POLICY GESTIONE "DATA BREACH"

Applicazione del Regolamento Europeo 679/2016 ("GDPR") in materia di protezione dei dati personali per la corretta gestione delle violazioni di dati personali ai sensi degli artt.33 e 34 del GDPR

Nome documento:	**POLICY DATA BREACH**	Versione:	**01.00**
Redatto da:	**DPO**	Verificato ed approvato da:	**Titolare del trattamento**

SOMMARIO

RIFERIMENTI NORMATIVI

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 "GDPR" relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE - Considerando n. 85, 86, 87, 88 artt. 33 e 34;
- Decreto Legislativo 30 giugno 2003 n. 196, come modificato e armonizzato dal Decreto Legislativo del 10 agosto 2018, n. 101;
- Linee guida sulla notifica delle violazioni di dati personali ai sensi del Regolamento UE 679/2016 ("on Personal Data Breach Notification under Regulation 2016/679), adottate dal Gruppo di lavoro Articolo 29 ("WP 29") - adottate il 3 Ottobre 2017 – Revisionate in via definitiva il 6 Febbraio 2018;
- Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali, Garante per la protezione dei dati personali (edizione aggiornata – Febbraio 2018)
- Linee guida concernenti la Valutazione di Impatto sulla Protezione dei Dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679, adottate dal WP29 - in via definitiva il 4 ottobre 2017;
- Linee guida sui Responsabili della Protezione dei Dati (WP243), adottate dal WP29;
- Guidelines 01/2021 EDBB on examples regarding personal Data Breach notification.

INTRODUZIONE

Il Regolamento Europeo 679/2016 (di seguito "GDPR"), prescrive per il Titolari del trattamento (si seguito "Titolare") un nuovo adempimento generalizzato che consiste nella violazione dei dati personali (c.d. "Data Breach").

In base al Considerando 85 del GDPR, una violazione dei dati personali potrebbe, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali e immateriali alle persone fisiche.

A seguito di un violazione possono derivare pregiudizi di varia natura dalla perdita di controllo dei dati personali alla limitazione diritti degli interessati compreso il furto o usurpazione di identità, pregiudizio alla propria reputazione e perdita di riservatezza, ma più in generale qualsiasi danno economico e/o sociale anche significativo agli interessati.

In particolare l'art. 32 del GDPR dispone che devono essere approntate misure tecniche e organizzative adeguate a garantire un livello adeguato di sicurezza dei dati personali. Individuare, indirizzare e segnalare tempestivamente una violazione di dati, è espressione dell'adeguatezza delle misure implementate dal Titolare. In tale contesto si ritiene necessario dotarsi di una procedura interna per la corretta gestione delle violazioni.

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

Inoltre, con specifico riferimento all'obbligo di cui all'art. 33 del GDPR n. 679/2016, il presente documento individua (non esaustivamente) quali siano le violazioni che ricadono nell'ambito della suddetta normativa, i casi in cui il Titolare deve notificare i c.d. "Data Breach" all'Autorità Garante ed agli interessati, le misure atte a trattare il rischio e la documentazione da produrre.

AMBITO APPLICATIVO

Le politiche descritte nel presente documento si applicano a tutti i dipendenti e collaboratori del Titolare (con particolare riferimento alla gestione di tutti gli archivi/documenti cartacei e di tutti i sistemi informatici/telematici), i quali durante lo svolgimento delle loro attività possono venire a conoscenza di una violazione dei dati personali.

Le presenti politiche si applicano anche ai fornitori nella misura in cui sono da considerarsi Responsabili del trattamento, ai sensi dell'articolo 28 del GDPR e compatibilmente con procedure adottate e applicate dagli stessi. In tal contesto è fatto obbligo loro di segnalare la violazione secondo le modalità indicate nella presente procedura.

DEFINIZIONI, TERMINI E ACRONIMI

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 (art. 4, punto 1).

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 (art. 4, punto 2).

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6).

Titolare del trattamento: 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 (artt. 4 e 24).

Designato al trattamento: la persona fisica che, secondo l'organizzazione aziendale, ricopre un ruolo gestionale e di responsabilità all'interno dell'Organizzazione (Art. 2-quaterdecies D.Lgs. 101/2018); [...] che può determinare specifiche modalità organizzative rispetto ad uno o più trattamenti.

Autorizzato al trattamento/Referente: la persona fisica, espressamente designata, che opera sotto l'autorità del Titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 29 e 4, punto 10).

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 (art. 28, punto 8).

