione venga eseguita una stampa in formato PFD del documento, che tale stampa sia firmata digitalmente dal Sindaco (legale rappresentante dell'ente) o da suo delegato e che il documento risultante sia denominato utilizzando un numero progressivo per evidenziarne la versione.

Di norma la frequenza delle registrazioni deve avvenire contestualmente alla conclusione di una delle fasi previste per la gestione dei "*data breach*" ed in precedenza evidenziate mentre la frequenza del versionamento del registro sia eseguita almeno al termine delle fasi di notifica al Garante (se dovuta) ed al termine della registrazione definitiva dell'evento.

Periodicamente si dovrà informare l'intera amministrazione delle operazioni svolte.

Per eseguire materialmente le registrazioni il Titolare può nominare o incaricare un dirigente o altro personale dell'ente anche diverso da quelli previsti nella seguente sezione titolata "MATRICE DI DISTRIBUZIONE DELLE RESPONSABILITÀ".

Possibile modello di Registro delle violazioni dei dati personali.

Un possibile modello di registro delle violazioni costituisce l'allegato n. 4 al provvedimento di approvazione del presente documento.

15. MATRICE DI ASSEGNAZIONE DELLE RESPONSABILITÀ'

In questa sezione del documento, sotto forma di matrice "RACI" sono poste in relazione le principali risorse umane con le attività delle quali sono responsabili per l'attuazione delle varie fasi del processo di "*data breach*".

Di seguito sono fornite due diverse matrici, la prima contempla le attività da eseguire in caso di "*data breach*" impattante su risorse informatiche mentre la seconda per le attività relative ad incidente su risorse analogiche.

Nel caso di "*data breach*" che impatti sia su risorse informatiche che analogiche si dovranno seguire entrambe le matrici per la parte di riferimento.

Per la definizione delle matrici si è preso spunto da quanto reso disponibile dalla Regione Piemonte in collaborazione con il CSI Piemonte, l'ANCI, l'UNCEM ed alcuni Enti Piemontesi.

Ruoli chiave

La matrice prende la propria denominazione dalle iniziali dei ruoli previsti (in lingua inglese) per l'esecuzione delle attività dei processi aziendali. I ruoli previsti dalla matrice sono:

- **A - (Accountable)** è il responsabile dell'attività e/o colui che la approva (ci può essere una sola A per ogni attività);
- **R - (Responsible)** è il responsabile dell'esecuzione dell'attività, la dirige o per conto del quale l'attività è eseguita (possono esserci più R per ogni attività);
- **C - (Consulted)** rappresenta i soggetti che i responsabili (A ed R) avranno bisogno di consultare o che eseguono attività sotto la loro supervisione;
- **I – (Informed)** sono i soggetti (fisici o giuridici, interni od esterni) che non hanno bisogno di essere coinvolti attivamente nella parte del progetto in capo all'ente ma che devono essere informate relativamente a come progredisce o alle quali è necessario rivolgersi per le parti non di competenza del comune.

Definizione delle figure coinvolte

Figura	Descrizione della figura
Titolare	Intera amministrazione comunale, le azioni sono compiute dal suo legale rappresentate (Sindaco) o suo sostituto
Segretario Comunale	Segretario Comunale
Resp. Anticorruzione e Trasparenza	Responsabile Anticorruzione e Trasparenza (art. 7 L. 190/2012 e art. 43D,Lgs n. 33/2013)
RPD	Responsabile della protezione dei dati (art. 37 GDPR)
Delegato al trattamento	Soggetto delegato dal Titolare per sovrintendere alle operazioni di trattamento

Figura	Descrizione della figura
Resp. Trattamento Esterno	Soggetto esterno nominato "Responsabile" dal Titolare (art. 28 GDPR)
Resp. Sistemi informativi	Soggetto delegato dal Titolare per sovrintendere alle operazioni di trattamento eseguite con strumenti informatici. La figura può coincidere con quella di responsabile per la transazione al digitale (art. 17 CAD)
Resp. Conservazione digitale/sostitutiva	Soggetto nominato ai sensi del DPCM 03/12/2013 (regole tecniche in materia di conservazione)
Resp. Archivi	Soggetto nominato Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (art. 3 DPCM 3/12/2013 e art. 61 D.P.R. 445/2000)
Resp. Violazione	Colui o coloro a cui è attribuibile la violazione di sicurezza
Garante Privacy	Autorità nazionale a tutela dei diritti derivanti dalle norme sulla protezione dei dati personali
CERT-PA	Struttura che opera all'interno dell'Agenzia ed è preposta al trattamento degli incidenti di sicurezza informatica verificatesi nelle PA e a cui queste ultime sono obbligate a segnalare l'incidente
Forze dell'ordine	Organo di polizia o Magistratura a cui viene denunciata la violazione di sicurezza se ne ricorrono gli estremi
Interessati	Persone fisiche i cui dati sono stati coinvolti nell'incidente

Una persona fisica può ricoprire anche simultaneamente più figure.

