ISTITUTO COMPRENSIVO STATALE ALTOPASCIO – LUCCA
Piazza D. Alighieri,1 Tel. 0583/25268-25817-216502
c.f. 80003820463 email LUIC84000P@istruzione.it
www.icaltopascio.edu.it

PROCEDURA DI GESTIONE DEL *DATA BREACH*

Originale	Il Titolare del trattamento
Revisione n. 1	

Sommario

1. PREMESSA

La violazione dei dati personali (*Data Breach*) è "***la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati***" dal Titolare del trattamento.

A norma dell'art. 33 del Regolamento Europeo 2016/679 (di seguito GDPR), ogni violazione di sicurezza, come sopra descritta, **deve essere notificata all'Autorità Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore, dal momento in cui si è venuti a conoscenza della violazione**. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, la stessa deve essere corredata dai motivi del ritardo. **La notifica al Garante non è necessaria quando sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**.

Il considerando 85 del G.D.P.R. chiarisce che lo scopo della notifica è quello di limitare i danni che possono derivare da una violazione a carico degli interessati e che l'efficacia di questa limitazione dipende dalla tempestività e dall'adeguatezza con cui la violazione è affrontata. E' importante quindi che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

Mentre l'obbligo di notifica sorge, in ogni caso, a fronte di una violazione di dati personali che sia suscettibile di presentare un rischio probabile per i diritti e le libertà delle persone fisiche, il dovere di comunicazione all'interessato emerge solo qualora tale rischio sia elevato.

Infatti, ai sensi dell'art.34 del GDPR, **quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento deve comunicare la violazione all'interessato senza ingiustificato ritardo**.

In altre parole, nel caso in cui dal data breach possa derivare un ingente pericolo per i diritti e le libertà delle persone interessate dal trattamento, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Non è richiesta la comunicazione all'interessato se:

a) sono state messe in atto tutte le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) la comunicazione richiederebbe sforzi sproporzionati: in tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui il titolare del trattamento ricorra ad un Responsabile del trattamento e sia quest'ultimo a venire a conoscenza di una violazione dei dati personali che sta trattando per conto del titolare, deve notificarla al titolare del trattamento senza ingiustificato ritardo.

In questa ipotesi il Responsabile del trattamento dovrà soltanto verificare se sia avvenuta una violazione e notificarla al Titolare del trattamento, sarà quest'ultimo che dovrà valutare la probabilità del rischio sui diritti e le libertà delle persone fisiche.

Per la omessa notifica di Data Breach all'Autorità di Controllo o per l'omessa comunicazione agli interessati o per entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, sono previste pesanti sanzioni amministrative (art. 83 GDPR), il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato totale annuo dell'esercizio precedente, se superiore, nonché le misure correttive di cui all'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati).

E' pertanto di fondamentale importanza rispettare la procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali, potendo così adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonchè danni economici per l'istituto stesso.

1.1 Momento dal quale decorrono le 72 ore per la notifica della violazione al Garante della protezione dei dati personali

L'obbligo di notifica sorge in concreto nel momento in cui il Titolare del trattamento diventa "consapevole" del data breach.

Un Titolare o un Responsabile del trattamento può considerarsi "*a conoscenza*" della violazione quando abbia conseguito un "*ragionevole grado di certezza che la violazione si sia verificata*" e che abbia causato una compromissione di dati personali.

Le linee guida EDPB 09/2022 versione 2.0 ha indicato, a titolo esemplificativo, una serie di "*situazioni-tipo*" reputate idonee a far cogliere con maggiore chiarezza i momenti di conoscenza di eventuali violazioni nella prassi.

Il Titolare e/o il Responsabile del trattamento può considerarsi "*a conoscenza*" della violazione nel caso in cui:

a) abbia ricevuto una e-mail da un utente che lo abbia avvisato di essere stato contattato da un soggetto terzo che impersonava il Titolare e che possa verosimilmente aver avuto accesso ai dati dell'organizzazione del Titolare medesimo.
Sia stata condotta una rapida indagine in grado di suffragare la segnalazione dell'utente, attraverso l'acquisizione di prove puntuali di un'intromissione nel sistema.

b) un terzo lo informi di aver ricevuto da suoi dipendenti/operatori, per errore, una comunicazione contenente i dati personali di altri utenti e fornisca la prova dell'intervenuta divulgazione non autorizzata (in tal caso, dal momento che il Titolare del trattamento è stato reso edotto, anche attraverso il supporto di prove evidenti, di una violazione della riservatezza, non possono sussistere dubbi circa il fatto che la stessa si sia verificata e che il Titolare stesso ne sia venuto a conoscenza).

c) in caso di smarrimento di una chiavetta USB contenente dati personali non criptati gestiti dall'organizzazione del Titolare (in tale evenienza, infatti, non essendo effettivamente possibile constatare con assoluta certezza se persone non autorizzate abbiano avuto o meno accesso a tali dati, si deve presumere un accesso non autorizzato possa essersi determinato).

Il momento esatto "di presa coscienza" da parte del Titolare e/o del Responsabile può quindi variare in base alle circostanze.

La conoscenza dovrà considerarsi immediata in tutti quei casi in cui il Titolare del trattamento dati sia stato informato di una violazione, tramite segnalazione documentata di un terzo, ovvero abbia rilevato, direttamente e/o per il tramite del Responsabile del trattamento eventualmente designato, l'evento.

Diversamente, potrebbero ricorrere situazioni in cui la consapevolezza/conoscenza della violazione non possa dirsi immediata, rendendosi necessario l'espletamento di apposite indagini volte ad appurare se il *data breach* abbia effettivamente avuto luogo.

In tali evenienze, secondo quanto affermato dall'EDPB, il Titolare del trattamento non può considerarsi pienamente "consapevole" *ab origine*. È, tuttavia, necessario che, in siffatte ipotesi, le indagini iniziali vengano avviate dal Titolare quanto prima e siano il più possibile dettagliate per permettere di stabilire rapidamente e con un ragionevole grado di certezza la sussistenza e la gravità della violazione.

2. NORMATIVA E DOCUMENTI DI RIFERIMENTO

➢ Regolamento UE 2016/679, considerando n. 85, 86, 87, 88, artt. 33, 34;

➢ Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) ai sensi del Regolamento 679/2016 (WP250) adottate dal Gruppo di lavoro art.29 (WP29), il 3/10/2017, versione emendata e adottata il 06/02/2018;

➢ Linee guida EDPB 01/2021 sugli esempi riguardanti la notifica di violazione dei dati;

➢ Linee guida EDPB 09/2022 sulla gestione e la notifica della violazione di dati personali;

➢ Best practices di settore sviluppatesi alla luce del Codice Privacy (D.Lgs.196/2003), del Regolamento Europeo 2016/679 e della giurisprudenza del Garante.

3. FINALITÀ

La finalità di questa procedura organizzativa interna è quella di fornire delle indicazioni pratiche ed operative, individuando la metodologia che consenta la gestione delle violazioni dei dati personali trattati dall'istituto in qualità di Titolare del trattamento.

4. DATI PERSONALI OGGETTO DELLA PROCEDURA DI DATA BREACH

I dati oggetto della procedura di data breach sono i dati personali trattati dal Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo.

Un **dato personale** è "*qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale, o sociale"* (art. 4 n. 1 del G.D.P.R. e art. 2, comma 1, lett. a), del D.Lgs 51/2018.
Sono quindi dati personali tutte quelle informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..
L'identificazione richiede elementi che permettono di distinguere una persona dalle altre. Il nome e il cognome, ad esempio, permettono di identificare una persona direttamente, mentre dati personali come il numero di telefono, il codice fiscale, l'indirizzo IP, la targa di un veicolo permettono di identificare una persona indirettamente.

In particolare, i dati personali si distinguono nelle seguenti categorie:
• **dati "comuni"** come i dati anagrafici (nome, cognome, data di nascita, luogo di nascita), i dati di contatto (indirizzo postale, indirizzo di posta elettronica, numero di telefono fisso o mobile), dati di accesso e di identificazione (*username, password*), dati di geolocalizzazione, dati di pagamento, le immagini, il codice fiscale, l'indirizzo IP, ecc;
• **dati rientranti in categorie particolari:** si tratta dei "*dati che rivelino l'origine razziale od etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale di una persona"* (art.9 GDPR);
• **dati relativi a condanne penali e reati**: si tratta dei dati c.d. *"giudiziari"*, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario o la qualità di imputato o di indagato. Sono compresi in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza (articolo 10 GDPR).

5. CLASSIFICAZIONE DEL DATA BREACH

Nel suo parere 03/2014 sulla notifica delle violazioni e nelle Linee-guida WP 250, il WP29 (Gruppo di lavoro ex art. 29) ha spiegato che le violazioni possono essere classificate in base ai seguenti tre noti principi di sicurezza delle informazioni:
➢ **Violazione della riservatezza:** in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali, come ad esempio:

• quando nella redazione di un atto non si rediga la versione con omissione dei dati da non pubblicare e l'atto viene pubblicato nella sua interezza;
• quando si inoltrano messaggi contenenti dati personali a soggetti non interessati al trattamento;
• quando un operatore abbandona la propria postazione di lavoro senza prima prendere le opportune precauzioni (riporre la documentazione, chiudere la sessione di lavoro sul gestionale utilizzato, ecc..) e terze persone prendano visione di informazioni;
• quando un soggetto in malafede comunichi dei dati non pubblici a terzi in modo non autorizzato.
➢ **Violazione dell'integrità:** in caso di alterazione non autorizzata o accidentale dei dati personali. L'alterazione è la situazione in cui i dati sono danneggiati, corrotti o non più completi. L'alterazione non autorizzata può essere la conseguenza di un attacco esterno o di una manipolazione inconsapevole da parte di personale non competente. Un'alterazione accidentale si può verificare per errore umano (ad es. nel momento di un aggiornamento delle informazioni) o per un disguido tecnico quando all'interno di una base dati si perdono i collegamenti a determinate informazioni (integrità referenziale);
➢ **Violazione della disponibilità:** in caso di perdita, accesso o distruzione di dati personali, accidentale o non autorizzata.
La "perdita di dati" è la situazione in cui i dati, presumibilmente, esistono ancora, ma il titolare ne ha perso il controllo o la possibilità di accedervi; la "distruzione" dei dati personali è la condizione in cui i dati non esistono più o non esistono più in un formato che sia utilizzabile dal titolare del trattamento.

La violazione dei dati può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione di documenti con dati personali (furto, etc.).

A seconda delle circostanze, una violazione può riguardare anche tutti gli aspetti sopra indicati o una combinazione di essi.
A titolo esemplificativo, l'oggetto della segnalazione di un data breach può essere:
➢ perdita della chiave di decriptazione;
➢ interruzione significativa di un servizio ("black out" elettrico o attacchi di tipo "denial of service");
➢ l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc;
➢ divulgazione non autorizzata dei dati personali;
➢ infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia e la distribuisce in ambiente pubblico);
➢ perdita o il furto di dati o di strumenti nei quali i dati sono memorizzati;
➢ perdita o il furto di documenti cartacei;
➢ perdita o distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
➢ banche dati alterate o distrutte senza autorizzazione;
➢ violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
➢ smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
➢ invio di e-mail contenenti dati personali e/o particolari ad erroneo destinatario.

6. EFFETTI DELLA VIOLAZIONE SULLE PERSONE FISICHE

Una violazione dei dati può avere potenzialmente effetti negativi significativi sulle persone fisiche che possono causare danni fisici, materiali o immateriali. Il G.D.P.R. spiega che ciò può includere la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari), nonché qualsiasi altro danno economico o sociale significativo per le persone fisiche interessate.

7. DESTINATARI DELLA PROCEDURA DI GESTIONE DEL DATA BREACH

La presente procedura interna è obbligatoria per tutti gli autorizzati al trattamento: lavoratori dipendenti e terzi non dipendenti che hanno accesso ai dati personali trattati nel corso della propria attività lavorativa presso l'istituto.
La mancata conformità alle regole di comportamento previste dalla stessa può comportare provvedimenti disciplinari a carico dei dipendenti inadempienti o la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

8. PROCEDURA DATA BREACH

Di seguito sono illustrate le fasi della procedura del data breach.

8.1 ACQUISIZIONE DEL DATA BREACH (rilevazione evento, segnalazione, raccolta informazioni).

Ogni Autorizzato al trattamento, qualora venga a conoscenza della concreta, sospetta e/o avvenuta violazione dei dati personali, la segnala immediatamente al Titolare del trattamento, al Responsabile Privacy se previsto, al DPO se nominato e, qualora si tratti di una violazione informatica, ad altre eventuali figure che gestiscono i sistemi informatici o che forniscono servizi di assistenza e consulenza informatica in modo da garantire la massima tempestività di intervento.