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

GDPR: Regolamento Generale per la protezione dei dati personali (Reg. UE 679/2016).

Violazione dei dati personali (c.d. Data Breach): 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 (art. 4, p. 12);

«Autorità di controllo/Autorità/Garante»: l'Autorità pubblica indipendente istituita da uno Stato membro; in Italia è il Garante per la protezione dei dati personali.

RAID - AdS (eventuali): Responsabile Area informatica/digitale – Amministratore di Sistema.

DEFINIZIONE DI DATA BREACH

L'art. 33 del GDPR recita che:

[…] "In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 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".

Per "Data Breach" si intende un evento in conseguenza del quale si verifica una "Violazione dei dati personali". Nello specifico, l'articolo 4 p.12 del GPDR definisce la violazione dei dati personali **come violazione di sicurezza che comporta accidentalmente o in modo illecito** la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Le Linee guida in materia di notifica delle violazioni di dati personali (*Data Breach Notification*), definite in base alle previsioni del GDPR, precisano la nozione di violazione come di seguito:

- Nel parere 03/2014 sulla notifica delle violazioni, il WP29 ha spiegato che le violazioni possono essere classificate in base a tre principi ben noti della sicurezza delle informazioni:
  a) "***Violazione della riservatezza***", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
  b) "***Violazione dell'integrità***", in caso di modifica non autorizzata o accidentale dei dati personali;
  c) "***Violazione della disponibilità***", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

N.B.: Va altresì osservato che, a seconda dei casi, una violazione può contemporaneamente riguardare la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Ci si potrebbe chiedere se una perdita temporanea della disponibilità dei dati costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica.

L'art. 32 del GDPR ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico".

Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo **costituisce una violazione**, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche.

Dettagli: Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'articolo 4, punto 12 del GDPR.

Nota Bene: qualsiasi violazione che implichi la perdita temporanea di disponibilità dovrebbe essere documentata, poiché ciò aiuta il Titolare a dimostrare l'assunzione di responsabilità all'autorità di controllo, che potrebbe chiedere di consultare tali registrazioni.

Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'autorità

di controllo e la comunicazione alle persone fisiche coinvolte. Il Titolare dovrà valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche.

Conformemente all'articolo 33, il Titolare dovrà effettuare la notifica **a meno che sia improbabile** che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso.

Va notato che, sebbene una perdita di disponibilità dei sistemi del Titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il Titolare stesso consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi. La mancata notifica può comportare ulteriori accertamenti da parte del Garante poiché può rappresentare un indizio di carenze che, se accertate, possono dar luogo a sanzioni.

Dettagli: Tutti gli eventi di Data Breach, compresi quelli per cui non sono necessarie le notifiche, devono essere documentati (art. 33 par. 5 del GDPR) su un **Registro delle Violazioni**.

Il Garante per la protezione dei dati personali può richiedere, in ogni caso, la notifica della violazione agli interessati. *La comunicazione della violazione agli interessati può essere ritardata nei casi in cui tale comunicazione possa pregiudicare le indagini su cause, natura e conseguenze della violazione, anche su indicazione delle varie Autorità di controllo.*

ESEMPI DI VIOLAZIONI

Tipologia Violazione	BREVE DESCRIZIONE
Accesso non autorizzato	Accesso (sia logico che fisico) a reti, sistemi, applicazioni, dati o altre risorse
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.
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.
Uso inappropriato	Violazione delle politiche di sicurezza e delle disposizioni su corretto utilizzo.
Codice malevolo	Un virus, worm, trojan, spyware, o qualsiasi altro codice malevolo che "infetti" un sistema
Data Leakage	Diffusione di informazioni riservate a seguito di un attacco informatico.
Alterazione delle informazioni	Modifica del contenuto di dati riservati a seguito di un attacco informatico.
Furto/smarrimento totale o parziale di apparecchiature	Furto o smarrimento di singoli dispositivi di memorizzazione che contengono dati personali (hard disk, memorie di massa rimovibili, etc) oppure dei computer/server che li ospitano.
Malfunzionamento Grave	Danneggiamento di un componente HW o SW, degrado delle performance per cause esterne che possano 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.
Multiplo	Incidente di sicurezza che comprende due o più di quelli sopra elencati.

PROCEDURA

Prima che si verifichi un Data Breach occorre predisporre le procedure, gli strumenti e l'organizzazione per gestire l'evento al meglio.