Ne caso di assenza o indisponibilità si devono utilizzare i criteri di sostituzione previsti dalla normativa o nei provvedimenti interni appositamente assunti, in particolare:

- il sindaco è sostituito dal Vicesindaco e nel caso dal Consigliere anziano o loro delegato;
- il Segretario Generale è sostituito dal Vice Segretario o loro delegato;
- i Delegati al trattamento ed il Delegato ai Sistemi informativi sino sostituite dai soggetti previsti con i decreti sindacali per la sostituzione delle figure dirigenziali.

Matrice RACI per "data breach" impattante su risorse informatiche

FASI	1	2	3	4	5	6	7
Figure coinvolte	Rilevazione Acquisizione	Gestione Tecnica e Analisi	Valutazione	Notifica al Garante	Segnalazioni (Forze dell'ordine e CERT-PA)	Comunicazioni interessati e riscontri	Registrazione della violazione
Titolare / Sindaco	I	I	A	A	A	R	A
Segretario Comunale	I	I	C	I	I	I	I
Resp. Anticorruzione e Trasparenza		C	C	I	I	I	I
RDP	C	C	C	R	C	R	C
Delegato/i al trattamento	R	R	R	R	R	R	R
Resp. Trattamento Esterno (se coinvolto)	R	R/A	R	R	R	R	C
Responsabile comunicazione		I	I	I		A	I
Resp. Sistemi Informativi	R	A/R	C	R	R	R	C
Resp. Conservazione digitale/sostitutiva	R	I	C	I	I	I	I
Resp. Archivi	A	C	C	R	R	R	I
Resp. Violazione		C	I		I		
Garante Privacy				I		I	I
CERT-PA					I		
Forze dell'ordine					I		
Interessati						I	

Matrice RACI per "data breach" impattante su risorse analogiche

FASI	1	2	3	4	5	6	7
Figure coinvolte	Rilevazione Acquisizione	Gestione Tecnica e Analisi	Valutazione	Notifica al Garante	Segnalazioni (Forze dell'ordine)	Comunicazioni interessati e riscontri	Registrazione della violazione
Titolare / Sindaco	I	I	A	A	A	R	A
Segretario Comunale	I	I	C	I	I	I	I
Resp. Anticorruzione e Trasparenza		C	C	I	I	I	I
RDP	C	C	C	R	C	R	C
Delegato/i interno al trattamento	R	R	R	R	R	R	R
Resp. Trattamento Esterno (se coinvolto)	R	R/A	R	R	R	R	C
Resp. comunicazione		I	I	I		A	I
Resp. Archivi	A	A/R	C	R	R	R	I
Resp. Violazione		C	I		I		
Garante Privacy				I		I	I
Forze dell'ordine					I		
Interessati						I	

16. ALLEGATI:

Si devono considerare come parte integrante di questo documento tutti gli allegati approvati con lo stesso suo provvedimento di approvazione, in particolare:

- **Allegato n. 1** – Il presente documento.
- **Allegato n. 2** – Modello di comunicazione al titolare di un "data breach".
- **Allegato n. 3** – Possibile modello di notifica all'autorità Garante nazionale per la protezione dei dati personali di una violazione.
- **Allegato n. 4** – Registro delle violazioni di dati personali.
- **Allegato n. 5** – Informativa da rendere a chi effettua una segnalazione di "*data breach*".

17. AGGIORNAMENTO DEL PRESENTE DOCUMENTO E DEGLI ALLEGATI

Sulla base dell'evolversi della normativa e del pensiero in materia di protezione dei dati personali potrà presentarsi la necessità di aggiornare o integrare il presente documento.

La frequenza di aggiornamento non può essere stabilita a priori.

Qualora le autorità o gli organismi pubblici mettessero a disposizione modelli di comunicazioni o metodologie dei comunicazione che sostituiscano i modelli qui riportati si dovranno immediatamente adottare le disposizioni pervenute ed il presente documento e/o i suoi allegati potranno essere modificati anche in tempi successivi.

Allo stesso modo ci si dovrà comportare se l'applicativo informatico per l'utilizzo del quale sono in corso di acquisizione i diritti fosse configurato in modo da produrre notifiche, segnalazioni, comunicazioni e registri utilizzando dei modelli diversi da quelli qui riportati.

