Allegato 3 alla Disposizione n. 40 del 01 Ottobre 2018

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

Versione del documento	1.0
Data emissione	01/10/2018
Stato del documento	Definitivo
Nome del file	*"Indicazioni operative per la redazione di linee guida per il processo di Data Breach.docx"*

Sommario

1 Contesto di riferimento

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

L'esigenza di una rivisitazione della normativa in materia di protezione dei dati personali si apprezza in relazione al mutato contesto politico, economico e sociale di riferimento del tutto differente rispetto a quello degli anni 90, periodo nel quale l'impatto e la cultura del dato non era così centrale come invece è oggi; ciò è dato dallo sviluppo repentino delle moderne tecnologie (in primis mobile devices, smartphone, tablet, social network, ecc.; in seconda battuta strumenti IOT (Internet of things), sistemi di Data Analytics e Big Data, Business Intelligence, ecc.) nemmeno immaginabile negli anni che chiudevano il secolo scorso, grazie alle quali è pensabile e apprezzabile anche il valore economico del dato.

Accanto a questa constatazione di tipo "sociologica" va da sé che il programma di integrazione europeo che vede come base di partenza la creazione di un mercato unico europeo, da realizzarsi inizialmente attraverso la libera circolazione di persone, servizi e merci, non possa non tenere in considerazione anche della libera circolazione del "dato personale" così come puntualmente sottolineato dai "considerando" del Regolamento fino anche alla maggiore rilevanza di questa libertà rispetto alla tutela del dato in sé come diritto soggettivo (considerando nr. 4).

A seguito di questa breve introduzione storica/sociologica ed avviando la riflessione sul terreno giuridico, in prima battuta 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 (Dlgs. 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 nel proseguo dell'elaborato 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.

Sotto il profilo dei soggetti attivi e protagonisti, in questo nuovo quadro, viene introdotta la figura del ***Data Protection Officer – DPO*** (obbligatorio per tutti gli enti pubblici) il quale si andrà a configurare da un lato come consulente per i Titolari e i Responsabili dei trattamenti, attraverso una continua verifica della *compliance* dell'organizzazione/ente rispetto ai dettami del GDPR, ma anche come punto di riferimento per i soggetti interessati rappresentando per questi ultimi il referente dell'organizzazione con il quale interfacciarsi in materia di protezione dei dati personali.

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

1.1 Oggetto e obiettivo del documento

A partire dal 25 maggio 2018, tutti i Titolari del trattamento – pubblici e privati – devono notificare all'autorità di controllo ("Garante") le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare o suo delegato. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazioni anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34.

I contenuti della notifica all'autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del regolamento.

Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati *(si veda art. 33, paragrafo 5)*; tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice per gli operatori di comunicazioni elettroniche. I titolari di trattamento devono pertanto adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

La presente indicazione operativa tiene quindi conto di quanto previsto dalla normativa di riferimento citata, ma resta comunque soggetta a possibili futuri aggiornamenti sulla base di eventuali interventi in materia da parte del Garante Privacy.

1.2 Ambito di applicazione del documento

La presente indicazione operativa ha lo scopo di descrivere il processo adottato dalla Regione Toscana e dagli Enti collegati per la gestione degli eventi di violazione dei dati personali.

Ai sensi dell'art. 4 par. 12 «violazione dei dati personali» ovvero per ***Data Breach*** si definisce: "*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"*.

Tale indicazione operativa pertanto si applica a tutti gli archivi/documenti cartacei e a tutti i sistemi sui cui sono conservati i dati personali degli interessati (Cittadini, dipendenti, fornitori, soggetti terzi ecc.) che la Regione e/o altri enti trattano, anche attraverso il supporto di Responsabili del Trattamento.

La presente indicazione operativa definisce le principali responsabilità ed attività relative agli obblighi di notifica verso gli Organismi di Controllo degli incidenti di Sicurezza delle Informazioni che abbiano come conseguenza la violazione di dati personali o che abbiano un impatto rilevante sulla continuità di Servizi Essenziali o sulla fornitura di Servizi Digitali.

1.3 Validità e Aggiornamento del documento

1.1.1 Soggetti Approvatori

Approvatore	Referente e Ruolo	Data

1.3.1 Soggetto verificatore

Verificatore	Referente e Ruolo	Data

1.3.2 Versione del documento

Stato	Versione	Autore	Descrizione	Data

2 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

2.1 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 è 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: il 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 quanto 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, il 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;

2.2 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 è 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 dovrà recare, 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, ecc.) e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni tipologie di record es numeri di passaporto, numeri di carte di credito, ecc.) 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 è 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 grado 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. E' 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.*"

2.3 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.

2.3.1 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.

3 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 ecc.)