Pianificazione

I Soggetti Competenti devono:

- Individuare e predisporre i mezzi tecnologici ed organizzativi per:
  - ✓ Individuare, Analizzare e Rispondere alle potenziali violazioni dei dati, coinvolgendo tutti i soggetti ritenuti essenziali e utili alla corretta procedura.

GESTIONE DELL'EVENTO

In caso di accertamento di violazione che rientra nella definizione di Data Breach, sarà opportuno seguire i seguenti steps:

Acquisizione della notizia da parte dei soggetti che sono venuti a conoscenza della violazione (o che l'hanno accidentalmente provocata);

La segnalazione di un può essere interna (personale dipendente, collaboratori, personale convenzionato/stagisti/tirocinanti, etc) o esterna (DPO, organi Pubblici quali Forze dell'Ordine, giornalisti o altri, Responsabili del trattamento, etc).

La segnalazione deve essere inoltrata mediante PEC/Email/avvertimento verbale e/o telefonico (comunque con il mezzo ritenuto più efficace e celere) direttamente al Titolare del trattamento e/o ai soggetti designati al trattamento (solitamente Dirigenti, Responsabili, figure di Vertice/apicali) o in alternativa al DPO che provvederà alla comunicazione di competenza.

Analisi tecnica dell'evento e contenimento del danno;

I Riceventi, effettuano una breve ***analisi preliminare*** (anche coinvolgendo il DPO) per comprendere se tale segnalazione si configuri effettivamente come un "Data Breach".

Qualora l'evento segnalato si configuri effettivamente come un "Data Breach" (a seguito appunto dell'analisi preliminare), è necessario raccogliere gli elementi per una valutazione e ***analisi approfondita*** dell'evento ai fini della notifica al Garante Privacy. Tale analisi è svolta insieme al segnalante richiedendo informazioni e facendo compilare apposito modello.

Nota bene: È importante sottolineare che, anche nel caso in cui dall'Analisi Preliminare emerga che la segnalazione non ha i caratteri del Data Breach, è consigliabile comunque registrarla nel Registro delle Violazioni.

Durante l'Analisi Approfondita, dovranno essere accertate le circostanze della violazione, le conseguenze e i relativi rimedi.

Si precisa che l'art. 33 paragrafo n. 4 del DGPR recita "Qualora nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo". Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni e, anche in caso queste non siano per il momento ritenute esaustive, effettuare la notificazione.

Nello specifico verrà effettuato, in un tempo consigliabile non superiore a 12 – 24 ore, almeno:

- Il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento;
- L'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
- L'identificazione degli interessati;
    - Il contenimento del danno (Limitazione degli effetti, Raccolta delle prove nel caso sia ipotizzato un reato, Determinazione delle azioni possibili di ripristino, Valutazione delle eventuali vulnerabilità collegate con l'incidente, Individuazione delle azioni di mitigazione delle vulnerabilità individuate, Valutazione dei tempi di ripristino, Ripristino dei dati, dei sistemi, dell'infrastruttura e delle configurazioni, Verifica dei sistemi recuperati).

Valutazione della gravità dell'evento;

Per identificare le modalità di gestione di una violazione e gli eventuali obblighi di notifica e/o di comunicazione, i soggetti che hanno ricevuto la segnalazione con il supporto del DPO (che in questa fase **va obbligatoriamente coinvolto**), effettuano la valutazione del rischio e della gravità/impatto, come di seguito indicato.

Il livello di rischio è definito sulla base di due parametri, gravità e probabilità:

- ❖ Gravità: rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati);
- ❖ Probabilità: grado di possibilità che si riverifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).

Ai fini della identificazione dei valori da attribuire ai due parametri, è possibile considerare i seguenti fattori:

- tipo di violazione;
- natura, sensibilità e volume dei dati personali;
- facilità nella identificazione degli interessati;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati (es. minori);
- numero degli interessati.

GRAVITÀ	<u>Impatto della violazione sui diritti e le libertà delle persone coinvolte:</u> • ***Basso***: nessun impatto • ***Medio***: impatto poco significativo, reversibile • ***Alto***: impatto significativo, irreversibile (o quasi)
PROBABILITÀ	<u>Possibilità che si verifichino nuovamente uno o più eventi temuti:</u> • ***Basso***: l'evento temuto non si rimanifesta • ***Medio***: l'evento temuto potrebbe rimanifestarsi • ***Alto***: l'evento temuto si è nuovamente manifestato

