CENTRO FORMATIVO PROVINCIALE
GIUSEPPE ZANARDELLI
Azienda Speciale della Provincia di Brescia

PROCEDURA DI DATA BREACH

Procedura da adottare in caso di violazione dei dati personali

Art. 4, 33, 34 del Regolamento UE 679/2016

Versione aggiornata al 5 Giugno 2019

SCOPO

La presente procedura regolamenta la gestione degli eventi di Data Breach o quelli che vengono, in prima battuta valutati come tali. Si considerano eventi di Data Breach quelli che comportano, in modo accidentale o illecito, la distruzione, la perdita, la modifica, la divulgazione non consentita o l'accesso non autorizzato ai dati personali trattati da Cfp Zanardelli. Tali eventi comportano rischi per i diritti e le libertà degli interessati. I principali rischi sono:

- *danni fisici, materiali o immateriali a persone fisiche*
- *perdita del controllo dei dati degli interessati*
- *limitazioni dei diritti/discriminazione*
- *furto o usurpazione di identità*
- *perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari)*

DEFINIZIONI

- **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.
- **Trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
- **Titolare del Trattamento**: 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.
- **Responsabile del Trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio, altro organismo che tratta dati personali per conto del titolare del trattamento.
- **Violazione del dato**: 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).

1. GENERALE

1.1 Team crisi

La presente procedura è condivisa con i membri del Team crisi all'atto della loro nomina. Il tema crisi di Cfp Zanardelli è composto da:

- DPO - Responsabile del team
- Titolare del trattamento

- Responsabile del Sistema informativo
- Ufficio marketing e comunicazione
- Affari Legali
- Specifica responsabilità qualità
- Nel caso in cui l'evento coinvolga le risorse umane si include anche la Specifica Responsabilità risorse umane

Fanno parte del Team anche altre funzioni, di volta in volta coinvolte in base all'evento (es. responsabile esterno o subresponsabile o Contitolare).

Il Team crisi o altri soggetti dallo stesso delegati, sono i soli autorizzati a trattare con il Garante e con gli interessati (vedi paragrafo "Comunicazione").
Il Team si occuperà di analizzare la gravità dell'evento prendendo in considerazione i dati, gli interessati coinvolti, la portata e l'arco temporale secondo precisi parametri individuati da Cfp Zanardelli.
A seguito di tale analisi l'Azienda realizzerà un'approfondita valutazione del rischio al fine di comprendere l'effettiva sussistenza della violazione.
In caso di esito positivo il Team procederà alla risoluzione del problema.
In caso di violazione dei dati potrebbe essere necessario dover comunicare al Garante Privacy l'evento entro 72 ore dal fatto.
Qualora la violazione dei dati abbia cagionato un rischio elevato dei diritti e libertà fondamentali, verrà fornita opportuna comunicazione al fine di consentire l'adozione di idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione.
Nella comunicazione verranno forniti:

- 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 dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Non vi è obbligo di comunicazione nel caso in cui siano state messe in atto adeguate misure tecniche ed organizzative di protezione dei dati oggetto della violazione o quando, successivamente, siano state adottate misure atte a scongiurare nuovi rischi elevati per i diritti oppure quando la comunicazione richiederebbe sforzi sproporzionati. In questo caso, si procederà con una comunicazione pubblica o misura simile. Verrà comunque valutata l'opportunità di effettuare la comunicazione di volta in volta.

1.1.1. Formazione del Team crisi

Almeno annualmente il Team crisi effettua una formazione mirata sull'applicazione della presente procedura; tale formazione è effettuata anche nel caso di introduzione di un nuovo membro nel Team. Nel corso della formazione, si valuta anche la necessità/opportunità di modificare e/o integrare la procedura nel caso di eventi verificatisi nel corso dell'anno. La formazione e la verifica dell'adeguatezza della procedura devono essere verbalizzate. Il documento viene archiviato nell'archivio "privacy" di Cfp Zanardelli.

