Camera di commercio, industria, artigianato, agricoltura di Lucca

Procedura di gestione dei data breach

ai sensi del Regolamento UE 679/2016

Camera di Commercio Industria Artigianato Agricoltura di Lucca - Corte Campana, 10 - 55100 Lucca - T +39 0583 9765 F +39 0583 199 99 82

cameracommercio@lu.camcom.it - p.e.c. camera.commercio.lucca@lu.legalmail.camcom.it - www.lu.camcom.it
C.F. 80004310464 - P.IVA 00427080460

Indice generale

RIFERIMENTI NORMATIVI

La presente procedura risponde ai seguenti requisiti normativi:

1. Notifica di una violazione dei dati personali all'autorità di controllo (art. 33 del GDPR)
2. Comunicazione di una violazione dei dati personali all'interessato (art. 34 del GDPR)
3. WP250rev.01, *Guidelines on Personal data breach notification under Regulation 2016/679*, adottate il 03/10/2017 e riemesse il 06/02/2018
4. Provv. del Garante 30 luglio 2019, n. 157, *sulla notifica delle violazioni dei dati personali (data breach).*

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice	D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018
Garante	Garante per la protezione dei dati personali
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati) – EDPB (European Data Protection Board)
DPO	Data Protection Officer
Delegato del Titolare	Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della *compliance* al GDPR
SG	Segretario Generale della Camera di commercio
Evento o incidente della sicurezza	Qualsiasi accadimento significativo per la gestione delle infrastrutture IT e per la gestione dell'operatività dei servizi o per la violazione di archivi cartacei
Violazione (data breach)	Qualsiasi incidente di sicurezza che soddisfi i presenti requisiti: • coinvolge dato/i trattati dalla Camera di Commercio di Lucca in modalità elettronica e/o cartacea; • costituisce una violazione della disponibilità e/o della riservatezza e/o dell'integrità del/i dato/i personali
Violazione della riservatezza	Si ha violazione della riservatezza quando il/i dato/i personale/i • sono accessibili a persone non autorizzate • sono resi accessibili a terzi con modalità illegali • sono comunicati a persone non autorizzate • sono diffusi in modo non conforme alla normativa Per comunicazione si intende mettere a conoscenza di uno o più dati un numero di destinatari definito a priori dal mittente. (Es invio di mail a destinatari errati) Per diffusione si intende mettere a conoscenza di uno o più dati un numero di utenti non definibile a priori. (Es pubblicazione sul siti internet, social, brochure, ecc)
Violazione della disponibilità	Si ha violazione della disponibilità quando • si perde/ono definitivamente uno o più dati personali • uno o più dati personali non sono disponibili in una delle modalità utilizzate in precedenza (es ho solo il documento cartaceo e non più la scansione o la

	rielaborazione dei dati in tabelle o altro) • uno o più dati personali non sono disponibili temporaneamente a causa di interventi illegali (es denial of service, criptovirus), di malfunzionamenti o di comportamenti organizzativi errati (es smarrimento credenziali) Gli interventi di manutenzione programmati non costituiscono violazione della disponibilità del dato
Violazione dell'integrità del dato	Si ha violazione dell'integrità del dato quando il dato è stato modificato in maniera definitiva accidentalmente o intenzionalmente (es uso un file come traccia per fare un altro documento e poi salvo solo la versione modificata)

MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Stato	Descrizione	Approvazione

OBIETTIVO E CAMPO DI APPLICAZIONE

Obiettivo della presente procedura è descrivere la gestione del data breach da parte della Camera di Commercio di Lucca.

La gestione di un data breach prevede due macrosettori di intervento:

- definizione dei compiti e delle responsabilità e degli strumenti per gestire un eventuale data breach
- definizione della gestione del data breach che si può riassumere nelle seguenti fasi: segnalazione di un incidente di sicurezza, verifica se si tratta di un data breach (triage) , studio delle cause ed adozione eventuale delle prime misure, conclusione del triage ed annotazione nel Registro data breach, costituzione del team di secondo livello (eventuale), valutazione del rischio, decisione se notificare al Garante, valutazione degli effetti delle misure adottate e se necessario implementare fissando compiti, notifica al Garante, annotazione nel Registro, decisione se notificare agli interessati, annotazione nel Registro, notifica agli interessati, annotazione nel Registro, follow up delle misure adottate e di eventuali richieste del Garante