		GRAVITÀ		
		A	**M**	**B**
PROBABILITÀ	**A**			
	M			
	B			

	DESCRIZIONE	**Notifica al Garante**	**Comunicazione agli interessati**
RISCHIO	Basso: nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	**NO**	**NO**
	Medio: possibile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	**SI/NO**	**NO**
	Alto: pregiudizio certo sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	**SI**	**SI**

Matrice della gravità - Indicazioni per la corretta valutazione

GRAVITÀ	DESCRIZIONE
Alta	Il grado di compromissione di servizi e/o sistemi è elevato. Si rilevano danni consistenti sugli asset. Il ripristino è di medio o lungo periodo. La violazione 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; • Frode o attività criminale che coinvolga servizi forniti dal Titolare; • Impossibilità tecnica di fornire uno o più servizi critici a un elevato numero di utenti per un intervallo di tempo superiore ai 30 minuti nell'arco di una giornata; • Impossibilità tecnica di fornire uno o più servizi di criticità media per un periodo di tempo superiore ai 2 giorni lavorativi; • Significativa perdita economica, di immagine e/o reputazione nei confronti del pubblico o degli utenti.
Media	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità Alta – Medio/Alta". Il grado di compromissione di servizi e/o sistemi è di una certa rilevanza e possono essere rilevati danni sugli asset di una certa consistenza. Il ripristino ha tempi che non compromettono la continuità del servizio L'incidente presenta una tra le seguenti condizioni: • Compromissione di server e/o PC; • Degrado di prestazioni relative ai servizi offerti con conseguente perdita di produttività da parte degli utilizzatori; • Attacchi che provocano il funzionamento parziale o intermittente della rete; • Impossibilità di fornire uno o più servizi critici ad un elevato numero di utenti per intervalli di tempo inferiori ai 30 minuti di tempo ripetuti su più giornate; • Impossibilità tecnica di fornire uno o più servizi critici ad una piccola parte di utenti per un periodo di tempo superiore ai 30 minuti di tempo nell'arco di una o più minuti ei tempo nell'arco di una o più giornate • Basso impatto in termini di perdita economica, di immagine e/o reputazione nei confronti degli utenti
Bassa	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità Alta o Media". Non vengono compromessi asset o servizi. La violazione presenta le seguenti condizioni: • Interruzione dell'attività lavorativa di un numero ristretto di dipendenti e per un breve periodo di tempo; • Contaminazioni da virus in un medesimo sito ma comunque identificate dai sistemi anti-intrusione; • Nessuna o limitata perdita di operatività o di business da parte di un ridotto numero di dipendenti

Sulla base degli elementi di cui sopra:

I. I Soggetti Designati coadiuvati dal DPO, stimano la gravità e la probabilità della violazione e classifica il rischio;

II. il Titolare, previa condivisione della valutazione con il DPO e i Soggetti Designati, documenta la decisione presa a seguito della valutazione nel "Registro delle violazioni";

III. Nel caso in cui il rischio sia considerato non elevato e non si ritenga necessario procedere con la comunicazione, il Titolare, unitamente al parere del DPO e dei Soggetti Designati, specifica la giustificazione per tale scelta, riservando la possibilità di comunicare la violazione in seguito.

IV. Nel caso il rischio lo richieda, il Titolare, su indicazione del DPO e dei Soggetti Designati, procede alla notifica della violazione all'Autorità garante, e ove necessario agli Interessati.

V. Gli elementi a supporto del procedimento e degli esiti della valutazione sono documentati.

Notifica al Garante "Privacy" (ove ritenuta necessaria);

La normativa prevede che, non appena si viene a conoscenza di una violazione dei dati personali che presenti un rischio per i diritti e le libertà delle persone coinvolte (pari o superiore al livello stabilito "Medio/Basso", è obbligatorio effettuare la notifica all'Autorità. Per le violazioni così identificate, l'invio (a cura del Titolare, il Titolare, con il supporto del DPO) avviene entro 72 ore dal momento in cui il Titolare del trattamento ne è venuto a conoscenza. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

A partire dal 1° luglio 2021, la notifica di una violazione di dati deve essere inviata al Garante tramite un'apposita **procedura telematica**, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/. N.B.: Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica ma utile per vedere in anteprima i contenuti che andranno comunicati.

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito strumento di autovalutazione (self assessment) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Il documento di notifica contiene i seguenti elementi:

- La natura della violazione dei dati, compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati in questione;
- Il nome e/o i dati di contatto del DPO o di altro contatto presso cui ottenere informazioni;
- Le probabili conseguenze della violazione dei dati personali;
- Le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione;
- I motivi del ritardo, qualora la notifica all'autorità non sia effettuata entro 72 ore;
- Eventualmente, una dichiarazione sulla mancanza di alcune delle informazioni necessarie e un impegno a fornire, il prima possibile, le informazioni aggiuntive, in una o più fasi successive.

