Linea guida/Policy per la gestione del “Data Breach”

Approvata con Determina dell’Amministratore Unico n. 25 del 22 Novembre 2018

CUP 2000 S.c.p.A. - Sede Legale
Via del Borgo di S. Pietro, 90/c
40126 Bologna
tel. +39 051 4208411
fax +39 051 4208511
cup2000@cup2000.it - cup2000@cert.cup2000.it - www.cup2000.it

C.F., P. IVA e Iscrizione al Registro delle Imprese di Bologna n. 04313250377 - Capitale Sociale €. 487.579,00 i.v.

1. Linea guida / Policy per la gestione del "Data Breach"

1.1. Premessa

L'art. 33 (*Notifica di una violazione dei dati personali all'autorità di controllo*) del **Regolamento Europeo 679/2016 (GDPR)** impone al titolare del trattamento di notificare all'autorità di controllo, ed in alcuni casi anche agli interessati, la violazione di dati personali (**data breach**) entro settantadue ore dal momento in cui ne viene a conoscenza.

Già in precedenza sussisteva l'obbligo di notifica delle violazioni di dati personali, per particolari categorie di titolari o per particolari categorie di trattamenti, ma la novità del GDPR è l'estensione dell'obbligo a tutti i titolari.

Il legislatore europeo richiede, quindi, che tutte le realtà toccate dal Regolamento siano in grado di rispettare i requisiti di trasparenza, evidenza e responsabilità. A tal proposito, si ricorda che ***l'art.24 punto 1 del GDPR*** richiede al titolare di "mettere in atto misure tecniche e organizzative adeguate a garantire ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR".

Il processo descritto nel documento vale per i **dati di cui CUP è Titolare**.

Rispetto ai dati trattati in qualità di Responsabile del Trattamento CUP 2000 - a fronte di un evento, rilevato direttamente e qualificabile quale violazione di dati personali ai sensi dell'art. 33 del GDPR - procederà tempestivamente ad informare il Titolare.

CUP 2000 fornirà in tutti i casi il necessario supporto tecnico nell'ambito delle istruzioni impartite dal Titolare.

1.2. Notifica/Comunicazione

L'obbligo di **notifica** all'Autorità di Controllo scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche; qualora il rischio sia elevato, oltre alla notifica, il titolare è tenuto a darne **comunicazione** anche all'interessato. Il termine per adempiere alla notifica è brevissimo, settantadue ore dal momento in cui il titolare ne viene a conoscenza, mentre l'eventuale comunicazione agli interessati deve essere fatta senza indugio.

L'eventuale **ritardo** nella notificazione deve essere giustificato; il **mancato** rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti ***dall'art. 58 GDPR*** (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati) e la imposizione di sanzioni amministrative secondo ***l'art. 83 GDPR***, il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Occorre in ogni caso tenere conto del fatto che la mancata **notifica** e/o **comunicazione**, può rappresentare per l'autorità di controllo un indizio di carenze più profonde e strutturali, quali ad esempio, carenze od inadeguatezza di misure di sicurezza; in tal caso, trattandosi di ipotesi separate ed autonome, l'autorità procederà per l'ulteriore irrogazione di sanzioni.

Il rispetto degli obblighi di notifica (***art. 33***) e di comunicazione (***art. 34***), in realtà già mediamente complesse (in termini di dimensioni ed articolazione dell'organizzazione del titolare e/o in termini di numero di interessati di cui sono trattati i dati personali e/o in termini di operazioni di trattamento, o di quantità, varietà, natura dei dati trattati), richiede al Titolare di strutturare il trattamento dei dati personali avvalendosi di un sistema di conformità e gestione del rischio che preveda **una procedura per la gestione degli incidenti e la continuità operativa.**

1.3. Violazione di dati

Per **"Violazione di dati"** si intende 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 GDPR***).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

Si possono distinguere tre tipi di violazioni:

- Violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.
- Violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
- Violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

In particolari circostanze le violazioni potrebbero essere combinate tra loro.