Si tenga conto inoltre che:

a) nei rapporti di contitolarità ciascun contitolare attua la sua procedura per quanto attiene al trattamento dei dati che svolge. Nell'accordo di contitolarità possono tuttavia essere disposte specifiche procedure e/o modalità relativi ad obblighi di comunicazione tra le parti e tra queste ed il Garante;

b) per quanto attiene ai data breach relativi alle ipotesi in cui la Camera di commercio opera in qualità di responsabile esterno del trattamento, ex art. 28 del GDPR, dovranno essere osservate anche le indicazioni ed istruzioni fornite dal Titolare nel documento di nomina/designazione.

La presente procedura è portata a conoscenza, anche attraverso attività di sensibilizzazione o formazione, di tutti i Dirigenti, Responsabili delle Unità organizzative, funzionari o, comunque, referenti delle Aree/Uffici/Servizi della Camera di Commercio.

La presente procedura è pubblicata nella Intranet nella sezione Documenti e modulistica, sottosezione Privacy.

COMPITI, STRUMENTI E RESPONSABILITÀ' PER GESTIRE UN DATA BREACH

Il Titolare deve essere in grado di determinare in tempi rapidi

- se l'incidente di sicurezza costituisce data breach perché coinvolge dati personali;
- se è necessario implementare ulteriori misure tecniche e/o organizzative;
- se il data breach costituisce un rischio per i diritti e le libertà degli interessati e, quindi, è necessario notificarlo al Garante;
- se il data breach costituisce una violazione grave per i diritti e le libertà degli interessati e, quindi, è necessario notificarlo agli interessati

IL TEAM

Dati i tempi ristretti (**entro 72 ore** da quando ne viene a conoscenza per la notifica al Garante) e la complessità della materia è necessario che il Titolare abbia definito a priori chi coinvolgere e con quali compiti cercando di unire competenze di vario tipo.

La soluzione adottata in questa procedura prevede la presenza di un Team a composizione variabile:

- Fase 1: il team è composto da Segretario Generale, Amministratore di Sistema, Responsabile Gestione documentale o delegato, DPO . Tra questi soggetti, escluso il DPO, va individuato il coordinatore che ha il compito di convocare, tenere i verbali.

- Fase 2: il team è allargato al Dirigente competente per l'ufficio o il servizio coinvolto, al Responsabile ex art 28 ove presente (per la Cciaa di Lucca al momento sono Lucense scrl, Infocamere scpa, Maggioli spa). Il Segretario Generale e/o il Dirigente competente potranno decidere di ampliare il team a legali o consulenti esterni.

GLI STRUMENTI DA USARE

Nel rispetto del principio di accountability sono fondamentali sia la tempestività delle comunicazioni che il tener traccia di quanto fatto e perché; per soddisfare queste esigenze sono necessari questi strumenti minimi:

- creazione di un gruppo di posta specifico dove far pervenire la stragrande maggioranza delle segnalazioni. Questo gruppo di posta deve contenere almeno i membri del Team della prima fase.

- Adozione di un modello di Registro del data breach che contenga tutte le informazioni richieste dalle Linee guida del WP29. La Camera di Commercio di Lucca ne dispone già di uno che potrebbe essere migliorato in base alle problematiche riscontrate nel suo utilizzo. (All.1 – Registro Data Breach)

- Adozione di un modello per la verbalizzazione. Si propone di usare il modello del Garante da compilare in parte o tutto a seconda dello stadio della procedura.(All.2 Modello notifica Data Breach)

- Adozione di un sistema per la conservazione della documentazione: si propone un fascicolo specifico in Gedoc con sotto fascicoli per ogni eventuale intervento. Il fascicolo deve essere visibile ai componenti del Team di primo livello. I documenti saranno estesi nella visibilità, ove necessario, dei componenti del Team di secondo livello.
- Predisposizione di un sistema per la valutazione del rischio e sua applicazione almeno per l'aspetto relativo al possibile danno in modo da velocizzare e standardizzare le operazioni di gestione della procedura (All.3 Valutazione rischio in Data Breach).
- Data base di referenti dei Responsabili ex art 28 che forniscono servizi IT continuativi. Il data base deve contenere l'indicazione di almeno un paio di referenti e l'eventuale DPO. Questi dati sono già contenuti nel Registro dei trattamenti consultabile all'indirizzo https://regi.infocamere.it/regi/ (browser consigliato Chrome)