Eventuali altre segnalazioni dovute;

Si dovrà verificare la necessità di informare altri organi quali ed esempio:

- Al Gestore di Identità Digitale e ad Agid nel caso in cui si individui un uso anomalo di un'identità SPID.

Segnalazioni allo CSIRT ed agli Organi di Polizia (ove ritenuta necessaria);

La comunicazione allo CSIRT

Dallo scorso 6 maggio 2020, il **CERT-PA** e il **CERT** Nazionale, strutture che hanno rispettivamente supportato le Pubbliche Amministrazioni ed il settore privato nella prevenzione e nella risposta agli incidenti cibernetici, hanno terminano tutti i servizi proattivi, reattivi e di risposta a tali incidenti, passando con gradualità le consegne allo **CSIRT Italia**, il nuovo team per gestire la cyber-difesa nazionale istituito presso il Dipartimento Informazioni per la Sicurezza (DIS).

Da tale data, inoltre, i due CERT cessano contestualmente di esistere come soggetti autonomi.

La decisione rientra nell'ambito del piano di attuazione della **Direttiva NIS** (Decreto legislativo 18 maggio 2018 n. 65), recante le misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione europea, che – tra le altre misure – prevede anche in Italia la costituzione di un ***Computer Security Incident Response Team unico*** (**cosiddetto CSIRT**).

L'attività dello CSIRT è disciplinata dal DPCM 8 agosto 2019 in materia di "Disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team – CSIRT italiano", pubblicato in Gazzetta Ufficiale l'8 novembre 2019. In tale quadro, i soggetti pubblici e privati, a partire dalla data menzionata, in caso di incidente cibernetico e/o di segnalazione di evento, hanno quale nuovo ed unico interlocutore lo **CSIRT Italia, che già riceve le notifiche obbligatorie e volontarie degli *operatori di servizi essenziali* (cosiddetti OSE) e *Fornitori di Servizi Digitali* (cosiddetti FSD) ai sensi della Direttiva NIS**.

→ Il sito di riferimento dello CSIRT Italia è disponibile al link https://csirt.gov.it.

→ La notifica di un incidente può essere effettuata online al link https://csirt.gov.it/segnalazione.

Segnalazione agli organi di polizia

Occorre sempre effettuare denuncia agli organi di polizia quando la violazione ai dati sia conseguenza di comportamenti illeciti o fraudolenti. Oltre alle modalità conosciute per eseguire comunicazione o denuncia agli organi di polizia, per certe tipologie di "Data Breach" è possibile eseguire una comunicazione telematica, infatti da tempo è stato attivato un **sito internet della Polizia Postale e delle Comunicazioni** raggiungibile all'indirizzo www.commissariatodips.it. All'interno di queste pagine è anche possibile reperire utili notizie sui tentativi di reato in corso ed eseguire denunce o segnalazioni di reati telematici previa registrazione.

Altre notizie su tentativi di frode sono ottenibili attraverso internet dal sito della struttura denominata CSIRT raggiungibile all'indirizzo https://csirt.gov.it.

Comunicazione agli Interessati (ove ritenuta necessaria);

Nel caso di accertamento di una violazione dei dati personali che sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare comunica la violazione all'interessato/i.

La comunicazione non è richiesta se è soddisfatta una delle seguenti condizioni:

- 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;
- 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;

- 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.

La comunicazione contiene almeno i seguenti elementi:

- La natura della violazione dei dati personali, descritta con linguaggio semplice e chiaro;
- Il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- Le probabili conseguenze della violazione dei dati personali;
- Le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione.

Per la comunicazione, è possibile identificare uno o più canali di comunicazione, a seconda delle circostanze, quali email, SMS, posta, comunicati pubblicitari, banner o notifiche su siti web, scegliendo il canale che massimizza la probabilità che tutti gli interessati siano raggiunti dal messaggio.