1.4. Identificazione dell'incidente di sicurezza

Il **considerando 85** offre utili elementi per determinare i rischi che possono determinare l'obbligo di notifica. In particolare, occorre valutare la possibilità che la violazione possa causare danni fisici, materiali o immateriali alle persone fisiche. La disposizione a titolo d'esempio elenca:

- perdita del controllo dei dati personali che li riguardano;
- limitazione dei loro diritti; discriminazione;
- furto o usurpazione di identità;
- perdite finanziarie;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale;
- o qualsiasi altro danno economico o sociale significativo per la persona interessata.

L'art. **33 p.5 del GDPR**, prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma. Ne discende che le generali attività di rilevazione dell'incidente, come le successive di trattamento, devono essere:

- documentate;
- adeguate (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi);
- tracciabili;
- replicabili.

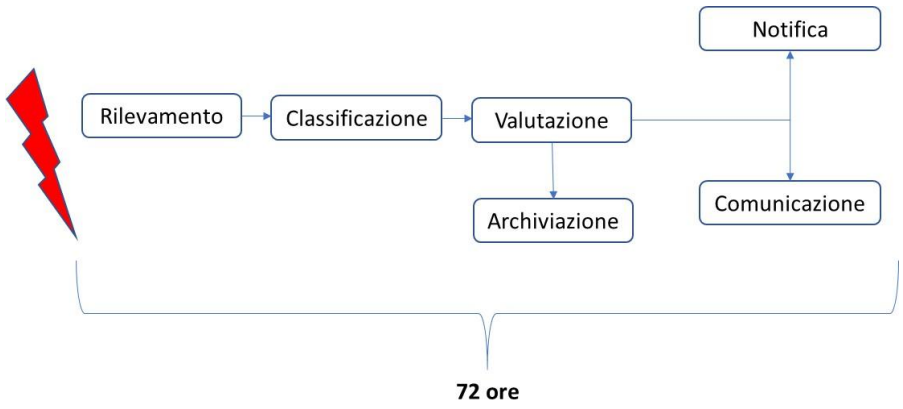
Di quanto sopra il titolare deve essere in grado di fornire evidenza nelle sedi competenti.

È importante, altresì, che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica; peraltro è rilevante considerare che scoprire l'incidente non è sufficiente, il titolare deve essere in grado di valutare la portata di questo in termini di impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati.

La rapida identificazione dell'incidente e la tempestività della adozione di contromisure possono consentire di limitare i danni derivanti da una violazione a carico degli interessati.

Nella definizione del processo di gestione del "data breach" diventa importante tenere conto di situazioni in cui il Titolare abbia affidato servizi a **Responsabili del trattamento**; preliminarmente, deve essere accertata la capacità del fornitore nel gestire tempestivamente e adeguatamente un incidente di sicurezza (art. 28 p.1 GDPR) e, quindi, è necessario prevedere idonee clausole contrattuali (art. 28 p.3 GDPR) che regolino il rapporto di fornitura in modo da garantire il rispetto del GDPR.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.



L'art. 34 del GDPR stabilisce che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve comunicare la violazione all'interessato senza ingiustificato ritardo. Il **considerando 86** del GDPR chiarisce che l'obbligo di comunicazione risponde allo scopo di consentire all'interessato, qualora sussista una violazione che presenta rischi elevati, di prendere le precauzioni necessarie.

La Notifica e la Comunicazione hanno un contenuto pressoché identico.

Notifica - Art. 33 p.3 GDPR

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 e/o i dati dell'Ufficio Affari Legali.
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 per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Comunicazione - Art. 34 p.2 GDPR

a) Descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali.
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 per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

La comunicazione dovrebbe essere data direttamente e personalmente agli interessati coinvolti dalla violazione, a meno che ciò comporti sforzi sproporzionati. In tal caso, si procede invece ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con la medesima efficacia.

1.5. Valutazione del livello di criticità della Violazione

Il considerando 76 del GDPR chiarisce che 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.

Il WP29 suggerisce ulteriori criteri per permettere una valutazione più accurata.

- Tipo di violazione;
- Natura, sensibilità e volume dei dati personali;
- Facilità di riconoscimento degli interessati;
- Serietà delle conseguenze per le persone fisiche;
- Caratteristiche specifiche delle persone fisiche;
- Quantità di persone fisiche coinvolte;
- Caratteristiche specifiche del titolare.