1.1.2 Nomina di responsabili esterni, Subresponsabili, Contitolari

Nei contratti con i responsabili esterni, nei rapporti con i contitolari e nelle autorizzazioni per i sub responsabili deve essere indicato:

- la richiesta di valutazione della loro procedura di Data Breach
- la specificazione dei tempi di comunicazione a Cfp Zanardelli che deve tener conto delle 72 ore a capo del Titolare per la segnalazione (es. 24 ore dalla rilevazione per i contitolari e responsabili e 12 ore per i subresponsabili)
- le conseguenze nel caso di mancata o ritardata comunicazione
- la figura di riferimento per la comunicazione (DPO – Privacy Officer) ed i riferimenti per contattala

1.1.3 Verbalizzazione delle attività

Tutte le attività e le riunioni del Team crisi devono essere verbalizzate; i verbali sono conservati, anche in modo elettronico, dal Responsabile del Team, nell'archivio "privacy" di Cfp Zanardelli e conservati per almeno 10 anni (o in relazione agli effetti che il Data Breach può avere sui diritti degli interessati). In ogni verbale (sottoscritto dai partecipanti alla riunione) deve essere indicato:

- chi partecipa (membro del Team/invitato all'incontro)
- decisioni assunte nel corso dell'incontro
- stato di avanzamento delle decisioni assunte nel corso di incontri precedenti

1.1.4 Disponibilità e posizione del Titolare del Trattamento

Il Titolare del trattamento è parte del Team e quindi informato degli sviluppi e delle decisioni, in ogni fase dell'indagine; ha potere di imporre misure più restrittive a tutela dei diritti degli interessati. Qualora il Titolare non fosse disponibile a fornire il contributo richiesto, il DPO ha l'autorità per procedere autonomamente nelle decisioni prese.

Qualora non condividesse la decisione presa dal Team e la valutasse eccessiva e che possa impattare negativamente sulla reputazione/immagine dell'azienda o ledere gli interessi economici della stessa, si assume la responsabilità di imporre la sua decisione. In questo caso il Team crisi verbalizzerà la decisione del Titolare nel MODULO Gestione del Data Breach Sezione S9 e la posizione del resto del Team. La documentazione verrà archiviata senza procedere ulteriormente, tramite comunicazioni con data certa (es. tramite PEC) al Titolare.

In ogni caso, il DPO è autonomo nel valutare, se in contrasto con il Titolare del Trattamento, di comunicare l'evento occorso direttamente al Garante nelle forme e modi che ritiene opportuni.

1.1.5 Ruolo di eventuali esperti esterni

Per le azioni previste dalla procedura possono essere coinvolti eventuali esperti esterni che verranno incaricati previa sottoscrizione di un vincolo di riservatezza.

1.2 Data Breach Policy

Nel sito di Cfp Zanardelli è pubblicata la presente procedura di Data Breach la cui finalità è quella di comunicare all'esterno la presenza di una modalità per la gestione delle segnalazioni che possono portare a situazioni di anomalia/sospetto o Data Breach.
Per effettuare le segnalazioni il contatto da utilizzare è **databreach@cfpzanardelli.it**.
Tale mail è reindirizzata nella casella di posta elettronica del DPO ed in quella del Responsabile Qualità.
La violazione dei dati personali può consistere nella distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale od illegale, a dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, causare danni alla persona fisica.
Ai sensi del Regolamento europeo, infatti, i principali rischi per i diritti e le libertà di tutti gli interessati, a seguito dell'avvenuta violazione dei dati, sono:

- *danni fisici, materiali o immateriali a persone fisiche*
- *perdita del controllo dei dati degli interessati*
- *limitazioni dei diritti/discriminazione*
- *furto o usurpazione di identità*
- *perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari)*

Le cause che possono portare a tale situazioni possono essere:

- *errore umano volontario o involontario*
- *circostanze impreviste come incendio, alluvione, terremoto, ecc.*
- *attacco hacker*
- *mancato funzionamento delle misure di mitigazione previste*

- *reati "blagging" in cui le informazioni sono ottenute ingannando l'organizzazione che lo detiene*

1.3 Individuazione dell'Autorità Garante competente

L'autorità competente per ogni comunicazione derivante dall'applicazione della policy data breach è il garante della protezione dei dati personali dello stato italiano.

1.4 Tempistica

Il calcolo della tempistica (considerando che il GDPR fornisce 72 ore al Titolare per la eventuale notifica al Garante e la comunicazione all'interessato) decorre dal ricevimento della segnalazione.