8.2 GESTIONE TECNICA (raccolta informazioni, definizione eventuali azioni correttive)

Il Titolare, unitamente al DPO, al Referente privacy ed alle figure che gestiscono i sistemi informatici, dovrà avviare tempestivamente una prima indagine interna. In particolare dovranno essere messe in atto le azioni correttive necessarie per gestire tecnicamente la violazione e per ripristinare, se del caso, la disponibilità e l'accesso dei dati personali (ad es. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso ecc.).
Dovranno anche essere desunte informazioni circa la natura dell'incidente occorso, le misure preventive poste in essere per evitarlo, le misure adottate per minimizzarne le conseguenze.

8.3 VALUTAZIONE DEL RISCHIO A SEGUITO DI DATA BREACH

Il Titolare, con l'ausilio dei soggetti sopra individuati, effettua una valutazione del rischio a seguito del data breach. Se necessario si avvarrà di eventuali altri professionisti per la corretta analisi della situazione.

8.3.1 METODOLOGIA PER LA VALUTAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Il modello di riferimento da adottare per la valutazione del rischio per le persone fisiche derivante da una violazione dei dati personali è quello elaborato da ENISA.
Secondo questo modello, gli elementi centrali che devono essere presi in considerazione quando si valuta la **gravità di una violazione di dati personali**, sono:

- **Contesto del trattamento e tipologia di dati**
- **Facilità di identificazione dell'individuo** sulla base dei dati violati
- **Circostanze della violazione** (che hanno ulteriore influenza sulla gravità della violazione)

Contesto del trattamento

Al fine di definire un punteggio al parametro relativo al **contesto del trattamento**, è attribuito un punteggio di base utilizzando come criterio la tipologia dei dati violati, adeguando poi il punteggio base analizzando altri fattori di contesto.

- È necessario individuare il tipo di dati personali violati e poi classificarli in una delle quattro tipologie previste:
  - **comuni;**
  - **comportamentali;**
  - **finanziari;**
  - **sensibili.**

- Adeguare il punteggio base (aumentandolo o diminuendolo) nel caso sussistano alcuni fattori di contesto (volume dei dati, caratteristiche speciali dei titolari o delle persone fisiche, invalidità/inesattezza dei dati, disponibilità pubblica (prima della violazione), natura dei dati come da seguente Tabella 1).

Tabella 1: Fattori di contesto		
Dati comuni	**Per esempio: dati anagrafici, recapiti, nome e cognome, dati sull'istruzione, sulla vita familiare, sull'esperienza professionale, ecc**.	
	Punteggio **base** preliminare: quando la violazione riguarda "dati semplici" e il titolare non è a conoscenza di eventuali aggravanti.	1
	Il punteggio base potrebbe essere **aumentato** di 1, ad es. quando il volume dei "dati semplici" e/o le caratteristiche del titolare del trattamento sono tali da consentire la profilazione dell'interessato o l'assunzione di ipotesi sullo stato socio-economico dell'interessato.	2
	Il punteggio base potrebbe essere **aumentato** di 2, ad es. quando i "dati semplici" e/o le caratteristiche del titolare possono indurre a supporre lo stato di salute, le preferenze sessuali, le convinzioni politiche o religiose dell'interessato.	3
	Il punteggio base potrebbe essere **aumentato** di 3, ad es. quando a causa di determinate caratteristiche dell'individuo (es. gruppi vulnerabili, minori), le informazioni possono essere critiche per la sua sicurezza personale o per le sue condizioni fisiche/psicologiche.	4
Dati comportamentali	**Per esempio: posizione, dati sul traffico, dati su preferenze e abitudini personali, ecc.**	
	Punteggio **base** preliminare: quando la violazione coinvolge "dati comportamentali" e il titolare non è a conoscenza di fattori aggravanti o attenuanti	2
	Il punteggio base potrebbe essere **ridotto** di 1, ad es. quando la natura del set di dati non fornisce alcuna visione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili al pubblico (ad es. combinazione di informazioni da ricerche web).	1
	Il punteggio base può essere **aumentato** di 1, ad es. quando il volume dei "dati comportamentali" e/o le caratteristiche del titolare del trattamento sono tali da consentire la creazione di un profilo dell'individuo, esponendo informazioni dettagliate sulla sua quotidianità e abitudini.	3
	Il punteggio base può essere **aumentato** di 2, ad es. se è possibile creare un profilo basato sui dati sensibili dell'individuo.	4
Dati Finanziari	**Qualsiasi tipo di dato finanziario (es. entrate, transazioni finanziarie, estratti conto bancari, investimenti, carte di credito, fatture, ecc.). Include i dati di assistenza sociale relativi alle informazioni finanziarie**.	
	Punteggio **base** preliminare: quando la violazione coinvolge "dati finanziari" e il titolare non è a conoscenza di fattori aggravanti o attenuanti.	3
	Il punteggio base potrebbe essere **ridotto** di 2, ad es. quando la natura del set di dati non fornisce informazioni sostanziali sulle informazioni finanziarie dell'individuo (ad esempio, il fatto che una persona sia cliente di una determinata banca senza ulteriori dettagli).	1
	Il punteggio base potrebbe essere **ridotto** di 1, ad es. quando il set di dati specifico include alcune informazioni finanziarie ma non fornisce ancora alcuna informazione significativa sulla situazione/situazione finanziaria dell'individuo (ad es. semplici numeri di conto bancario senza ulteriori dettagli).	2

	Il punteggio base potrebbe essere **aumentato** di 1, ad es. quando, a causa della natura e/o del volume del set di dati specifico, vengono divulgate informazioni finanziarie complete (ad es. carta di credito) che potrebbero consentire frodi o viene creato un profilo sociale/finanziario dettagliato	4
Dati sensibili	**Qualsiasi tipo di dato sensibile (es. salute, appartenenza politica, vita sessuale)**	
	Punteggio **base** preliminare: quando la violazione coinvolge "dati sensibili" e il titolare non è a conoscenza di fattori attenuanti.	4
	Il punteggio base potrebbe essere **ridotto** di 3, ad es. quando la natura del set di dati non fornisce alcuna visione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili al pubblico (ad es. combinazione di informazioni da ricerche web).	1
	Il punteggio base potrebbe essere **ridotto** di 2, ad es. quando la natura dei dati può portare a ipotesi generali.	2
	Il punteggio base potrebbe essere **ridotto** di 1, ad es. quando la natura dei dati può portare a ipotesi su informazioni sensibili.	3

Se i dati corrispondono a più di una categoria, i passaggi sopra indicati devono essere seguiti per ciascuna categoria applicabile. In questi casi **il valore da utilizzare per il calcolo complessivo della gravità sarà il punteggio più alto raggiunto.**

Facilità di identificazione

La **facilità di identificazione** valuta quanto sarà facile per un soggetto che ha accesso ai dati abbinarli univocamente a una determinata persona.
Sono previsti quattro livelli di identificabilità (trascurabile, limitato, significativo, massimo), il cui valore sarà utilizzato come moltiplicatore sul punteggio del contesto del trattamento.
Il punteggio più basso viene assegnato quando la possibilità di identificare l'individuo è trascurabile, il che significa che è estremamente difficile abbinare i dati a una determinata persona, ma potrebbe comunque essere possibile a determinate condizioni. Il punteggio più alto viene selezionato quando l'identificazione è possibile direttamente dai dati violati senza che siano necessarie ricerche speciali per scoprire l'identità dell'individuo.

Facilità di identificazione	
Livello di identificabilità	*Moltiplicatore*
Trascurabile	0,25
Limitato	0,5
Significativo	0,75
Massimo	1

Circostanze della violazione

Gli elementi che sono considerati nelle **circostanze della violazione** sono la perdita di sicurezza (riservatezza, integrità, disponibilità) e gli intenti dolosi:

Perdita di riservatezza: la perdita di riservatezza si verifica quando accedono alle informazioni soggetti che non sono autorizzati o che non hanno uno scopo legittimo per accedervi. L'entità della perdita di riservatezza varia in base al potenziale numero e tipo di soggetti che potrebbero avere accesso illegale alle informazioni.

Perdita di integrità: la perdita di integrità si verifica quando le informazioni originali vengono alterate e la sostituzione dei dati può essere pregiudizievole per l'individuo. La situazione più grave si verifica quando vi sono serie possibilità che i dati alterati siano stati utilizzati in un modo che potrebbero danneggiare l'individuo.

Perdita di disponibilità: la perdita di disponibilità si verifica quando non è possibile accedere ai dati originali quando ce n'è bisogno. Può essere temporanea (i dati sono recuperabili ma ci vorrà un periodo di tempo e questo può essere dannoso per l'individuo) o permanente (i dati non possono essere recuperati).

Intento doloso: questo elemento esamina se la violazione è stata causata da un errore, umano o tecnico, o se è stata causata da un'azione intenzionale. Le violazioni non dolose includono casi di perdita accidentale, smaltimento inadeguato, errore umano e bug del software o errata configurazione. Le violazioni dolose includono casi di furto e pirateria informatica volti a danneggiare le persone (ad esempio esponendo i loro dati personali a terzi non autorizzati). In altri casi l'intento doloso potrebbe includere il trasferimento di dati personali a terzi a scopo di lucro (ad esempio la vendita di elenchi di dati personali). In alcuni casi l'intento doloso potrebbe anche essere dedotto da azioni volte a danneggiare il titolare del trattamento (ad esempio attraverso il furto e l'esposizione dei dati personali a soggetti non autorizzati). L'intento doloso è un fattore che aumenta la probabilità che i dati vengano utilizzati in modo dannoso, poiché questo era lo scopo iniziale della violazione.

Circostanze della violazione	
Circostanza	*Correzione*
Perdita di riservatezza	da +0 a 0,50
Perdita di integrità	da +0 a 0,50
Perdita di disponibilità	da +0 a 0,50
Intenzioni malevole	+0,50

Per quanto riguarda il punteggio delle circostanze di violazione **i punti ottenuti per ciascun elemento** "circostanze della violazione" **sono sommati per ottenere il punteggio finale**, poiché nella stessa violazione possono verificarsi circostanze diverse.

Calcolo della gravità di una violazione

Utilizzando tutti gli elementi sopra indicati, si calcola la gravità di una violazione di dati personali attraverso la formula **Gravità = (Contesto x Facilità di identificazione) + Circostanze.**

Il risultato ottenuto sarà valutato secondo quanto riportato nella seguente tabella.

GRAVITÀ	RISCHIO	DESCRIZIONE
Minore di 2	Basso	Gli interessati non incontreranno inconvenienti o potrebbero incontrare alcuni inconvenienti che supereranno senza alcun problema (tempo passato a reinserire informazioni, fastidio, irritazione, ecc.)
Compreso tra 2 e 3	Medio	Gli interessati potranno incontrare inconvenienti significativi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici lievi, ecc.)
Compreso tra 3 e 4	Alto	Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione, peggioramento della salute, ecc.)
Maggiore di 4	Molto alto	Gli interessati possono incontrare conseguenze significative o addirittura irreversibili che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità al lavoro, disturbi psicologici a lungo termine o disturbi fisici, morte, ecc.)

Una volta definito il livello di gravità, vanno considerati alcuni "fattori" che, pur non incidendo a priori sul punteggio, sono rilevanti ai fini della valutazione finale. Ai fini della metodologia sono stati considerati due fattori:

Il <u>numero di individui violati supera i 100</u>. I dati di un individuo, violato nel contesto di un incidente più grande, possono potenzialmente essere divulgati più facilmente, mentre allo stesso tempo un numero elevato di individui interessati influenza la portata complessiva della violazione.

<u>Dati incomprensibili</u>. L'incomprensibilità (ad esempio sotto forma di crittografia forte e senza compromissione della chiave) può ridurre sostanzialmente l'impatto sulle persone, poiché riduce notevolmente la possibilità che parti non autorizzate accedano ai dati.

8.3.2 ADEMPIMENTI SUCCESSIVI ALLA VALUTAZIONE DEL RISCHIO A SEGUITO DI DATA BREACH

Si procede alla notifica del data breach al Garante e/o agli interessati come indicato dalla seguente tabella:

	DESCRIZIONE	NOTIFICA AL GARANTE	COMUNICAZIONE AGLI INTERESSATI	REGISTRAZIONE SUL REGISTRO DELLE VIOLAZIONI
RISCHIO	BASSO	NO	NO	SI
	MEDIO	SI	NO	SI
	ALTO	SI	SI	SI
	MOLTO ALTO	SI	SI	SI

Nel caso in cui si constati <u>l'assenza di rischi</u>, il Titolare del trattamento o il Referente privacy, se previsto, è tenuto a **registrare la violazione sul registro delle violazioni**, annotando le motivazioni che hanno portato a non notificare l'evento al Garante Privacy (vedi punto 8.6).

Nel caso sia necessario eseguire la notifica al Garante e la comunicazione agli interessati si proceda secondo quanto indicato rispettivamente al punto 8.4 al punto 8.5.