COMPITI PREDEFINITI

La Camera di Commercio di Lucca con la Delibera di Giunta n° 34 del 4/5/2018 ha deciso di

- Affidare la tenuta del Registro del data breach all'Amministratore di Sistema.
- Affidare al SG sia la notifica al Garante che quella agli interessati

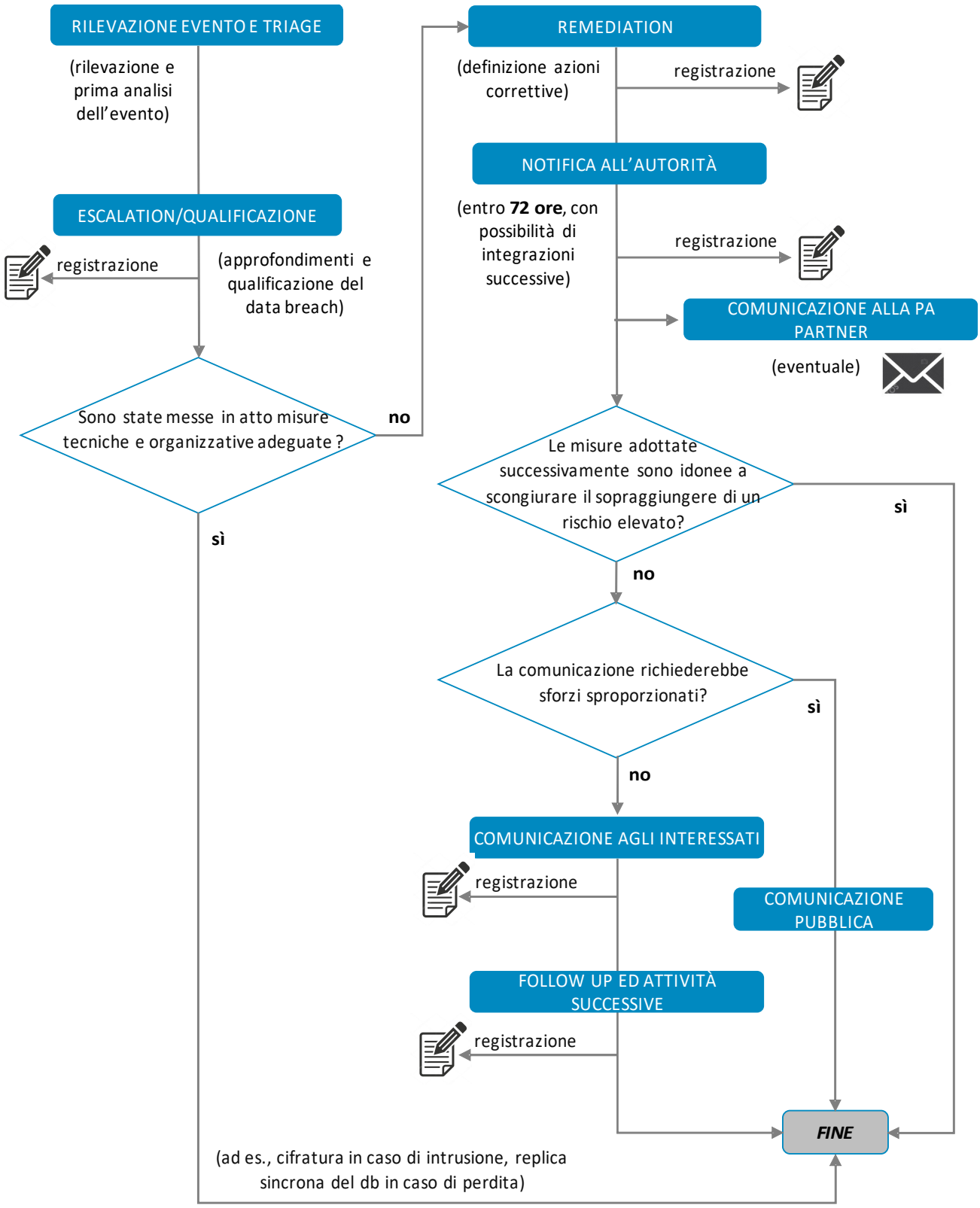
La normativa prevede che il DPO sia il punto di contatto tra il Garante ed il Titolare per la gestione del follow up di un eventuale data breach