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.

b) **Perdita:** Perdita del supporto fisico di memorizzazione dei dati (dischi esterni, pendrive ecc.) in termini di privazione, sottrazione, smarrimento dei dispositivi contenenti i dati degli interessati oppure dei documenti cartacei. La perdita può essere anche temporanea ma superiore a sette giorni. Può riguardare le copie o gli originali dei supporti contenenti i dati personali dei soggetti interessati.

c) **Modifica:** Modifiche improprie dei dati degli interessati non autorizzate, effettuate al di fuori dei processi operativi di trattamento dei dati svolti dagli incaricati autorizzati, oppure modifiche con finalità fraudolente eseguite dagli incaricati autorizzati all'accesso.

d) **Rivelazione:** Distribuzione non autorizzata o impropria dei dati personali degli interessati verso terze parti (persone fisiche, persone giuridiche, gruppi di soggetti, pubblico) anche non precisamente identificabili.

e) **Accesso:** Accesso non autorizzato o improprio ai dati degli interessati. Accessi ai dati (anche in sola visualizzazione, sia in caso di accessi logici ai sistemi informatici sia agli archivi cartacei) effettivamente avvenuti al di fuori dei processi operativi di trattamento dei dati previsti e autorizzati.

3.1 Tassonomia eventi

La Regione Toscana ha individuato, in maniera esemplificativa e non esaustiva, una tassonomia dei possibili eventi causa delle violazioni dei dati personali sopra specificate. Il verificarsi di uno degli eventi di seguito descritti non costituisce tuttavia condizione sufficiente per stabilire l'effettivo Data Breach**.**

3.2 Trattamenti elettronici

3.2.1 Eventi accidentali:

Eventi anomali determinati da fatti fortuiti che causano la perdita delle caratteristiche di sicurezza dei dati personali dei clienti (confidenzialità, integrità o disponibilità) in caso di trattamenti informatizzati. Rientrano in tali casistiche eventi generati nella gestione dei sistemi ICT (gestiti internamente oppure in outsourcing) quali:

- ***Esecuzione erronea di comandi e/o procedure per distrazione:*** ad esempio pubblicazione erronea delle informazioni personali (non di dominio pubblico) su portali web pubblici; erroneo invio di informazioni a enti esterni alla Società, formattazione di dispositivi di memorizzazione, errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi; divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato ecc.
- **Rottura delle componenti HW:** a titolo di esempio distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e di elettricità, umidità, corto circuito, caduta accidentale, eventi catastrofici/incendi, ecc.
- **Malfunzionamenti Software**: ad esempio esecuzione di uno script automatico non autorizzato; errori di programmazione che causano output errati, ecc.

- **Visibilità errata di dati sul sito web della Società:** ad esempio visibilità da parte di clienti di dati di altri clienti anche per casi di omonimia.
- **Fornitura dati a persona diversa dall'interessato:** a titolo di esempio comunicazioni di dati di interessati a destinatari errati; gestione di informazioni avanzate da persone diverse dal Titolare o suo delegato;
- **Guasti alla rete aziendale**: a titolo di esempio caduta delle comunicazioni durante il trasferimento di dati e perdita di dati durante la trasmissione, ecc.

3.2.2 Eventi dolosi:

Eventi dolosi causati da personale interno o soggetti esterni realizzati tramite:

1) accesso non autorizzato ai dati con lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione;

2) compromissione o rivelazione abusiva di credenziali di autenticazione;

3) utilizzo di software malevolo. In tale casistica rientrano gli incidenti di sicurezza ICT che comportano la violazione dei dati personali dei clienti quali:

   - **Furto:** furto di supporti di memorizzazione e/o elaborazione contenenti dati personali dei clienti (es: furto laptop, hard disk, chiavette USB, smartphone, tablet ecc)
   - **Truffa informatica esterna:** tutti i casi di frodi realizzate da un soggetto esterno all'azienda rivolto a procurare a sé o ad altri un profitto o, comunque, un vantaggio in termini economici, pubblicitari, ideologici/politici, qualora tali frodi causino perdita delle caratteristiche di sicurezza dei dati personali dei soggetti interessati (confidenzialità, integrità o disponibilità) trattati dall'ente/organizzazione o da suoi fornitori. Ad esempio: accesso non autorizzato ed illecito alle basi dati dei sistemi contenenti i dati dei soggetti interessati tramite sfruttamento di vulnerabilità dei sistemi; appropriazione dei dati di carta di credito; appropriazione (e diffusione) delle credenziali di autenticazione ai servizi dei clienti.
   - **Truffa informatica interna:** tutti i casi di frodi realizzate da personale interno all'azienda che comportano la violazione dei dati personali. Tali eventi possono derivare dall'utilizzo illecito e/o illegittimo delle informazioni a cui un incaricato del trattamento accede anche se autorizzato.

3.3 Trattamenti Cartacei

3.3.1 Eventi accidentali

Eventi anomali causati nell'ambito dei trattamenti non automatizzati effettuati su archivi cartacei dei dati personali dei clienti dell'ente/organizzazione quali:

- **Distruzione accidentale di documenti:** ad esempio *incendio/ allagamento dei locali dove sono presenti archivi cartacei*, causati da eventi fortuiti e non dolosi presso le sedi dell'ente/organizzazione, dei partners commerciali e dei locali, degli outsourcers di archiviazione contratti e dei corrieri per la raccolta dei contratti, dei partners cessati dai quali si attende la restituzione della documentazione

contrattuale; *distruzione per errore di documenti originali*, senza eventuale copia, da parte di dipendenti interni, di partners commerciali.