8.4 NOTIFICA AL GARANTE

All'esito della valutazione, qualora si sia ritenuto probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento, con l'ausilio del DPO e degli altri soggetti coinvolti, procede alla notifica all'Autorità Garante mediante l'apposita procedura telematica resa disponibile nel portale dei servizi online dell'Autorità pubblicato all'indirizzo "https://servizi.gpdp.it/".

La notifica deve avere il contenuto previsto dall'art. 33 del GDPR e pertanto deve:

1. descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie ed il numero approssimativo di registrazioni dei dati personali in questione;

2. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

3. descrivere le probabili conseguenze della violazione dei dati personali;

4. descrivere 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.

Per verificare di essere in possesso di tutte le informazioni necessarie per procedere alla notifica del data breach si veda l'allegato 1) del presente documento (fac-simile Data Breach).

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in <u>fasi successive</u> senza ulteriore ingiustificato ritardo.

Nel caso in cui si debba effettuare una <u>notifica per fasi</u> il Titolare del trattamento dovrà eseguire una prima e rapida notifica di *alert* all'Autorità Garante (avendo cura di informare l'Autorità che la notifica ha un contenuto

soltanto parziale) e successivamente dovrà comunicare tutte le informazioni aggiuntive acquisite attraverso l'invio di successive notifiche integrative.

Nel caso in cui la notifica all'Autorità Garante avvenga oltre il termine delle 72 ore, la notifica deve essere corredata anche delle ragioni del ritardo.

È opportuno precisare che se, dopo aver completato le attività di notifica, una successiva indagine dimostri che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione, il Titolare del trattamento può informarne l'autorità di controllo. Tali informazioni possono quindi essere aggiunte alle informazioni già fornite all'autorità di controllo e l'incidente può essere quindi registrato come un evento che non costituisce una violazione (o falso positivo). Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione.

Nel caso in cui si verifichino violazioni ripetute, ravvicinate e di natura simile che interessano un numero elevato di soggetti è possibile eseguire un'unica "notifica aggregata" di tutte le violazioni occorse nel breve periodo di tempo (anche se superi le 72 ore), purché la notifica motivi le ragioni del ritardo.

Per maggiori informazioni sulla procedura telematica da seguire per la comunicazione al Garante del data breach si veda l'allegato 2) del presente documento ("istruzioni per la procedura telematica di notifica").

8.5 COMUNICAZIONE AGLI INTERESSATI

Nel caso in cui si valuti che il *data breach* presenti un elevato rischio per i diritti e le libertà delle persone fisiche, occorre effettuare la comunicazione agli interessati della predetta violazione dei dati, da inviarsi nei tempi e nei modi più opportuni come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

In tal caso, nella eventuale comunicazione si dovranno indicare i seguenti dati:
a) la natura della violazione dei dati personali, descritta con linguaggio semplice e chiaro;
b) il nome e i dati di contatto del D.P.O. o di altro punto di contatto presso cui ottenere più informazioni;
c) le probabili conseguenze della violazione dei dati personali;
d) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e, se del caso, per attenuarne i possibili effetti negativi (ivi inclusi i consigli agli individui interessati per mitigare gli effetti della violazione, come ad es. un rapido aggiornamento delle credenziali).

Nel comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard.
Ciò contribuisce a rendere la comunicazione della violazione chiara e trasparente.
Esempi di metodi trasparenti di comunicazione sono: la messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto), banner o notifiche su siti web di primo piano, comunicazioni postali e pubblicità di rilievo sulla stampa. Una semplice comunicazione all'interno di un comunicato stampa o di un blog aziendale non costituirebbe un mezzo efficace per comunicare una violazione all'interessato.
Il titolare del trattamento deve scegliere un mezzo che massimizzi la possibilità di comunicare correttamente le informazioni a tutte le persone interessate. A seconda delle circostanze, ciò potrebbe significare che il titolare del trattamento dovrebbe utilizzare diversi metodi di comunicazione, anziché un singolo canale di contatto.
Inoltre il titolare del trattamento potrebbe dover garantire che la comunicazione sia accessibile in formati alternativi appropriati e lingue pertinenti al fine di assicurarsi che le persone fisiche siano in grado di comprendere le informazioni fornite loro. Ad esempio, nel comunicare una violazione a una persona, sarà di norma appropriata la lingua utilizzata durante il precedente normale corso degli scambi commerciali con il destinatario.
Tuttavia, se la violazione riguarda interessati con i quali il titolare del trattamento non ha precedentemente interagito o, in particolare, interessati che risiedono in un altro Stato membro o in un altro paese non UE diverso da quello nel quale è stabilito il titolare del trattamento, la comunicazione nella lingua nazionale locale potrebbe essere accettabile, tenendo conto della risorsa richiesta. L'obiettivo principale è aiutare gli interessati a comprendere la natura della violazione e le misure che possono adottare per proteggersi.

Il titolare del trattamento è nella posizione migliore per stabilire il canale di contatto più appropriato per comunicare una violazione agli interessati, soprattutto se interagisce frequentemente con i suoi clienti.

Tuttavia, è chiaro che il titolare del trattamento dovrebbe essere cauto nell'usare un canale di contatto compromesso dalla violazione, in quanto tale canale potrebbe essere utilizzato anche da autori di attacchi che si fanno passare per il titolare del trattamento.

8.6 REGISTRAZIONE DELLA VIOLAZIONE

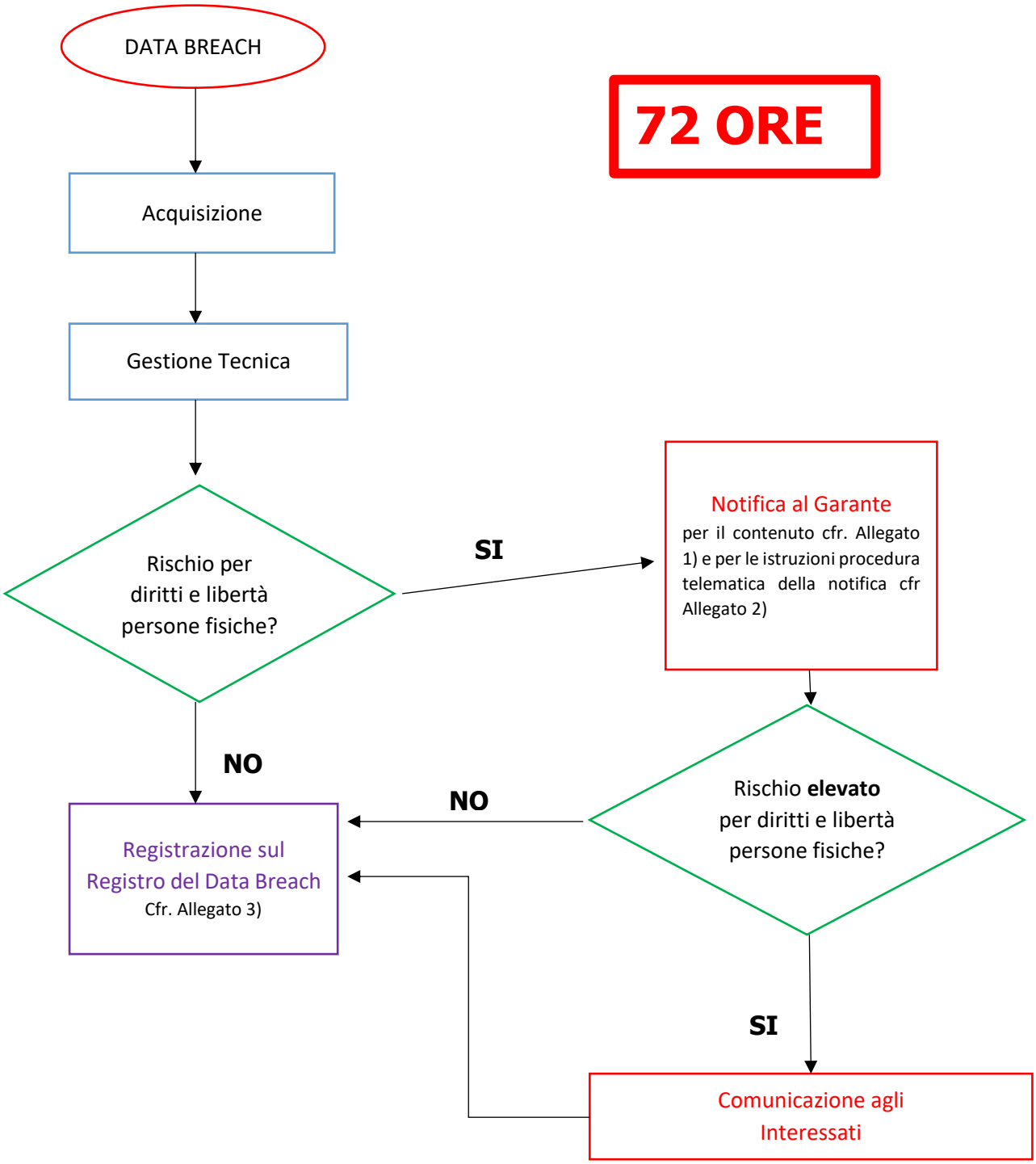
Il Titolare del trattamento o il Referente Privacy, se previsto, in caso di una violazione dei dati, deve procedere alla registrazione del data breach nell'apposito Registro delle violazioni (art.33, comma 5 del GDPR), da compilare secondo quanto indicato nell'allegato 3) del presente documento (Registro del data breach istruzioni), documentando in tal modo qualsiasi violazione dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

La violazione, anche se non notificata al Garante, dovrà comunque essere annotata nel **registro del data breach** annotando i motivi della mancata notifica al Garante Privacy in modo da comprovare la effettiva assenza dei rischi.

8.7 RECEPIMENTO DELLA EVENTUALE RISPOSTA DEL GARANTE

Il Titolare dispone ulteriori indagini o eventuali misure correttive, secondo le disposizioni ricevute dal Garante.

SCHEMA PROCEDURA DATA BREACH



9. ESEMPI RIGUARDANTI LA NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI

Si riportano i casi presentati nelle linee guida 01/2021 adottate il 14.12.2021 dall'EDPB.
Si tratta di casi fittizi che si basano su casi tipici tratti dall'esperienza collettiva delle autorità di controllo in materia di notifiche di violazioni dei dati. Qualsiasi modifica delle circostanze riferite alle fattispecie descritte di seguito può comportare livelli di rischio diversi o più significativi, e quindi rendere necessarie misure diverse o supplementari.
I casi descritti nelle linee guida sono presentati in base a determinate categorie di violazioni (ad esempio "attacchi ransomware"). Alcune misure di mitigazione sono necessarie in tutte le fattispecie appartenenti a una determinata categoria di violazioni. Tali misure non sono necessariamente ripetute in ciascuna analisi riferita a un caso appartenente alla stessa categoria di violazioni.
Per i casi appartenenti alla stessa categoria sono indicate solo le differenze. Pertanto è necessario tenere conto dell'intera casistica riferita alla pertinente categoria di violazione al fine di individuare e distinguere tutte le misure corrette da adottare.

9.1 RANSOMWARE

Una causa frequente di notifica di violazione dei dati è un attacco ransomware subito dal titolare del trattamento. In questi casi un codice malevolo cifra i dati personali e successivamente l'autore dell'attacco chiede al titolare del trattamento un riscatto in cambio della chiave di decifratura. Questo tipo di attacco può di norma essere classificato come una violazione della disponibilità, ma spesso potrebbe comportare anche una violazione della riservatezza.

9.1.1 Caso n. 01: Ransomware in presenza di backup adeguato e senza esfiltrazione

I sistemi informatici di una piccola impresa manifatturiera sono stati esposti a un attacco ransomware e i dati memorizzati in tali sistemi sono stati cifrati. Il titolare ha utilizzato la cifratura dei dati memorizzati (at rest), per cui tutti i dati ai quali ha avuto accesso il ransomware erano conservati in forma cifrata utilizzando un algoritmo di cifratura conforme allo stato dell'arte. La chiave di decifratura non è stata compromessa nell'attacco, ossia l'autore dell'attacco non ha potuto accedervi né utilizzarla indirettamente. Di conseguenza, l'autore dell'attacco ha avuto accesso solo a dati personali cifrati. In particolare, né il sistema di posta elettronica della società né i sistemi clienti utilizzati per accedervi sarebbero stati interessati.
L'impresa si avvale delle competenze di una società esterna di cybersecurity per indagare sull'incidente.
Sono disponibili le registrazioni (log) di tutti i flussi dati in uscita dall'impresa (compresa la posta elettronica in uscita). Dopo aver analizzato i log e i dati raccolti dai sistemi di rilevazione utilizzati dall'impresa, un'indagine interna supportata dalla società esterna di cybersecurity ha stabilito *con certezza* che l'autore del reato si è limitato a cifrare i dati, senza esfiltrarli. I log non mostrano alcun flusso di dati verso l'esterno nell'arco di tempo dell'attacco. I dati personali interessati dalla violazione riguardano i clienti e i dipendenti dell'impresa, per un totale di poche decine di persone. Un backup era prontamente disponibile e i dati sono stati ripristinati poche ore dopo l'attacco. La violazione non ha avuto alcuna conseguenza sull'operatività del titolare del trattamento. Non vi sono stati ritardi nei pagamenti dei dipendenti o nella gestione delle richieste dei clienti.
In questo caso, rispetto alla definizione di "violazione dei dati personali" si sono concretizzati i seguenti elementi: una violazione della sicurezza ha comportato una modifica illecita e l'accesso non autorizzato ai dati personali conservati.

