Comune di Rimini

Allegato alla deliberazione di Giunta comunale n.

COMUNE DI RIMINI
PROCEDURA DI GESTIONE DATA BREACH
AI SENSI DEL REGOLAMENTO UE
2016/679

Indice generale

1. CONTESTO APPLICATIVO

Il presente documento rappresenta il riferimento del Comune di Rimini per la regolamentazione della gestione degli incidenti di sicurezza informatica e cartacea che possono occorrere nello svolgimento delle proprie attività e, in particolare, per l'individuazione delle violazioni che ricadono nell'ambito del Regolamento UE 2016/679, per i casi in cui l'Ente deve notificare i *data breach* all'Autorità Garante ed agli interessati, per le misure atte a trattare il rischio e la relativa documentazione da produrre.

La procedura di gestione data breach costituisce allegato al Modello organizzativo dell'Ente.

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

La presente regolamentazione riguarda sia i supporti cartacei che i sistemi ICT facenti parte del Sistema Informatico del Comune di Rimini e sono presi in considerazione incidenti che possono scaturire sia attraverso l'azione attivata da elementi esterni all'organizzazione (ad esempio di un attacco informatico portato per la dimensione ICT) sia generati da un eventuale comportamento negligente o scorretto, di natura ostile con obiettivi frodatori da parte di un collaboratore dell'ente.

Il presente documento, inoltre, è applicabile alle risorse ed ai servizi di tipo informatico gestiti in modo diretto oppure esternalizzato da parte del Comune di Rimini. In relazione ai servizi di tipo informatico gestiti tramite esternalizzazione, le modalità di gestione degli incidenti vengono garantite dai soggetti esterni in quanto Responsabili del trattamento, mentre le modalità di comunicazione al Comune Titolare, e di collaborazione nella gestione della violazione, vengono indicate all'interno dell'accordo di nomina del Responsabile, in base a quanto di seguito indicato.

2. RIFERIMENTI NORMATIVI

La presente procedura viene redatta in ottemperanza a quanto disposto da

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR);
- 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)

In relazione al Regolamento UE si richiamano, in particolare, i considerando n. 85, 86, 87, 88 e gli artt. 32, 33, 34. L'art. 32 del Regolamento UE dispone di approntare tutte le misure tecniche e organizzative 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.

In caso di violazione dei dati personali, l'art. 33 del Regolamento UE 2016/679 impone al titolare del trattamento la notifica della violazione all'autorità di controllo competente a norma dell'articolo 55 del Regolamento UE, che in Italia è individuata nel Garante Privacy, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore è corredata dei motivi del ritardo.

Non tutte le violazioni di dati personali comportano la notifica al Garante Privacy, ma solo quelle che, ai sensi dell'art. 34 del Regolamento UE, sono suscettibili di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

L'attività di prevenzione degli incidenti è contenuta nel Modello organizzativo sulla protezione dei dati personali e nelle policy di sicurezza vigenti nel Comune di Rimini.

3. DEFINIZIONI

Dato personale: Si fa riferimento a qualsiasi informazione riguardante una persona fisica identificata o identificabile (qualificata come Interessato). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Sono ricompresi nella definizione, a titolo di esempio, data di nascita, indirizzo di residenza o domicilio, codice fiscale, numeri di telefono, posta elettronica, indirizzo IP, dati di log, video, audio, immagini, dati di geolocalizzazione, IBAN, P.IVA, stato di disagio economico, contributi economici, agevolazioni tributarie/tariffarie e simili, abusi/accertamenti edilizi, permessi a costruire.

Trattamento: Si considera trattamento qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Titolare del trattamento: Il titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Il Comune di Rimini è titolare in tutti i casi in cui determina le finalità e i mezzi del trattamento di dati personali. Talvolta anche il Sindaco, nella sua veste di Ufficiale di Governo, può rivestire il ruolo di titolare del trattamento, in base a quanto previsto per legge.