- **Smarrimento di documenti:** ad esempio perdita di documenti contenenti dati dei cittadini, degli outsourcers (es. archiviazione contratti e dei corrieri per la raccolta dei contratti), ecc.
- **Fornitura involontaria di dati a persona diversa dal contraente:** ad esempio invio lettera ad Ente senza mandato, gestione ed evasione reclami/richieste di informazioni avanzate da persone diverse dal titolare della linea non delegato, comunicazione di dati dal subentrato al subentrante e viceversa, invio/visualizzazione di fatture a soggetti diversi dal titolare della linea.

3.3.2 Eventi dolosi

Comportamenti dolosi da parte di personale interno o soggetti esterni realizzati, attraverso accessi non autorizzati, nell'ambito di trattamenti effettuati su archivi cartacei di dati personali della Regione e/o Enti collegati quali:

- **Distruzione dolosa dei documenti:** ad esempio incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati dei clienti; accesso non autorizzato da parte di terzi ad archivi interni della Società e distruzione volontaria di documenti contenenti dati dei client.
- **Accesso non autorizzato:** ad esempio accesso non autorizzato da parte di personale interno o soggetti esterni, con lettura e/o copia dei documenti, ad archivi documentali presso le sedi dell'ente/organizzazione, dei partners commerciali. Non si verifica violazione se si ha la ragionevole certezza che non vi è stata lettura o copia dei documenti contenenti dati degli interessati.
- **Furto (cartacei):** Furto da parte di personale interno o soggetti esterni (o non identificati) di documenti cartacei contenenti dati dei soggetti interessati.

4 Panoramica sul processo operativo

Al fine di assicurare l'attuazione dei nuovi obblighi di legge sulle violazioni dei dati personali all'interno della Regione Toscana, dovrà essere definito una macro Processo di *Incident Management* atto a individuare le violazioni, valutarle e comunicarle secondo quanto previsto dalla norma.

Le comunicazioni interne fra le varie funzioni coinvolte nel processo di gestione delle violazioni dovranno essere inviate tramite i normali canali di comunicazione aziendale.

Sarà, in particolare, creata una web form destinata a gestire le sole comunicazioni inerenti l'evento di violazione dal momento in cui l'evento è stato accertato come Data Breach (Cfr. sotto paragrafo 7.3).

L'Ownership della piattaforma sopra specificata compete al Security manager e/o al Responsabile Conservazione documentale la quale è supportata dal settore IT nella gestione del processo di valutazione degli incidenti di sicurezza.

Il macro processo di gestione delle violazioni si potrebbe articolare nelle fasi di seguito descritte.

4.1 Segnalazione degli eventi di violazione dei dati personali

In questa fase si acquisisce la notizia di una possibile violazione di dati personali.

La segnalazione di un possibile Data Breach può provenire dall'esterno (cittadini, fornitori esterni, enti istituzionali ecc.) o dall'interno, da parte delle varie funzioni di settore durante il normale svolgimento dell'attività lavorativa (più frequentemente tali eventi vengono evidenziati da funzioni che svolgono attività di verifica e /o di controllo).

Il Referente interno che riceve la segnalazione dall'esterno o che rileva dall'interno l'evento anomalo di violazione di dati personali, deve segnarlo al ***Security manager e/o al Responsabile Conservazione documentale*** che si attiverà per acquisire elementi necessari per l'effettiva rilevazione del Data Breach.

4.2 Rilevazione degli eventi di violazione dei dati personali

In questa fase si acquisiscono gli elementi necessari per condurre la fase successiva di valutazione al fine di escludere o confermare la sussistenza del Data Breach.

Nella pratica, rilevazione e valutazione dell'evento sono interconnesse; ma è solo al termine della fase di valutazione che si considera accertata o meno la violazione dei dati personali. Da questo momento decorrono le tempistiche per la comunicazione al Garante.

Resta inteso che la fase di rilevazione deve avvenire in tempi brevi.

Il Security Manager e/o Responsabile Conservazione documentale inserisce i dati relativi all'evento nell'Applicativo *Data Breach e Incident Management (vedi cap. 6)* per una prima analisi di identificazione della tipologia di violazione e raccolta informazioni per la fase di valutazione.

Il Security manager e/o il Responsabile Conservazione documentale, se necessario, per integrare l'analisi, coinvolge altre funzioni aziendali responsabili di attività da cui possono derivare ulteriori elementi conoscitivi, le quali devono garantire tempestivamente il supporto richiesto.

Se dalla prima analisi emergono elementi tali da escludere la possibile violazione dei dati personali, l'anomalia viene gestita secondo i processi aziendali standard.

Se invece dalla prima analisi emergono gli estremi per una probabile violazione dei dati personali il Security Manager attiva la fase di valutazione confrontandosi con il Referente Data Protection.

4.3 Valutazione degli eventi di violazione ai dati personali.

Scopo di questa fase è quello di confermare o meno l'avvenuta violazione, di circostanziare in modo completo l'evento e fornire una valutazione del possibile pregiudizio per i clienti.

Il Security Manager supportato dal Referente Data Protection e, ove necessario e opportuno, anche da altre funzioni aziendali coinvolte, effettua una analisi di dettaglio, raccoglie informazioni aggiuntive e valuta il livello di rischio dell'evento e il livello di pregiudizio per gli eventuali clienti impattati dalla violazione.