Misure in essere e valutazione del rischio

Come per tutti i rischi posti da attori esterni, la probabilità che un attacco ransomware abbia successo può essere drasticamente ridotta rafforzando la sicurezza dei dati mediante controllo del contesto. La maggior parte di queste violazioni può essere evitata garantendo l'adozione di adeguate misure di sicurezza organizzative, fisiche e tecnologiche. Esempi di tali misure sono la corretta gestione delle patch e l'uso di un adeguato sistema di rilevamento di malware. Disporre di un backup adeguato e separato contribuirà ad attenuare le conseguenze di un eventuale attacco riuscito. Inoltre, un programma di istruzione, formazione e sensibilizzazione dei dipendenti in materia di sicurezza (SETA) contribuirà a prevenire e riconoscere questo tipo di attacco. (Un elenco di misure consigliate è riportato nel punto 9.1.5) Tra tali misure, una delle più importanti è una corretta gestione delle patch che assicuri che i sistemi siano aggiornati e che tutte le vulnerabilità note dei sistemi installati siano state corrette poiché la maggior parte degli attacchi ransomware sfrutta proprio vulnerabilità ben note.
Nel valutare i rischi, il titolare del trattamento dovrebbe indagare sulla violazione e individuare il tipo di codice malevolo per comprendere le possibili conseguenze dell'attacco. Tra i rischi da considerare figura il rischio che i dati siano stati esfiltrati senza lasciare traccia nei log dei sistemi.

In questo esempio, l'attaccante ha avuto accesso ai dati personali ed è stata compromessa la riservatezza del testo cifrato contenente dati personali in forma cifrata. Tuttavia, i dati che potrebbero essere stati esfiltrati non possono essere letti o utilizzati dall'autore dell'attacco, almeno per il momento. La tecnica di cifratura utilizzata dal titolare è conforme allo stato dell'arte. La chiave di decifratura non è stata compromessa e presumibilmente non può essere determinata con altri mezzi. Di conseguenza, i rischi in termini di riservatezza per i diritti e le libertà delle persone fisiche sono ridotti al minimo, salvi i progressi delle tecniche crittografiche che in futuro potrebbero rendere i dati cifrati intelligibili.
Il titolare del trattamento dovrebbe considerare il rischio per le persone fisiche dovuto alla violazione. In questo caso, sembra che i rischi per i diritti e le libertà degli interessati derivino dalla mancanza di disponibilità dei dati personali e che la riservatezza dei dati personali non sia compromessa. In questo esempio, gli effetti negativi della violazione sono stati attenuati in tempi contenuti dopo il verificarsi della violazione stessa.
Disporre di un adeguato regime di backup riduce gli effetti negativi della violazione e in questo caso il titolare del trattamento è stato in grado di avvalersene in modo efficace.
Per quanto riguarda la gravità delle conseguenze per gli interessati, è stato possibile individuare solo conseguenze minori, poiché i dati sono stati ripristinati in poche ore e la violazione non ha avuto conseguenze sull'operatività del titolare del trattamento né effetti significativi sugli interessati (ad esempio pagamenti ai dipendenti o gestione delle richieste dei clienti).

Misure di mitigazione e obblighi

In assenza di un backup, il titolare del trattamento può adottare poche misure per porre rimedio alla perdita di dati personali e i dati devono essere nuovamente raccolti. In questo caso particolare, tuttavia, gli effetti dell'attacco potrebbero essere contenuti efficacemente "ripulendo" tutti i sistemi compromessi dal codice malevolo, correggendo le vulnerabilità e ripristinando i dati interessati entro breve tempo dall'attacco. In assenza di backup, i dati sarebbero andati persi e la gravità può aumentare di pari passo con i rischi o gli impatti per le persone.
La tempestività di un ripristino efficace dei dati utilizzando un backup prontamente disponibile è una variabile fondamentale nell'analisi della violazione. La definizione di una tempistica adeguata per il ripristino di dati compromessi dipende dalle circostanze specifiche della violazione. Il regolamento generale sulla protezione dei dati stabilisce che una violazione dei dati personali deve essere notificata senza ingiustificato ritardo e, ove possibile, entro 72 ore. Si potrebbe pertanto stabilire che in nessun caso è consigliabile superare il termine di 72 ore, ma quando si tratta di casi caratterizzati da un rischio elevato, anche il rispetto di tale termine può risultare insoddisfacente.
In questo caso, grazie a procedure dettagliate per la valutazione d'impatto e la risposta agli incidenti, il titolare del trattamento ha stabilito che era improbabile che la violazione comportasse un rischio per i diritti e le libertà delle persone fisiche; pertanto non è necessaria alcuna comunicazione agli interessati, né la violazione richiede una notifica all'autorità di controllo. Tuttavia, come tutte le violazioni dei dati, è necessario conservarne la documentazione conformemente all'articolo 33, paragrafo 5. La struttura del titolare potrebbe anche necessitare di (o essere successivamente tenuta a effettuare, su disposizione dell'autorità di controllo) aggiornamenti e correzioni delle misure e procedure organizzative e tecniche messe in atto per la gestione della sicurezza dei dati personali e la mitigazione dei rischi. Nell'ambito di tale aggiornamento e revisione, si dovrebbe indagare approfonditamente sulla violazione individuandone le cause e definendo i metodi utilizzati dall'autore dell'attacco al fine di prevenire eventi analoghi in futuro.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	X

9.1.2 Caso n. 02: Ransomware senza un adeguato backup

Uno dei computer utilizzati da un'azienda agricola è stato esposto a un attacco ransomware e i dati sono stati cifrati dall'attaccante. L'impresa si avvale delle competenze di una società esterna di cybersecurity per monitorare la propria rete. Sono disponibili log che tracciano tutti i flussi di dati in uscita dall'impresa (comprese le e-mail in uscita). Dopo aver analizzato i log e i dati raccolti dagli altri sistemi di rilevamento, l'indagine interna condotta con l'ausilio dell'impresa di cybersecurity ha stabilito che l'autore dell'attacco ha soltanto cifrato i dati, senza esfiltrarli. I log non mostrano alcun flusso di dati verso l'esterno nell'arco di tempo dell'attacco. I dati personali interessati dalla violazione riguardano i dipendenti e i clienti dell'impresa, per un totale di poche decine di persone. Non sono state interessate categorie particolari di dati. Non era disponibile alcun backup in formato elettronico. La maggior parte dei dati è stata ripristinata da backup cartacei. Il

ripristino dei dati ha richiesto 5 giorni lavorativi e ha comportato lievi ritardi nella consegna degli ordini ai clienti.

Misure in essere e valutazione del rischio

Il titolare del trattamento avrebbe dovuto adottare le stesse misure di cui al punto 9.1.1 e 9.1.5. La principale differenza rispetto al caso precedente è la mancanza di un backup in formato elettronico e la mancanza di cifratura dei dati memorizzati (at rest). Ciò comporta differenze critiche nelle fasi successive.

Nel valutare i rischi, il titolare del trattamento dovrebbe indagare sul metodo di infiltrazione e individuare la tipologia di codice malevolo per comprendere le possibili conseguenze dell'attacco. In questo esempio il ransomware cifrava i dati personali senza esfiltrarli. Di conseguenza, i rischi per i diritti e le libertà degli interessati sembrano derivare dalla mancanza di disponibilità dei dati personali e la riservatezza dei dati personali non risulterebbe compromessa. Per determinare il rischio è essenziale un esame approfondito dei log dei firewall e delle relative implicazioni. Su richiesta, il titolare del trattamento dovrebbe presentare le risultanze documentate di tali indagini.

Il titolare del trattamento deve tenere presente che, se l'attacco è più sofisticato, il malware è in grado di modificare i file di log e rimuovere le tracce. Pertanto, poiché i log non sono trasmessi o replicati a un server centrale, anche dopo un'indagine approfondita che ha accertato che i dati personali non sono stati esfiltrati dall'attaccante, il titolare del trattamento non può affermare che l'assenza di log dimostri l'assenza di esfiltrazione; ne consegue l'impossibilità di escludere in via assoluta la probabilità di una violazione della riservatezza.

Il titolare del trattamento dovrebbe valutare i rischi di questa violazione se l'attaccante ha avuto accesso ai dati. Nel corso della valutazione del rischio, il titolare dovrebbe tenere conto anche della natura, della sensibilità, del volume e del contesto dei dati personali interessati dalla violazione. In questo caso non sono coinvolte categorie particolari di dati personali e la quantità di dati violati e il numero di interessati colpiti sono ridotti.

La raccolta di informazioni esatte sull'accesso non autorizzato è fondamentale per determinare il livello di rischio e prevenire un nuovo attacco o la prosecuzione di un attacco in corso. Se i dati fossero stati copiati dalla banca dati, ciò sarebbe stato ovviamente un fattore di incremento del rischio. In caso di incertezza circa le specificità dell'accesso illegittimo, si dovrebbe prendere in considerazione lo scenario peggiore e il rischio dovrebbe essere valutato in termini conseguenti.

L'assenza di un backup può essere considerata un fattore di incremento del rischio a seconda della gravità delle conseguenze derivanti per gli interessati dall'indisponibilità dei dati.

Misure di mitigazione e obblighi

In assenza di un backup, sono poche le misure che il titolare del trattamento può adottare per porre rimedio alla perdita di dati personali e i dati devono essere nuovamente raccolti, a meno che sia disponibile un'altra fonte (ad esempio, e-mail di conferma degli ordini). Senza un backup, i dati possono andare persi e la gravità dipenderà dall'impatto per le persone.

Il ripristino dei dati non dovrebbe rivelarsi eccessivamente problematico se i dati sono ancora disponibili su supporto cartaceo; tuttavia, data la mancanza di un backup in formato elettronico , si ritiene necessaria una notifica all'autorità di controllo, in quanto il ripristino dei dati ha richiesto un certo tempo e potrebbe causare ritardi nella consegna degli ordini ai clienti mentre potrebbe risultare impossibile recuperare una notevole quantità di metadati (ad esempio log, marcatura temporale).

La comunicazione agli interessati in merito alla violazione può dipendere anche dal periodo di indisponibilità dei dati personali e dalle difficoltà che ne potrebbero derivare per l'operatività del titolare del trattamento (ad esempio ritardi nel trasferimento dei pagamenti ai dipendenti). Poiché tali ritardi nei pagamenti e nelle consegne possono comportare perdite finanziarie per le persone i cui dati sono stati compromessi, si potrebbe anche sostenere che la violazione comporti un rischio elevato. Inoltre, potrebbe risultare impossibile evitare di informare gli interessati se il loro contributo è necessario per ripristinare i dati cifrati.

Questo caso è un esempio di attacco ransomware con rischi per i diritti e le libertà degli interessati, senza che si raggiunga un rischio elevato. La violazione dovrebbe essere documentata conformemente all'articolo 33, paragrafo 5, e notificata all'autorità di controllo a norma dell'articolo 33, paragrafo 1. La struttura del titolare può anche necessitare di (o ricevere disposizioni dall'autorità di controllo per) aggiornare e correggere le misure e procedure organizzative e tecniche di gestione della sicurezza dei dati personali e di mitigazione dei rischi.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	X

9.1.3 Caso n. 03: Attacco ransomware nei confronti di un ospedale con backup e senza esfiltrazione

Il sistema informativo di un ospedale/centro sanitario è stato esposto a un attacco ransomware e una parte significativa dei dati è stata cifrata dall'attaccante. L'azienda sanitaria si avvale delle competenze di una società esterna di cybersecurity per monitorare la propria rete. Sono disponibili log che tracciano tutti i flussi di dati in uscita dall'azienda (comprese le e-mail in uscita). Dopo aver analizzato i log e i dati raccolti dagli altri sistemi di rilevamento, l'indagine interna svolta con l'ausilio della società di cybersecurity ha stabilito che l'autore dell'attacco ha soltanto cifrato i dati senza esfiltrarli. I log non mostrano alcun flusso di dati verso l'esterno nell'arco di tempo dell'attacco. I dati personali interessati dalla violazione riguardano i dipendenti e i pazienti, complessivamente varie migliaia di persone. I backup erano disponibili in formato elettronico. La maggior parte dei dati è stata ripristinata, ma questa operazione ha richiesto 2 giorni lavorativi, causando notevoli ritardi nelle cure rese ai pazienti con annullamento o rinvio di interventi chirurgici e un abbassamento del livello di servizio a causa dell'indisponibilità dei sistemi.