18. ELEMENTI DI SUPPORTO ALLE FASI DI VERIFICA TECNICA E VALUTAZIONE

<u>Identificazione della tipologia della violazione</u>

Tra i parametri ritenuti necessari dal WP29 per consentire la valutazione dei fattori che determinano il rischio per le libertà e i diritti degli interessati è ricompreso il tipo di violazione. Questo è un parametro necessario per la valutazione del rischio (la violazione dei dati sanitari di tutti i pazienti di un ospedale è ben diversa dalla perdita dei dati sanitari di un singolo paziente).

Nella fase di gestione tecnica precedentemente descritta è necessario stabilire se la violazione appartiene ad una o più categorie tra quelle individuate dal WP29 come di seguito meglio descritto:

Violazione di riservatezza:

Questo tipo di violazione può manifestarsi in diversi modi, a puro titolo di esempio:

- quando un incaricato nella redazione di un atto non rediga la versione con omissione dei dati da non pubblicare e l'atto viene pubblicato nella sua interezza;
- quando si inoltrano messaggi contenenti dati a soggetti non interessati al trattamento;
- quando un operatore abbandona la propria postazione di lavoro senza prima prendere le opportune precauzioni (riporre la documentazione, lasciare attive procedure sulla risorsa informatica utilizzata, ecc..) e terze persone possono prendere visione di informazioni;
- quando un soggetto in malafede comunica dei dati non pubblici a terzi in modo non autorizzato (ad esempio elenchi di residenti estratti dai sistemi informatici comunicati a società operanti in campo pubblicitario).

Nei casi in cui la violazione sia eseguita in modo consapevole difficilmente può essere rilevata dall'interno (può emergere per segnalazione dell'interessato o di altri organismi pubblici, ad esempio dalle forze dell'ordine o dal Garante oppure può essere rilevata durante l'esecuzione di indagini o verifiche).

La violazione di integrità:

Questa tipologia di violazione si verifica quando avviene un'alterazione di dati personali non autorizzata o accidentale. Un'alterazione accidentale si può verificare per errore umano (ad es. nel momento di un aggiornamento delle informazioni), per un disguido tecnico quando all'interno di una base dati si perdono i collegamenti a determinate informazioni (integrità referenziale) mentre l'alterazione non autorizzata può essere la conseguenza di un attacco esterno o di una manipolazione inconsapevole da parte di personale non competente.

La violazione di disponibilità:

La valutazione di questa tipologia di violazioni è particolarmente delicata in quanto può essere falsata da alcuni fattori.

La casistica è molto amplia, il WP29 nelle sue linee guida riporta gli esempi di:

- dati cancellati accidentalmente o da soggetti non autorizzati;
- perdita della chiave di decriptazione;
- quando i dati persi dall'ambiente di produzione non possano essere ripristinati integralmente dalle copie di sicurezza e si debba provvedere manualmente alla loro ricostruzione;
- quando si verifica un'interruzione significativa di un servizio ("*black out*" elettrico o attacchi di tipo "d*enial of service*").

In proposito occorre ricordare che l'art. 32 del GDPR richiede al titolare di mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; in particolare:

- alla lettera b) è richiesta: "la capacità di assicurare su base permanente la disponibilità dei sistemi e dei servizi di trattamento";
- alla lettera c) è richiesta "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".

Determinare se vi è stata una violazione della riservatezza o dell'integrità è relativamente chiaro mentre determinare se ci sia stata una violazione della disponibilità potrebbe essere meno ovvio.

Una violazione sarà sempre considerata come una violazione della disponibilità in caso di perdita o distruzione permanente dei dati personali, ma nel caso in cui l'indisponibilità sia solo temporanea la si deve considerare o meno un "*data breach*" e quindi richiedere la notificata al Garante?

Il gruppo WP29 precisa che: "un incidente di sicurezza con conseguente indisponibilità dei dati personali per un certo periodo di tempo è anche un tipo di violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e libertà delle persone fisiche. Per essere chiari, dove i dati personali non sono disponibili a causa del sistema pianificato manutenzione effettuata non è una violazione della sicurezza".