Con l'adozione della presente procedura si stabilisce che

- Nel caso di data breach relativi a trattamenti cartacei (ad esempio in caso di violazione fisica ad archivio, a cassetti/porte forzate) oppure in caso di smarrimenti di dispositivi fisici (ad esempio chiavette usb, pc, etc.) al Team di primo livello partecipa, se è il caso, il Provveditore.
- Il Delegato del Responsabile della gestione documentale è il Responsabile dell'Ufficio Segreteria Protocollo Relazioni esterne
- Il coordinamento dei team (convocazioni, verbalizzazioni, ecc) è affidato al Delegato del Responsabile della gestione documentale

LA GESTIONE DEL DATA BREACH

La gestione di un data breach può riassumersi nelle fasi di seguito rappresentate



FASE 1: RILEVAZIONE EVENTO E TRIAGE

La rilevazione di un evento può avvenire da diverse fonti:

↘ SEGNALAZIONE AUTOMATICA: sistemi di segnalazione automatica come le violazioni derivanti da superamento dei sistemi di Firewall della Camera di Commercio (gestiti direttamente o tramite soggetti esterni), ovvero gestiti da InfoCamere.

↘ SEGNALAZIONE INTERNA: attività di monitoraggio degli eventi da parte degli Amministratori di sistema o; comunicazione da parte del personale

↘ SEGNALAZIONE ESTERNA: nell'ambito dell'attività di monitoraggio, assistenza e manutenzione da parte di fornitori esterni di applicativi, supporto sistemistico, servizi di consulenza, etc. ovvero da parte di utenti finali dei servizi della Camera di Commercio, ovvero da parte di Responsabili nominati ex art. 28 del GDPR.

In particolare, in tutti i contratti che attribuiscano funzioni di amministrazione di sistemi o deleghino trattamenti di dati personali a soggetti esterni qualificati o qualificabili come responsabili esterni del trattamento ex art. 28 GDPR, devono essere inserite clausole contrattuali che prevedono l'obbligo:

- di comunicazione immediata di eventuali eventi di sicurezza che abbiano coinvolto i dati oggetto di trattamento, specificando le azioni correttive poste in atto e gli esiti delle stesse. Nello standard contrattuale è previsto che la segnalazione pervenga alla pec camerale (camera.commercio.lucca@lu.legalmail.camcom.it)
- di fornire, in caso di necessità, anche attraverso il DPO eventualmente nominato, la massima disponibilità e collaborazione per l'analisi e risoluzione di eventuali criticità emergenti per l'ambito di trattamento assegnato.

Secondo il WP 29, il Regolamento "impone tanto al titolare quanto al responsabile del trattamento di disporre di misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati. Tali soggetti dovrebbero tenere conto: dello stato dell'arte e dei costi di attuazione; della natura, dell'oggetto, del contesto e delle finalità del trattamento; del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Inoltre, il regolamento impone di mettere in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali, il che a sua volta consente di stabilire se scatta l'obbligo di notifica"

A chi arrivano le segnalazioni?

- Le segnalazioni automatiche arrivano all'Amministratore di Sistema o ad altro referente indicato nel contratto con il Responsabile ex art 28.
- Le segnalazioni interne arrivano ad una casella dedicata violazioni@lu.camcom.it che è visibile a Segretario Generale, Amministratore di Sistema, Responsabile gestione documentale o suo delegato, DPO, Coordinatore del Team di primo intervento (se non compreso nei soggetti sopra indicati).
- Le segnalazioni esterne arrivano alla pec camerale e in copia conoscenza a violazioni@lu.camcom.it

Cosa succede a seguito delle segnalazioni?

Le segnalazioni sono senza indugio portate a conoscenza del Team della prima fase tramite inoltro alla casella dedicata creata se non sono arrivate già da quella.

Il coordinatore provvede ad aprire apposito fascicolo in Gedoc.

Il team di primo intervento, sotto la responsabilità del SG, ha il compito di verificare il perimetro dell'evento, ovvero almeno le seguenti informazioni:

1. sistema, infrastruttura, base dati oggetto dell'evento;
2. tipologia dell'evento verificatosi;

3. tipologia e volume dei dati e degli interessati coinvolti:
4. misure di sicurezza applicate;
5. attività di remediation (azioni correttive) ipotizzabili.