1.5 Rendicontazione delle attività del Team Crisi

Almeno annualmente il DPO predispone una relazione sulla attività del Team Crisi nel corso dell'anno. Tale relazione viene trasmessa al Legale rappresentante di Cfp Zanardelli.
La relazione, per quanto possibile è integrata da dati numerici per comprendere l'entità degli eventi ed i tempi di reazione.

2. GESTIONE EVENTO DI DATA BREACH

Alla gestione di evento di Data Breach è richiesta la massima attenzione e sensibilità da parte di tutte le funzioni coinvolte.

2.1 Segnalazione

La segnalazione di un evento può provenire:

- Interno – ogni autorizzato al trattamento deve, nel caso abbia anche il sospetto di una violazione di dati (compiuta dall'interno o dall'esterno), o sia a conoscenza di una comunicazione da parte di un interessato/terzo (anche esterno), effettuare la segnalazione **nel minor tempo possibile**, tramite l'indirizzo **databreach@cfpzanardelli.it** o con qualsiasi altra forma, ad uno dei membri del Team di crisi in modo da attivare la procedura di valutazione dell'evento.
- Esterno (interessato/Garante/stampa/soggetti terzi)
    - il DPO raccoglie le segnalazioni di possibile Data Breach provenienti dall'esterno in qualsiasi forma
    - il DPO consulta regolarmente il sito del Garante e gli organi di stampa specializzata per verificare eventuali situazioni di potenziale rischio che potrebbero riguardare anche Cfp Zanardelli
    - il DPO verifica l'autenticità della comunicazione ricevuta analizzando: fonte nota/registrata, informazione tramite canali regolari, messaggio con intestazione completa. Per altre indicazioni richiamarsi al doc. ENISA
- Responsabile esterno trattamento/sub responsabile/contitolare - il DPO riceve le segnalazioni di possibili Data Breach provenienti da figure esterne con le quali è in essere un contratto di responsabile esterno/sub responsabile/contitolare; attraverso i canali definiti in tali contratti.

  In tutti i casi il DPO comunica via mail con gli altri membri del Team crisi utilizzando la loro casella di posta e quella di databreach@cfpzanardelli.it (al fine di lasciare una traccia).
  Tutte le comunicazioni che provengono da fonte interna o da Responsabili esterni devono essere identificate con data e ora.
  Nel caso il DPO non fosse presente in azienda, la specifica responsabilità qualità, informa lo stesso DPO entro 12 ore dalla comunicazione.

2.1.1 ID segnalazione

Ad ogni segnalazione è assegnato un numero (ID) formato dal numero progressivo/anno. Questo numero permetterà di identificare in modo univoco tutta la documentazione che riguarda l'incidente e, per quanto possibile, deve essere sempre indicato.

Appena ricevuta la segnalazione deve essere aggiornato, da parte del DPO, il registro degli incidenti.

2.2 Valutazione di pertinenza della segnalazione

Raccolta la segnalazione, attraverso le forme sopra indicate, il responsabile del Team crisi convoca entro massimo 12 ore dalla segnalazione[1], una riunione coinvolgendo tutti i membri ed eventuali altri soggetti potenzialmente coinvolti sulla base delle informazioni disponibili. Qualora qualche membro non fosse disponibile, si procederà comunque con la riunione.

Il team compila il MODULO Gestione del Data Breach nella sezione S1. Se necessario, il Team procede alla raccolta di eventuali ulteriori informazioni (es. tramite organi di stampa, richieste di approfondimento) al fine di chiarire la veridicità, la portata e la reale sussistenza dell'evento segnalato.

Il Team crisi valuta prioritariamente eventuali azioni per contenere gli effetti dell'evento; attivando le risorse necessarie e documentando tali azioni nel MODULO Gestione del Data Breach nella sezione S2.

Qualora si verificasse, anche dopo eventuali approfondimenti, l'insussistenza di situazioni che mettono a rischio i dati degli interessati, il Team compila il MODULO Gestione del Data Breach nella sezione S6. Il Team comunica la decisione al Titolare, qualora quest'ultimo non fosse presente alla riunione del team e valuta la necessità di procedere ad una eventuale azione correttiva, come indicato nella sezione S8 del MODULO Gestione del Data Breach. Infine, aggiorna il Registro degli incidenti.

