Allegato 3 al decreto n. 66 del 23.11.2023

Indicazioni operative per la redazione di linee guida per il processo di Data Breach

Versione del documento 1.0

Data emissione 23/11/2023
Stato del documento Definitivo
Nome del file ALL.3_def.docx"

Sommario

1 Contesto di riferimento

La presente introduzione è necessaria al fine di inquadrare sotto un profilo contestuale il Regolamento Europeo n. 679/2016 (General Data Protection Regulation meglio noto come GDPR), entrato in vigore il 24 maggio 2016 ma pienamente applicato a partire dal 25 maggio 2018, che uniforma ed armonizza le legislazioni dei Paesi Europei con riguardo alla materia di protezione dei dati personali.

Preme precisare che la scelta di tipologia di intervento del legislatore Europeo risulta alquanto significativa nella misura in cui, con la scelta di un Regolamento, non viene lasciata agli Stati membri alcuna possibilità di intervento (se non in termini di adozione di provvedimenti volti ad armonizzare la normativa nazionale) stante la piena applicabilità del Regolamento a dispetto della presenza, come successo invece in passato in materia di protezione di dati personali, di direttiva europea (95/46) che necessitava di un atto di recepimento (Digs. 196/2003, meglio noto come codice della privacy).

In riferimento invece ai contenuti della presente legge si sottolinea come l'approccio che propone il Regolamento sia del tutto differente rispetto a quello proposto dal codice privacy nazionale.

Principio fondamentale che impernia l'intera normativa è infatti quello di accountability (la capacità di rendere conto delle azioni) il quale illustra, di fatto, una responsabilizzazione dei soggetti coinvolti in materia di protezione di dati personali; questi infatti secondo il dettato normativo non dovranno più ragionare in termini di mero adempimento alla norma di riferimento, come invece accaduto fino ad oggi con riferimento ai dettami del codice della privacy.

In tal senso il principio di accountability deve essere letto sotto un duplice profilo: esso non solo è il principio che ispira l'adeguamento/l'adempimento degli enti alla normativa europea, ma è anche il punto di partenza per dimostrare la compliance (il rispetto, l'aderenza) dell'ente/organizzazione alla norma europea.

Ciò significa che un ente/organizzazione può disattendere una prescrizione del Regolamento, avendo tuttavia cura di indicare in apposito documento le ragioni in forza delle quali si ritiene di non dover seguire il dettato normativo.

Oltre quindi a lasciare uno spazio di intervento ai soggetti Titolari del trattamento in ordine alla scelta di adozione delle novità introdotte dal GDPR, obbligandoli comunque ad una seria riflessione in ordine alle politiche da adottare per essere conformi al Regolamento, si segnalano a titolo esemplificativo alcuni istituti del tutto lontani dalla logica "burocratica" del Codice Privacy.

Si richiama inevitabilmente quindi al processo di istituzione e conservazione del registro di trattamenti in capo ai titolari e responsabili del trattamento che consente quindi di avere una chiara panoramica dei trattamenti di dati personali che vengono effettuati all'interno dell'organizzazione che fa per l'appunto capo al titolare o al responsabile; a ciò si aggiunga l'organizzazione del processo che porta il titolare o responsabile del trattamento in contatto con l'autorità garante e con i soggetti interessati in caso di "violazione di dati" nota anche come Data Breach, che come sarà meglio trattato nell'apposito documento non si limita al solo furto di dati.

Ancora, la previsione di una conduzione di Valutazione di impatto per quei trattamenti che presentino un rischio elevato per i diritti e le libertà degli interessati.

In conclusione, come già emerso dalla disamina condotta, a mutare è l'atteggiamento della normativa rispetto alla tematica della protezione dei dati personali, esso infatti impone una riflessione preventiva rispetto alla materia de qua, che porta quindi ad adattare la propria organizzazione in base alle opportunità che si intendono cogliere, lasciando non solo ampi spazi di autonomia ai soggetti Titolari/Responsabili ma anche abbandonando quell'approccio di mero adempimento richiesto dalla normativa. In sintesi, non è sufficiente avere "le carte a posto".

