CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

Articolo Scientifico

LA GESTIONE DEL DATA BREACH. COMPLIANCE NORMATIVA E PROCEDURE AZIENDALI

La gestione delle violazioni di dati personali rappresenta uno degli aspetti più delicati e complessi da gestire nell'ambito di ogni modello organizzativo per la protezione dei dati personali. Attraverso un'analisi storica dell'evoluzione della materia nella letteratura dell'European Data Protection Board, ai tempi Gruppo di Lavoro 29, si analizzerà la necessità dell'azione dell'approccio basato sul rischio per la corretta gestione delle violazioni di dati personali nelle sue varie fasi alla luce della casistica elaborata dalla letteratura più recente. Nel presente contributo, verranno esaminate la differenza fra incidente di sicurezza e violazione, l'attività di registrazione delle violazioni e le successive procedure di notificazione all'autorità di controllo e di comunicazione agli inte

di **Giacomo Conti**
IUS/01 - DIRITTO PRIVATO
Estratto dal n. 2/2023 - ISSN 2532-9871

Direttore responsabile
Alessio Giaquinto

Pubblicato, Lunedì 13 Febbraio 2023

CamminoDiritto.it
ISSN 2532-9871

Abstract ENG

Data breaches management is one of the most delicate and complex aspects to handle within any data protection compliance model. Through an historical analysis of the evolution of the literature of the European Data Protection Board, at the time Working Group 29, the present article will focus on the risk-based approach regarding the correct management of personal data breaches in its various phases in the light of the most recent literature. The difference between a security incident and a violation will be analysed, as well as the activity of recording violations and the subsequent procedures for notifying the supervisory authority and communicating them to the interested data subjects, as well as the centrality of the " Handbook on Handling Personal Data Breach" where procedures, respons

Sommario: 1. L'evoluzione storica del concetto di violazione di dati personali nella letteratura dell'european data protection board e del working party; 2. Il concetto di violazione di dati personali e i rischi derivanti dalla stessa; 3. La sicurezza del dato come concetto relativo; 4. Incidente di sicurezza e violazione di dati personali: la registrazione delle violazioni; 5. La notificazione della violazione al garante e la comunicazione agli interessati; 6. Le procedure per la documentazione, la notifica e la comunicazione della violazione; 7. Il manuale per la gestione delle violazioni di dati personali.

1. L'evoluzione storica del concetto di violazione di dati personali nella letteratura dell'european data protection board e del working party 29

Per comprendere a fondo il concetto di violazione di dati personali le disposizioni del GDPR e i Considerando agli stessi devono essere studiate alla luce delle opinioni e linee guida dell'European Data Protection Board che ne rappresentano un fondamentale complemento.

Prima ancora dell'istituzione dell'EDPB, la principale letteratura in materia era stata elaborata dal Gruppo di Lavoro (Working Party) istituito ai sensi dell'articolo 29 della direttiva 95/46/CE: un organo consultivo europeo indipendente composto sui dati protezione e riservatezza i cui compiti sono descritti all'articolo 30 della direttiva 95/46/CE e dall'articolo 15 della direttiva 2002/58/CE poi sostituito dall'EDPB con l'entrata in vigore del GDPR.

Già nell'Opinion 03/2014 on Personal Data Breach Notification del 25 marzo 2014, il Gruppo di Lavoro aveva posto le pietre miliari della materia e posto le basi per l'art. 33

CamminoDiritto.it
ISSN 2532-9871

del futuro General Data Protection Regulation. In questa sede, il gruppo di lavoro aveva proposto un'interessante casistica presentando ipotesi in cui gli interessati al trattamento avrebbero dovuto essere notificati in caso di violazione. Ad esempio, l'opinione affronta il caso di furto di quattro computer di un istituto pediatrico, di un accesso non autorizzato sfruttando una vulnerabilità di una web application di una compagina assicuratrice, di comunicazione non autorizzata di username e password a terzi non autorizzati che pone il rischio di accesso non autorizzato a un data base aziendale o, ancora, nel caso in cui delle carte di credito siano state gettate dall'organizzazione senza avere adottato sistemi di distruzione sicura dei supporti[1].