Misure in essere e valutazione del rischio

Il titolare del trattamento avrebbe dovuto adottare le stesse misure di cui al punto 9.1.1 e 9.1.5. La principale differenza rispetto al caso precedente è l'elevata gravità delle conseguenze per un numero sostanziale di interessati. La quantità di dati violati e il numero di interessati colpiti dalla violazione sono elevati, in quanto gli ospedali generalmente trattano grandi quantità di dati. L'indisponibilità dei dati ha un forte impatto su una parte sostanziale degli interessati. Esiste inoltre un rischio residuo di elevata gravità per la riservatezza dei dati dei pazienti.

La tipologia della violazione, la natura, la sensibilità e il volume dei dati personali interessati dalla violazione sono importanti. Sebbene esistesse un backup per i dati e questi abbiano potuto essere ripristinati in pochi giorni, sussiste un rischio elevato a causa della gravità delle conseguenze per gli interessati derivanti dall'indisponibilità dei dati al momento dell'attacco e nei giorni successivi.

Misure di mitigazione e obblighi

Si ritiene necessaria una notifica all'autorità di controllo, in quanto si tratta di categorie particolari di dati personali e il ripristino dei dati potrebbe richiedere molto tempo, con notevoli ritardi nelle cure dei pazienti.

Comunicare la violazione agli interessati è necessario a causa dell'impatto sui pazienti, anche dopo il ripristino dei dati cifrati. Anche se sono stati criptati dati relativi a tutti i pazienti trattati in ospedale negli ultimi anni, la violazione ha interessato soltanto i dati relativi ai pazienti che dovevano essere sottoposti a terapie in ospedale durante il periodo di indisponibilità del sistema informatico. Il titolare del trattamento dovrebbe comunicare la violazione dei dati direttamente a tali pazienti. L'eccezione di cui all'articolo 34, paragrafo 3, lettera c), può non rendere necessaria la comunicazione diretta agli altri pazienti, alcuni dei quali possono non essere stati ricoverati in ospedale da più di venti anni. In tal caso, si procede invece a una comunicazione pubblica o a una misura analoga, tramite la quale gli interessati sono informati con pari efficacia. In tal caso, l'ospedale dovrebbe rendere pubblico l'attacco ransomware e i suoi effetti.

Questo caso serve da esempio di un attacco ransomware con un rischio elevato per i diritti e le libertà degli interessati. La violazione dovrebbe essere documentata conformemente all'articolo 33, paragrafo 5, notificata all'autorità di controllo in conformità dell'articolo 33, paragrafo 1, e comunicata agli interessati in conformità dell'articolo 34, paragrafo 1. L'azienda sanitaria deve inoltre aggiornare e correggere le misure e procedure organizzative e tecniche di gestione della sicurezza dei dati personali e di mitigazione dei rischi.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

9.1.4 Caso n. 04: Attacco ransomware senza backup e con esfiltrazione

Il server di una società di trasporto pubblico è stato esposto a un attacco ransomware e i dati sono stati cifrati dall'autore dell'attacco. Secondo i risultati dell'indagine interna, l'autore dell'attacco non solo ha cifrato i dati,

ma li ha anche esfiltrati. La tipologia dei dati violati consiste nei dati personali di clienti e dipendenti e delle diverse migliaia di persone che utilizzano i servizi della società (ad esempio, per l'acquisto di biglietti online). Oltre ai dati identificativi di base, sono coinvolti nella violazione i numeri dei documenti d'identità e dati finanziari come i dati della carta di credito. Era disponibile un backup, ma anch'esso è stato criptato dall'aggressore.

Misure in essere e valutazione del rischio

Il titolare del trattamento avrebbe dovuto adottare le stesse misure di cui al punto 9.1.1 e 9.1.5. Sebbene disponibile, anche il backup è stato compromesso dall'attacco. Questa circostanza di per sé solleva interrogativi sulla qualità delle misure di sicurezza informatica in essere e dovrebbe essere oggetto di approfondimenti ulteriori durante l'indagine poiché, in un regime di backup ben progettato, devono essere conservati in modo sicuro più backup senza consentire l'accesso dal sistema principale, altrimenti potrebbero essere compromessi nello stesso attacco. Inoltre, gli attacchi ransomware possono rimanere occulti per giorni cifrando lentamente dati utilizzati di rado. Ciò può rendere inutile l'esecuzione di più backup, per cui dovrebbero essere eseguiti anche backup periodici e poi essere isolati. In tal modo si aumenterebbe la probabilità di recupero seppur con una perdita maggiore di dati.

La violazione riguarda non solo la disponibilità dei dati, ma anche la riservatezza, in quanto l'autore dell'attacco può aver modificato e/o copiato i dati dal server. Pertanto, il tipo di violazione comporta un rischio elevato.

La natura, la sensibilità e il volume dei dati personali aumentano ulteriormente i rischi, poiché il numero di persone interessate è elevato, così come la quantità complessiva di dati personali compromessi. Al di là dei dati identificativi di base, sono coinvolti anche documenti di identità e dati finanziari come i dati della carta di credito. Una violazione dei dati relativa a queste categorie di informazioni presenta di per sé un rischio elevato e i dati oggetto di compromissione, se utilizzati congiuntamente, potrebbero servire, tra l'altro, a realizzare furti di identità o frodi.

A causa di errori dei controlli logici o organizzativi del server, i backup sono stati compromessi dal ransomware e ciò ha impedito il ripristino dei dati e aumentato il rischio.

Questa violazione dei dati presenta un rischio elevato per i diritti e le libertà delle persone, in quanto potrebbe comportare sia un danno materiale (ad esempio una perdita finanziaria dovuta alla compromissione dei dati della carta di credito) sia immateriale (ad esempio furto o usurpazione d'identità in quanto i dati della carta d'identità sono stati compromessi).

Misure di mitigazione e obblighi

La comunicazione agli interessati è essenziale affinché possano adottare le misure necessarie per evitare danni materiali (ad esempio bloccare le loro carte di credito).

Oltre a documentare la violazione ai sensi dell'articolo 33, paragrafo 5, anche in questo caso la notifica all'autorità di controllo è obbligatoria (articolo 33, paragrafo 1) e il titolare del trattamento è altresì tenuto a comunicare la violazione agli interessati (articolo 34, paragrafo 1). Quest'ultima comunicazione potrebbe essere effettuata a ogni singolo interessato, ma per le persone in cui i dati di contatto non sono disponibili, il titolare del trattamento dovrebbe dare pubblica comunicazione purché ciò non sia suscettibile di determinare ulteriori conseguenze negative per gli interessati - ad esempio mediante una notifica sul suo sito web. In quest'ultimo caso è necessaria una comunicazione chiara e precisa, ben visibile sulla homepage del titolare del trattamento, con riferimenti esatti alle pertinenti disposizioni del GDPR. La società può inoltre dover aggiornare e correggere le misure e procedure organizzative e tecniche di gestione della sicurezza dei dati personali e di mitigazione dei rischi.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

9.1.5 Misure organizzative e tecniche per prevenire/mitigare gli effetti degli attacchi di ransomware

Il fatto che si sia verificato un attacco ransomware è solitamente la spia dell'esistenza di una o più vulnerabilità del sistema del titolare del trattamento. Ciò vale anche nei casi di attacchi ransomware con cifratura dei dati personali ma senza esfiltrazione. Indipendentemente dall'esito e dalle conseguenze dell'attacco, non si evidenzierà mai a sufficienza quanto sia cruciale una valutazione complessiva del sistema di sicurezza dei dati, con particolare riguardo alla sicurezza informatica. Le debolezze individuate e le lacune di sicurezza devono essere documentate e affrontate senza indugio.

Misure consigliate:
(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)
• Mantenere aggiornato il firmware, il sistema operativo e il software applicativo sui server, sui client, sui componenti attivi di rete e su ogni altra macchina presente sulla stessa LAN (compresi i dispositivi Wi-Fi).
Garantire l'esistenza di adeguate misure di sicurezza informatica, accertarne l'efficacia e mantenerle regolarmente aggiornate quando il trattamento o le circostanze cambiano o evolvono. Ciò comprende la conservazione di log dettagliati dei patch applicati e della rispettiva marcatura temporale.
• Progettazione e organizzazione di sistemi e infrastrutture di trattamento in modo da segmentare o isolare sistemi e reti di dati per evitare la propagazione di software malevolo all'interno dell'organizzazione e verso sistemi esterni.
• Esistenza di una procedura di backup aggiornata, sicura e testata. I mezzi di supporto per il back-up a medio e lungo termine dovrebbero essere tenuti separati dalla conservazione dei dati operativi e fuori dalla portata di soggetti terzi anche in caso di attacco riuscito (per esempio, un backup incrementale giornaliero e un backup settimanale completo).
• Disporre di/procurarsi un software antimalware adeguato, aggiornato, efficace e integrato.
• Disporre di un firewall e sistemi per il rilevamento e la prevenzione delle intrusioni adeguati, aggiornati, efficaci e integrati. Instradare il traffico di rete attraverso il firewall/il sistema rilevamento intrusioni, anche in caso di lavoro agile o in mobilità (ad esempio utilizzando connessioni VPN dotate di meccanismi organizzativi di sicurezza per l'accesso a Internet).
• Formazione dei dipendenti sui metodi di riconoscimento e prevenzione degli attacchi informatici. Il titolare del trattamento dovrebbe fornire gli strumenti per stabilire se le e-mail e i messaggi ottenuti con altri mezzi di comunicazione siano autentici e affidabili. I dipendenti dovrebbero essere formati per riconoscere quando si verifica un attacco del genere, sapere come rimuovere dalla rete l'endpoint ed essere tenuti a segnalarlo immediatamente al responsabile della sicurezza.
• Sottolineare la necessità di individuare il tipo di codice malevolo per comprendere le conseguenze dell'attacco ed essere in grado di individuare le misure giuste per attenuare il rischio. Nel caso in cui un attacco ransomware abbia avuto successo e non sia disponibile alcun back-up, per recuperare i dati possono essere utilizzati strumenti come quelli del progetto "no more ransom" (nomoreransom.org).
Tuttavia, nel caso in cui sia disponibile un backup sicuro, è consigliabile ripristinare i dati attraverso il backup.
• Inoltrare o replicare tutti i log a un server centrale (compresa eventualmente la marcatura temporale crittografica o la firma delle registrazioni dei log).
• Cifratura robusta e autenticazione a più fattori, in particolare per l'accesso amministrativo ai sistemi informatici, adeguata gestione delle chiavi e delle password.
• Test di vulnerabilità e di penetrazione a cadenze regolari.
• Istituire un gruppo di risposta agli incidenti di sicurezza (CSIRT) o un gruppo di risposta alle emergenze informatiche (CERT) all'interno dell'organizzazione o aderire a un CSIRT/CERT collettivo. Creare un piano di risposta agli incidenti, un piano di *disaster recovery* (ripristino in caso di evento catastrofico) e un piano di continuità operativa e assicurarsi che tali piani siano testati in modo approfondito.
• Nel valutare le contromisure, si dovrebbe riesaminare, testare e aggiornare l'analisi dei rischi.

9.2 ATTACCHI DI ESFILTRAZIONE DEI DATI

Gli attacchi che sfruttano le vulnerabilità dei servizi offerti dal titolare del trattamento a terzi su Internet, ad esempio mediante attacchi di *injection* (es. attacchi SQL *injection*, *path traversal*), compromissione di siti web e simili, possono assomigliare ad attacchi ransomware in quanto il rischio deriva dall'azione di un terzo non autorizzato, ma mirano generalmente a copiare, esfiltrare e utilizzare dati personali per fini dolosi. Si tratta quindi principalmente di violazioni della riservatezza e, eventualmente, anche dell'integrità dei dati. Allo stesso tempo, se il titolare del trattamento è a conoscenza delle caratteristiche di questo tipo di violazioni, vi sono numerose misure che possono ridurre considerevolmente il rischio di un attacco efficace.

9.2.1 Caso n. 05: Esfiltrazione dei dati delle domande di impiego da un sito web

Un'agenzia per l'impiego è stata vittima di un attacco informatico, che ha inserito un codice malevolo sul suo sito web. Questo codice ha reso accessibili a soggetti non autorizzati le informazioni personali contenute nei moduli di richiesta di impiego conservati sul server web. 213 di tali moduli potrebbero essere interessati, e le analisi hanno accertato che nessuna categoria particolare di dati era oggetto della violazione. Il malware

installato aveva funzionalità che consentivano all'attaccante di rimuovere qualsiasi traccia di esfiltrazione e di monitorare il trattamento effettuato sul server e di carpire dati personali. Il malware è stato individuato solo un mese dopo la sua installazione.