2 PREMESSA

2.1 Oggetto e obiettivo del documento

Il GDPR riforma il precedente impianto normativo in materia di protezione dei dati personali - Codice Privacy, inserendo come elementi cardine il principio di Accountability o Responsabilizzazione in capo al Titolare, e di eventuali Responsabili o Contitolari del trattamento, nell'adozione di misure tecniche ed organizzative adeguate ed efficaci, con l'onere di dimostrare la conformità delle attività di trattamento al GDPR stesso, garantendo la tutela ai diritti dell'interessato, nonché mettendo in atto procedure per riesaminare e aggiornare le misure stesse.

In tale contesto assume rilievo il cambio di approccio al "tema privacy" da parte del Titolare del trattamento, oggi chiamato a rimodulare i processi di flusso dei dati personali secondo i principi di privacy "by design" e "by default", per avere la certezza che le misure tecniche e organizzative siano adottate ed integrate fin dall'inizio del trattamento; per valutare i rischi che possono violare i dati personali o la tutela della vita privata (come riporta l'art. 1 § 2 del GDPR "il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali"); per prioritizzare gli interventi, per avere la garanzia della liceità del trattamento, per monitorare costantemente le misure di sicurezza ed i trattamenti, per rendere i collaboratori consapevoli del valore del dato attraverso la formazione ed infine per garantire che quest'ultimi si impegnino alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza.

Pertanto, diventa prioritaria la riorganizzazione dell'ente/organizzazione cercando di ridistribuire compiti e responsabilità tra i soggetti coinvolti nel trattamento dei dati personali (vedi Titolare del trattamento, Responsabile del trattamento, persona istruita e autorizzata - ex incaricato del trattamento nel codice privacy).

2.2 Ambito di applicazione del documento

Il presente documento ha lo scopo di fornire indicazioni in grado di coadiuvare Regione Toscana e gli Enti ad essa collegati nella definizione delle Linee Guida per l'aggiornamento del Sistema Organizzativo, ai fini dell'applicazione di quanto previsto dal GDPR.

Le presenti indicazioni si applicano a Regione Toscana e a tutti gli Enti che condividono le indicazioni del medesimo DPO come da decreto regionale nr. 387 del 12.01.2023 e nel rispetto della Delibera della Giunta Regionale n. 250 del 7 marzo 2022.

2.3 Validità e Aggiornamento del documento

2.3.1 Soggetti Approvatori

Approvatore	Referente e Ruolo	Data

2.3.2 Soggetto verificatore

Verificatore	Referente e Ruolo	Data

2.3.3 Versione del documento

Stato	Versione	Autore	Descrizione	Data

3 QUADRO NORMATIVO

REGOLAMENTO 2016/679/UE: Articoli 4, 33 e 34

Considerando C85, C86, C87, C88

WP250 - Guidelines on Personal Data Breach Notification under Regulation 2016/679 - Adopted on 3 October 2017

3.1 Definizioni normative di riferimento

Anonimizzazione: tecnica di trattamento dei dati personali tramite la quale i dati personali non possano più essere attribuiti a un interessato specifico, nemmeno attraverso l'utilizzo di informazioni aggiuntive.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Autorità di controllo: è l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

Cifratura: tecnica di trattamento dei dati personali tramite la quale i dati personali vengono resi non intellegibili a soggetti non autorizzati ad accedervi.

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Contitolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altri determina le finalità e i mezzi di trattamento dei dati personali.

Data Breach: è un incidente di sicurezza in cui i dati personali vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato o persi accidentalmente.

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («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;

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

DPIA: acronimo di Data Protection Impact Assessment (valutazione di impatto sulla protezione dei dati).

Interessato: persona fisica identificata o identificabile. 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.

Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

Misure di sicurezza: misure tecniche ed organizzative adeguate per garantire un livello di sicurezza dei dati trattati adeguato al rischio.

Nuovo trattamento: trattamento di dati personali che comporta l'utilizzo di nuove tecnologie o/e di nuovo tipo e in relazione al quale il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.