Già in questa sede, il WP ha analizzato le conseguenze della violazione sotto i profili della riservatezza, integrità e disponibilità. L'opinion, per quanto ben strutturata e ancora attuale sotto molti profili, non ha il grado di completezza e approfondimento delle successive Linee Guida adottate dallo stesso WP nell'ottobre del 2017.

Nonostante le linee guida del 2017, nella versione emendata e adottata in data 6 febbraio 2018, siano ancora attuali e applicabili sia nei loro principi generali che nella casistica sicuramente ancora più che attuale; l'evoluzione dei rischi e delle minacce ha reso necessario un nuovo intervento da parte dell'EDPB che è intervenuto da ultimo nelle "Guidelines 01/2021 on Examples regarding Data Breach Notification" adottate in data 14 gennaio 2021. In questa sede, l'EDPB ha presentato una corposa e aggiornata casistica in tema di gestione delle violazioni.

Attraverso un'analisi delle disposizioni di legge e delle linee guida è, pertanto, possibile tracciare un quadro completo e articolato per gestire una violazione di dati personali a norma di Legge.

2. Il concetto di violazione di dati personali e i rischi derivanti dalla stessa

Il GDPR definisce come violazione dei dati personali una 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.

In linea generale, si parla di "distruzione" dei dati quando questi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento. I dati personali sono, invece, danneggiati quando sono stati modificati, corrotti o non sono più completi dopo l'avvenuta violazione. Si parla di "perdita" di dati personali quando il titolare del trattamento non ne possiede più il controllo, non è più in grado di accedervi piuttosto che quando questi non sono più in suo possesso[2]. Diverso è, infine, il concetto

CamminoDiritto.it
ISSN 2532-9871

di trattamento non autorizzato o illecito che può includere la divulgazione o accesso ai dati personali da parte di soggetti non autorizzati al trattamento. Una violazione particolarmente grave potrebbe interessare anche due oppure tutti e tre i profili di protezione del dato.

Si legge nei considerando alla norma che una violazione se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche che ne sono state coinvolte le quali possono, ad esempio, subire la perdita del controllo dei dati personali che li riguardano o una limitazione dei loro diritti o altri pregiudizi di tipo patrimoniale e non patrimoniale. Dalla violazione potrebbero, inoltre, derivare altre conseguenze pregiudizievoli quali la discriminazione, il furto o l'usurpazione d'identità, piuttosto che perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, un pregiudizio alla reputazione, la perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata[3]. La violazione potrebbe, inoltre, comportare anche pregiudizi atipici che potrebbero articolarsi in altri vantaggi economici e sociali che dovrebbero essere individuati e valutati dall'organizzazione che l'ha subita.

Pertanto, uno degli obblighi più importanti del titolare del trattamento è quello valutare tali rischi per i diritti e le libertà degli interessati e attuare misure appropriate misure tecniche e organizzative per affrontarli.

3. La sicurezza del dato come concetto relativo

Le problematiche relative alla sicurezza delle informazioni e alle violazioni non possono essere affrontate a livello meramente teorico od accademico, ma è necessario adottare un approccio necessariamente pragmatico basato su un'analisi dei rischi specifici che l'organizzazione incontra che è l'approccio che permea le Linee Guida dell'EDPB.

Ogni organizzazione deve, infatti, porre in essere misure di organizzazione e sicurezza adeguate a prevenire il rischio del verificarsi delle violazioni oltre che misure di mitigazione degli effetti dei data breach quando questi si verificano, ma nessuna misura di sicurezza per quanto aggiornata e sofisticata può eliminare integralmente il rischio del verificarsi di incidenti di sicurezza e di violazione dei dati personali.

La sicurezza dei dati personali, ma delle informazioni più in generale, si configura pertanto come un processo continuo, costante e laborioso che richiede il necessario intervento di diverse professionalità che devono gestire le complessità operative a livello informatico, gestionale e legale e coordinare una significativa complessità operativa.

CamminoDiritto.it
ISSN 2532-9871

Occorre, quindi, sfatare o meglio inquadrare realisticamente il concetto di "sicurezza" partendo da esempi pratici.