Misure in essere e valutazione del rischio

La sicurezza dell'ambiente del titolare del trattamento è estremamente importante, dal momento che la maggior parte di queste violazioni può essere evitata garantendo che tutti i sistemi siano costantemente aggiornati, che i dati sensibili siano cifrati e che le applicazioni siano sviluppate secondo elevati standard di sicurezza quali autenticazione forte, misure contro attacchi di forza bruta, "escape" (evasione) o "sanitizing" (sanificazione) degli input degli utenti, ecc.. Anche gli audit periodici di sicurezza informatica, le valutazioni delle vulnerabilità e i test di penetrazione sono necessari per individuare e correggere tali tipi di vulnerabilità. Nel caso specifico, l'impiego di strumenti di monitoraggio dell'integrità dei file nell'ambiente di produzione avrebbe potuto facilitare l'individuazione dell'iniezione del codice (un elenco delle misure consigliate figura nel punto 9.2.4).

Nell'indagare sulla violazione, il titolare del trattamento dovrebbe sempre partire dall'identificazione della tipologia e della metodica dell'attacco, al fine di valutare le misure da adottare. Per garantire rapidità ed efficacia di tale valutazione, il titolare dovrebbe disporre di un piano di risposta agli incidenti che specifichi le misure necessarie da adottare rapidamente per assumere il controllo dell'incidente. In questo caso particolare, il tipo di violazione costituiva un fattore di incremento del rischio, in quanto non solo veniva compromessa la riservatezza dei dati, ma il soggetto infiltrato era anche in grado di apportare modifiche al sistema cosicché veniva messa in discussione anche l'integrità dei dati.

Si dovrebbe tenere conto della natura, della sensibilità e del volume dei dati personali colpiti dalla violazione per determinare in che misura quest'ultima abbia inciso sugli interessati. Sebbene non siano state compromesse categorie particolari di dati personali, i dati oggetto della violazione contengono importanti informazioni sulle persone che hanno compilato i moduli online e tali dati potrebbero essere utilizzati impropriamente in vari modi (marketing indesiderato, furto di identità, ecc.), per cui la gravità delle conseguenze dovrebbe aumentare il rischio per i diritti e le libertà degli interessati.

Misure di mitigazione e obblighi

Se possibile, una volta risolto il problema, la banca dati dovrebbe essere confrontata con quella memorizzata in un backup sicuro. Le esperienze tratte dalla violazione dovrebbero essere utilizzate per aggiornare l'infrastruttura informatica. Il titolare del trattamento dovrebbe riportare tutti i sistemi informatici interessati a uno stato pulito noto, porre rimedio alla vulnerabilità e attuare nuove misure di sicurezza per evitare analoghe violazioni dei dati in futuro, ad esempio controlli di integrità dei file e audit di sicurezza. Se i dati personali sono stati non solo esfiltrati, ma anche cancellati, il titolare del trattamento deve intraprendere un'azione sistematica per ripristinare i dati personali nello stato in cui si trovavano prima della violazione.

Potrebbe essere necessario applicare backup completi, modifiche incrementali ed eventualmente ripetere il trattamento dall'ultimo backup incrementale, il che richiede che il titolare sia in grado di replicare le modifiche apportate dopo l'ultimo backup. Ciò potrebbe necessitare che il titolare del trattamento disponga di un sistema progettato per conservare i file di input giornalieri nel caso in cui questi debbano essere nuovamente elaborati; tutto ciò richiede una tecnica robusta di memorizzazione e un'adeguata politica di conservazione prolungata dei dati.

Alla luce di quanto precede, poiché la violazione può comportare un rischio elevato per i diritti e le libertà delle persone fisiche, gli interessati dovrebbero esserne informati (articolo 34, paragrafo 1), il che significa naturalmente che anche le autorità di controllo competenti dovrebbero essere coinvolte attraverso una notifica di violazione dei dati. Documentare la violazione è obbligatorio ai sensi dell'articolo 33, paragrafo 5, del regolamento generale sulla protezione dei dati e facilita la valutazione del caso specifico.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

9.2.2 Caso n. 06: Esfiltrazione da un sito web di password sottoposte ad hashing

Una vulnerabilità SQL Injection è stata sfruttata per accedere a un database sul server di un sito web dedicato alla cucina. Agli utenti è stato consentito di scegliere solo pseudonimi arbitrari come nomi utente.

È stato scoraggiato l'uso di indirizzi di posta elettronica a tal fine. Le password memorizzate nella banca dati sono state sottoposte ad hashing con un algoritmo robusto e il *salt* non è stato compromesso. Dati interessati:

password *hashed* di 1.200 utenti. Per motivi di sicurezza, il titolare del trattamento ha informato gli interessati della violazione tramite posta elettronica e ha chiesto loro di modificare le password, soprattutto se la stessa password è stata utilizzata per altri servizi.

Misure in essere e valutazione del rischio

In questo caso particolare, la riservatezza dei dati è compromessa, ma le password nel database sono state sottoposte ad hashing con un metodo conforme allo stato dell'arte, il che ridurrebbe il rischio per quanto riguarda la natura, la sensibilità e il volume dei dati personali. Il caso non presenta rischi per i diritti e le libertà degli interessati.

Inoltre, non sono state compromesse le informazioni di contatto (ad esempio indirizzi di posta elettronica o numeri di telefono) degli interessati, il che significa che non vi è alcun rischio significativo per gli interessati di essere oggetto di tentativi di frode (ad esempio, messaggi di posta elettronica di phishing o telefonate e SMS fraudolenti). Non sono state coinvolte categorie particolari di dati personali.

Alcuni nomi utente potrebbero essere considerati dati personali, ma la materia trattata dal sito web non genera connotazioni negative. Tuttavia, si deve osservare che la valutazione del rischio può essere diversa se la natura del sito web e i dati consultati possono rivelare categorie particolari di dati personali (ad esempio il sito web di un partito politico o di un sindacato). L'uso di tecniche di cifratura conformi allo stato dell'arte potrebbe attenuare gli effetti negativi della violazione. Consentire un numero limitato di tentativi di login impedirà il successo degli attacchi di forza bruta sul login, riducendo in larga misura i rischi generati da i attaccanti che già conoscono i nomi utente.

Misure di mitigazione e obblighi

In alcuni casi la comunicazione agli interessati potrebbe essere considerata un fattore di mitigazione del rischio, dal momento che anche gli interessati sono in grado di adottare le misure necessarie per evitare ulteriori danni derivanti dalla violazione, ad esempio modificando la loro password. In questo caso, la comunicazione non era obbligatoria, ma in molti casi può essere considerata una buona pratica.

Il titolare del trattamento dovrebbe correggere la vulnerabilità e implementare nuove misure di sicurezza per evitare in futuro analoghe violazioni dei dati, ad esempio attraverso audit sistematici di sicurezza sul sito web. La violazione dovrebbe essere documentata conformemente all'articolo 33, paragrafo 5, ma non è necessaria alcuna notifica o comunicazione.

Inoltre, è fortemente consigliabile comunicare agli interessati una violazione che riguardi password anche se le password sono state memorizzate utilizzando un hash con l'impiego di *salt* attraverso un algoritmo conforme allo stato dell'arte. È preferibile utilizzare metodi di autenticazione che evitino la necessità di trattare password lato server. Gli interessati dovrebbero avere la possibilità di adottare misure adeguate per quanto riguarda le proprie password.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	X

9.2.3 Caso n. 07: Attacco del tipo *credential stuffing* su un sito web bancario

Una banca ha subito un attacco informatico contro uno dei suoi siti web di servizi bancari online. L'attacco mirava a elencare tutti gli identificativi utente di accesso possibili utilizzando una banale password fissa. Le password sono composte da 8 cifre. A causa di vulnerabilità del sito web, in alcuni casi l'autore dell'attacco ha potuto accedere a informazioni riguardanti gli interessati (nome, cognome, sesso, data e luogo di nascita, codice fiscale, codici di identificazione dell'utente), anche se la password utilizzata non era corretta o il conto bancario non era più attivo. Ciò ha interessato circa 100.000 soggetti. Fra questi, l'autore dell'attacco si è connesso con successo a circa 2.000 account che utilizzavano la password banale da questi processata.

Successivamente il titolare del trattamento è stato in grado di individuare tutti i tentativi illegittimi di log-on.

Il titolare ha potuto verificare che, in base ai controlli antifrode, su tali account non è stata effettuata alcuna transazione durante l'attacco. La banca era a conoscenza della violazione dei dati in quanto il suo centro operativo di sicurezza ha individuato un numero elevato di richieste di log-in dirette verso il sito web.

In risposta, il titolare del trattamento ha disattivato temporaneamente la possibilità di connettersi al sito web e ha forzato il cambio password degli account compromessi. Il titolare ha comunicato la violazione solo agli utenti con account compromessi, ossia agli utenti le cui password sono state compromesse o i cui dati sono stati divulgati.

Misure in essere e valutazione del rischio

È importante ricordare che i titolari che trattano dati di natura estremamente personale (informazioni degli interessati relative a metodi di pagamento come numeri di carta, conti bancari, pagamenti on-line, cedolini degli stipendi, estratti conto bancari, studi economici o qualsiasi altro elemento che possa rivelare informazioni economiche relative agli interessati) hanno maggiori responsabilità in termini di garanzia di un'adeguata sicurezza dei dati, ad esempio predisponendo un centro operativo di sicurezza e attuando altre misure di prevenzione, rilevamento e risposta agli incidenti. Il mancato rispetto di questi standard più elevati comporterà certamente l'adozione di misure più severe durante l'indagine di un'autorità di controllo.
La violazione riguarda dati finanziari che vanno al di là dell'identità e delle informazioni identificative dell'utente, il che la rende particolarmente grave. Il numero di persone interessate è elevato.
Il fatto che una violazione possa verificarsi in un ambiente così sensibile segnala la presenza di notevoli lacune della sicurezza dei dati nel sistema del titolare del trattamento e può essere un indicatore della necessità di un riesame e di un aggiornamento delle misure in questione, in linea con gli articoli 24 (1), 25 (1) e 32 (1) del GDPR. I dati violati consentono l'identificazione univoca degli interessati e contengono altre informazioni su di essi (tra cui sesso, data e luogo di nascita); inoltre possono essere utilizzati dall'autore dell'attacco per ricavare le password dei clienti o per condurre una campagna di phishing mirata ai clienti della banca.
Per questi motivi, la violazione dei dati è stata ritenuta suscettibile di comportare un rischio elevato per i diritti e le libertà di tutti gli interessati. Pertanto, è ipotizzabile il verificarsi di un danno materiale (ad esempio una perdita finanziaria) e immateriale (ad esempio furto d'identità o frode) in conseguenza della violazione.

Misure di mitigazione e obblighi

Le misure del titolare del trattamento menzionate nella descrizione del caso sono adeguate. A seguito della violazione, ha inoltre corretto la vulnerabilità del sito web e ha adottato altre misure per prevenire analoghe violazioni dei dati in futuro, come l'aggiunta di un'autenticazione a due fattori al sito web interessato e il passaggio a un'autenticazione forte del cliente.
In questo scenario la documentazione della violazione a norma dell'articolo 33, paragrafo 5, del GDPR e la notifica all'autorità di controllo non sono lasciate alla discrezione del titolare. Inoltre, il titolare del trattamento dovrebbe informare tutti i 100.000 interessati (compresi gli interessati i cui account non sono stati compromessi) a norma dell'articolo 34 del GDPR.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

9.2.4 Misure organizzative e tecniche per prevenire/mitigare gli effetti degli attacchi di hacker

Come nel caso degli attacchi ransomware, indipendentemente dall'esito e dalle conseguenze dell'attacco, i titolari sono tenuti a riconsiderare le misure di sicurezza dei sistemi informativi in casi analoghi.

Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

• Cifratura e gestione delle chiavi conformi allo stato dell'arte, in particolare quando si trattano password, dati sensibili o finanziari. L'hashing e l'utilizzo di salt crittografici sono sempre preferibili in caso di informazioni riservate (password) rispetto alla cifratura delle password. È preferibile utilizzare metodi di autenticazione che evitino la necessità di trattare password lato server.
• Aggiornamento del sistema (software e firmware). Garantire l'applicazione di tutte le misure di sicurezza informatica, garantirne l'efficacia e mantenerle regolarmente aggiornate quando il trattamento o le circostanze cambiano o evolvono. Per essere in grado di dimostrare la conformità all'articolo 5, paragrafo 1, lettera f), a norma dell'articolo 5, paragrafo 2, del GDPR, il titolare del trattamento dovrebbe conservare un registro di tutti gli aggiornamenti effettuati, compreso il momento in cui sono stati applicati.
• Uso di metodi di autenticazione forte quali autenticazione a due fattori e server di autenticazione, integrati da una politica aggiornata in materia di password.
• Gli standard sicuri di sviluppo comprendono l'applicazione di un filtro agli input utente (utilizzando per quanto possibile una *white list*), la sanificazione degli input utente e misure di prevenzione degli attacchi di forza bruta (come limitare il numero massimo di tentativi ripetuti). L'impiego di Web Application Firewall (WAF - firewall per le applicazioni web) può supportare l'implementazione efficace di questa tecnica.