La valutazione dei rischi non sempre è semplice; a tal proposito il WP29 raccomanda al titolare, in caso di dubbio, di scegliere la strada di maggior tutela procedendo alla notifica.

1.6. Procedura di identificazione e gestione degli incidenti

La tempestività nella notifica può essere assicurata se preesiste un sistema di comunicazione interno adeguato e tutti coloro che operano per il titolare abbiano ricevuto adeguata formazione.

La stessa comunicazione può essere fatta solo se sono disponibili le informazioni necessarie, aspetto possibile solo se precedentemente è stato strutturato un sistema di report dell'incidente, è stata fatta una ricognizione adeguata dell'organizzazione del titolare, sono state condotte le Valutazioni di impatto sui dati personali (DPIA).

Infine, è possibile mostrare la stessa documentazione delle violazioni, che la norma prescrive di conservare, (anche per quelle che non determinano obbligo di notifica), solo se è stato strutturato un sistema di gestione degli incidenti.

2. Processo di gestione degli incidenti di sicurezza

Di seguito si riporta una proposta di flusso di processo relativo alla gestione degli incidenti nonché la procedura di gestione dei data breaches prevista dal Regolamento Privacy.

2.1. Premessa

Il trattamento degli incidenti di sicurezza presuppone, a monte, l'esistenza di un sistema di sicurezza delle informazioni che offra tutti gli strumenti necessari.

- La scoperta dell'incidente presuppone un sistema di monitoraggio che, a sua volta, presuppone l'organizzazione della sicurezza all'interno della società (definizione degli obiettivi, politiche, compiti e responsabilità, classificazione di dati e processi, individuazione e definizione dei rischi, individuazione dei rimedi).
- La valutazione dell'incidente presuppone la definizione dei criteri di valutazione, la formazione del personale incaricato, la predisposizione di procedure.
- La tempestività nella notifica può essere assicurata se preesiste un sistema di comunicazione interno adeguato e tutti coloro che operano per il titolare abbiano ricevuto adeguata formazione.
- La stessa comunicazione può essere fatta solo se sono disponibili le informazioni necessarie, aspetto possibile solo se precedentemente è stato strutturato un sistema di report dell'incidente, è stata fatta una ricognizione adeguata dell'organizzazione del titolare, sono state condotte le Valutazioni di impatto sui dati personali (DPIA).
- Infine, è possibile mostrare la stessa documentazione delle violazioni, che la norma prescrive di conservare, (anche per quelle che non determinano obbligo di notifica), solo se è stato strutturato un sistema di gestione degli incidenti.

Una corretta gestione delle problematiche di Data breach deve anche basarsi su una serie di presupposti organizzativi. In particolare:

- Tutti gli attori coinvolti devono essere allineati su cosa sia un incidente di sicurezza.
- Tutti gli attori devono essere allineati sulla classificazione e la casistica relativa agli incidenti di sicurezza.
- Tutti gli attori devono essere allineati sul fatto che gli incidenti di sicurezza devono essere gestiti da un team con apposite competenze e che tale funzione opera sotto la responsabilità del Responsabile Ufficio Affari Legali con il controllo della Divisione Data Center e Cloud.
- In qualunque punto del processo, laddove non ci sia risposta sollecita da parte di utenti e funzioni interne o del Responsabile del trattamento, sarà compito del Responsabile Ufficio Affari Legali attivare le necessarie escalation sul Titolare del Trattamento, identificato nel Legale Rappresentante della Società, con il coinvolgimento del DPO.

2.2. Fasi della procedura

Nel seguito è riportata una sintetica descrizione del processo suddiviso in fasi come indicato nello schema che segue.

- *Rilevamento e Segnalazione*
- *Analisi e Classificazione*
- *Trattamento incidente*
- *Chiusura incidente*
- *Follow up e Reporting*

Rilevamento e Segnalazione

La fase di rilevazione del processo di gestione degli incidenti ha la principale finalità di intercettare ed identificare tutti i possibili eventi che possano essere correlati ad un potenziale incidente.