Pensiamo a Fort Knox, dove si trovano le riserve monetarie degli USA, che è generalmente individuato come uno dei luoghi più sicuri al mondo. Le misure di sicurezza implementate integrano sofisticati sensori, barriere perimetrali e allarmi sono tutti ai massimi livelli nonché un comando di Marines pronti a intervenire per qualsiasi problema. Fort Knox può, pertanto e di buon diritto, porsi come l'emblema del luogo sicuro per eccellenza.

Nonostante le misure di protezione adottate, gli esperti di sicurezza hanno elaborato un interessante esperimento e si sono domandati se Fort Knox resistere all'impatto con un meteorite di un chilometro di diametro e si sono dati la risposta in senso negativo[4].

Questo evento, per quanto improbabile, vanificherebbe, o meglio polverizzerebbe, tutte le misure di sicurezza adottate dal Governo del Stati Uniti d'America. Tuttavia, data la scarsissima probabilità del verificarsi di un simile evento l'adozione di uno scudo di protezione contro meteoriti non dovrebbe ritenersi una misura adeguata al rischio e non dovrebbe essere adottata.

Dall'esempio proposto emerge, pertanto, il carattere relativo del concetto di sicurezza che deve partire dall'individuazione della minaccia contro cui l'organizzazione si vuole e deve proteggere. Pertanto, il conseguente processo di gestione del rischio e il seguente processo di adozione delle relative misure di sicurezza non è in grado di prevenire in termini assoluti qualunque violazione.

Anche l'organizzazione più diligente può, pertanto, subire incidenti di sicurezza e anche violazioni di dati personali in quanto ogni misura di sicurezza, per quanto aggiornata e sofisticata, viene costantemente messa sotto pressione da minacce che si trovano sia all'esterno che all'interno dell'organizzazione.

Le minacce si fanno tanto più sofisticate e agguerrite quanto maggiore è il valore dei dati trattati.

Solo nei primi sei mesi del 2022 sono stati dagli esperti Clusit 1.141 gli attacchi cyber gravi, ovvero con un impatto sistemico in diversi aspetti della società, della politica, dell'economia e della geopolitica.

CamminoDiritto.it
ISSN 2532-9871

Rispetto al primo semestre 2021si è registrata una crescita dell'8,4%, per una media complessiva di 190 attacchi al mese, con un picco di 225 attacchi a marzo 2022, il valore più alto mai verificato.

I ricercatori di Clusit[5] hanno valutato, inoltre, e classificato i livelli di impatto dei singoli incidenti, sulla base di aspetti economici, sociali e relativi all'immagine e alle ripercussioni dal punto di vista geopolitico e hanno evidenziato che il trend di crescita degli attacchi riguarda anche la "qualità" degli stessi messa a punto dai cyber criminali, che agisce da moltiplicatore dei danni.

Confermando una tendenza già evidente nel 2021, gli attacchi gravi con effetti molto importanti sono stati nel primo semestre 2022 il 45% del totale, mentre quelli con impatto "critico" arrivano nei primi sei mesi di quest'anno a rappresentare un terzo di tutti gli attacchi. Nel complesso, gli attacchi con impatto Critical e High sono stati il 78% del totale.

È stata registrata una crescita percentuale seguono le categorie "Telecommunication" (+77,8%), "Financial / Insurance" (+76,7%), "News / Multimedia" (+50%), "Manufacturing" (+34%), "Other Services" (+30,8%) ed "ICT" (+11,5%), "Energy / Utilities" (+5,3%) ed "Healthcare" (+2,2%).

Per quanto riguarda la distribuzione delle vittime, le categorie più colpite dopo i "Multiple targets" sono i settori "Healthcare" e Governativi ciascuna con circa il 12% degli attacchi totali. Al quarto posto segue Information Technology - "ICT" (11%) e "Financial / Insurance" (9%)[6].

Emerge, pertanto, come le minacce e gli attacchi siano una costante con cui ogni organizzazione deve convivere e contro le quali deve combattere.