Privacy by-design / by-default: l'incorporazione della privacy a partire dalla progettazione di un processo aziendale, con le relative applicazioni informatiche di supporto. La prima introduce la protezione dei dati fin dalla progettazione per caso specifico, la seconda per impostazione

predefinita di una pluralità di casi tra loro omogenei.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Pseudonimizzazione: ii trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanta riguarda gli obblighi rispettivi a norma del regolamento.

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.

Responsabile della Conservazione documentale: si tratta della figura preposta alla gestione e supervisione del processo di conservazione dei documenti (digitali o cartacei).

Security Manager: è la figura preposta alla gestione e supervisione del processo di Security Incident Management.

Sub responsabile: persona fisica o giuridica designata dal responsabile del trattamento previa autorizzazione scritta del titolare del trattamento.

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare o suo delegato del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Titolare del trattamento o suo delegato: 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, ii titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

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.

Violazione dei dati personali: 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.

3.2 Adempimenti prescritti dalla normativa

Ai sensi dell'art. 33 del GDPR "Notifica di una violazione dei dati personali all'autorità di controllo":

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione

all'autorità di controllo competente a norma dell'articolo 55 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.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 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.

4. 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.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Ai sensi dell'art Articolo 34 "Comunicazione di una violazione dei dati personali all'interessato":

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

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) 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.

4. 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 o può decidere che

una delle condizioni di cui al paragrafo 3 sia soddisfatta.

In capo alla Regione Toscana e agli enti collegati, in caso di violazione dei dati personali degli interessati (a titolo esemplificativo e non esaustivo: cittadini, dipendenti, soggetti terzi ecc.) vige:

A) **Obbligo di comunicazione della violazione al Garante Privacy senza ingiustificato ritardo**: a tale adempimento il Titolare o suo delegato del trattamento dei dati personali deve provvedere non appena venuto a conoscenza della violazione e, comunque entro 72 ore, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Si evidenzia quindi che la notifica all'Autorità è obbligatoria quando vi è:

- **un rischio probabile per i diritti e le libertà delle persone fisiche.**

(Tale parametro deve essere desunto dall'analisi dei rischi effettuata)

- **Ritardo nella notifica**. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore dal momento in cui ne è venuto a conoscenza è possibile effettuarla in ritardo corredandola con i motivi del ritardo.

- **Notifica non completa**. Qualora la notifica effettuata nelle 72 ore non sia completa è possibile integrarla in una o più fasi successive (ad es. nel caso di violazioni complesse per le quali occorrono indagini approfondite) corredandola con i motivi (analogamente come in caso di notifica in ritardo).

Nello specifico della notifica al Garante, dall'avvenuta conoscenza dell'evento, si dovranno dare, attraverso un modulo o comunicazione ad hoc, almeno le seguenti informazioni:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie (clienti, dipendenti, categorie vulnerabili, minori, etc.) e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni con tipologie di record (ad es. numeri di passaporto, numeri di carte di credito, etc.) 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 o suo delegato per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Inoltre, nel caso in cui la scoperta della violazione non sia contestuale al verificarsi dell'evento che l'ha generata, devono essere indicate nella comunicazione le motivazioni che non hanno consentito l'immediata rilevazione dell'evento stesso e le misure adottate o che si intende adottare affinché ciò non si ripeta in futuro.

B) **Obbligo di comunicazione senza ingiustificato ritardo all'interessato (cittadino, dipendente, soggetto terzo ecc.), quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.**

La comunicazione a tali soggetti deve avvenire senza ingiustificato ritardo, il prima possibile.

Il Garante Privacy può autorizzare il differimento di tale comunicazione qualora quest'ultima rischi di compromettere gli accertamenti relativi al Data Breach.

La predetta comunicazione, infine, non è dovuta:

a) se si dimostra al Garante di aver applicato ai dati oggetto della violazione misure tecnologiche di protezione che li hanno resi inintelligibili a chiunque non sia autorizzato ad accedervi quali la cifratura;

b) il Titolare del trattamento o suo delegato ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati (ad esempio sono state immediatamente intraprese azioni contro colui che ha avuto acceso ai dati oggetto della violazione);

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 (ad es. in caso di perdita di documenti conservati solo in formato cartaceo potrebbero esser predisposte procedure o soluzioni tecniche che rendano le informazioni agli interessati fruibili su richiesta degli stessi)

Analisi dei rischi

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.