Negli altri casi il Team procede a:

- informare il Titolare del trattamento, nel caso non fosse presente alla riunione.
- valutare le conseguenze dell'evento [dati personali colpiti, portata (n. e/o % interessati e n. dati), arco temporale, dati/interessati coinvolti].

Sulla base degli elementi raccolti, valuta la presenza o meno della violazione o presunta tale, tenendo presente che, in caso di dubbio, si deve assumere un atteggiamento prudenziale a difesa dei diritti dell'interessato, e la documenta nel MODULO Gestione del Data Breach nella sezione S2.

In caso di esito positivo procede con la analisi del rischio. In caso negativo procede con la compilazione del MODULO Gestione del Data Breach nella sezione S6.

L'esito della valutazione di pertinenza della segnalazione deve essere riportato, a cura del DPO, nel REGISTRO degli incidenti. Se la segnalazione non risulta pertinente il DPO traccerà una riga per annullare la compilazione degli altri campi previsti dal REGISTRO.

2.3 Analisi del rischio

Il Team crisi procede all'analisi del rischio ed alla sua documentazione compilando il MODULO Gestione del Data Breach nella sezione S3. Nella compilazione del modulo deve tenere conto del significato associato a:

- Riservatezza: stima del danno/impatto che la perdita di riservatezza riguardante l'asset comporterebbe per il business di Cfp Zanardelli/tutela interessato (1-4)
- Integrità: stima del danno/impatto che la perdita di integrità riguardante l'asset comporterebbe per il business di Cfp Zanardelli/tutela interessato (1-4)

[1] Considerare che, nel caso di comunicazione da parte del subresponsabie (situazione più critica) l'azione si avvia entro 36 ore dalla sua rilevazione

- Disponibilità: stima del danno/impatto che la perdita di disponibilità riguardante l'asset comporterebbe per il business di Cfp Zanardelli/tutela interessato (1-4)

Per la valutazione della stima della perdita di Riservatezza, Integrità e Disponibilità viene utilizzata la seguente tabella (fonte www.cesaregallotti.it).

Liv[2].	R- Riservatezza	I - Integrità	D- Disponibilità
1 - Basso	**Organizzazione** I dati non presentano particolari requisiti di riservatezza. I dati sono pubblici. **Interessati** La mancanza di riservatezza ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie. **Interessati** La mancanza di integrità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti. **Interessati** La mancanza di disponibilità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.
2 - Medio	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti. **Interessati** La mancanza di disponibilità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.

[2] Fonte www.cesaregallotti.it

3 - Alto	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine) e un'eventuale loro diffusione ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti. **Interessati** La mancanza di **disponibilità** ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.
4 - Critico	**Organizzazione** La diffusione delle informazioni ha elevati impatti sul business dell'organizzazione o sul rispetto della normativa vigente o sull'immagine dell'organizzazione tali da compromettere la sostenibilità dell'organizzazione. **Interessati** La mancanza di riservatezza ha impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** La mancanza di integrità delle informazioni ha elevati impatti sul business aziendale o sul rispetto della normativa vigente tali da compromettere la sostenibilità dell'organizzazione. **Interessati** La mancanza di integrità ha impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali che mettono in pericolo la sostenibilità economica e di immagine o hanno impatti sulla sicurezza delle persone fisiche. **Interessati** La mancanza di disponibilità ha impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.

2.4 Esito della analisi del rischio e decisioni

Le valutazioni associate agli eventi di Data Breach possono variare in base al contesto in cui si trova l'organizzazione.