Si pensi alla temporanea indisponibilità di una rete di comunicazione ed al disservizio che ne consegue:

- se il disservizio si limita all'impedimento temporaneo di inviare una "*newsletter*" non vi sarebbe impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati. Quindi non vi sarebbero gli obblighi di notifica e comunicazione agli interessati ma rimarrebbero comunque l'obbligo di registrazione nell'evento nel registro degli incidenti informatici e sarebbero da valutare la necessità di comunicazione dell'incidente a CERT-PA e la necessità di segnalazione agli organi di polizia.
- Se però il disservizio temporaneo può causare (anche solo potenzialmente) impatto rispetto ai dati personali ed ai diritti dell'interessato, come nel caso in cui il temporaneo impedimento di accesso ad un archivio cartaceo per reperire dati da utilizzare per rendere una certificazione necessaria all'interessato per concludere degli adempimenti contrattuali (e per la quale l'interessato non può ricorrere ad autocertificazione) l'incidente è da considerare un "*data breach*" dovrà essere necessariamente notificato al Garante e registrato sul registro degli incidenti mentre è da valutare la necessità di eseguire la comunicazione all'interessato e alle forze dell'ordine (l'incidente potrebbe non essere di natura dolosa) ed è da escludersi la segnalazione a CERT-PA.

Nella gestione tecnica di questa tipologia di incidenti dovrà emergere l'impatto che il disservizio ha causato o potrebbe causare rispetto ai dati personali ed ai diritti degli interessati. Dovranno anche essere desunte informazioni circa la natura dell'incidente occorso, le misure preventive poste in essere per evitarlo e le misure adottate per minimizzarne le conseguenze. Infatti al punto c) dell'art. 32 del GDPR è richiesta al Titolare la "capacità di ripristinare l'accesso ai dati personali".

In questo caso si dovranno comunicare al Titolare notizie aggiuntive, tra queste:

- la causa e la natura del disservizio o della rottura;
- tempi previsti per la riparazione;
- i tempi e le modalità per il ripristino della disponibilità dei dati;
- l'esistenza di misure adottate precedentemente all'evento per contrastare il rischio;
- l'eventualità di perdita di dati durante il ripristino, la loro tipologia, se i dati sono reperibili in altre aree dei sistemi o presso terzi e le tempistiche per il recupero.

Da quanto sopra si ricava che un incidente che determini la non disponibilità di dati per un periodo di tempo, anche breve, deve essere comunque considerato violazione e, dunque, deve essere comunque

documentato, mentre l'obbligo di notifica e quello aggiuntivo delle comunicazione devono essere valutati caso per caso in relazione ai diritti ed alla libertà degli interessati.

19. ELEMENTI DI SUPPORTO PER VALUTARE LA NECESSITA' DI NOTIFICA AL GARANTE E DI COMUNICAZIONE AGLI INTERESSATI

Il gruppo WP29 chiarisce che la responsabilità del titolare deve essere commisurata secondo la sua capacità di scoprire tempestivamente un incidente ed indagarlo al fine di valutare l'obbligatorietà della notifica e della comunicazione agli interessati.

Allo scopo, il WP29, ha reso disponibile in appendice alle linee guida per la gestione dei "*data breach*" una tabella che fornisce diversi scenari ed evidenzia la necessità o meno di eseguire una notifica al garante e/o una comunicazione agli interessati.

Si riporta di seguito la tabella di cui sopra tradotta in lingua italiana.

Esempio	Notifica garante ?	Comunicaz. interessati ?	Note e raccomandazioni
i. Un soggetto ha memorizzato il backup di un archivio di dati personali in modo crittografato su una chiavetta USB. La chiave viene rubata.	No	No	Fino a quando: i dati rimangono crittografati con un buon algoritmo, il backup dei dati esiste, la chiave non è compromessa e idati possono essere ripristinati in breve tempo, non può essere considerata una violazione notificabile. Tuttavia se successivamente viene meno uno di questi elementi la notifica è richiesta.
ii. Un soggetto mantiene un servizio online. In conseguenza di un attacco informatico a quel servizio i dati personali sono rubati. Il soggetto ha i clienti in un singolo Stato membro dell'UE.	Si, se ci sono probabili conseguenze per gli individui.	Si, a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per gli individui è alta.	
iii. A causa di una interruzione elettrica di diversi minuti in un call center causa l'impossibilità di ricevere aiuto da parte di alcuni clienti e di accedere ai loro dati.	No	No	Questo non è una violazione notificabile, ma l'incidente deve essere registrato per effetto dell' Art. 33, paragrafo 5 del GDPR. Registrazioni appropriate devono essere mantenute dal responsabile.
iv. In seguito ad un attacco "ransoware" tutti i dati vengono criptati e non sono disponibili dei salvataggi dai quali sia possibile eseguirne il	Si, se ci sono probabili conseguenze per gli individui e vi è una perdita di disponibilità dei dati.	Si, se la natura dei dati personali interessati ed il possibile effetto della perdita di disponibilità comportino probabili conseguenze per gli	Se vi fosse stato un backup disponibile e dati potessero essere ripristinati in tempo utile non sarebbe necessaria la notifica e la comunicazione