In ogni caso, lungi dall'essere un evento definitivo, irreversibile o paralizzante, il verificarsi di una violazione o incidente di sicurezza rappresenta un evento accidentale nell'attività di trattamento di dati personali.

Il verificarsi di una violazione, pertanto, fa sorgere degli specifici obblighi in capo all'organizzazione che non solo deve essere in grado di gestire adeguatamente la violazione e di mitigarne i rischi, ma deve essere anche in grado di dimostrarlo strutturando procedure e misure di sicurezza adeguate a gestire i rischi che affronta.

4. Incidente di sicurezza e violazione di dati personali: la registrazione delle

CamminoDiritto.it
ISSN 2532-9871

violazioni

Si legge nelle Linee Guida del 2017 del WP29 che violazione di dati personali rappresenta un tipo di incidente di sicurezza[7].

Se non tutti gli incidenti di sicurezza integrano una violazione di dati personali, al contrario tutte le violazioni di dati personali presuppongono il verificarsi di un incidente di sicurezza. Pertanto, la violazione si pone come conseguenza dei più gravi incidenti di sicurezza.

Ne consegue che quando l'organizzazione rileva oppure viene informata di un incidente di sicurezza, ad esempio dal reparto IT interno, deve stabilire se si è verificata o meno una violazione dei dati personali sorgono specifici obblighi che riguardano sia la documentazione che la gestione della violazione. Ad esempio, un attacco ai sistemi di un'azienda potrebbe essere stato schermato dalle misure di sicurezza adottate oppure le misure adottate dall'organizzazione sono state idonee a ridurne gli impatti in una maniera talmente significativa tale da rendere improbabile il verificarsi di un rischio per i diritti e per le libertà delle persone fisiche coinvolte nel trattamento.

Se prima si è parlato di attacchi hacker, in ogni caso è bene tenere a mente che un incidente di sicurezza non è sempre e solo un evento organizzato dall'esterno dell'organizzazione, come nel caso di un cryptolocker o un tentativo di phising posto in essere da soggetti esterni contro una risorsa aziendale, ma può riguardare anche incidenti che si verificano all'interno dell'organizzazione. Si pensi al mancato rispetto di una procedura, allo smarrimento di un documento aziendale contenenti dati particolari o alla cancellazione accidentale di informazioni da parte di un soggetto autorizzato. È bene, pertanto, distinguere le minacce in due grandi macrocategorie: quelle esterne e quelle interne e ogni organizzazione dovrebbe comprendere se è maggiore la probabilità che le minacce che deve affrontare siano di tipo interno od esterno.

Indipendentemente dal fatto che una violazione debba o meno essere notificata all'autorità di controllo, il titolare del trattamento deve conservare la documentazione di tutte le violazioni, come spiegato all'articolo 33, paragrafo 5 GDPR.

La documentazione della violazione subita è, infatti, cruciale posto che senza una completa annotazione degli elementi descrittivi della violazione subita, non si può determinarne né la gravità né le conseguenze per gli interessati né, per l'effetto, stabilire se la stessa sia da notificare al Garante o meno. Pare, pertanto, opportuno adottare il registro delle violazioni che risponde all'esigenza di documentare le violazioni subite al fine di procedere alla loro valutazione secondo quanto esige l'art. 33 comma 5 GDPR.

CamminoDiritto.it
ISSN 2532-9871

L'organizzazione, inoltre, deve documentare anche il ragionamento alla base delle decisioni prese in risposta a una violazione; a maggior ragione se una violazione non viene notificata deve essere documentata la motivazione dove il titolare ha valutato che la violazione è improbabile che presenti un rischio per i diritti e per le libertà delle persone fisiche[8].

5. La notificazione della violazione al garante e la comunicazione agli interessati

Dopo avere documentato la violazione nonché individuato vanno individuati e valutati i rischi che possono discendere dalla stessa.

Sebbene il regolamento introduca l'obbligo di notificare una violazione, non è obbligatorio farlo in tutte le circostanze. In particolare, 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, mentre la comunicazione di una violazione agli interessati diventa necessaria soltanto laddove la violazione possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte[9].