Il risultato del calcolo del rischio deve essere interpretato come segue, considerando che, in base ai criteri assegnati, il valore minimo è 3 ed il massimo è 27:

A. Valore Data Breach - da 1 - 3 = nessun rischio – MISURE: non fare NOTIFICA e COMUNICAZIONE. Valutare eventuale AC - vedi S8 nel MODULO Gestione del Data Breach.
B. Valore Data Breach - da 3 a 8 = rischio - MISURE: non fare NOTIFICA e COMUNICAZIONE all'interessato. Effettuare il trattamento dell'evento - vedi S7 ed eventuale AC vedi S8 del MODULO Gestione del Data Breach.
C. Valore Data Breach - da 9 a 15 = rischio - MISURE: fare NOTIFICA, non fare la COMUNICAZIONE all'interessato. Effettuare il trattamento dell'evento - vedi S7 ed eventuale AC vedi S8 del MODULO Gestione del Data Breach.
D. Valore Data Breach – oltre 15 = rischio - MISURE: fare NOTIFICA, fare la COMUNICAZIONE all'interessato. Effettuare il trattamento dell'evento - vedi S7 ed eventuale AC vedi S8 del MODULO Gestione del Data Breach.

Nel caso in cui il valore anche di uno solo tra **riservatezza, integrità** e **disponibilità** sia uguale o superiore a 3, il Team crisi deve valutare se le misure corrispondenti siano adeguate.

I risultati dell'esito dell'analisi del rischio vanno riportati nel MODULO Gestione del Data Breach nella sezione S3 massimo entro 4 ore[3], dall'inizio della riunione del Team crisi. Dell'esito della decisione si informa il Titolare del trattamento (vedi parte Generale).

L'esito della casistica in cui cade la segnalazione deve essere riportato, a cura del DPO, nel REGISTRO degli incidenti.

2.5 Azioni a seguito delle decisioni

Sulla base della casistica in cui si ricade, devono essere svolte le seguenti azioni:

- Caso A – si aggiorna il MODULO Gestione del Data Breach Sezione 3; l'evento si chiude; non vengono effettuate ulteriori comunicazioni.
- Caso B - si aggiorna il MODULO Gestione del Data Breach Sezione 3; si procede con le eventuali AC; si comunica internamente con il Responsabile dell'area interessata dall'evento; l'adozione di trattamento dell'evento (vedi paragrafo dedicato).
- Caso C - si aggiorna il MODULO Gestione del Data Breach Sezione 3 ed il REGISTRO degli incidenti; si procede con l'adozione del trattamento dell'evento (vedi paragrafo dedicato), con le AC; si comunica internamente con il Responsabile dell'area interessata dall'evento; si NOTIFICA all'autorità di controllo (vedi paragrafo dedicato). Il Responsabile Marketing e Comunicazione prepara un comunicato stampa (vedi paragrafo dedicato) che verifica con DPO e Titolare del trattamento. Quest'ultimo ne darà comunicazione al Consiglio di amministrazione.
- caso D – implica, oltre a quanto previsto dal caso C, anche la COMUNICAZIONE obbligatoria agli interessati coinvolti preparata a cura del Responsabile Marketing e Comunicazione: secondo il Modello (vedi paragrafo dedicato) e verificata da DPO e Titolare del trattamento. Quest'ultimo ne darà comunicazione al Consiglio di amministrazione.

Per i casi C e D, le comunicazioni (NOTIFICA e COMUNICAZIONE obbligatorie agli interessati) devono avvenire massimo entro 8 ore[4] dalla decisione presa.

Per le comunicazioni agli interessati ed al Garante vedi specifiche sezioni.

Da considerare che il trattamento dell'evento senza l'avvio della AC deve essere una situazione eccezionale: di norma contenere semplicemente la violazione e continuare con lo *status quo*, non è accettabile.

[3] Considerare che, nel caso di comunicazione da parte del sub responsabile o contitolare (situazione più critica), l'azione si conclude entro 52 ore dalla sua rilevazione

[4] Considerare che, nel caso di comunicazione da parte del subresponsabie (situazione più critica), l'azione si conclude entro 60 ore dalla sua rilevazione

2.6 Indicizzazione sui motori di ricerca

Nel caso in cui il Data Breach abbia riguardato la pubblicazione di dati in rete (ad esempio per errore sono state messe on line delle pagine), deve essere verificato, sui principali motori di ricerca che le pagine contenenti tali dati non siano stati indicizzati e, nel caso in cui fosse avvenuto, richiedere, ai motori di ricerca la rimozione (diritto all'oblio). Tale indagine deve essere fatta sia appena a monte del Data Breach sia ripetuta a distanza di una settimana, due settimane ed un mese dall'evento.