Data Protection Officer: la persona fisica o giuridica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (artt. 37, 38, 39 del Regolamento).

Delegato al trattamento: il Dirigente delegato dal Sindaco allo svolgimento di compiti e funzioni connesse al trattamento dei dati personali in relazione al Servizio affidatogli. Il Dirigente si considera responsabile del procedimento ai fini della presente procedura.

Referente privacy: il Dirigente preposto alle attività di coordinamento relativamente alla protezione dei dati personali.

Incaricato al trattamento: la persona fisica, espressamente designata dal Dirigente, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali.

Gruppo Privacy: gruppo permanente di dipendenti che assicura il presidio per le strutture dell'Ente, ciascuno per la propria, in relazione agli adempimenti continuativi, lo studio e l'approfondimento degli aspetti normativi, organizzativi e procedurali, derivanti delle disposizioni normative in materia di protezione dei dati personali.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento, secondo quanto definito in appositi accordi.

ITbreach: la struttura tecnica a cui è demandata la gestione degli incidenti di sicurezza in ambito ICT. Tale struttura si avvale della collaborazione del Gruppo Privacy (o di un suo referente) nell'assolvimento di tutti gli aspetti di natura formale previsti e/o scaturenti dal processo di gestione dell'incidente.

4. Definizione di violazione di dati personali (c.d. data breach)

La violazione dei dati personali consiste nella 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.

Si ha violazione quando si perde il controllo sulla:

Riservatezza dei dati: cioè gestione della sicurezza in modo tale da mitigare il rischio di accesso ai dati o di loro utilizzo non autorizzato.

Integrità dei dati: intesa come garanzia che i dati non vengano alterati, ossia non subiscano modifiche o cancellazioni a seguito di eventi esterni e/o di azioni deliberate e non (es. malfunzionamenti o danni degli asset che contengono i dati stessi).

Disponibilità dei dati: ossia salvaguardia dei dati in modo che ne sia garantito l'accesso, l'usabilità e la confidenzialità. Da un punto di vista di gestione dei rischi, significa ridurre a livelli accettabili i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, ecc.) garantendone la sicurezza.

Non tutte le violazioni vengono considerate di gravità tale da essere notificate al Garante, cui vanno comunicate solo le violazioni di dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali.

Le violazioni di dati personali si intendono sia quelle relative a dati trattati o conservati su supporto informatico che a dati trattati o conservati su supporto cartaceo.

Di seguito vengono indicati alcuni esempi, non esaustivi, di violazioni di dati personali.

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	I furto o smarrimento di singoli dispositivi di memorizzazione (hard disk, memorie di massa rimovibili ecc) oppure dei computer/server che li ospitano. 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, in alcuni casi,

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.

5. GESTIONE DELL'INCIDENTE INFORMATICO

Nel caso in cui un ufficio riscontri una violazione di dati personali su supporto informatico dovrà informare tempestivamente, e comunque non oltre 24 ore dalla scoperta della violazione, il proprio Dirigente, che dovrà inoltrare una comunicazione al Dirigente dei sistemi informativi mediante invio alla scrivania predisposta per le pratiche di privacy e, per conoscenza, all'indirizzo di posta elettronica privacy@comune.rimini.it, fornendo una sintetica spiegazione dell'accaduto, affinché il Dirigente dei sistemi informativi possa attivare la struttura cui è demandata la gestione degli incidenti di sicurezza, denominata ITbreach, che prende contatto con l'ufficio segnalante e acquisisce tutte le informazioni necessarie ad un'esaustiva rappresentazione della violazione.

Rilevato l'incidente, è compito dell'ITbreach:

- svolgere l'analisi sulla violazione;
- valutare il livello di rischio conseguente alla violazione e attribuirgli un bollino di rilevanza, validato dal Responsabile Unità Operativa Sistemi Informativi;
- minimizzare i danni relativi all'incidente ed impedirne la propagazione;
- acquisire le eventuali evidenze digitali di reato prima che queste possano essere compromesse;
- redigere un rapporto intermedio e finale sulla violazione;
- supportare il Delegato nella notifica al Garante;
- conservare tutta la documentazione relativa alla violazione.