• Politiche robuste per i privilegi utente e la gestione del controllo degli accessi.
• Uso di sistemi di protezione, di rilevamento delle intrusioni e di difesa perimetrale adeguati, aggiornati, efficaci e integrati.
• Audit sistematici della sicurezza informatica e valutazioni delle vulnerabilità (test di penetrazione).
• Revisioni e test periodici per garantire l'utilizzabilità dei backup al fine di ripristinare i dati la cui integrità o disponibilità siano state compromesse.
• Nessun identificativo di sessione nell'URL in chiaro.

9.3 FONTI DI RISCHIO INTERNE LEGATE AL FATTORE UMANO

Occorre evidenziare il ruolo dell'errore umano nelle violazioni dei dati personali a causa della sua frequenza. Poiché queste violazioni possono essere sia intenzionali che accidentali, è molto difficile per i titolari del trattamento individuare le vulnerabilità e adottare misure per evitarle. La Conferenza internazionale delle autorità per la protezione dei dati e la privacy ha riconosciuto l'importanza di affrontare tali fattori umani e ha adottato, nell'ottobre 2019, una risoluzione concernente il ruolo dell'errore umano nelle violazioni dei dati personali. La risoluzione sottolinea la necessità di adottare misure di salvaguardia adeguate al fine di prevenire gli errori umani e fornisce un elenco non esaustivo di garanzie e approcci.

9.3.1 Caso n. 08: Esfiltrazione di dati aziendali da parte di un dipendente

Durante il suo periodo di preavviso, il dipendente di una società copia i dati aziendali dalla banca dati della società. Il dipendente è autorizzato ad accedere ai dati solo per svolgere le sue mansioni. Vari mesi dopo aver cessato il lavoro alle dipendenze della società, utilizza i dati così ottenuti (dati di contatto di base) per alimentare un nuovo trattamento dei dati per il quale è il titolare, al fine di contattare i clienti della società e invitarli a rivolgersi alla sua nuova impresa.

Misure in essere e valutazione del rischio

Nel caso di specie non sono state adottate misure preventive per impedire al dipendente di copiare i dati di contatto della clientela della società, in quanto il dipendente aveva bisogno legittimamente di accedere – e di fatto accedeva – a tali informazioni per le sue mansioni. Poiché la gestione dei clienti richiede nella maggior parte dei casi un qualche tipo di accesso dei dipendenti ai dati personali, tali violazioni possono essere le più difficili da prevenire. Limitando la portata dell'accesso si rischia di limitare il lavoro che il dipendente è in grado di svolgere. Tuttavia, politiche di accesso ben concepite e un controllo costante possono contribuire a prevenire tali violazioni.

Come di consueto, durante la valutazione del rischio devono essere presi in considerazione il tipo di violazione e la natura, la sensibilità e il volume dei dati personali interessati. Queste violazioni sono generalmente violazioni della riservatezza, in quanto la banca dati è solitamente lasciata intatta e il suo contenuto è "semplicemente" copiato in vista di un ulteriore utilizzo. La quantità di dati interessati è solitamente bassa o media. In questo caso particolare non sono state coinvolte categorie particolari di dati personali, il dipendente aveva bisogno soltanto delle informazioni di contatto dei clienti per essere in grado di contattarli dopo aver lasciato la società. Pertanto, i dati in questione non sono sensibili.

Sebbene l'unico obiettivo dell'ex-dipendente che ha copiato in modo fraudolento i dati possa consistere nell'ottenere le informazioni di contatto della clientela della società per i propri scopi di natura commerciale, il titolare del trattamento non può considerare basso il rischio per gli interessati poiché non dispone di alcuna certezza sulle intenzioni del dipendente. Pertanto, sebbene le conseguenze della violazione possano limitarsi all'esposizione alle attività di autopromozione svolte dall'ex-dipendente, non è escluso un ulteriore e più grave abuso dei dati copiati, a seconda della finalità del trattamento messo in atto dall'ex-dipendente.

Misure di mitigazione e obblighi

Nel caso di specie è difficile mitigare gli effetti negativi della violazione. Potrebbe essere necessario avviare un'azione legale immediata per impedire all'ex-dipendente di utilizzare impropriamente e diffondere ulteriormente i dati. In seconda battuta, l'obiettivo dovrebbe essere quello di evitare situazioni analoghe in futuro. Il titolare del trattamento potrebbe chiedere un'ingiunzione che imponga all'ex-dipendente di astenersi dall'utilizzo dei dati, ma le probabilità che ciò risulti efficace sono, nella migliore delle ipotesi, opinabili. Possono essere utili misure tecniche adeguate, come l'impossibilità di copiare o scaricare dati su dispositivi amovibili.

Non esiste una soluzione unica per tutti i casi di questo tipo, ma un approccio sistematico può contribuire a prevenirli. Ad esempio, l'impresa può prendere in considerazione, ove possibile, la limitazione degli accessi per i dipendenti che hanno segnalato l'intenzione di licenziarsi, oppure prevedere log degli accessi in modo da registrare e segnalare ogni accesso indesiderato. Il contratto firmato con i dipendenti dovrebbe includere clausole che vietino attività del genere descritto.

Nel complesso, poiché la violazione in questione non comporterà un rischio elevato per i diritti e le libertà delle persone fisiche, è sufficiente una notifica all'autorità di controllo. Tuttavia, informarne gli interessati potrebbe essere vantaggioso anche per il titolare del trattamento, in quanto sarebbe meglio che gli interessati ricevano la notizia della violazione dall'azienda piuttosto che apprenderla quando l'ex-dipendente cercherà di contattarli. La documentazione della violazione a norma dell'articolo 33, paragrafo 5, è un obbligo giuridico.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	X

9.3.2 Caso n. 09: Trasmissione accidentale di dati a un terzo fidato

Un agente assicurativo ha notato che — a causa dalle impostazioni difettose di un file Excel ricevuto per posta elettronica — era in grado di accedere alle informazioni relative a una ventina di clienti non appartenenti al suo portafoglio. Egli è vincolato dal segreto professionale ed è stato l'unico destinatario del messaggio di posta elettronica. L'accordo tra il titolare del trattamento e l'agente assicurativo obbliga quest'ultimo a segnalare senza ingiustificato ritardo una violazione dei dati personali al titolare stesso.
Pertanto, l'agente ha immediatamente segnalato l'errore al titolare, che ha corretto il file e lo ha inviato nuovamente, chiedendo all'agente di cancellare il messaggio precedente. In base all'accordo di cui sopra, l'agente deve confermare la cancellazione per iscritto, cosa che ha fatto. Le informazioni raccolte non comprendono categorie particolari di dati personali, solo dati di contatto e dati relativi all'assicurazione stessa (tipo di assicurazione, importo). Dopo aver analizzato i dati personali interessati dalla violazione, il titolare del trattamento non ha individuato elementi particolari, sia per quanto riguarda gli interessati sia per quanto riguarda lo stesso titolare, tali da incidere sul livello di impatto della violazione.

Misure in essere e valutazione del rischio

In questo caso la violazione non deriva da un'azione deliberata di un dipendente, ma da un errore umano accidentale causato da disattenzione. Questo tipo di violazione può essere evitato o reso meno frequente: a) applicando programmi di formazione, istruzione e sensibilizzazione cosicché i dipendenti acquisiscano una migliore comprensione dell'importanza della protezione dei dati personali; b) riducendo lo scambio di file tramite posta elettronica, e utilizzando invece sistemi dedicati per il trattamento dei dati dei clienti; c) verificando due volte i file prima dell'invio; d) separando il momento della creazione da quello dell'invio di file. La violazione riguarda solo la riservatezza dei dati, e l'integrità e l'accessibilità degli stessi non sono compromesse. La violazione dei dati riguardava solo una ventina di clienti, per cui è contenuto il volume dei dati interessati. Inoltre, non sono coinvolti dati sensibili. Il fatto che il responsabile del trattamento abbia contattato immediatamente il titolare dopo essere venuto a conoscenza della violazione dei dati può essere considerato un fattore di mitigazione del rischio. (Sarebbe da valutare anche l'eventualità che i dati siano stati trasmessi ad altri agenti assicurativi e, in caso di conferma, si dovrebbero adottare misure adeguate.) Grazie alle misure appropriate adottate successivamente alla violazione dei dati, probabilmente quest'ultima non avrà alcun impatto sui diritti e sulle libertà degli interessati.
Il basso numero di persone interessate, la rilevazione immediata della violazione e le misure adottate per minimizzarne gli effetti rendono il caso in questione privo di rischi.

Misure di mitigazione e obblighi

Vi sono altri elementi di mitigazione del rischio nel caso in esame: l'agente è vincolato al segreto professionale; egli stesso ha segnalato il problema al titolare del trattamento e ha cancellato il file su richiesta. La sensibilizzazione ed eventualmente la previsione di ulteriori misure di controllo dei documenti contenenti dati personali potranno contribuire a evitare il ripetersi di situazioni simili in futuro.
Oltre a documentare la violazione a norma dell'articolo 33, paragrafo 5, non sono necessarie altre azioni.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	X

9.3.3 Misure organizzative e tecniche per prevenire/attenuare l'impatto delle fonti interne di rischio legate al fattore umano

L'applicazione congiunta delle misure indicate di seguito, in funzione delle caratteristiche specifiche del caso, dovrebbe contribuire a ridurre le probabilità di una recidiva analoga.

Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

• Attuazione periodica di programmi di formazione, istruzione e sensibilizzazione per i dipendenti sugli obblighi in materia di privacy e sicurezza e sulla rilevazione e la segnalazione di minacce alla sicurezza dei dati personali. Messa a punto di un programma di sensibilizzazione per ricordare ai dipendenti gli errori più comuni che portano a violazioni dei dati personali e come evitarli.
• Istituzione di pratiche, procedure e sistemi solidi ed efficaci in materia di protezione dei dati e di tutela della vita privata.
• Valutazione delle pratiche, delle procedure e dei sistemi in materia di tutela della vita privata per garantirne l'efficacia nel tempo.
• Elaborazione di adeguate politiche di controllo dell'accesso e obbligo per gli utenti di rispettare le norme.
• Tecniche per forzare l'autenticazione dell'utente quando accede a dati personali sensibili.
• Disabilitazione dell'account aziendale non appena il dipendente lascia l'azienda.
• controllo dei flussi di dati insoliti tra il file server e le postazioni di lavoro dei dipendenti.
• impostazione della sicurezza dell'interfaccia I/O nel BIOS o mediante l'uso di software che controlla l'uso delle interfacce del computer (blocco o sblocco, ad esempio USB/CD/DVD, ecc.).
• revisione delle politiche in materia di accesso dei dipendenti (ad esempio, registrare l'accesso a dati sensibili chiedendo all'utente di inserire una motivazione di ordine aziendale, in modo che sia disponibile per gli audit).
• Disabilitazione dei servizi di cloud aperti.
• Vietare e impedire l'accesso a servizi di posta elettronica aperta noti.
• Disattivazione della funzione *print screen* [stampa schermata] nel sistema operativo (OS).
• Applicazione rigorosa di una politica della "scrivania sgombra" (c.d. *clean desktop*).
• Blocco automatico di tutti i computer dopo un certo periodo di inattività.
• Utilizzo di meccanismi (ad esempio token (wireless) per accedere a/aprire account bloccati) per cambi rapidi di utente in ambienti condivisi.
• Utilizzo di sistemi dedicati per la gestione dei dati personali che prevedano adeguati meccanismi di controllo dell'accesso e siano in grado di prevenire errori umani, come l'invio di comunicazioni al soggetto sbagliato. L'uso di fogli di calcolo e di altri documenti d'ufficio non è adeguato al fine di gestire i dati dei clienti.

9.4 SMARRIMENTO O FURTO DI DISPOSITIVI O DI DOCUMENTI CARTACEI

Un caso frequente è lo smarrimento o il furto di dispositivi portatili. In questi casi, il titolare del trattamento deve prendere in considerazione le circostanze del trattamento, quali le categorie dei dati conservati sul dispositivo, nonché le risorse di supporto, e le misure adottate precedentemente alla violazione per garantire un livello di sicurezza adeguato. Tutti questi elementi incidono sui potenziali impatti della violazione dei dati.
La valutazione dei rischi potrebbe risultare difficile, in quanto il dispositivo non è più disponibile.
Questo tipo di violazione può essere classificato in tutti i casi come violazione della riservatezza. Tuttavia, se non esiste un backup per il database sottratto, può configurarsi anche una violazione della disponibilità e dell'integrità.
Gli scenari descritti di seguito illustrano in che modo le circostanze di cui sopra determinano la probabilità e la gravità della violazione dei dati.

9.4.1 Caso n. 10: Furto di supporti sui quali sono memorizzati dati personali cifrati

A seguito di un'effrazione compiuta in un asilo, sono stati rubati due tablet. Nei tablet era installata un'app contenente dati personali sui bambini che frequentano l'asilo: nome, data di nascita, dati personali relativi alle attività educative. Sia i tablet cifrati, che erano spenti al momento dell'effrazione, sia l'app erano protetti da una password robusta. Per il titolare era prontamente ed efficacemente disponibile il back-up. Subito dopo essere venuto a conoscenza dell'effrazione, l'asilo ha inviato un comando a distanza per rimuovere il contenuto dei tablet.