2.7 Trattamento dell'evento

Quando è previsto un trattamento dell'evento, ovvero una o più azioni volte a minimizzare gli impatti per gli interessati e ripristinare la situazione precedente all'evento (laddove possibile), il Team crisi definisce: modalità, responsabilità e tempi. Il Team tiene sotto controllo lo stato di avanzamento delle azioni di trattamento previste e tiene aggiornato il MODULO Gestione del Data Breach Sezione 7 ed il REGISTRO degli incidenti (sezione data di completamento del trattamento).
Per il trattamento di eventi che riguardano la sicurezza dei sistemi informatici (v. anche documento ENISA)

2.8 Azione correttiva

Quando sono previste una o più azioni correttive volte a rimuovere la causa dell'evento, il Team crisi definisce: modalità, responsabilità e tempi. Il Team tiene sotto controllo lo stato di avanzamento delle azioni e l'efficacia delle stesse. Viene valutata la necessità di aggiornare l'analisi dei rischi ed eventualmente la PIA, se prevista per tale trattamento e la documentazione (es. procedure di riferimento nomina a responsabile esterno del trattamento). Il Team crisi tiene aggiornato il MODULO Gestione del Data Breach Sezione 8 ed il REGISTRO degli incidenti (sezione data di completamento della Azione correttiva).

2.9 Comunicazione al Garante ed agli interessati

Nei casi previsti, a seguito di un evento di Data Breach, deve essere effettuata la comunicazione al Garante ed agli interessati. La comunicazione è coordinata dal Team Crisi. Le evidenze di tutte le comunicazioni devono essere conservate.

2.9.1 Comunicazioni al Garante

La comunicazione al Garante deve contenere almeno i seguenti elementi:

- Riferimenti dell'Azienda, del Titolare e del DPO
- Indirizzo PEC e/o EMAIL per eventuali comunicazioni
- Recapito telefonico per eventuali comunicazioni
- Eventuali Contatti (altre informazioni)
- Natura della comunicazione
- Breve descrizione della violazione dei dati personali trattati
- Quando si è verificata la violazione dei dati personali trattati. Specificare l'arco temporale o se la violazione è ancora in corso.
- Luogo dove è avvenuta la violazione dei dati (es. se avvenuta a seguito di smarrimento di dispositivi o di supporti portatili).
- Tipo di violazione
    - Lettura (presumibilmente i dati non sono stati copiati)
    - Copia (i dati sono ancora presenti sui sistemi del titolare)
    - Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
    - Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
    - Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
    - Dispositivo oggetto della violazione ed eventuale ubicazione (es. Computer, Rete, Dispositivo mobile, Archivio/File o parte di un archivio/file, Strumento di *backup,* Documento cartaceo)
    - Altro

- Quanti interessati sono state colpiti dalla violazione dei dati personali? N. interessati ed incidenza % sull'universo della popolazione/Un numero (ancora) sconosciuto di interessati
- Che tipo di dati sono oggetto di violazione?
- Misure tecniche e organizzative applicate ai dati oggetto di violazione
- Eventuali azioni già intraprese per contenere la violazione
- Eventuali azioni già intraprese per ripristinare lo status quo (ove possibile)
- Eventuali azioni correttive
- La violazione è stata comunicata anche agli interessati?
- Data e mezzo di comunicazione
- Eventuale motivazione della non comunicazione.
- Analisi del rischio estrapolata dal MODULO Gestione del Data Breach e l'eventuale comunicazione inviata agli interessati

2.9.2 Comunicazione agli interessati

La comunicazione agli interessati può avvenire con modalità diverse tra cui:

- comunicazione diretta agli interessati (mailing list, posta elettronica, sms, newsallert)
- comunicato stampa
- comunicazione tramite sito WEB/social media

La comunicazione deve essere congruente con quanto indicato nella Data Breach Policy (vedi paragrafo dedicato).