Nell'effettuare l'analisi sulla violazione, l'ITbreach 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 datti personali;

- 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, la struttura deve valutare l'opportunità o la necessità di coinvolgere le strutture di riferimento regionali e nazionali. Inoltre, la struttura 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, la struttura 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.

Il tempo di conservazione di tale documentazione è stabilito in 24 mesi nel caso in cui siano presenti dati personali, allo spirare del quale i dati devono essere cancellati e senza limiti di tempo nel caso non siano presenti dati personali.

In ogni caso, la documentazione relativa agli incidenti di sicurezza, comprensiva delle evidenze e delle valutazioni effettuate, viene elaborata in maniera tale da non indicare dati personali.

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 IT coinvolta;
- 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 IT/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.

6. RATING DEI RISCHI CONSEGUENTI A VIOLAZIONE DI DATI PERSONALI

Sia che si tratti di violazioni informatiche, sia che si tratti violazioni cartaceee, il rischio può essere catalogato secondo diversi livelli di gravità, che devono tenere conto del numero di dati violati, della sensibilità delle informazioni, del disagio causato, del contenimento o non-contenimento della violazione, della possibilità di recuperare i dati e dell'eventuale applicazione di dispositivi di cifratura.

I livelli di rischio che possono presentarsi sono i seguenti:

Se si ritiene che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.
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;
- smarrimento o furto di dispositivi dell'ente su cui sono presenti banche dati contenenti dati personali.

ARANCIONE

L'incidente non presenta nessuna condizione che porti alla catalogazione del rischio come ROSSO. Il grado di compromissione di servizi e/o sistemi è di una certa rilevanza e possono essere rilevati danni sugli asset di una certa consistenza.
Il ripristino ha tempi che non compromettono la continuità del servizio L'incidente presenta una tra le seguenti condizioni:

- compromissione di server;
- degrado di prestazioni relativo ai servizi offerti dall'ente con conseguente perdita di produttività da parte degli utilizzatori;
- attacchi che provocano il funzionamento parziale o intermittente della rete;
- impossibilità tecnica di fornire uno o più servizi critici ad un elevato numero di utenti per intervalli di tempo inferiori ai 30 minuti di tempo ripetuti su più giornate;
- impossibilità tecnica di fornire uno o più servizi critici ad una piccola parte di utenti per un periodo di tempo superiore ai 30 minuti di tempo nell'arco di una o più minuti di tempo nell'arco di una o più giornate;
- basso impatto in termini di perdita economica, di immagine e/o reputazione nei confronti degli utenti

GIALLO

L'incidente non presenta nessuna condizione che porti alla catalogazione del rischio come ROSSO O ARANCIONE.
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 identificate dai sistemi anti-malware;
- nessuna o limitata perdita di operatività o di business da parte di un ridotto numero di dipendenti;
- smarrimento o furto di dispositivi dell'ente su cui non sono presenti banche dati contenenti dati personali.

L'ITbreach, per gli incidenti informatici, e il Delegato, per gli incidenti cartacei, a seguito dell'analisi della violazione attribuiscono un bollino in base alla gravità del rischio conseguente all'incidente.
Nel caso di violazione informatica il bollino è attribuito dal Dirigente dei sistemi informativi, in base alla proposta avanzata dall'ITbreach, mentre per le violazioni cartacee è il Delegato stesso a decidere quale bollino attribuire.
Relativamente alle violazioni informatiche, il Dirigente dei servizi informativi informa l'ufficio da cui è originata la violazione, gli Assessori di riferimento e quello afferente al servizio presso cui è avvenuta la violazione, nonché il Delegato da cui è originata la comunicazione, indicando il bollino attribuito all'incidente. Azione analoga viene svolta dal Delegato nel caso di violazione cartacea.