Inserimento dell'evento nel Registro delle violazioni;

Il Titolare avvalendosi dei Designati/Autorizzati coadiuvati dal DPO, coordinano e supervisionano l'aggiornamento del Registro delle violazioni, ai sensi dell'art. 33, c. 5 del GDPR, verificando che siano state annotate tutte le informazioni utili e necessarie per la gestione della possibile violazione dei dati, ovvero almeno:

- Data rilevazione della violazione;
- Natura della violazione e categorie di dati personali coinvolti;
- Servizio/Area/Settore/Ufficio coinvolti;
- Categorie (numero ove possibile) degli interessati coinvolti;
- Cause della violazione;
- Probabili conseguenze della violazione;
- Rischio (derivante dalla stima della gravità e della probabilità);
- Misure adottate o di cui si propone l'adozione per mitigare i rischi e possibili effetti negativi;
- Notifica Autorità Garante per la Protezione dei dati (data e ora, rifermento per reperire la notifica);
- Comunicazione agli interessati (data e ora, modalità di comunicazione);
- Verifica attuazione ed efficacia delle misure adottate e data di verifica.

Ad integrazione di quanto riportato nel Registro, il Titolare coadiuvato dai Designati/Autorizzati e dal DPO, raccoglie e conserva tutti i documenti relativi ad ogni violazione, compresi quelli inerenti le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione è resa disponibile all'Autorità di controllo per le verifiche di competenza.

CONTROLLI, AZIONI CORRETTIVE SPECIFICHE (E/O PER ANALOGIA) POST INCIDENTE

In seguito alla comunicazione e "chiusura" del Data Breach, dovranno essere valutate tutte le operazioni eseguite per la gestione dello stesso, evidenziando sia i punti in cui queste sono state eseguite in armonia con le procedure e le aspettative, sia eventuali problemi sorti durante lo svolgimento delle operazioni.

È fondamentale che i punti critici rilevati durante l'esecuzione delle operazioni siano immediatamente condivisi con i componenti del team di gestione dei Data Breach e si provveda nel più breve tempo possibile a predisporre quanto può essere necessario per eliminarli o mitigarli, migliorando quindi sia la procedura tecnica di gestione sia la capacità di operare dei Soggetti preposti, sia agendo sulle infrastrutture e i sistemi.

Di seguito alcuni esempi di punti critici che possono essere rilevati:

- mancanza delle competenze per operare correttamente;
- mancanza degli opportuni strumenti;
- errori nella valutazione della gravità dell'incidente o nelle sue capacità di diffusione;
- errori o difficoltà nell'interazione con soggetti interni (ed esterni);
- errori nella comunicazione verso terze parti o verso dipendenti e collaboratori.

In particolare può essere utile porsi le seguenti domande:

- La procedura è stata correttamente eseguita? È risultata adeguata al contesto?
- Si sono presentati aspetti che hanno rallentato la risoluzione del Data Breach?
- Si sono presentati elementi che si ritiene siano da cambiare in modo da rendere il processo più efficace ed efficiente?
- È necessario aggiornare il metodo di analisi della gravità a valle del Data Breach?
- Sono necessarie delle azioni correttive da intraprendere in fase di mitigazione dei rischi onde evitare che il Data Breach possa riaccadere?
- È necessario modificare le policy interne dal punto di vista tecnico?
- È necessario aggiornare e/o migliorare gli interventi formativi al fine di istruire il personale sulle problematiche inerenti la sicurezza e la protezione dei dati?
- Sono necessarie risorse addizionali (es.: personale, tools, strumenti hardware o software) per rendere il processo più efficace ed efficiente?
- Sono necessarie modifiche e/o riconfigurazioni del software (es.: aumentare frequenza di aggiornamento delle firme dei software antivirus e/o anti-intrusione e, modificare il livello di dettaglio fornito dai sistemi di difesa perimetrali)?

Questa operazione ha lo scopo di verificare che il processo di gestione del Data Breach sia risultato adeguato a fronteggiare la situazione e far sì che le considerazioni che ne scaturiscono debbano divenire patrimonio comune.

Per questo motivo occorre che entro breve termine dalla chiusura formale di un Data Breach, il Titolare convochi tutte le risorse che sono state parte attiva nella gestione, con l'obiettivo di valutare collegialmente l'efficacia della procedura di gestione tenere traccia delle le considerazioni e le operazioni che possono portare a migliorare l'intera procedura. Inoltre, qualora siano identificati più Titolari del trattamento (o casi in cui siano coinvolti Responsabili del trattamento o Contitolari), verificare se i ruoli e le responsabilità tra le parti siano state correttamente definite (ad esempio con la "Designazione del Responsabile del trattamento" ovvero con apposite "clausole privacy"), per la corretta gestione degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali, concordandone puntualmente le modalità, al fine di garantire il rispetto dei termini di notifica e comunicazione, di cui il Titolare del trattamento resta legalmente responsabile.