Ove dall'analisi non si ravvisi l'esistenza di una violazione, l'evento anomalo viene gestito secondo le procedure aziendali vigenti.

Nel caso in cui, invece, dall'analisi, si accerti che l'evento costituisce una violazione dei dati personali, da questo momento decorrono le tempistiche previste dalla normativa (dal momento della conoscenza – 72 h) in tema di comunicazioni al Garante.

4.4 Comunicazione

In questa fase si procede all'invio formale delle informazioni inerenti il Data Breach al Garante Privacy e, ove previsto, ai soggetti interessati dalla violazione, nel rispetto delle disposizioni previste dall' art 33 e 34 del GDPR.

a) Comunicazione verso il Garante Privacy

Le tempistiche di comunicazione nei confronti dell'Autorità Garante ed eventualmente nei confronti dei cittadini decorrono dal momento in cui il Security manager e/o dal Responsabile Conservazione documentale la segnalazione dell'evento di violazione. E pertanto:

- **Senza ingiustificato ritardo dalla segnalazione e comunque entro 72 ore** viene comunicato via Pec al Garante le informazioni disponibili relative al Data Breach mediante il modulo predisposto dallo stesso (ovvero con nota formulata sulla base dello stesso modulo) sottoscritto digitalmente dal Titolare o suo delegato del Trattamento dei Dati Personali della Società ed archivia la notifica e le evidenze della violazione nell'*inventario violazioni;*
- **Ove la notifica venga effettuata oltre le 72 ore** deve essere corredata dai motivi del ritardo;
- **Se la prima notifica entro le 72 ore non è completa** (es. nei casi di violazioni molto complesse) la stessa può essere integrata successivamente ed accompagnata dai motivi del ritardo in aderenza a quanto previsto dall'art 33 par. 1.

Il dettaglio delle informazioni che devono essere comunicate al Garante ***(Modulo per la notifica al Garante del Data Breach).***

b) Comunicazione verso l'interessato

In caso violazione dei dati che comporti un elevato pregiudizio per i diritti e le libertà degli interessati (cittadini, dipendenti, soggetti terzi, ecc.) e quindi la violazione deve essere comunicata agli interessati impattati dal Security manager e/o dal Responsabile della Conservazione Documentale dovrà supportare il Referente Data Protection, nel reperire ulteriori informazioni, nel predisporre e concordare il testo della comunicazione e nella scelta della modalità di diffusione.

Prima di procedere alla notifica della violazione ai soggetti interessati il testo della comunicazione, la modalità di notifica e le evidenze che attestano il reale livello di pregiudizio, dovranno essere validate dal Titolare del Trattamento o suo delegato.

Nel caso in cui la comunicazione dovesse pregiudicare lo svolgimento delle verifiche sull'evento Data Breach, il Referente Data Protection può chiedere al Garante l'autorizzazione a ritardare la citata comunicazione per il tempo necessario all'espletamento di tali verifiche.

La comunicazione dovrà descrivere con un linguaggio semplice e chiaro la natura della violazione e contenere almeno le informazioni e le misure di cui all'art 33 par. 3, lett b, c).

5 Inventario violazioni

L'art 33 paragrafo 5 del GDPR prevede "*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".*

L'**Applicativo Data Breach e Incident Management** è un tool interno alla Regione Toscana e/o agli enti collegati, realizzato tenendo conto del modulo di comunicazione Data Breach istituito dal Garante, utilizzato come strumento di raccolta e identificazione di un possibile Data Breach e per la valutazione del livello di rischio dello stesso.

Nel registro saranno annotate tutte le informazioni richieste dalla normativa vigente, quali, ad es.: (a) le circostanze relative alla violazione; (b) le conseguenze; (c) i provvedimenti adottati per contrastarla e limitarne gli effetti; (d) i dati personali coinvolti, ecc.

6 Gestione dei soggetti terzi

La normativa disciplina anche l'ipotesi in cui sia il Responsabile, ad esempio il fornitore di un servizio, a venire a conoscenza della violazione dei dati personali ed in tal caso il fornitore dovrà informare il Titolare del trattamento o suo delegato (rectius Regione Toscana) senza ingiustificato ritardo, art 33 par. 2 *"Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione".*

Precisamente, il fornitore deve - appena venuto a conoscenza dell'evento- avvertire il Security manager e/o il responsabile della conservazione documentale fornendo alcune primarie indicazioni del *Breach* (es. Database colpito, misure di sicurezza adottate, grado di rischio sui diritti degli interessati, ecc.).

Questo aspetto non è di secondaria importanza, infatti si consiglia di richiamarlo non solo nell'atto di designazione a Responsabile ex art. 28, ma anche nel contratto di fornitura di servizio.

6.1 Processo Gestione delle segnalazioni di violazioni di dati personali da parte di fornitori.

Gli adempimenti relativi alla gestione delle violazioni dei dati personali ex art 33 del GDPR **-** *sono disciplinati all'interno dei contratti di fornitura stipulati tra committente (La Regione) e soggetti terzi nella clausola adempimenti privacy e/o negli allegati e/o negli addendum contrattuali.*

1) ***Segnalazione dell'evento di violazione dei dati personali oggetto del servizio di commessa.***

Il fornitore esterno nel caso in cui si verifichi un evento di violazione dei dati personali trattati nell'erogazione del servizio oggetto della commessa, effettua una prima analisi dell'accaduto e ove accerti che si tratti di un Data Breach, invia la segnalazione alla Referente interno per la quale eroga il servizio, senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. La segnalazione deve contenere tutti gli elementi utili alla comprensione/identificazione dell'evento.