In caso di mancato coinvolgimento di dati personali, il Team di primo intervento attribuisce le responsabilità per l'avvio delle eventuali azioni correttive e registra nell'apposito Registro indicando la motivazione per cui non costituisce data breach. Dato che i documenti in uscita della Camera di Commercio sono originali informatici, non costituisce mai data breach la distruzione anche parziale di un documento cartaceo che costituisce copia analogica di originale informatico.

Ad esito delle azioni correttive, la fase si chiude con il follow up di remediation [annotazione nel Registro del Data Breach (All. 1 - Registro Data Breach) ed eventuali allegati], inserimento dei documenti nel fascicolo di Gedoc e sua chiusura.

Questa fase deve concludersi entro 24 ore dalla rilevazione dell'evento.

Per una migliore chiarezza si riproducono alcune indicazioni del WP29.

Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

Esempi

1. In caso di perdita di una chiave USB contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati. Tuttavia, anche se il titolare del trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, tale caso deve essere notificato, in quanto sussiste una ragionevole certezza del fatto che si è verificata una violazione della disponibilità; il titolare del trattamento si considera venuto "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB.

2. Un terzo informa il titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata. Dato che al titolare del trattamento è stata presentata una prova evidente di una violazione della riservatezza, non vi è dubbio che ne sia venuto "a conoscenza".

3. Un titolare del trattamento rileva che c'è stata una possibile intrusione nella sua rete. Controlla quindi i propri sistemi per stabilire se i dati personali ivi presenti sono stati compromessi e ne ottiene conferma. Ancora una volta, dato che il titolare del trattamento ha una chiara prova di una violazione non può esserci dubbio che sia venuto "a conoscenza" della stessa.

4. Un criminale informatico viola il sistema del titolare del trattamento e lo contatta per chiedere un riscatto. In tal caso, dopo aver verificato il suo sistema per accertarsi dell'attacco, il titolare del trattamento dispone di prove evidenti che si è verificata una violazione e non vi è dubbio che ne sia venuto a conoscenza.

Se una persona, un'organizzazione di comunicazione o un'altra fonte informa il titolare del trattamento di una potenziale violazione o se egli stesso rileva un incidente di sicurezza, il titolare del trattamento può effettuare una breve indagine per stabilire se la violazione si sia effettivamente verificata. Durante il periodo di indagine il titolare del trattamento non può essere considerato "a conoscenza". Tuttavia, si prevede che l'indagine iniziale inizi il più presto possibile e stabilisca con ragionevole certezza se si è verificata una violazione; può quindi seguire un'indagine più dettagliata.

Dopo che il titolare del trattamento è venuto a conoscenza di una violazione soggetta a notifica, la stessa deve essere notificata senza ingiustificato ritardo e, ove possibile, entro 72 ore. Durante questo

periodo il titolare del trattamento dovrebbe valutare il rischio probabile per le persone fisiche al fine di stabilire se è soddisfatto il requisito per la notifica e quali siano le azioni necessarie per far fronte alla violazione. Tuttavia, il titolare del trattamento potrebbe già disporre di una valutazione iniziale del rischio potenziale che potrebbe derivare da una violazione come parte di una valutazione d'impatto sulla protezione dei dati effettuata prima dello svolgimento del trattamento interessato. Tuttavia, tale valutazione può essere più generale rispetto alle circostanze specifiche di un'effettiva violazione e, pertanto, in ogni caso dovrà essere effettuata una valutazione aggiuntiva che tenga conto di tali circostanze.