All'interno del Cfp Zanardelli il Team di crisi ha la responsabilità di individuare la forma ed il contenuto della comunicazione da utilizzare.
Nel caso in cui il Legale Rappresentante non fosse presente alla riunione del team di crisi sarà necessario avere la sua approvazione della comunicazione.
Quindi il Team crisi decide la strategia di *crisis communication* da mettere in atto, da quando è a conoscenza dell'evento di Data Breach, fino alla sua risoluzione.
Di seguito le linee guida da considerare per la redazione delle comunicazioni verso gli interessati:

Aspetti generali:

- definire il tono della comunicazione che può essere più informale (comunicato) o più formale (dichiarazione ufficiale);
- fornire un titolo "giornalistico" che, per quanto possibile, rassicuri gli interessati o perlomeno riducano il livello di allarme, utilizzare parole chiave facilmente rintracciabili sui motori di ricerca, qualora venissero cercate informazioni;
- le comunicazioni potrebbero non riguardare solo il Data Breach (rilevazione), ma anche le informazioni sull'andamento dello stesso nel tempo;
- assicurare forme di comunicazione oneste, concrete e trasparenti;
- fare riferimento al Team crisi, al suo ruolo ed al suo impegno;
- mettere in evidenza la storia, l'impegno dell'Azienda nell'assicurare l'attenzione al tema, gli investimenti fatti e le misure applicate;
- descrivere l'evento in modo facilmente comprensibile [quale impatto ha avuto sui dati (o quale impatto presumibile può avere – informazioni perse, violate, comunicate a terzi non autorizzati, diffuse, ecc), come lo si sta affrontando/come è stato affrontato] e specificare cosa l'azienda sta facendo concretamente per proteggere i dati degli interessati;
- indicare se, come e quando, è stato coinvolto il Garante della Protezione dei dati;
- inserire un contatto diretto per rivolgersi all'organizzazione;
- valutare l'eventualità di attivare un numero verde per rispondere agli interessati.

Aspetti specifici per il comunicato stampa/dichiarazione ufficiale:

- prevedere il link alla pagina del sito web dove sono reperibili le informazioni sul Data Breach. Fornire lo stato dell'andamento dello stesso nel tempo.

Aspetti specifici per la comunicazione tramite sito WEB/social media:

- considerare di pubblicare (per le situazioni più gravi) anche un messaggio di scuse/spiegazioni coinvolgendo il Consiglio di Amministrazione e il Direttore Generale;
- affidarsi ad un esperto, qualora non si disponesse internamente di tali competenze, per evitare errori o creare più allarme del necessario;
- valutare l'eventualità di attivare una APP dedicata all'evento.

2.10 Comunicazione al Consiglio di Amministrazione del Cfp Zanardelli

A seguito di un evento che ricade nei casi C e D, ed in ogni caso qualora il Titolare del trattamento lo ritenesse opportuno, deve essere tenuto aggiornato il Consiglio di amministrazione. Tale attività è a cura del Titolare del trattamento e deve avvenire con modalità, per quanto possibili, rintracciabili.

2.12 Formazione al personale

A seguito di eventi che hanno comportato delle violazioni o delle possibili violazioni, deve essere valutata una attività di formazione ad hoc, per il personale coinvolto o che sarebbe stato potenzialmente coinvolto nella violazione. I temi dovranno essere definiti di volta in volta rispetto agli eventi accorsi.

2.13 Situazioni anomale o di emergenza

In caso di segnalazioni in situazioni anomale o di emergenza, quali:

- chiusura temporanea della sede di Cfp Zanardelli (es. periodo di ferie)
- mancanza di figure apicali del Team crisi
- mancanza di collegamenti (es. internet)/energia/situazioni di emergenza dovute a cause di forza maggiore)

Devono essere considerate le seguenti misure:

- Il Team crisi può operare anche con una sola persona tra quelle che compongono il Team.
- Le riunioni del Team possono essere effettuate in luoghi diversi dalla sede di Cfp Zanardelli ed eventualmente con strumenti quali skype, ecc.
- Indisponibilità del server (per manutenzione programmata) o altri eventi che possono non garantire il presidio dei sistemi deve essere comunicato anche nella sezione Data Breach Policy del sito internet (quando possibile).

3. ALLEGATI

- MODULO Gestione del Data Breach
- REGISTRO degli incidenti
- Esempi comunicazione

4. FONTI

Procedura ENISA Doc. WP2006/5.1.