Il fornitore garantisce inoltre assistenza al referente interno del servizio fornendo eventuali informazioni aggiuntive per la corretta valutazione e gestione dell'evento.

2) ***Rilevazione – Valutazione – Comunicazione di violazione dei dati personali oggetto del servizio di commessa.***

La Referente aziendale che riceve la segnalazione è il referente del contratto di fornitura, il quale usufruisce del servizio oggetto della commessa.

Il referente aziendale del contratto inoltra la segnalazione al Security Manager e/o Responsabile Conservazione documentale.

7 Aspetti sanzionatori

7.1 Violazioni

Le linee guida che il Titolare del trattamento o suo delegato dovrà predisporre, per le proprie verifiche periodiche, quanto meno l'individuazione della casistica delle possibili violazioni con riguardo ai diversi trattamenti e con riferimento agli obblighi giuridici del Titolare del trattamento così come delineati dalla normativa in materia di protezione dei dati personali.

Questo anche al fine di agevolare il controllo della compliance e l'adozione delle misure di contenimento del relativo rischio.

7.2 Sanzioni

In conformità del paragrafo 2 dell'art. 83 GDPR, la violazione da parte del Titolare del trattamento o del Responsabile del trattamento delle disposizioni legate al Data Breach è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente,

Altresì, secondo il paragrafo 2 dell'articolo 83 GDPR, l'inosservanza di un ordine da parte dell'Autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

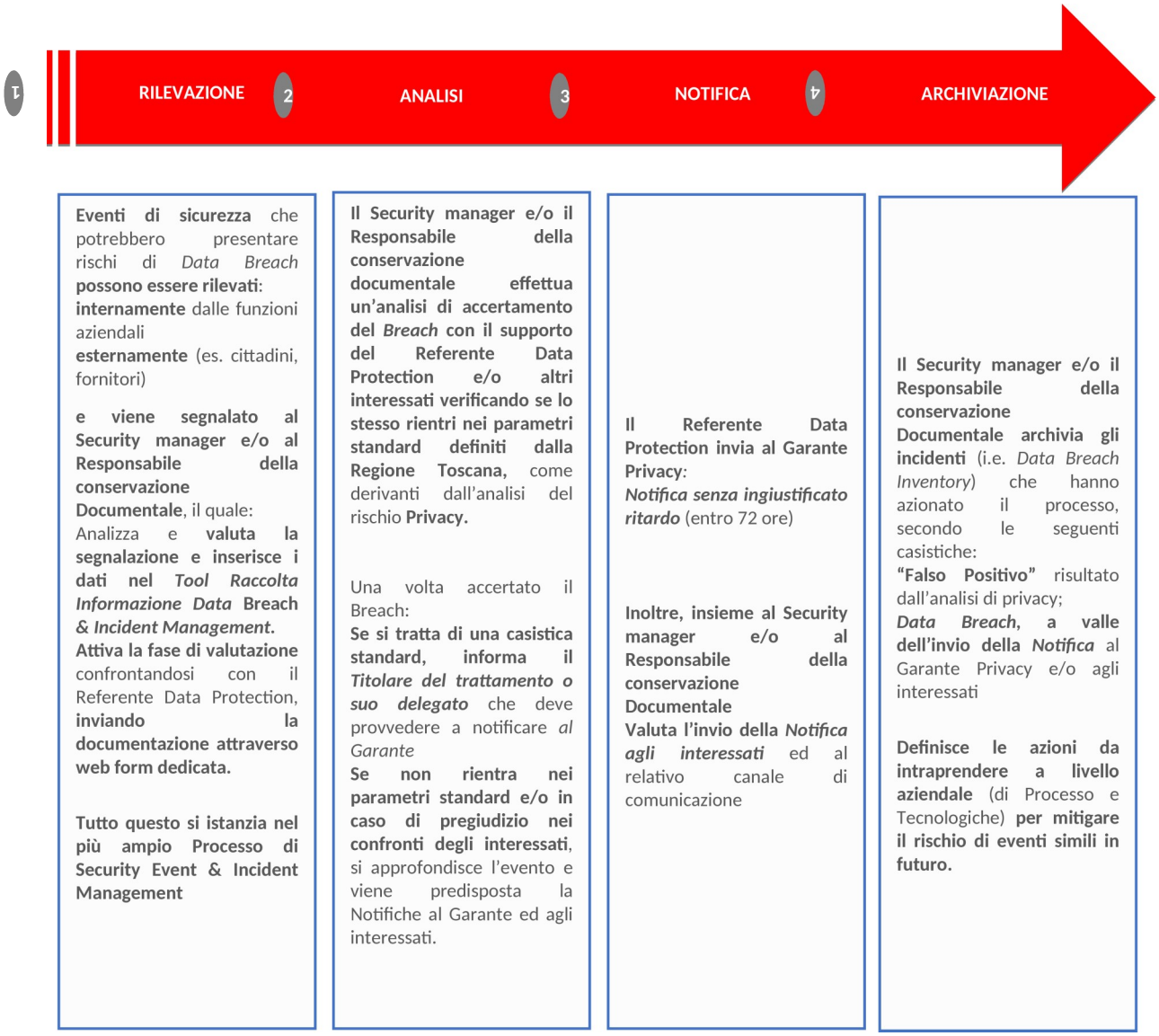
Fatti salvi i poteri correttivi delle Autoritàà di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

A ciò si deve aggiungere, in via generale, che l'art.82 GDPR prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile).