FASE 2: ESCALATION, QUALIFICAZIONE DELLA VIOLAZIONE E REMEDIATION

Stabilito che l'evento costituisce un data breach, in seguito alla ricezione della scheda di segnalazione, il Dirigente dell'Area di riferimento costituisce il Team di secondo intervento (T2I) costituito dai componenti del Team di primo intervento a cui si aggiungono:

- il Responsabile dell'Ufficio in relazione al quale si ipotizza la violazione di dati;
- Eventuale legale o consulente di fiducia;
- lo specialista della società o soggetto che ha realizzato/fornito il prodotto/servizio interessato dall'incidente e/o il DPO (ove nominato) o altro referente specializzato della Società in house coinvolta nel trattamento.[1]

Il Team ha il compito di verificare, a norma dell'art. 33, par. 1, del GDPR, la probabilità che la violazione dei dati personali presenti un rischio (soprattutto se questo può qualificarsi come "elevato") per i diritti e le libertà delle persone fisiche e, di conseguenza, decidere le misure di risposta all'emergenza.
A tal fine:

a) si individua/no il/i Trattamento/i di riferimento in base al Registro adottato e si acquisisce la valutazione di impatto già presente;
b) sono raccolte o consolidate/approfondite le informazioni di cui al format per la comunicazione al Garante (All.2 - Modello notifica Data Breach), ove disponibili, anche al fine di minimizzare i tempi di risposta;
c) sono effettuate le seguenti valutazioni:
    - se la violazione costituisce un rischio per i diritti e le libertà delle persone fisiche, compilando la parte finale della scheda di valutazione del rischio (si veda All.3 - Valutazione rischio in Data Breach) con il volume di dati, i tempi di ripristino (solo per violazione dell'integrità o della disponibilità), le modalità della comunicazione/diffusione/accesso non autorizzato.

Per valutare il rischio si utilizzano in parte gli esiti del sistema di valutazione del rischio: questa metodologia valuta il rischio di un data breach incrociando gravità dell'impatto e probabilità dell'accadimento. Questa valutazione serve per determinare l'adeguatezza o meno delle misure tecniche ed organizzative scelte. Gli esiti, però, possono in parte essere recuperati in caso di data breach creando un sistema che incrocia la gravità della violazione (impatto) con la sua esposizione; l'impatto è già stabilito a priori sulla base dei dati contenuti nel Registro dei trattamenti, mentre il grado di esposizione dipende dalle caratteristiche dell'evento.
La gravità è calcolata sulla base di matrici distinte per tipologia di violazione e che tengono conto dei seguenti elementi:

- tipologia di dati trattati
- effetti per gli interessati
- effetti per l'ente (solo per violazione disponibilità)
- caratteristiche interessati
- conoscibilità del dato (solo per violazione della riservatezza)

L'impatto è espresso nel Registro dei Trattamenti con una scala che va da 1 a 5: Trascurabile. Basso. Medio. Alto e Molto Alto.

Il grado di esposizione è calcolato tenendo conto dei seguenti elementi:

- volume dei dati
- numerosità degli interessati coinvolti
- durata dell'evento (solo per violazione della disponibilità)
- capacità delle misure adottate in prima battuta di annullare o minimizzare gli effetti negativi per gli interessati (solo per violazione della riservatezza)

L'esposizione si esprime su una scala da 1 a 3: bassa, media, alta

1 Cfr. nota n. 1.

Qui di seguito si riportano le tabelle per valutazione dell'esposizione nelle due ipotesi di violazione della riservatezza e violazione della disponibilità/integrità

	parametro			
opzioni e valori	Volume dati	le misure adottate possono eliminare gli effetti negativi	interessati coinvolti	tipo di accesso
1	Limitato ed identificato o identificabile con certezza	si	singolo o limitato identificabile a priori	non autorizzato da parte di dipendenti interni
2	Ampio ed identificabile con difficoltà	solo in parte	limitato non identificabile a priori	non autorizzato o non corretto da parte di esterni
3	Ampio e non identificabile	no o non nell'immediato	Ampio identificabile o larga scala	illegale

esposizione per violazione della disponibilità/integrità

	parametro		
valore ed opzioni	Volume dati	Durata evento o tempi di recupero del dato	interessati coinvolti
1	Limitato ed identificato o identificabile con certezza	Inferiore alle tre ore	singolo o limitato identificabile a priori
2	Ampio ed identificabile con difficoltà	Giornata lavorativa	limitato non identificabile a priori
3	Ampio e non identificabile	Oltre la giornata lavorativa	Ampio identificabile o larga scala

Dall'incrocio tra impatto ed esposizione si determina il rischio che sarà basso (verde), medio (giallo), alto(rosso)
come esposto qui sotto[2]