La rilevazione e segnalazione può essere riconducibile, in particolare, a due principali fonti:

- **Rilevazione Interna proveniente da personale della società (utenti owner del trattamento o personale IT)** - Il personale della società può identificare:
  - eventi di sicurezza sui sistemi o componenti di sistema gestiti internamente;
  - eventi di sicurezza relativi ai sistemi eventualmente gestiti da Responsabili del trattamento;
  - possibili eventi di sicurezza per altri servizi gestiti da altri fornitori.
- **Rilevazione Esterna** – Eventuali fornitori esterni, a prescindere che siano stati o meno nominati, l'interessato, Responsabili del trattamento che identificano eventi di sicurezza mediante rilevazione e "segnalazione" automatica con informazioni che provengono da sistemi di monitoraggio o mediante "notifica" attraverso sistema di ticketing.

Le segnalazioni possono essere generate automaticamente dai sistemi mediante *alert* o manualmente.

Segnalazione automatica

L'attività di identificazione proattiva degli eventi di sicurezza rientra nell'attività di monitoraggio continuo che una società o un fornitore esterno di servizi realizza sulla propria infrastruttura attraverso apposite piattaforme tecniche di monitoraggio degli eventi.

Ricevuto l'allarme dalle proprie piattaforme di monitoraggio, qualora ritenuto che l'evento possa generare un *evento di sicurezza*, la società attraverso la sua funzione preposta alla gestione degli incidenti, analizza l'allarme e ricerca e raccoglie eventuali altri eventi che in qualche modo potrebbero essere collegati o riconducibili all'evento di sicurezza segnalato.

Qualora la segnalazione sia riconducibile a un *evento di sicurezza*, tale funzione aprirà il ticket su un apposito sistema. Una volta inseriti in tale coda, i ticket acquisiranno di conseguenza la tipologia di "Incidente".

Segnalazione manuale

Segnalazioni di eventi di sicurezza possono sorgere all'interno della società, anche da parte di funzioni interne o di partner/fornitori esterni con i quali la stessa collabora.

Tali segnalazioni, una volta analizzate e filtrate dalla struttura IT che le ha ricevute - ove si ritenga che l'evento possa generare un incidente - sono oggetto di specifica verifica per controllare se già esista una

segnalazione aperta riconducibile all'evento segnalato e ricercare/raccogliere eventuali altri eventi collegati o riconducibili all'evento di sicurezza segnalato.
Qualora la segnalazione sia riconducibile a un *evento di sicurezza*, tale funzione aprirà il ticket su apposito sistema.

Processo

Tutte le segnalazioni che pervengono sia da fonti interne alla società sia da eventuali fornitori esterni di cui la società si avvale, vengono raccolte ed analizzate preliminarmente dall'Ufficio Affari Legali supportato dalla Divisione Data Center e Cloud al fine di effettuare una prima analisi e filtrare quelle ritenute non significative.
Le informazioni necessarie alla valutazione dell'incidente devono comprendere:

- gli asset impattati sia in numero che in tipologia;
- la criticità, la classificazione del processo di gestione del rischio, degli asset coinvolti;
- i processi, i servizi e i soggetti impattati dall'evento;
- eventuali danni prodotti dall'evento (es. malfunzionamenti, blocchi o degradi di servizi, corruzione di dati, fughe di informazioni, etc);
- in caso di attacco da Internet, sorgenti (es. indirizzi IP), estensione e modalità di attacco;
- altre segnalazioni/allarmi correlati all'evento in esame;
- modalità di propagazione/evoluzione dell'evento;
- altre informazioni ritenute utili.

Tutte le informazioni suddette hanno la finalità di consentire la classificazione dell'evento e di attivare tutte le misure di contrasto e contenimento necessarie.

Qualora la segnalazione sia riconducibile a un evento di sicurezza, la Divisione Data Center e Cloud aprirà un ticket sulla specifica coda "Incidenti" dell'apposito sistema.
Nel caso di "*evento di sicurezza*", saranno coinvolte le funzioni costituenti il Team Privacy (Ufficio Affari Legali, la Divisione Data Center e Cloud, il DPO, il Direttore Generale) per la successiva classificazione di dettaglio. In tal caso tutte le funzioni delegate e i loro collaboratori, essendo informati della segnalazione dell'evento di sicurezza, potranno già intraprendere le azioni opportune per la gestione e la risoluzione dell'incidente.