8 Allegati

8.1 Schema "Processo Data Breach"

Al fine di rendere maggiormente esemplificativa la procedura in analisi, si riporta di seguito uno schema esemplificativo dell'intero processo dalla fase di rilevazione sino alla fase di archiviazione del *Data Breach*.

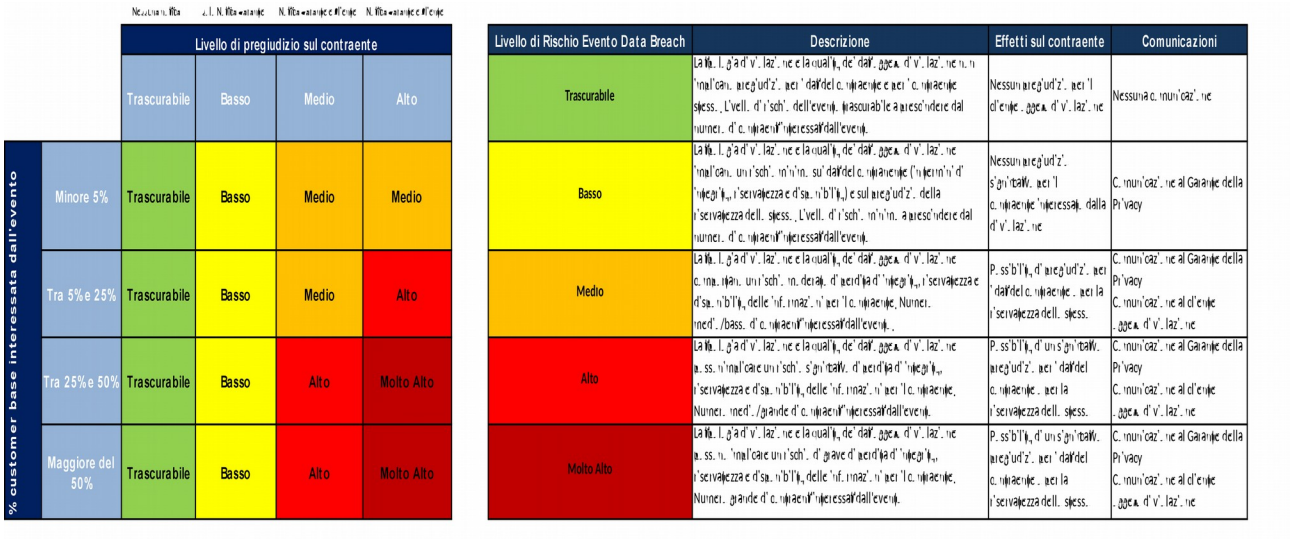


8.2 Tabella di valuzione del livello del rischio

Occorre rapportare la casistica di cui alla tabella alle specifiche valutazioni interne del Titolare del trattamento o suo delegato in termini di criticità dell'evento e di livello del rischio.

È importante che quando viene rilevata una violazione venga segnalato il livello appropriato di gestione in quanto la notifica all'Autorità è obbligatoria solo laddove vi sia un rischio probabile per i diritti e le libertà delle persone fisiche.

Laddove poi vi sia un anche rischio **elevato** per i diritti e le libertà delle persone fisiche anche gli interessati devono essere informati.



% customer base interessata dall'evento	Livello di pregiudizio sul contraente			
	Trascurabile	Basso	Medio	Alto
Minore 5%	Trascurabile	Basso	Medio	Medio
Tra 5% e 25%	Trascurabile	Basso	Medio	Alto
Tra 25% e 50%	Trascurabile	Basso	Alto	Molto Alto
Maggiore del 50%	Trascurabile	Basso	Alto	Molto Alto