L'esempio classico di violazione da non notificare è quella che riguarda dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica.

In linea generale, se i dati personali sono stati resi sostanzialmente incomprensibili ai soggetti non autorizzati e se esiste una copia o un backup, una violazione della riservatezza che coinvolga dati personali correttamente crittografati potrebbe non dover essere notificata all'autorità di controllo[10].

Secondo l'approccio basato sul rischio, la gravità della violazione va valutata. principalmente, in ragione dei dati violati, ad esempio sulla natura particolare o comune degli stessi, e delle misure di sicurezza adottate per gestire il rischio. Ad esempio, nel caso di smarrimento di un dispositivo l'organizzazione deve valutare se i dati all'interno dello stesso erano stati criptati e stimare se sia probabile che gli stessi vengano decriptati.

Nel caso in cui lo scenario di rischio sia non improbabile, ad esempio se dati idonei a rivelare lo stato di salute della persona, si pensi a dati relativi a infezioni da HIV o altre malattie infettive, sono stati protetti da una password non adeguatamente robusta, l'organizzazione deve provvedere a notificare la violazione all'autorità di controllo e a comunicarla all'interessato nel caso in cui il rischio per i diritti e per le libertà degli

CamminoDiritto.it
ISSN 2532-9871

interessati si presenti come elevato.

In ogni caso, la violazione dovrebbe essere notificata anche quando il rischio si presenta anche in linea astratta come probabile. La letteratura ha specificato come non sia necessario attendere un esame forense dettagliato piuttosto che di adottare misure di mitigazione del rischio che può essere fornito anche in un momento successivo.

Per comprendere quale tipo di rischio la violazione presente, dopo avere provveduto alla registrazione della sessa è necessario qualificarla, ossia valutare quale aspetto della protezione e sicurezza del dato personale è stato inciso.

Nell'opinione del 2014 e nelle Linee Guida del 2017 viene presentata la differenza fra "violazione della riservatezza", "violazione dell'integrità" e "violazione della disponibilità", mentre nella precedente opinione questo aspetto era marcato sotto il profilo delle conseguenze della violazione che veniva presentata come un concetto ancora unitario. Più specificatamente la violazione della riservatezza si articola in un accesso, divulgazione o diffusione non autorizzata o accidentale di dati personali, la violazione all'integrità viene integrata da un'alterazione non autorizzata o accidentale dei dati personali ancora dalla, mentre la violazione alla disponibilità ha ad oggetto la perdita accidentale o non autorizzata dell'accesso o la distruzione di dati personali.

In particolare, "l'accesso" al dato rappresenta una componente fondamentale della "disponibilità"[11]. Si pensi al caso di indisponibilità ad accedere ai dati salvati in cloud. Nel caso in cui i servizi siano indisponibili o si perdano le credenziali di accesso ai servizi, viene integrata una violazione alla disponibilità del dato personale i cui rischi possono essere adeguatamente gestiti avendo una copia in locale dei dati trattati.

In ogni caso come sopra accennato, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse. Si pensi a un cryptolocker installato a seguito di un'esfiltrazione dei dati trattati. In questa ipotesi, i cybercriminali, dopo avere acquisito i dati trattati violandone la riservatezza, hanno criptato gli stessi rendendoli indisponibili all'organizzazione che li tratta e anche agli interessati. Questo tipo di violazione può essere particolarmente grave laddove riguardi dati particolari degli interessati quali, ad esempio, il fascicolo sanitario elettronico.

6. Le procedure per la documentazione, la notifica e la comunicazione della violazione

CamminoDiritto.it
ISSN 2532-9871

Ogni organizzazione, per essere compliant al GDPR e dimostrare il rispetto della norma deve, quindi, dotarsi di procedure che le consentano di documentare eventuali violazioni, le circostanze relative alle stesse oltre che gli effetti e le azioni correttive intraprese. A tal fine, occorre dotarsi di piani e procedure per la gestione di eventuali violazioni dei dati con designazione di responsabilità anche in ordine al processo di recupero (recovery process).