7. Continuità 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, cartacei e informatici, e dell'infrastruttura ICT preposta all'erogazione dei servizi informatici.

8. Gestione dell'incidente cartaceo

In relazione alla gestione delle violazioni di dati personali su supporto cartaceo è responsabile ciascun Delegato, cui compete la predisposizione di tutte le misure idonee a garantire la gestione, il ripristino e il monitoraggio successivo alla gestione della violazione.

Ciascun Delegato predispone un rapporto nel quale registra i dati rilevati in occasione all'incidente occorso, le operazioni svolte dall'ente, i soggetti coinvolti, le analisi condotte e i risultati rilevati fino alla conclusione della gestione dell'incidente.

Nell'effettuare questa analisi, la struttura 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 datti personali;

- 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, la struttura deve valutare l'opportunità o la necessità di coinvolgere le strutture di riferimento regionali e nazionali. Inoltre, la struttura deve prevedere il coinvolgimento dei propri fornitori di servizi 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, la struttura 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.

La valutazione sull'impatto dell'incidente ai fini della sua adeguata classificazione viene effettuata in base ad alcuni parametri di seguito elencati:

- il numero di dati coinvolti;
- il numero di utenti o postazioni di lavoro potenzialmente impattati dalla indisponibilità dei dati personali violati;
- l'eventuale coinvolgimento di risorse/utenti/fornitori esterni all'organizzazione;
- 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.

Durante la gestione dell'incidente, fino alla chiusura dello stesso, il Delegato, tramite i propri uffici, 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.

Il tempo di conservazione di tale documentazione è stabilito in 24 mesi nel caso in cui siano presenti dati personali, allo spirare del quale i dati devono essere cancellati e senza limiti di tempo nel caso non siano presenti dati personali.

In ogni caso, la documentazione relativa agli incidenti di sicurezza, comprensiva delle evidenze e delle valutazioni effettuate, viene elaborata in maniera tale da non indicare dati personali.

9. Gestione della notifica al Garante Privacy

Accertato il data breach di rating rosso, il Dirigente dei sistemi informativi, o il Delegato del trattamento in caso di violazione cartacea, provvede senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui l'ufficio competente ne è venuto a conoscenza, a notificare la violazione al Garante per la protezione dei dati personali.

Il Dirigente dei servizi informativi, o il Delegato del trattamento attraverso il Referente privacy, segnala tempestivamente al DPO le violazioni dei dati personali ai fini della notifica al Garante per la protezione dei dati personali.

Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo. La motivazione verrà fornita dall'ufficio comunale da cui è originata la violazione o dal Dirigente dei servizi informativi, in ragione dell'imputabilità del ritardo.

La notifica al Garante deve contenere le informazioni presenti nel modulo pubblicato nella intranet comunale, conforme ai provvedimenti del medesimo Garante Privacy in materia.

Essa deve, in ogni caso, contenere le seguenti informazioni:

A. informazioni di sintesi

B. Informazioni di dettaglio

C. Possibili conseguenze e gravità della violazione

D. Misure adottate a seguito della violazione

E. Comunicazione agli interessati

F. Altre informazioni generali

10. Modalità di comunicazione agli interessati

Nel caso in cui dal data breach possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

A tal fine, il Delegato informa il rappresentante politico afferente al relativo servizio presso cui è avvenuta la violazione e predispone una comunicazione, che deve contenere un linguaggio chiaro e comprensibile agli utenti e deve riportare 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, la comunicazione dell'avvenuta violazione di dati viene divulgata tramite il sito istituzionale.