Livello di Rischio Evento Data Breach	Descrizione	Effetti sul contraente	Comunicazioni
Trascurabile	La vi. l. g'ard' v'. laz'. ne e la qual'i, de' dall'. ggea. d' v'. laz'. ne n. n 'nal'can. ureg'urd'z'. ueri 'dall'del c. nuraenje e ueri 'c. nuraenje sjess.. L'vell. d' i'sch'. dell'evenj. nascrab'le a uresc'ndere dal nurner. d' c. nuraenj" njecessar'dall'evenj.	Nessun ureg'urd'z'. ueri 'l cl'enje. ggea. d' v'. laz'. ne	Nessuna c. nuni'caz'. ne
Basso	La vi. l. g'ard' v'. laz'. ne e la qual'i, de' dall'. ggea. d' v'. laz'. ne 'nal'can. uni'sch'. n'u'n. su' dall'del c. nuraenje ('nje n'u' d' 'njegi'i,, i'servajezza e d'sa. n'b'l'i,) e sul ureg'urd'z'. della i'servajezza dell. sjess.. L'vell. d' i'sch'. n'u'n. a uresc'ndere dal nurner. d' c. nuraenj" njecessar'dall'evenj.	Nessun ureg'urd'z'. s'gn'tativ. ueri 'l c. nuraenje 'njecessarj. dalla d' v'. laz'. ne	C. nuni'caz'. ne al Garanje della Pi'vacy
Medio	La vi. l. g'ard' v'. laz'. ne e la qual'i, de' dall'. ggea. d' v'. laz'. ne c. nu. nan. uni'sch'. n. derarj. d' ueri'fja d' 'njegi'i,, i'servajezza e d'sa. n'b'l'i, delle 'nf. nraz'. n' ueri 'l c. nuraenje, Nurner. ned'. /bass. d' c. nuraenj" njecessar'dall'evenj..	P. ss'b'l'i, d' ureg'urd'z'. ueri 'dall'del c. nuraenje. ueri la i'servajezza dell. sjess.	C. nuni'caz'. ne al Garanje della Pi'vacy C. nuni'caz'. ne al cl'enje. ggea. d' v'. laz'. ne
Alto	La vi. l. g'ard' v'. laz'. ne e la qual'i, de' dall'. ggea. d' v'. laz'. ne a. ss. n 'nal'cane uni'sch'. s'gn'tativ. d' ueri'fja d' 'njegi'i,, i'servajezza e d'sa. n'b'l'i, delle 'nf. nraz'. n' ueri 'l c. nuraenje, Nurner. ned'. /grande d' c. nuraenj" njecessar'dall'evenj.	P. ss'b'l'i, d' uni s'gn'tativ. ureg'urd'z'. ueri 'dall'del c. nuraenje. ueri la i'servajezza dell. sjess.	C. nuni'caz'. ne al Garanje della Pi'vacy C. nuni'caz'. ne al cl'enje. ggea. d' v'. laz'. ne
Molto Alto	La vi. l. g'ard' v'. laz'. ne e la qual'i, de' dall'. ggea. d' v'. laz'. ne a. ss. n. 'nal'cane uni'sch'. d' grave d' ueri'fja d' 'njegi'i,, i'servajezza e d'sa. n'b'l'i, delle 'nf. nraz'. n' ueri 'l c. nuraenje, Nurner. grande d' c. nuraenj" njecessar'dall'evenj.	P. ss'b'l'i, d' uni s'gn'tativ. ureg'urd'z'. ueri 'dall'del c. nuraenje. ueri la i'servajezza dell. sjess.	C. nuni'caz'. ne al Garanje della Pi'vacy C. nuni'caz'. ne al cl'enje. ggea. d' v'. laz'. ne

8.3 Casi pratici di sussistenza o meno di un Data Breach

Esempi riportati nel documento WP 250 edito dal Gruppo dei Garanti europei ex art.29.

Esempio 1

Viene effettuato un back up di un archivio di dati personali su una chiavetta USB criptata. La chiavetta viene rubata.

Notifica della data breach al Garante?

NO

Notifica della data breach all'interessato?

NO

Note/Raccomandazioni

Nella misura in cui: (1) è stata utilizzata una tecnologia crittografica basata su algoritmi aggiornati e sicuri in base allo stato dell'arte; (2) esistono altri back up dell'archivio su altri supporti; (3) la chiavetta USB non è stata compromessa; (4) può essere comunque effettuato in tempo utile un *restore* dei dati personali, l'evento **non** rappresenta una ipotesi di *data breach* da notificare.

Tuttavia, se successivamente si verifica una compromissione della chiavetta o dell'algoritmo di crittografia, tale ipotesi comporterà l'obbligo di notifica.

Esempio 2

Un Titolare del trattamento gestisce un servizio on line agli utenti. A seguito di un attacco hacker contro tale servizio, i dati degli utenti vengono diffusi. Il gestore di questo servizio ha clienti in un solo Stato membro.

Notifica al Garante?

SI, poiché vi è un probabile rischio per i diritti e le libertà degli interessati (gli utenti del servizio i cui dati sono diffusi a seguito dell'attacco).

Notifica all'interessato?

SI, laddove vi sia un rischio elevato per i diritti e le libertà degli interessati (gli utenti del servizio i cui dati sono diffusi a seguito dell'attacco), in base alla natura dei dati oggetto dell'attacco e alle

conseguenze.

Esempio 3

Una temporanea interruzione di corrente elettrica causa l'impossibilità di resa dei servizi da parte di un call center gestito da un Titolare del trattamento. Gli utenti non sono in grado di chiamare il call center né di accedere ai propri records.

Notifica della data breach al Garante?

NO

Notifica della data breach all'interessato?

NO

Note/Raccomandazioni

Anche se tale incidente non è soggetto a nessuna notifica, resta l'obbligo per il Titolare del trattamento di riportare, descrivere e conservare i riferimenti all'incidente nell'Inventario Incidenti di cui all'art. 33, comma 5 del GDPR.