Le Linee guida del 2017 rappresentano una pietra miliare della materia e sono fondamentali nell'interpretazione generale e sistematica degli articoli 33 e 34 GDPR, sviluppando quanto elaborato nella precedente Opinion del 2014, alla luce dell'adozione del GDPR vengono approfonditi temi essenziali quali la notifica all'autorità di controllo, la comunicazione all'interessato dalla violazione, la valutazione dell'esistenza di un rischio o di un rischio elevato, il principio di responsabilizzazione e la tenuta dei registri.

In questa sede, il WP29 ha elaborato una corposa casistica distinguendo le ipotesi in cui una violazione deve essere notificata all'autorità di controllo piuttosto che comunicata agli interessati.

Viene posto il caso di un'organizzazione che ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB che viene rubata durante un'effrazione. Secondo quanto ritenuto dal WP29, fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare o da comunicare agli interessati. Tuttavia, laddove la chiave di criptazione venisse successivamente compromessa, la notifica della stessa si rende necessaria.

Il secondo caso proposto riguarda una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del trattamento e accedere alle proprie registrazioni. Secondo il gruppo di lavoro, questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. Pertanto, l'organizzazione deve conservare in ogni caso adeguate registrazioni in merito alle violazioni e incidenti di sicurezza subiti[12].

Le Linee Guida del 2017 sono intervenute a disciplinare l'aspetto normativo di gestione della violazione, hanno sviluppato e articolato la necessità di adottare un approccio basato sul rischio e valorizzato il principio di accountability, mettendo in luce l'importanza di adottare un registro per la gestione delle violazioni dei dati personali.

In particolare, il WP29 ha messo in luce come vi sia un obbligo di conservare la

CamminoDiritto.it
ISSN 2532-9871

documentazione interna relativa all'incidente e come questo obbligo sia indipendente dai profili di valutazione del rischio che l'incidente presenta per gli interessati.

Nelle Linee Guida si legge inoltre che, nell'ottica di assicurare un'efficiente ed efficace gestione delle violazioni, dovrebbero essere intraprese, al riguardo, attività di formazione e sensibilizzazione sui temi della protezione dei dati del personale del titolare del trattamento con approfondimenti relativi alla gestione dei data breach, avuto riguardo dei processi di identificazione dell'incidente, le azioni da intraprendere e ogni altro elemento utile come, ad esempio, l'annotazione e la valutazione delle stesse. Inoltre, l'attività di formazione dovrebbe essere ripetuta regolarmente, tenuta nella dovuta considerazione il rischio del trattamento valutato in ragione della dimensione del titolare oltre che delle attività realizzate.

In ogni caso, l'organizzazione deve affrontare le ultime tendenze e gli avvisi più recenti provenienti da attacchi informatici o altri incidenti di sicurezza.

Preliminarmente, l'organizzazione è tenuta a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate.

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.

Ad esempio, nell'ipotesi di smarrimento di una chiave USB contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati, l'organizzazione viene "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB.

Per contro, nel caso di richiesta di riscatto dopo la rivendicazione di un attacco informatico l'organizzazione arriva ad avere conoscenza della violazione dopo che ha operato le dovute verifiche. Ad esempio, un'analisi dei file di log che dimostrano l'avvenuta esfiltrazione dei dati. Ugualmente, se la notizia dell'avvenuta violazione proviene da terzi.

Laddove sia necessario procedere alla notifica della violazione, l'art 33 del GDPR stabilisce che il titolare del trattamento notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui

CamminoDiritto.it
ISSN 2532-9871

ne è venuto a conoscenza. Durante questo periodo il titolare del trattamento dovrebbe valutare il rischio probabile per le persone fisiche al fine di stabilire se è soddisfatto.

In ogni caso, se la notifica avviene oltre le 72 ore, il titolare del trattamento deve essere in grado di fornire i motivi del ritardo e la documentazione relativa a tale circostanza potrebbe contribuire a dimostrare che il ritardo nella segnalazione è giustificato e non eccessivo. Al contrario, se il titolare del trattamento non agisce in maniera tempestiva e risulta evidente che si è verificata una violazione, la sua inazione potrebbe essere considerata una mancata notifica ai sensi dell'articolo 33.