11. RIPRISTINO DELLE ATTIVITÀ INFORMATICHE E CARTACEE

A seguito della presentazione del Rapporto di Incidente di Sicurezza da parte della struttura cui è demandata la gestione degli incidenti di sicurezza ciascun Delegato valuta la sussistenza dei presupposti per la redazione di una valutazione di impatto sulla protezione dei dati personali (c.d. DPIA *Data Protecion Impact Assessment*) allo scopo di individuare le modalità adeguate di protezione dei dati in merito alla specifica attività in relazione alla quale è avvenuta la violazione.

Nel caso si violazione di dati personali su supporto cartaceo, il Dirigente preposto, a conclusione dell'analisi della violazione medesima, valuta la sussistenza dei presupposti per la redazione di una DPIA allo scopo di individuare le modalità adeguate di protezione dei dati in merito alla specifica attività in relazione alla quale è avvenuta la violazione.

Non è necessario effettuare una DPIA nel caso in cui il trattamento sia obbligatorio per legge o effettuato nell'interesse pubblico o nell'esercizio di pubblici poteri, se a monte l'Ente ha già effettuato una valutazione di impatto generale, o la legge esclude l'obbligo di effettuarla. Tuttavia, l'avvento di un data breach comporta un'analisi da parte del Delegato interessato dalla violazione che, partendo dal Rapporto di Incidente di Sicurezza permetta di:
- 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, anche tramite l'acquisizione di osservazioni da parte di tutti i servizi coinvolti nella violazione dei dati e nella gestione di essa.

In tutti gli altri casi, la DPIA è obbligatoria per i seguenti trattamenti:

- trattamenti valutativi o con assegnazione di punteggi su larga scala;
- profilazione anche online o tramite app di aspetti legati al rendimento professionale, situazione economica, salute, preferenze, interessi personali, affidabilità o comportamento;
- monitoraggio sistematico anche tramite reti o app;
- trattamento di identificativi univoci che identifichino utenti di servizi web, rispetto ad abitudini di consumo e di visione per periodi prolungati;
- trattamento di metadati per ragioni organizzative, sicurezza, upgrade tecnologico, previsioni di budget e miglioramento delle reti;
- trattamenti automatizzati che hanno effetti giuridici (es. esercizio di un diritto, uso di un servizio o di un contratto);
- sorveglianza sistematica su larga scala di zone accessibili al pubblico;
- trattamenti su larga scala di dati estremamente personali (es. vita familiare, dati finanziari, ubicazione);
- trattamenti nell'ambito del rapporto di lavoro con uso di sistemi tecnologici che permettono il controllo a distanza (anche videosorveglianza e geolocalizzazione);
- trattamenti non occasionali di dati relativi a soggetti vulnerabili (es. dipendenti, minori, disabili);
- trattamenti che implicano l'uso di tecnologie innovative:
  - per la valutazione o l'assegnazione di un punteggio;
  - che implichino un processo decisionale automatizzato con effetto giuridico;
  - per il monitoraggio sistematico;
  - per il trattamento di dati sensibili o aventi carattere altamente personale;
  - per il trattamento di dati su larga scala;
  - per la creazione di corrispondenze o combinazioni di dati;

- per il trattamento di dati relativi a soggetti vulnerabili;
- per trattamenti che possono impedire di esercitare un diritto o avvalersi di un servizio o di un contratto.

- trattamenti che comportano lo scambio tra titolari diversi di dati su larga scala in modalità telematica;
- trattamenti che comportano la creazione di correlazioni o combinazioni di determinati set di dati (es. trattamenti ulteriori rispetto alle originarie finalità o dati raccolti da diversi titolari);
- trattamenti di dati particolari o relativi a condanne penali e reati interconnessi con altri dati personali raccolti per fini diversi;
- trattamenti di dati biometrici o genetici raccolti in grande volute o trattati per lungo tempo.

La DPIA deve essere sottoposta a validazione del Dirigente preposto al servizio e del Dirigente preposto alla sicurezza dei dati personali all'interno dell'Ente.

I risultati della DPIA vanno trasmessi al RPD/DPO per la sua validazione.