MATRICE DI ASSEGNAZIONE DELLE RESPONSABILITÀ

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

Ruoli chiave

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

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

Definizione delle figure coinvolte

FIGURA	DESCRIZIONE DELLA FIGURA
Titolare del trattamento	Intera organizzazione, le azioni sono compiute dal suo legale rappresentate o suo sostituto
Responsabile Anticorruzione e Trasparenza – "RPCT", se presente	Responsabile Anticorruzione e Trasparenza (art. 7 L. 190/2012 e art. 43D, Lgs n. 33/2013)
RPD o DPO, se presente	Responsabile della protezione dei dati (art. 37 GDPR)
Privacy Officer, se presente	Consulente privacy
Designato al trattamento, se presente (in alternativa Autorizzato al trattamento / referente privacy, ex art. 29 GDPR)	Soggetto designato dal Titolare per sovrintendere alle operazioni di trattamento (ex art. 2-quaterdecies del D.Lgs. 196/2003 come novellato dal D.Lgs. 101/2018)

Responsabile del Trattamento, se presenti	Soggetto esterno nominato "Responsabile" dal Titolare (art. 28 GDPR)
Responsabile Sistemi informativi / Amministratore di Sistema, se presente	Soggetto individuato dal Titolare per sovrintendere alle operazioni di trattamento eseguite con strumenti informatici (Provvedimento Garante del 27 novembre 2008). La figura può coincidere con quella di Responsabile per la Transazione al Digitale (art. 17 CAD)
Responsabile Conservazione digitale/sostitutiva, se presente	Soggetto nominato ai sensi del DPCM 03/12/2013 (regole tecniche in materia di conservazione)
Responsabile Archivi, se presente	Soggetto nominato Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (art. 3 DPCM 3/12/2013 e art. 61 D.P.R. 445/2000)
Responsabile Violazione, se individuabile	Colui o coloro a cui è attribuibile la violazione di sicurezza
Autorità Garante per la protezione dei dati personali – "Garante Privacy"	Autorità nazionale a tutela dei diritti derivanti dalle norme sulla protezione dei dati personali
CSIRT	Il CSIRT italiano è istituito presso il Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri. I compiti del CSIRT sono definiti dal Decreto Legislativo 18 maggio 2018, n. 65 e dal Decreto del Presidente del Consiglio dei ministri 8 agosto 2019 art. 4. Essi includono: • il monitoraggio degli incidenti a livello nazionale; • l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; • l'intervento in caso di incidente; • l'analisi dinamica dei rischi e degli incidenti; • la sensibilizzazione situazionale; • la partecipazione alla rete dei CSIRT.
Forze dell'ordine	Organo di polizia o Magistratura a cui viene denunciata la violazione di sicurezza se ne ricorrono gli estremi
Interessati	Persone fisiche i cui dati sono stati coinvolti nell'incidente

N.B.: Una persona fisica può ricoprire anche simultaneamente più figure. Ne caso di assenza o indisponibilità si devono utilizzare i criteri di sostituzione previsti dalla normativa o nei provvedimenti interni appositamente assunti.