Il seguente articolo 34, paragrafo 1, stabilisce l'obbligo di comunicazione agli interessati delle violazioni che presentano un rischio elevato per i diritti e per le libertà delle persone fisiche. Questa comunicazione è da operarsi senza indebito ritardo in quanto l'obiettivo principale di questa attività è quella di fornire ai soggetti coinvolti nella violazione informazioni per proteggersi dalle conseguenze della violazione e attenuarne le conseguenze[13]

La violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. Ad esempio, tramite e-mail o SMS e attraverso il canale di contatto più immediato e diretto per operare la comunicazione.

L'organizzazione potrebbe contattare e consultare l'autorità di controllo non soltanto per chiedere consiglio sull'opportunità di informare gli interessati in merito a una violazione ai sensi dell'articolo 34, ma anche sui messaggi appropriati da inviare loro e sul modo più opportuno per contattarli.

L'articolo 34, paragrafo 3, stabilisce tre condizioni che, se soddisfatte, non richiedono la comunicazione agli interessati in caso di violazione, ossia quando:

il titolare del trattamento ha applicato misure tecniche e organizzative adeguate a proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, come la protezione dei dati personali con cifratura allo stato dell'arte; immediatamente dopo una violazione, il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche. Ad esempio, se l'organizzazione ha immediatamente individuato e intrapreso un'azione contro il soggetto che ha avuto accesso ai dati personali prima che questi fosse in grado di utilizzarli in qualsiasi modo; contattare gli interessati richiederebbe uno sforzo sproporzionato[14] **7. Il manuale per la gestione delle violazioni di dati personali**

CamminoDiritto.it
ISSN 2532-9871

L'approccio pragmatico e basato sul caso richiesto per la gestione della violazione richiede l'adozione di procedure interne adeguate a gestire la criticità.

Ogni organizzazione che ha intrapreso il processo di adeguamento al GDPR dovrebbe, pertanto, già essersi munita di procedure adeguate a gestire la violazione di legge anticipando quanto richiesto dall'EDPB.

In ogni caso, l'EPBD ha riconosciuto nelle proprie linee guida la centralità del manuale per la gestione delle violazioni di dati personali (Handbook on Handling Personal Data Breach) di cui ogni organizzazione dovrebbe munirsi oltre ad aggiornare la casistica nelle ultime Linee Guida adottate.

Il manuale rappresenta, del resto, una procedura interna dove il titolare di trattamento fornisce e stabilisce le indicazioni operative per registrare, valutare i rischi derivanti dalle violazioni di dati personali nonché per operare le modalità operative per gestire i processi di notifica all'autorità di controllo e di comunicazione agli interessati coinvolti ove necessarie.

E', in ogni caso, importante sottolineare come il manuale non dovrebbe limitarsi alle mere indicazioni dell'EDPB, ma dovrebbe contenere anche altre informazioni utili, anche sulla base del settore di riferimento, a gestire le violazioni.

Ad esempio, il designato aziendale con l'ausilio del DPO potrebbero inserire anche casistiche specifiche tipiche del settore oppure precedenti violazioni subite e già affrontate al fine di prevenire ulteriormente il rischio del loro verificarsi o ripetersi e anche prevedere un piano di azione per affrontare e gestire nuove minacce.

L'implementazione del "Manuale sulla gestione della violazione dei dati personali" all'interno del Modello Organizzativo per la Protezione dei Dati consente di definire ruoli e responsabilità e permette una più rapida gestione di ogni incidente e rappresenta una pietra cardine all'interno del sistema di compliance al GDPR.

Inoltre, è bene precisare come l'organizzazione non dovrebbe munirsi di questo manuale dopo aver subito la violazione, bensì prima.

La preparazione anticipata di questo manuale rappresenta, infatti, una fonte di informazioni molto più rapida per consentire alle organizzazioni di mitigare i rischi e ottemperare agli obblighi di Legge senza indebito ritardo[15].