Esempio 4

Un Titolare del trattamento subisce un attacco di tipo ransomware che determina il blocco e la crittografia di tutti i suoi dati sui sistemi. Non sono disponibili back-up e i dati non possono dunque essere ripristinati. Dopo le opportune verifiche e investigazioni, risulta che lo scopo del ransomware è esclusivamente quello di crittografare i dati e che nessun malware è presente nei sistemi del Titolare del trattamento.

Notifica della data breach al Garante?

SI, in quanto vi è una data breach rappresentata da una perdita di disponibilità dei dati personali che impatta sugli interessati.

Notifica della data breach all'interessato?

SI, in quanto vi è una data breach rappresentata da una perdita di disponibilità dei dati personali che impatta sugli interessati. Vi potrebbero essere altresì anche altre conseguenze in base alla natura dei dati personali.

Note/Raccomandazioni

Ove fossero stati disponibili back up e fosse stato possibile ripristinare i dati personali in breve tempo, tale incidente non avrebbe comportato l'obbligo di notifica della violazione né all'Autorità né agli interessati poiché non vi sarebbe stata perdita permanente di disponibilità dei dati medesimi né di confidenzialità (data la crittografia). In tali casi, ove non fosse stato notificato all'Autorità l'incidente, comunque l'Autorità avrebbe potuto – ove ne fosse venuta a conoscenza – avviare una indagine presso il Titolare per verificare la conformità delle misure di sicurezza da questi adottate all'articolo 32 GDPR.

Esempio 5

Il cliente di una banca chiama la sua agenzia per informarla di un data breach: dichiara di aver ricevuto l'estratto conto mensile di un altro correntista. Nelle 24 ore successive la banca effettua gli

accertamenti del caso e stabilisce che molto probabilmente si è verificata una violazione di dati personali e se tale incidente è sistemico e può interessare anche altri clienti della banca.
Notifica della data breach al Garante? **SI**.
Notifica della data breach all'interessato? **SI**, ma solo agli interessati effettivamente coinvolti, non anche agli altri che potrebbero essere coinvolti.
Note/Raccomandazioni Se dopo le prime investigazioni emerge che sono coinvolti anche altri clienti della banca, il Titolare del trattamento dovrà integrare la notifica di violazione già svolta all'Autorità con le ulteriori informazioni e dovrà notificare anche agli interessati.

Esempio 6 *Il gestore di un marketplace on line, con clienti di diversi Stati europei, è vittima di un cyber attacco a seguito del quale usernames, passwords e storico degli acquisiti della clientela sono pubblicati on line.*
Notifica della data breach al Garante? **SI**. Nel caso siano coinvolte più autorità privacy – data la natura cross-border della violazione dei dati personali – andrà effettuata la notifica della violazione alla leading Authority (individuabile in base alle)
Notifica della data breach all'interessato? **SI**, poiché è elevato il rischio per i diritti e le libertà dei clienti coinvolti.
Note/Raccomandazioni Il gestore del marketplace dovrebbe prendere immediate misure volte a mitigare il rischio. Ad esempio forzando il reset delle password dei clienti.

Esempio 7 *Il fornitore di servizi di hosting per siti web che agisce quale Responsabile esterno del trattamento si avvede di un errore nel codice di controllo delle autorizzazioni a seguito del quale qualsiasi utente può accedere all'account di qualsiasi altro utente.*
Notifica della data breach al Garante? Come Responsabile esterno del trattamento e fornitore dei servizi di hosting ai suoi clienti (i Titolari del trattamento), la società di hosting deve immediatamente informare e senza ritardo della violazione i suoi clienti (i Titolari del trattamento). Assumendo che la società di hosting abbia condotto le propri investigazioni, nel momento in cui i Titolari sono informati dal Responsabile esterno, è questo il momento in cui essi diventano consapevoli della violazione e dunque da tale momento decorre il termine di 72 ore per effettuare la notifica all'Autorità.
Notifica della data breach all'interessato? Se non vi è un rischio elevato, non vi è obbligo di notificare la violazione agli interessati.
Note/Raccomandazioni

Esempio 8 *Per errore di un addetto del Titolare del trattamento le schede anagrafiche dei partecipanti a un corso*

di formazione sono trasmesse ad una mailing list errata di più di mille destinatari.
Notifica della data breach al Garante? SI.
Notifica della data breach all'interessato? SI. Va comunque valutato il livello di gravità la severità delle conseguenze dell'errato invio.
Note/Raccomandazioni

Esempio 9 *Una email di direct marketing è inviata in copia palese e non nascosta a molti destinatari, che dunque possono vedere i recapiti di posta elettronica di ciascun destinatario in copia..*
Notifica della data breach al Garante? SI, ma solo nel caso in cui sia coinvolto un elevato numero di interessati, vi sia una natura delicata (es: la mailing list dei pazienti di uno studio medico) o il contenuto del messaggio sia rischioso (es: invio del primo pin o password per accedere a un servizio).
Notifica della data breach all'interessato? SI. Va comunque valutato il livello di gravità la severità delle conseguenze dell'errato invio.
Note/Raccomandazioni Potrebbe non esservi alcun obbligo di notifica, né all'Autorità né agli interessati, ove sia molto limitato il numero di interessati coinvolti e la natura dei dati sia ordinaria e non delicata.