PROVINCIA DI RAVENNA
SISTEMI INFORMATIVI, DOCUMENTALI E SERVIZI DIGITALI

PROCEDURA DI GESTIONE DI DATA BREACH AI SENSI DEL REGOLAMENTO UE 679/2016 NELLA PROVINCIA DI RAVENNA

TITOLO I– DISPOSIZIONI COMUNI E PRINCIPI GENERALI

ARTICOLO 1 - FINALITÀ

Una violazione dei dati personali (c.d. *data breach*) può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Il presente documento rappresenta il riferimento della Provincia di Ravenna per la regolamentazione della gestione degli incidenti di sicurezza informatica che possono occorrere ai servizi.

La corretta gestione degli incidenti di sicurezza permette di evitare o minimizzare la compromissione dei dati dell'organizzazione in caso di incidente; permette inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, di migliorare continuamente la capacità di risposta agli incidenti.

Inoltre, con specifico riferimento all'obbligo di cui all'art. 33 del GDPR n. 679/2016, il presente documento individua quali siano le violazioni che ricadono nell'ambito della suddetta normativa, i casi in cui l'Ente deve notificare i data breach all'Autorità Garante ed agli interessati, le misure atte a trattare il rischio e la documentazione da produrre.

Si rappresenta che l'art. 32 del Regolamento dispone che devono essere approntate misure tecniche e organizzative adeguate per garantire un livello adeguato di sicurezza dei dati personali. Individuare, indirizzare e segnalare tempestivamente un incidente di sicurezza, come una violazione di dati, è espressione dell'adeguatezza delle misure implementate dall'Ente.

L'ambito di applicazione è rappresentato da sistemi ICT facenti parte del Sistema Informatico della Provincia di Ravenna (di seguito SInfP) dell'Ente e sono presi in considerazione incidenti che possono scaturire sia attraverso l'azione di un attacco informatico portato da elementi esterni all'organizzazione sia generati da un eventuale comportamento negligente o scorretto, di natura ostile con obiettivi frodatori da parte di un collaboratore dell'ente.

Tutte le violazioni dei dati personali sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

L'obbligo di cui agli artt. 33 e 34 del Regolamento trova applicazione nei soli casi in cui la violazione riguardi dati personali, come definiti dall'art. 4 n. 1).

Il presente documento è applicabile alle risorse ed ai servizi di tipo informatico gestiti in modo diretto oppure esternalizzato da parte della Provincia di Ravenna.

ARTICOLO 2 - RIFERIMENTI NORMATIVI

La presente procedura è stata redatta in ottemperanza a quanto disposto dalle norme sotto riportate:

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Guidelines on Personal data breach notification under Regulation 2016/679 – article 29 data protection working party (Adopted on 3 October 2017 – as last Revised and Adopted on 6 February 2018)

TITOLO II – DEFINIZIONI

ARTICOLO 3 - INCIDENTE DI SICUREZZA

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

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

Al fine di aumentare la sicurezza dei sistemi ICT e di ridurre al minimo gli incidenti di sicurezza, l'Ente promuove l'adozione e l'attuazione di comportamenti, attività e regolamenti volti a ridurre il livello di rischio e l'esposizione a possibili attacchi informatici.

ARTICOLO 4 - DATA BREACH

Il Regolamento generale sulla protezione dei dati (GDPR 2016/679/UE) definisce la violazione dei dati personali come "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Le violazioni declinate dalla norma sono sintetizzabili come

- "**Violazione della riservatezza**", che si ha in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.
- "**Violazione dell'integrità**", che si ha in caso di alterazione non autorizzata o accidentale dei dati personali
- "**Violazione della disponibilità**", che si ha in caso di perdita o distruzioni di dati personali o di impossibilità di accesso ai dati personali da parte di soggetti autorizzati

Va sottolineato che una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione di queste.

Gli effetti di una violazione possono causare danni fisici, materiali o immateriali, ovvero sia la perdita del controllo sui propri dati personali, la limitazione dei loro diritti, discriminazione, furto d'identità o frode, perdita finanziaria, inversione non autorizzata di pseudonimizzazione, danno alla reputazione e perdita di riservatezza dei dati personali protetti dal segreto professionale . Può anche includere qualsiasi altro significativo svantaggio economico o sociale per tali individui.

ARTICOLO 5 - NOTIFICA AL GARANTE E AGLI INTERESSATI

In caso di data breach l'Ente deve valutare i rischi per i diritti e le libertà delle persone fisiche, registrando le evidenze di tale analisi.