	Esposizione		
Impatto o gravità	Bassa	Media	Alta

2 Si è messo valore medio nel caso in cui una gravità elevata si incrocia con un'esposizione bassa perché tale fattispecie si verifica solo nel caso in cui con le prime misure adottate si è in grado di eliminare o minimizzare gli effetti negativi della violazione (es perdita/furto di credenziali per pochi utenti).

in verticale			
trascurabile			
bassa			
media			
alta			
molto alta			

Ad esito dell'analisi il Team decide cosa fare sulla base della seguente tabella di riferimento:

	Descrizione	Notifica al Garante	Comunicazione interessati
Rischio	Basso: è improbabile che la violazione arrechi un pregiudizio ai diritti ed alle libertà degli interessati	no	no
	Medio: la violazione arreca un pregiudizio non elevato ai diritti ed alle libertà degli interessati	si	no
	Alto: la violazione arreca un pregiudizio elevato ai diritti ed alle libertà degli interessati	**si**	**si**

A) La valutazione è condivisa dai membri del team di secondo livello e si tiene traccia dei pareri espressi. Nel caso in cui la violazione non costituisca un rischio per i diritti e le libertà degli interessati e le misure adottate si ritengano adeguate, il Dirigente o suo delegato provvede a verbalizzare gli esiti dell'analisi riportando esplicitamente il parere formalizzato dal DPO; copia del verbale deve essere inviato al DPO.

B) Nel caso in cui sia stato valutato che la valutazione costituisce un rischio per i diritti e le libertà degli interessati e le misure implementate siano insufficienti :

- il team provvede ad identificare le possibili azioni correttive da implementare, selezionandole tra quelle di cui sia valutata la fattibilità immediata ed il miglior esito ai fini della minimizzazione del possibile danno agli interessati
- il Dirigente provvede a:
- definire ed assegnare responsabilità e tempistiche per la remediation, compresi i soggetti esterni coinvolti;
- provvede a comunicare all'Amministratore di sistema cosa annotare nel Registro del data breach. allegando eventuali pareri dell'Amministratore di Sistema stesso o dei Referenti di Responsabili ex art 28 circa la non adeguatezza delle misure;
- Il Segretario Generale provvede, con il supporto del team, a compiere le seguenti attività:
- compilare o completare il Modello per la notificazione al Garante (riportato nell'Allegato al presente documento- All. 2 Modello notifica Data Breach), indicando se le azioni correttive (c.d. attività di remediation) sono già concluse od ancora in itinere;

- inviare il modello al Garante nei tempi e nei modi previsti
- predisporre, qualora ne ricorrano le condizioni, la comunicazione da inviare all'interessato (ovvero la comunicazione pubblica), contenenti le indicazioni riportate nell'All.2 Modello notifica Data Breach

Questa fase deve concludersi entro ulteriori 56 ore dalla rilevazione dell'evento.

FASE 3: INVIO DELLE NOTIFICAZIONI

Il Garante, con il provv. 30 luglio 2019, n. 157, ha definito il Modello per la notifica delle violazioni dei dati personali, ai sensi dell'art. 33 del GDPR e dell'art. 26 del D.Lgs. n. 51/2018. Il Modello, secondo le modalità di cui all'art. 65 del D.Lgs. n. 82/2005 (CAD), è riprodotto nell'Allegato 2 al presente documento.

La notifica avviene mediante la compilazione del Modello nell'ambito dei sistemi telematici indicati nel sito istituzionale del Garante.

Il Modello deve essere sottoscritto con firma digitale dal SG e trasmesso al Garante nel più breve tempo possibile, **possibilmente entro 72 ore** dall'avvenuta conoscenza da parte del Titolare, di un evento qualificabile come Data breach[3].

Ove avvenga oltre tale limite temporale è necessario corredarla dei motivi del ritardo[4].

Qualora non si disponga di tutte le informazioni si procede ad inviare una prima notifica parziale, da completare non appena disponibili le ulteriori informazioni.

Il Dirigente dell'Area di riferimento invia il verbale e copia del Modello sottoscritto dal SG:

- al DPO;
- all'Amministratore di Sistema, che aggiorna o provvede a far aggiornare il "Registro dei Data Breach";
- al referente dell'Amministrazione Pubblica da cui eventualmente la Camera di Commercio ha ricevuto l'incarico di trattare i dati personali[5], previa valutazione di opportunità condotta congiuntamente con il SG ed a seguito dell'avvenuta notifica al Garante.