12. ATTIVITÀ DI MONITORAGGIO POST INCIDENTE

L'incidente si considera chiuso nel momento in cui il Dirigente dei sistemi informativi, o il Delegato del trattamento in caso di violazione cartacea, lo dichiara tale, a seguito delle verifiche operate in fase di ripristino delle attività e degli strumenti di lavoro.

A seguito della dichiarazione di chiusura dell'incidente, per la parte informatica, l'ITbreach monitora il corretto funzionamento dei sistemi per un periodo di tempo adeguato. A tal fine, possono essere attivati ulteriori controlli utilizzando gli strumenti di monitoraggio in uso, oppure aumentando il livello di profondità degli eventi da registrare nei file di log applicativi o dei sistemi operativi. In quanto senso, l'ITbreach ha facoltà di richiedere la modifica o l'implementazione di nuove regole di *monitoring* ai soggetti preposti, in accordo con il Dirigente dei sistemi informativi.

L'attività di monitoraggio dei supporti cartacei, successiva all'incidente, avviene nelle modalità che ciascun Delegato ritiene più opportune in considerazione dei luoghi di allocazione e delle disponibilità economiche a disposizione.

E', in ogni caso, fatta salva la previsione dell'art. 32, Regolamento UE 2016/679, in considerazione della quale il Titolare del trattamento fa sì che chiunque agisca sotto la sua autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri. Ciascun Delegato è, pertanto, responsabile della formazione del proprio personale, salvo iniziative di carattere generale promosse dal Gruppo Privacy.

La dichiarazione di chiusura dell'incidente viene adeguatamente comunicata agli Interessati e ai rappresentanti politici afferenti ai relativi servizi presso cui è avvenuta la violazione.

13. DATA BREACH DEL RESPONSABILE DEL TRATTAMENTO

All'interno di ciascun accordo, sottoscritto ai sensi dell'art. 28 del Regolamento UE 2016/679, vengono indicate le modalità di gestione dei data breach occorsi al Responsabile del Trattamento.
In ogni caso, esso deve tempestivamente comunicare al Titolare, e comunque non più tardi di 48 ore dall'accadimento dell'evento, tramite posta elettronica certificata indicata nella nomina a Responsabile del trattamento, gli eventi di *data breach* che comportano effetti avversi significativi sugli individui, indicando ogni informazione utile alla gestione dell'evento, in conformità alle indicazioni del Garante per la Protezione dei Dati Personali, oltre a:

- descrivere la natura della violazione dei dati personali;

- indicare le categorie e il numero approssimativo di interessati in questione nonché le categorie;
- indicare il numero approssimativo di registrazioni dei dati personali in questione;
- indicare i recapiti del DPO nominato o del soggetto competente alla gestione del data breach;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o che si intende adottare per affrontare la Violazione della sicurezza, compreso, ove opportuno, misure per mitigare i suoi possibili effetti negativi;

Il Responsabile del trattamento ha l'onere di fornire i medesimi elementi anche in relazione al proprio sub-responsabile del trattamento.

14. REGISTRO DATA BREACH

Il Delegato al trattamento e il Dirigente dei servizi informativi, tramite l'ITbreach, a prescindere dalla notifica al Garante, documenta tutte le violazioni dei dati personali.
Le sole violazioni notificate al Garante vanno comunicate al Referente privacy, attraverso i propri referenti del Gruppo Privacy, in modo che siano inserite all'interno di un apposito Registro dei *data breach* tenuto dal Referente.

15. RIFERIMENTI

I riferimenti dell'ITbreach (nominativi, indirizzo e-mail, numero di telefono ecc.) sono riportati nella sezione intranet relativa al GDPR, e tempestivamente aggiornati in caso di mutamento.

I riferimenti del Gruppo Privacy (nominativi, indirizzo e-mail, numero di telefono ecc.) sono riportati nella sezione intranet relativa al GDPR, e tempestivamente aggiornati in caso di mutamento.