Nell'eventualità che tale valutazione rappresenti elementi di rischio per i diritti e le libertà delle persone fisiche l'Ente effettua la notifica al Garante delle violazioni di dati personali.

Quando le violazioni di dati comportano un rischio che è valutato come elevato per i diritti e le libertà delle persone fisiche, le stesse devono essere comunicate agli interessati senza ingiustificato ritardo, fornendo loro specifiche informazioni in ordine alle salvaguardie che devono adottare per proteggere loro stessi dalle conseguenze della violazione.

Questo rischio esiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone i cui dati sono stati violati. Tale rischio è presunto quando il data breach riguarda le categorie particolari di dati di cui all'art. 9 del GDPR 2016/679/UE.

I criteri che devono guidare la valutazione del suddetto rischio sono i seguenti:

- la tipologia di violazione
- la natura dei dati violati
- il volume dei dati violati
- il numero di individui cui si riferiscono i dati violati
- caratteristiche speciali degli individui cui si riferiscono i dati violati
- il grado di identificabilità delle persone
- la gravità delle conseguenze per gli individui

La valutazione deve essere condotta secondo una metodologia operativa adeguata che viene dettagliata nel seguito.

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

ARTICOLO 6 - RUOLI E RESPONSABILITA’

Al SIDD (unità operativa della Provincia di Ravenna dedicata alla gestione della sicurezza informatica del Sistema Informatico della Provincia di Ravenna) compete la gestione, in accordo con il Data Protection Officer (DPO), di tutte le attività inerenti l’analisi e la gestione di un incidente di sicurezza, ivi comprese quelle relative alla sua notifica e documentazione; garantendo che il processo di gestione incidenti sia sempre adeguato alle esigenze dell’Ente.
In particolare pone in essere tutte le misure organizzative necessarie per poter garantire la facilità e tempestività di contatto (es. contatto reperibile H24, indirizzo e-mail, numero di telefono, link presente nella Intranet) in caso di segnalazione di un data breach.

ARTICOLO 7 - SEGNALAZIONE DI UN INCIDENTE

Nel caso si rilevi un potenziale incidente oppure un comportamento sospetto, il personale deve rivolgersi al SIDD (unità operativa della Provincia di Ravenna dedicata alla gestione della sicurezza informatica del Sistema Informatico della Provincia di Ravenna), nelle modalità opportuna indicate nella Intranet dell’Ente.
Nel caso di segnalazioni di incidente da parte di soggetti terzi, l’Ente avvia senza indugio un’indagine volta a verificare che sia avvenuta effettivamente la violazione di dati segnalata.

ARTICOLO 8 - GESTIONE DELL'INCIDENTE

Ricevuta la segnalazione, è compito del SIDD attivarsi per valutare se un evento riscontrato sia effettivamente riconducibile ad un incidente di sicurezza oppure si tratti di un cosiddetto falso positivo. Le operazioni di identificazione (Detection and Analysis) devono permettere di verificare, per ogni caso di evento anomalo o sintomo di un incidente, se si è in presenza di un incidente reale di sicurezza.

Il SIDD, durante le operazioni relative alla gestione dell'incidente di sicurezza, provvede alla redazione di un rapporto (di seguito Rapporto) nel quale registra i dati rilevati relativamente all'incidente occorso, tutte le operazioni effettuate, i soggetti coinvolti, le analisi condotte e i risultati rilevati fino alla conclusione della gestione dell'incidente.

Nell'effettuare questa analisi, il SIDD, può:

- coinvolgere il DPO che, nel caso di data breach esercita le proprie funzioni di monitoraggio della conformità, fornendo il proprio parere in ordine alla necessità di effettuare la notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali e, quindi, sulle valutazioni precedentemente descritte.
- coinvolgere, a seconda della gravità dell'incidente, i vertici dell'Ente o i Dirigenti competenti per gli aspetti di comunicazione interna ed esterna e nel caso, durante la gestione dell'incidente, emergano responsabilità da parte di personale interno dell'Ente coinvolgere la struttura che si occupa di gestione del personale.
- nel caso in cui le attività di analisi dell'incidente di sicurezza evidenzino particolari difficoltà oppure impatti che si estendono al di fuori del perimetro dell'Ente, il SIDD deve valutare l'opportunità o la necessità di coinvolgere le strutture di riferimento regionali e nazionali (ad esempio LepidaSpA considerando il proprio ruolo nell'ambito della sicurezza della Community Network, CERT-PA, …). Inoltre, il SIDD deve prevedere il coinvolgimento dei propri fornitori di servizi ICT per il supporto all'analisi e per l'ottenimento di informazioni utili oltre alle autorità di pubblica sicurezza nel caso in cui l'incidente possa presentare risvolti dal punto di vista penale.