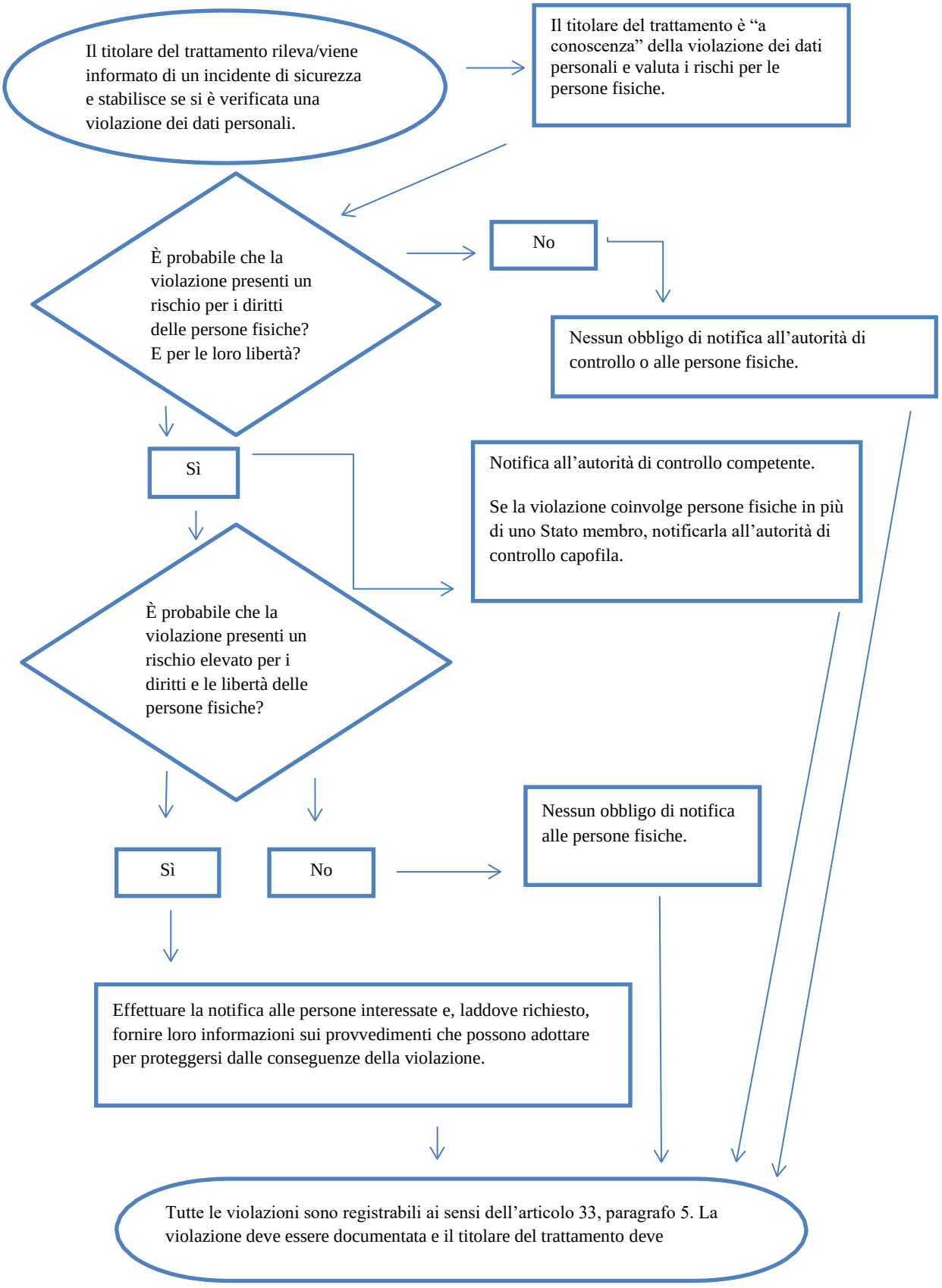
Matrice RACI

FASI / FIGURE	Rilevazione/ Acquisizione	Gestione Tecnica e Analisi	Valutazione	Notifica al Garante	Altre Segnalazioni	Comunicazioni interessati e riscontri	Registrazione della Violazione
Titolare	**I**	**I**	**A**	**A**	**A**	**R**	**A**
RPCT		**C**	**C**	**I**	**I**	**I**	**I**
DPO	**C**	**C**	**C**	**R**	**C**	**R**	**C**
Designato	**R**	**R**	**R**	**R**	**R**	**R**	**R**
Responsabile trattamento (se coinvolto)	**R**	**R/A**	**R**	**R**	**R**	**R**	**C**
Responsabile comunicazione		**I**	**I**	**I**		**A**	**I**
Responsabile archivi	**A**	**A/R**	**C**	**R**	**R**	**R**	**I**
Responsabile violazione		**C**	**I**		**I**		
Garante privacy				**I**		**I**	**I**
CSIRT/Forze dell'Ordine					**I**		
Interessati						**I**	

AGGIORNAMENTO DEL PRESENTE DOCUMENTO E DEGLI ALLEGATI

Sulla base dell'evolversi della normativa e del pensiero in materia di protezione dei dati personali potrà presentarsi la necessità di aggiornare o integrare il presente documento. La frequenza di aggiornamento non può essere stabilita a priori. Qualora le autorità o gli organismi pubblici mettessero a disposizione modelli di comunicazioni o metodologie di comunicazione che sostituiscano i modelli qui riportati si dovranno immediatamente adottare.

DIAGRAMMA DI FLUSSO OBBLIGHI DI NOTIFICA



ALLEGATI

- ® Modello Segnalazione Data Breach
- ® Tabella accertamenti e ispezioni preliminari Data Breach
- ® Modello di comunicazione all'Interessato del Data Breach
- ® Registro Data Breach