I criteri per valutare il rischio elevato, ai fini della comunicazione all'utente finale, dovranno basarsi su:

• il grande di pregiudizio che la violazione può comportare (danno alla reputazione, furto di identità ecc.);

• l'attualità dei dati (i dati più recenti potrebbero essere considerati più interessanti);

• la qualità dei dati coinvolti (dati sanitari, dati finanziari, dati giudiziari, credenziali di autenticazione);

• la quantità dei dati coinvolti;

• la tipologia di violazione (accesso non autorizzato, distruzione dei dati, perdita, furto);

• la capacità di identificare le persone coinvolte nella violazione.

Ai sensi del dell'art 33 par. 5 "Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo".

La Regione e/o gli Enti collegati sono pertanto tenuti ad adottare

• un inventario aggiornato delle violazioni contenente tutte le informazioni necessarie a chiarire le circostanze nelle quali si sono verificate, le conseguenze che le stesse hanno avuto e i provvedimenti adottati per porvi rimedio, la tenuta di tale inventario consente al Garante di verificare il rispetto delle disposizioni di legge. È comunque opportuno che l'inventario tenga traccia anche delle varie fasi di gestione dell'evento, dalla rilevazione, all'analisi e alla sua risoluzione e

conclusione. L'inventario dovrà essere dotato di idonee misure di sicurezza atte a garantire l'integrità e l'immodificabilità dei dati in esso registrati.

La normativa prevede inoltre l'ipotesi in cui il Responsabile designato sia informato della violazione ex art 33, comma 2,"il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione."

3.3 Soggetti attivi

I soggetti attivi sono tutti coloro che si occuperanno sin dalla fase di rilevazione sino alla fase di notifica al Garante del Data Breach.

3.3.1 Ruoli coinvolti

Ruolo aziendale	Responsabilità principali nella Procedura Data Breach
Security Manager	• Rilevare, analizzare e notificare gli incidenti di Sicurezza IT che si verificano sui Sistemi informativi.
Responsabile della Conservazione Documentale	• Rilevare, analizzare e notificare gli incidenti di Sicurezza che si verificano sui documenti/fascicoli cartacei.
Fornitori (Responsabili ex art.28 GDPR)	• Rilevare e registrare gli incidenti di Sicurezza IT che si verificano sui Sistemi informativi da essi gestiti; • Valutare l'impatto dell'incidente di Sicurezza IT sulla fornitura dei Servizi Digitali forniti; • Provvedere - se necessario - a notificare l'incidente al CSIRT Italiano.
Referente interno	• Comunica l'incidente, rilevato dai fornitori o soggetti terzi esterni, al Security Manager e/o al Responsabile della Conservazione Documentale.
Titolari del trattamento o suo delegato	• Provvedere - se necessario - a notificare l'incidente all'Autorità Garante per la protezione dei dati personali; • Procedere - se necessario - a comunicare l'incidente agli Interessati.
Referente Data Protection	• Fornire supporto giuridico ai summenzionati Ruoli / Strutture nell'attuazione delle operazioni di valutazione e notifica degli incidenti di Sicurezza IT.

4 Tipologie di violazioni dei dati

Le violazioni dei dati personali si considerano tali se hanno un reale impatto sulla confidenzialità, integrità o disponibilità dei dati personali degli interessati (cittadini, dipendenti, soggetti terzi etc.).

Di seguito una breve descrizione delle varie tipologie di violazione dei dati personali:

a) Distruzione: indisponibilità definitiva di dati personali dei clienti con impossibilità di ripristino degli stessi entro sette giorni. La violazione può essere determinata da una eliminazione logica (es. cancellazione dei dati) oppure fisica (es. rottura dei supporti di memorizzazione) non autorizzata e relativa impossibilità di ripristinare i dati entro i sette giorni.