Durante la gestione dell'incidente fino alla chiusura dello stesso, il SIDD provvede alla redazione di un Rapporto di Incidente di Sicurezza contenente tutte le informazioni rilevate, le operazioni eseguite e i soggetti coinvolti.
Tale rapporto sarà opportunamente conservato in formato elettronico in una cartella assoggettata a backup periodico e ad accesso opportunamente limitato.

ARTICOLO 9 - EVENTI VERIFICABILI

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

Tipologia Incidente	Descrizione

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

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

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

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

ARTICOLO 10 - GRAVITA' DEGLI INCIDENTI

E' necessario stabilire la gravità dell'incidente di sicurezza; per fare ciò inizialmente ci si può avvalere della seguente matrice contraddistinta da una valutazione di tipo qualitativo, ma la classificazione della gravità dell'incidente è comunque discrezionale, dipendente dal evento effettivamente occorso.

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

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

Gravità incidente di sicurezza	*Descrizione*
	• Nessuna o limitata perdita di operatività o di business da parte di un ridotto numero di dipendenti.

Per alcuni incidenti può risultare difficile assegnare un livello di gravità definitivo prima che l'analisi sia completa; in tal caso occorre valutarla sulla base delle evidenze note sino a quel momento, assumendo che la gravità potrebbe molto probabilmente aumentare nel caso non si effettui alcuna operazione di contenimento.

In ogni caso, è opportuno verificare ciclicamente, nel periodo in cui l'incidente è in corso, la gravità assegnata allo stesso in quanto essa può variare nel tempo.

ARTICOLO 11 - VALUTAZIONE DEI RISCHI DERIVANTI DAL VERIFICARSI DEL DATA BREACH

In caso di data breach l'Ente valuta i rischi per i diritti e le libertà delle persone fisiche, utilizzando i criteri di seguito indicati:

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

personali siano nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose il livello di rischio potenziale sarà più elevato.

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

ARTICOLO 12 - NOTIFICA AL GARANTE

Nei casi in cui l'incidente consista in una violazione di dati personali, l'Ente deve notificare l'incidente al Garante per la protezione dei dati personali se, sulla scorta della valutazione approfondita, strutturata e documentata si assuma come probabile che la violazione dei dati personali presenti effettivamente un rischio per i diritti e le libertà delle persone fisiche.
La comunicazione al Garante, a cura del DPO, deve ricomprendere ogni informazione utile; l'elenco seguente, non esaustivo, comprende le informazioni inviate:

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

ARTICOLO 13 - NOTIFICA DELLA VIOLAZIONE AGLI INTERESSATI

Le violazioni che comportano un rischio elevato per i diritti e le libertà delle persone fisiche sono comunicate agli interessati senza ingiustificato ritardo, con un linguaggio chiaro e comprensibile agli utenti; nella comunicazione devono essere riportate almeno le seguenti informazioni:

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

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

ARTICOLO 14 - CONTINUITA' OPERATIVA

Nel caso si verifichi un incidente di sicurezza che possa pregiudicare per un periodo sufficientemente lungo la disponibilità delle informazioni, occorre porre in essere le

misure volte a garantire la continuità operativa al fine di garantire la disponibilità dei dati e dell'infrastruttura ICT preposta all'erogazione dei servizi informatici.

ARTICOLO 15 - CONTENIMENTO, RIMOZIONE E RIPRISTINO

Rilevato l'incidente, è compito del SIDD, quale unità responsabile della sicurezza informatica:

- minimizzare i danni relativi all'incidente ed impedirne la propagazione;
- acquisire le eventuali evidenze digitali di reato prima che queste possano essere compromesse;
- documentare in modo dettagliato tutte le operazioni eseguite riportandole nel Rapporto di cui all'articolo precedente;
- gestire correttamente il processo di ripristino dei sistemi e delle applicazioni;
- acquisire nel modo appropriato le eventuali evidenze digitali di reato;
- formulare proposte volte a migliorare la procedura stessa.

ARTICOLO 16 - ATTIVITA' POST INCIDENTE

Il Rapporto, di cui all'articolo precedente, dovrà essere opportunamente conservato, comprensivo di tutta l'ulteriore documentazione prodotta e raccolta (es. notifica all'Autorità del Garante).
Nell'ottica di migliorare e incrementare la sicurezza, l'Ente, compatibilmente con le proprie risorse finanziarie e tecniche, provvede a porre in essere misure volte ad evitare incidenti futuri con caratteristiche analoghe a quello accaduto.