CamminoDiritto.it
ISSN 2532-9871

L'adozione del manuale, lungi dall'essere una novità per gli interpreti e operatori della materia, rappresenta un'applicazione pratica ed operativa del principio di accountability e di data protection by design.

Ogni organizzazione, pertanto, dovrebbe valutare di adottare questo manuale oppure di aggiornarlo.

CamminoDiritto.it
ISSN 2532-9871

Note e riferimenti bibliografici

[1] V. WP213, 25 March 2014, Opinion 03/2014 on Personal Data Breach Notification, p. 5, {https/URL}

[2] Il Gruppo di Lavoro nelle linee guida citate alla nota 1 scrive quanto segue: "Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del titolare del trattamento. Un altro esempio può essere il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un ransomware (malware del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso".

[3] Cons. 86 GDPR.

[4] V. Cesare Gallotti; "Sicurezza delle informazioni - Edizione 2022 Gestione del rischio I sistemi di gestione per la sicurezza delle informazioni La norma ISO/IEC 27001:2022 I controlli della ISO/IEC 27002:2022" pag. 1.

[5] Clusit è l'Associazione Italiana per la Sicurezza Informatica. Nata nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, rappresenta oggi oltre 600 organizzazioni, appartenenti a tutti i settori del Sistema-Paese. Clusit collabora con la Presidenza del Consiglio, con diversi Ministeri, Authority, Istituzioni e organismi di controllo, tra cui Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali.

[6] V. comunicato stampa Rapporto Clusit ottobre 2022 disponibile in {https/URL}

[7] G29 WP250 rev.1, 6 February 2018, Guidelines on Personal data breach notification under Regulation 2016/679 - endorsed by the EDPB, {https/URL}

[8] V. Giacomo Conti, "La tenuta dei registri: consapevolezza, accountability, substance over form e documentazione delle scelte. Sintesi della relazione dell'Avv. Giacomo Conti all'evento summer meeting GDPR Italia – Operatori e Consulenti. Milano in data 29 giugno 2018 – aggiornata in data 9 ottobre 2018 all'esito dei chiarimenti forniti dall'Autorita' Garante per la protezione dei dati personali)"; Ed. Il Foro Padano – Rivista di giurisprudenza e di dottrina – Fabrizio Serra Editore, Pisa – Roma – N. Rivista 1/2019.

[9] V. Pag 25 G29 WP250 rev.1, 6 February 2018, Guidelines on Personal data breach notification under Regulation 2016/679 - endorsed by the EDPB, {https/URL}

[10] V. pag. 20 Linee Guida 2017 WP29 dove viene spiegato che "nel caso in cui dati personali, quali password, siano stati codificati in modo sicuro con un hash e un salt, il valore hash sia stato calcolato con una funzione di hash con chiave crittografica all'avanguardia, la chiave utilizzata per l'hashing dei dati non sia stata compromessa nell'ambito di una violazione della sicurezza e sia stata generata in maniera tale da non poter essere individuata con i mezzi tecnologici a disposizione di qualcuno che non è autorizzato ad accedervi".

[11] V. sul punto il documento NIST SP800-53rev4, che definisce la "disponibilità" come la "garanzia di un accesso e un uso tempestivi e affidabili delle informazioni", disponibile all'indirizzo {https/URL}://{https/URL}#160;Anche la norma ISO/IEC 27000:2016 definisce la "disponibilità" come la "proprietà di essere accessibile e utilizzabile su richiesta da un soggetto autorizzato": {https/URL}#iso:std:iso-iec:27000:ed-4:v1:en

[12] G29 WP250 rev.1, 6 February 2018, Guidelines on Personal data breach notification under Regulation 2016/679 - endorsed by the EDPB, {https/URL}

[13] Cfr. Art. 86 GDPR

[14] G29 WP250 rev.1, 6 February 2018, Guidelines on Personal data breach notification under Regulation 2016/679 - endorsed by the EDPB, {https/URL}

[15] V. Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on 14 January 2021 Version 1.0 pag. 6 "People in the organisation would know what to do, and the incident would more than likely be handled

CamminoDiritto.it
ISSN 2532-9871

quicker than if there were no mitigations or plan in place".

---

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=9241