Analisi e Classificazione

L'analisi e la classificazione di dettaglio degli eventi di sicurezza ad opera del personale della Divisione Data Center e Cloud ha la principale finalità di avviare le necessarie attività volte a raccogliere le informazioni indispensabili per la corretta classificazione dell'evento di sicurezza. L'attività di classificazione tipizza l'evento in "falso positivo" o in caso di "incidente" effettivo lo categorizza in modo più granulare, sulla base della gravità (in incidente operativo, incidente di sicurezza informatica, incidente grave, crisi) guidando così le attività necessarie per il suo trattamento.

In caso di incidente di sicurezza che preveda un impatto Privacy, il Team Privacy segnala tempestivamente (telefonicamente e/o via sms) l'incidente al Direttore Generale e al DPO.
Sulla base delle informazioni fornite riguardanti l'entità dell'incidente sarà cura del Titolare del Trattamento col supporto del DPO provvedere alla valutazione d'impatto dell'incidente sul proprio

contesto operativo e prendere una decisione in merito alla necessità di procedere alla “Notifica” e alla “Comunicazione”.

Trattamento

La fase di trattamento del processo di gestione degli incidenti ha la principale finalità di attivare tutte le azioni necessarie a gestire l’evento segnalato.

Una volta ricevuta la segnalazione dell’evento, la fase di trattamento consiste nella presa in carico dell’incidente e nell’attuazione di tutte le misure di contenimento e riduzione degli impatti da porre in essere.

Nel caso di incidente di sicurezza dovrà essere mantenuto un opportuno aggiornamento mediante canali tempestivi (telefonicamente e/o via sms) tra le Funzioni del Team Privacy e il Titolare del Trattamento e il DPO ai fini di consentire agli stessi visibilità costante sullo stato di avanzamento della gestione e risoluzione dell’incidente e di rispettare le tempistiche stringenti previste dal Regolamento.

Il Direttore Generale procederà, nel rispetto dei tempi richiesti, ad attivare la notifica all'autorità di controllo competente con il supporto del DPO.

Analoga azione dovrà essere fatta, sempre a cura del Direttore Generale, nel caso in cui si evidenzi la necessità di comunicazione dell’incidente al / ai soggetti interessati.

Chiusura incidente

Nel momento in cui l’evento viene risolto, la Divisione Data Center e Cloud effettua la verifica di quanto risolto e procede all’aggiornamento del sistema di gestione degli incidenti.

Il sistema di gestione degli incidenti di sicurezza Privacy dovrà contenere tutte le informazioni raccolte anche per quelle segnalazioni che non hanno determinato un obbligo di notifica o di comunicazione

Follow up e Reporting

La fase di Follow-up & Reporting ha la finalità di analizzare le cause che hanno determinato il verificarsi dell’incidente e di identificare gli interventi necessari affinché lo stesso non si ripeta.

Il Team Privacy in accordo con la Divisione Data Center e Cloud, a tal fine predispone e protocolla la relazione tecnica di chiusura dell’intervento da inviare al Direttore Generale indicando le cause che hanno determinato l’evento/incidente, gli interventi e le eventuali contromisure adottate, nonché tutte le informazioni raccolte in fase di classificazione e analisi e, per quanto riguarda gli incidenti, le azioni di contrasto, contenimento e ripristino adottate, le vulnerabilità/minacce riscontrate, con indicazione della relativa gravità.

Gli eventi qualificati come 'data breach' ai sensi dell'art. 33 vengono tracciati mediante annotazione su apposito Registro (allegato alla presente procedura) recante le seguenti voci:

- data e tipo di evento;
- numero di risorse informatiche coinvolte;
- numero di utenti/postazioni di lavoro potenzialmente impattati dalla indisponibilità del servizio informatico;
- risorse ICT /utenti esterni coinvolti;
- tipo di danno arrecato;
- enti/organizzazioni coinvolti nell'incidente;
- modalità di gestione dell'incidente.

L'Amministratore Unico
Dott. Alessandro Saccani
(sottoscritto con firma digitale)