Esempio	Notifica garante ?	Comunicaz. interessati ?	Note e raccomandazioni
ripristini. Dalle indagini condotte è risultato presente sul sistema il solo il virus che ha criptato i dati e non ci sono altre infezioni.		interessati.	agli individui perché non ci sarebbe stata perdita permanente di disponibilità o confidenzialità. Però, se il titolare è diventato consapevole dell'incidente da in seguito a segnalazione da parte di terzi, significa che può far eseguire un'indagine per valutare la conformità dei sistemi ai dettami dell'art, 32.
v. Un individuo telefona alla call center della propria banca per segnalare un data breach. L'individuo ha ricevuto un estratto mensile di qualcun altro. Il titolare esegue una breve verifica (es. completata entro 24 ore) e stabilisce con una ragionevole fiducia che la violazione dei dati personali si è effettivamente verificata e ha trovato un difetto nei sistemi che fa pensare che altri individui sono stati o potrebbero essere colpiti.	Si	Si, solo agli interessati colpiti se esiste un rischio alto ed è chiaro che altri soggetti non siano stati colpiti.	Se dipo successive indagini, si identifica che più individui sono stati colpiti dalla violazione deve essere fatta un a notifica al Garante di aggiornamento ed il Titolare deve eseguire una ulteriore comunicazione agli interessati se esiste un alto rischio per i loro diritti e libertà.
VI. Un titolare gestisce un mercato online ed ha clienti in più Stati membri. Il sistema viene attaccato e vengono diffusi sul web utenze, password e cronologia degli acquisti.	Sì, segnalare anche all'autorità di controllo europea se la violazione coinvolge processi cross-border.	Si, perché potrebbe comportare un altro rischio	Il titolare dovrebbe eseguire azioni di mitigazione del rischio. Ad es. forzare la reimpostazione delle password degli account interessati. Il titolare dovrebbe anche considerare se vi sono altri obblighi di notifica, per esempio quelli previsti dalla direttiva NIS, per i fornitori di servizi digitali.
vii. Un sito web di una società di servizi in hosting che agisce per l'elaboratore di dati identifica un errore nel codice che controlla le autorizzazioni utente. L'effetto del difetto causa che qualsiasi utente può accedere ai dettagli dell'account di qualsiasi altro utente.	Come il titolare anche, il fornitore in hosting del sito web deve avvisare i suoi clienti interessati (il titolare) senza indebito ritardo. Supponendo che il fornitore in hosting del sito web abbia condotto proprie indagini i Titolari interessati dovrebbero essere ragionevolmente sicuri in	Si	Il fornitore dell'hosting deve considerare se vi sono altri obblighi di notifica, per esempio quelli previsti dalla direttiva NIS, per i fornitori di servizi digitali. Se non ci sono evidenze che questa vulnerabilità sia stata sfruttata, la violazione potrebbe non essersi verificata e non sia necessaria

Esempio	Notifica garante ?	Comunicaz. interessati ?	Note e raccomandazioni
	quanto se ognuno ha ha subito una violazione è probabile che sia considerato come "Diventare consapevole" una volta sia stato notificato dal fornitore dell'hosting. Il titolare quindi deve avvisare l'autorità.		la notifica ma è probabile che debba essere registrata o che evidenzi una situazione di non conformità ai sensi dell'articolo 32.
viii. In un ospedale non sono disponibili le cartelle cliniche per un periodo di 30 ore a causa di un attacco informatico.	Si la notifica è obbligatoria	Si, segnalate ad ogni individuo coinvolto	
ix. I dati personali di un Gran numero di studenti lo sono stati inviati per errore ad una mailing list con più di 1000 destinatari.	Si	Sì, la comunicazione agli interessati deve essere eseguita in base allo scopo ed al tipo di dati personali coinvolti e il livello di gravità delle possibili conseguenze.	
x. Una mail commerciale è stata inviata a destinatari nel campo "a:" anziché per conoscenza "cc:" quindi ogni destinatario può vedere l'indirizzo degli altri.	Si, la notifica al Garante potrebbe essere obbligatoria se: sono interessati un gran numero di individui, se la mail conteneva dati sensibili (ad es. la mailing list di uno psicoterapeuta) o se esistono altri fattori che presentino alti rischi (ad es la posta contiene le password iniziali).	Sì, segnalare agli individui se lo scopo e il tipo di dati personali coinvolti ha una gravità che possa determinare possibili conseguenze.	La notifica potrebbe non essere necessaria se non sono stati rivelati dati sensibili e se è stato rivelato solo un minor numero di indirizzi.