Ove le misure di cui al punto B) del paragrafo precedente siano adottate immediatamente, la fase si chiude con il follow up di remediation (mediante verbalizzazione degli esiti da parte del Dirigente dell'Area di riferimento)[6]

Nel caso in cui tali misure necessitino di maggior tempo per l'implementazione ovvero non siano in grado di minimizzare i rischi per gli interessati, il Dirigente dell'Area di riferimento:

- provvede a definire i contenuti della comunicazione agli interessati, che – con linguaggio semplice e chiaro - deve contenere almeno i seguenti elementi:
  A. la natura della violazione dei dati personali;
  B. le probabili conseguenze della violazione dei dati personali;
  C. le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione;
  D. il nome e i dati di contatto del responsabile della protezione dei dati.

3 Nelle fasi indicate in precedenza sono disponibili 12 ore che possono essere distribuite come si ritenga maggiormente opportuno.

4 Ad es., data breach particolarmente complesso, serie di attacchi/violazioni consecutive che necessitano di una reazione complessa.

5 Ad es., sulla base di una convenzione/protocollo d'intesa.

6 "Non è richiesta la comunicazione all'interessato… se 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" (art. 34, par. 3, lett. b del GDPR).

La comunicazione – un cui esempio è riportato nell'All. 4 - Comunicazione a interessato – è sottoposta a parere del DPO e ad approvazione del SG.

- verifica la fattibilità di reperimento dei dati di contatto degli interessati coinvolti o potenzialmente coinvolti; nel caso in cui si valuti che la comunicazione agli interessati possa essere sostenuta senza sforzi sproporzionati (ad es., disponibilità di email/pec), provvede all'invio massivo della comunicazione.
- ove non vi sia disponibilità di dati di contatto ovvero si valuti che la comunicazione richieda sforzi sproporzionati, provvede a darne pubblicità nelle modalità concordate con SG e DPO (ad es., pubblicazione in evidenza sul sito istituzionale, comunicati stampa, etc.).

La comunicazione agli interessati deve essere formalizzata "senza ingiustificato ritardo".

Dell'avvenuta comunicazione è data informazione al DPO.

E' bene ricordare che:

- la notifica all'autorità di controllo competente è obbligatoria a meno che sia improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche;

- la comunicazione di una violazione alle persone fisiche diventa necessaria soltanto laddove la violazione possa presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche.

FASE 4: ATTIVITÀ' SUCCESSIVE

Se durante le fasi precedenti si sospetta che la violazione possa essere stata provocata in maniera intenzionale da un esterno o da un utente interno si attiva il processo di raccolta delle evidenze o prove con ulteriori investigazioni anche difensive.

L'attività, ove necessario, può essere gestita secondo quanto previsto dall'art. 391 nonies[7] o dall'art. 327 bis c.p.p.[8] e deve rispettare gli standard e le normative (raccolta e "catena di custodia") in termini di analisi forense, al fine di poter intraprendere successivamente un'azione legale nei confronti dell'eventuale responsabile.

Qualora non si riscontrasse questa condizione, l'analisi post-violazione sarà finalizzata all'apprendimento delle cause che hanno generato l'evento al fine di imparare dai propri errori e per fornire ulteriori informazioni per la risoluzione di eventuali criticità collegate o ricorrenti.

Ad esito delle notificazioni al Garante ed agli interessati, il DPO deve:

- gestire in prima persona le relazioni e gli eventuali feedback pervenuti dal Garante e dalle altre Istituzioni coinvolte, coordinando – con l'ausilio della sua struttura di supporto – l'aggiornamento del "Registro dei Data Breach" (un cui modello è riportato nell'All.1 - Registro Data Breach);
- supportare il Dirigente competente a gestire le comunicazioni, istanze e richieste da parte degli Interessati, anche attraverso un referente del Servizio Staff, ovvero dell'Ufficio legale o, ancora, dell'Area/Ufficio di riferimento interessata dalla la violazione.

FORMAZIONE

Nell'ambito del programma di formazione sulla sicurezza, nonché di quello permanente sulla tutela dei dati personali, L'Ente svolge attività di informazione e formazione con riferimento ai contenuti del presente documento.

7 Se precedente all'instaurazione di un procedimento penale.

8 Se già instaurato il procedimento.