Misure in essere e valutazione del rischio

In questo caso particolare, il titolare del trattamento ha adottato misure adeguate per prevenire e mitigare gli effetti di una potenziale violazione dei dati utilizzando la cifratura dei dispositivi, introducendo un'adeguata

protezione delle password e garantendo il back-up dei dati conservati sui tablet. (Un elenco delle misure consigliate figura nel punto 9.4.4).
Dopo essere venuto a conoscenza di una violazione, il titolare del trattamento dovrebbe valutare la fonte di rischio, i sistemi a supporto del trattamento dei dati, il tipo di dati personali coinvolti e gli impatti potenziali della violazione sulle persone interessate. La violazione dei dati sopra descritta avrebbe riguardato la riservatezza, la disponibilità e l'integrità dei dati; tuttavia, grazie alle idonee misure adottate dal titolare precedentemente e successivamente alla violazione dei dati, nessuna di tali compromissioni si è verificata.

Misure di mitigazione e obblighi

La riservatezza dei dati personali sui dispositivi non è stata compromessa grazie alla protezione delle password robuste sia sui tablet che sulle app. I tablet sono stati configurati in modo tale che la l'impostazione di una password comporti la cifratura dei dati nel dispositivo. A ciò si aggiunga il tentativo del titolare di cancellare da remoto tutte le informazioni nei tablet rubati.
Grazie alle misure adottate, anche la riservatezza dei dati non è stata compromessa. Inoltre, il backup garantiva la costante disponibilità dei dati personali, pertanto non si sarebbe potuto verificare alcun potenziale impatto negativo.
Ne deriva l'improbabilità che la violazione dei dati sopra descritta comporti un rischio per i diritti e le libertà degli interessati, pertanto non occorre alcuna notifica all'autorità di controllo o agli interessati. Tuttavia, anche una violazione di questo tipo deve essere documentata, a norma dell'articolo 33, paragrafo 5.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	X

5.2 Caso n. 11: Furto di supporti sui quali sono memorizzati dati personali non cifrati

Il computer portatile di un dipendente di una società di servizi è stato rubato. Il notebook rubato conteneva nomi, cognomi, sesso, indirizzi e data di nascita di oltre 100.000 clienti. A causa dell'indisponibilità del dispositivo rubato non è stato possibile individuare se fossero interessate anche altre categorie di dati personali. L'accesso al disco rigido del notebook non era protetto da alcuna password. È possibile ripristinare i dati personali attraverso i backup giornalieri disponibili.

Misure in essere e valutazione del rischio

Poiché il titolare del trattamento non ha adottato alcuna misura di sicurezza, i dati personali memorizzati nel notebook rubato erano facilmente accessibili all'autore del furto o a qualsiasi altra persona che successivamente entrasse in possesso del dispositivo.
Questa violazione riguarda la riservatezza dei dati conservati sul dispositivo rubato.
In questo caso il notebook contenente i dati personali era vulnerabile in quanto non disponeva di alcuna password di protezione né di cifratura. La mancanza di misure di sicurezza di base aumenta il livello di rischio per gli interessati. Un'ulteriore criticità è rappresentata dall'identificazione degli interessati, il che aumenta anche la gravità della violazione. Il numero considerevole di persone interessate comporta un incremento del rischio; tuttavia, nella violazione non sono coinvolte categorie particolari di dati personali.
Nel corso della valutazione del rischio, il titolare del trattamento dovrebbe prendere in considerazione le potenziali conseguenze e gli effetti negativi della violazione della riservatezza. A causa della violazione, gli interessati possono subire furti di identità sulla base dei dati disponibili nel notebook sottratto, per cui il rischio è da ritenersi elevato.

Misure di mitigazione e obblighi

La cifratura del dispositivo e l'uso della protezione di una password robusta del database memorizzato nel dispositivo avrebbero potuto impedire che la violazione dei dati comportasse un rischio per i diritti e le libertà degli interessati.
Alla luce di tali circostanze, è necessaria la notifica all'autorità di controllo competente nonché la comunicazione agli interessati.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati

✓	✓	✓

9.4.3 CASO n. 12 – FURTO DI FASCICOLI CARTACEI CONTENENTI DATI SENSIBILI

Un registro cartaceo è stato rubato da un centro per la riabilitazione dalle tossicodipendenze. Il registro conteneva dati identificativi e sanitari di base relativi ai pazienti del centro. I dati erano memorizzati solo sul supporto cartaceo e i medici che trattavano i pazienti non dispongono di un backup. Il registro non era conservato in un cassetto chiuso a chiave né in una stanza chiusa a chiave; il titolare non aveva previsto politiche per il controllo degli accessi né altre misure a protezione della documentazione cartacea.

Misure in essere e valutazione del rischio

Poiché il titolare del trattamento dei dati non ha adottato alcuna misura di sicurezza, i dati personali conservati nel registro erano facilmente accessibili alla persona che lo ha trovato. Inoltre, la natura dei dati personali conservati nel registro rende la mancanza di un backup un fattore di rischio molto grave.

Questo caso esemplifica una violazione dei dati ad alto rischio. A causa della mancanza di adeguate precauzioni a, sono andati perduti dati sanitari sensibili a norma dell'articolo 9, paragrafo 1, del GDPR. Poiché in questo caso si trattava di una categoria particolare di dati personali, i rischi potenziali per gli interessati sono maggiori, e tale circostanza deve essere tenuta in considerazione anche dal titolare del trattamento nell'effettuare la valutazione del rischio.

La violazione riguarda la riservatezza, la disponibilità e l'integrità dei dati personali in questione. La violazione compromette la segretezza del rapporto medico-paziente, e terzi non autorizzati possono accedere alle informazioni sanitarie riguardanti i pazienti, il che può avere gravi ripercussioni sulla loro vita. La violazione della disponibilità può anche compromettere la continuità delle cure prestate. Non potendosi escludere la modifica/cancellazione di parti del contenuto del registro, risulta compromessa anche l'integrità dei dati personali.

Misure di mitigazione e obblighi

In fase di valutazione delle misure di salvaguardia dovrebbe essere presa in considerazione anche la natura del supporto utilizzato. Poiché il registro dei pazienti era un documento fisico, la sua protezione avrebbe dovuto essere organizzata in modo diverso rispetto a un dispositivo elettronico. La pseudonimizzazione dei nomi dei pazienti, la conservazione del registro in un locale protetto e in un cassetto o una stanza chiusi a chiave, e un adeguato controllo degli accessi che prevedesse l'autenticazione al momento dell'accesso avrebbero potuto impedire la violazione dei dati.

La violazione dei dati di cui sopra può avere gravi ripercussioni sugli interessati; di conseguenza, la notifica dell'autorità di controllo e la comunicazione della violazione agli interessati sono obbligatorie.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

9.4.4 Misure organizzative e tecniche per prevenire/attenuare le conseguenze della perdita o del furto di dispositivi

L'applicazione congiunta delle misure indicate di seguito, in funzione delle caratteristiche specifiche del caso, dovrebbe contribuire a ridurre la probabilità del ripetersi di incidenti analoghi.

Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

- Attivare sistemi di cifratura del dispositivo (come BitLocker, Veracript o DM-Crypt).
- Utilizzare un codice di accesso/password su tutti i dispositivi. Cifrare tutti i dispositivi elettronici mobili prevedendo l'inserimento di una password complessa per la decifratura.
- Utilizzare l'autenticazione a più fattori.
- Attivare le funzionalità dei dispositivi ad alta mobilità che ne consentono la localizzazione in caso di perdita o smarrimento.
- Utilizzare software/app e localizzazione MDM (Mobile Devices Management). Utilizzare filtri antiriflesso. Chiudere tutti i dispositivi incustoditi.

• Se possibile e opportuno per il trattamento dei dati in questione, salvare i dati personali non su un dispositivo mobile, ma su un server centrale di back-end.
• Se la postazione di lavoro è collegata alla LAN aziendale, eseguire un backup automatico dalle cartelle di lavoro, a condizione che sia ineludibile che i dati personali siano ivi conservati.
• Utilizzare una VPN sicura (ad esempio, che richieda un secondo fattore di autenticazione separato per stabilire una connessione sicura) per collegare i dispositivi mobili ai server back-end.
• Fornire dispositivi di blocco fisico ai dipendenti per consentire loro di mettere fisicamente in sicurezza i dispositivi mobili che utilizzano quando rimangono incustoditi.
• Corretta regolamentazione dell'uso del dispositivo al di fuori dell'azienda.
• Corretta regolamentazione dell'uso dei dispositivi all'interno dell'azienda.
• Utilizzare software/app MDM (Mobile Devices Management) e attivare la funzione wipe da remoto.
• Utilizzare una gestione centralizzata dei dispositivi con diritti minimi per l'installazione di software da parte degli utenti finali.
• Installare controlli di accesso fisico.
• Evitare di conservare informazioni sensibili in dispositivi mobili o dischi rigidi. Se è necessario accedere al sistema interno dell'impresa, si dovrebbero utilizzare canali sicuri come indicato in precedenza.

9.5 ERRATO INVIO DI CORRISPONDENZA

Anche in questo caso la fonte di rischio è un errore umano interno, ma nessun atto doloso ha portato alla violazione. È il risultato di una disattenzione. Ben poco può fare il titolare del trattamento una volta che la violazione si sia verificata, pertanto la prevenzione in questi casi è ancora più importante.

9.5.1 Caso n. 13: Errore nella corrispondenza postale

Due ordini per l'acquisto di calzature sono stati evasi da una società di vendita al dettaglio. A causa di un errore umano, è stata fatta confusione con le due fatture per cui sia i prodotti che le relative fatture sono stati inviati alla persona sbagliata. Ciò significa che i due clienti hanno ricevuto gli ordini l'uno dell'altro, comprese le fatture contenenti i dati personali. Dopo essere venuto a conoscenza della violazione, il titolare del trattamento ha richiamato gli ordini e li ha inviati ai destinatari corretti.

Misure in essere e valutazione del rischio

Le fatture contenevano i dati personali necessari per la consegna (nome, indirizzo, oltre all'articolo acquistato e il suo prezzo). È importante individuare in primo luogo come abbia potuto verificarsi l'errore umano e, se del caso, come avrebbe potuto essere evitato. Nel caso specifico, il rischio è basso, poiché non sono state coinvolte categorie particolari di dati personali o altri dati il cui abuso potrebbe avere effetti negativi rilevanti, la violazione non consegue a un errore sistemico da parte del titolare del trattamento e sono interessate solo due persone. Non sono stati rilevati effetti negativi sugli interessati.

Misure di mitigazione e obblighi

Il titolare del trattamento dovrebbe prevedere la restituzione gratuita degli articoli e delle relative fatture, nonché chiedere ai destinatari errati di distruggere/cancellare tutte le eventuali copie delle fatture contenenti i dati personali dell'altro destinatario.
Anche se la violazione non comporta di per sé un rischio elevato per i diritti e le libertà delle persone interessate e, di conseguenza, la comunicazione agli interessati non è richiesta ai sensi dell'articolo 34 del GDPR, tale comunicazione di fatto è inevitabile in quanto è necessaria la cooperazione degli interessati per la mitigazione del rischio.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	X

9.5.2 Caso n. 14: Dati personali altamente riservati inviati erroneamente per posta elettronica

Il dipartimento risorse umane di una pubblica amministrazione ha inviato un messaggio di posta elettronica — sulle attività formative previste — alle persone registrate nel sistema come in cerca di occupazione. Per errore, all'e-mail è stato allegato un documento contenente tutti i dati personali di tali soggetti (nome, indirizzo e-mail, indirizzo postale, numero di previdenza sociale). Gli interessati coinvolti sono oltre 60.000.
Successivamente, l'Ufficio ha contattato tutti i destinatari chiedendo loro di cancellare il messaggio precedente e di non utilizzare le informazioni in esso contenute.

Misure in essere e valutazione del rischio

Per l'invio di messaggi di questo genere avrebbero dovuto essere applicate regole più rigorose. Occorre prendere in considerazione l'introduzione di meccanismi di controllo supplementari.

Il numero di persone interessate è considerevole e il coinvolgimento del loro numero di previdenza sociale, insieme ad altri dati personali più basilari, aumenta ulteriormente il rischio, che può essere classificato come elevato. Il titolare non può implementare misure tese a contenere l'eventuale diffusione dei dati da parte di uno qualsiasi dei destinatari.

Misure di mitigazione e obblighi

Come indicato in precedenza, sono pochi gli strumenti utili a mitigare efficacemente i rischi di una violazione analoga. Sebbene il titolare del trattamento abbia chiesto la cancellazione del messaggio, non può costringere i destinatari a farlo e, di conseguenza, non può essere certo che essi adempiano a quanto richiesto.

In un caso del genere non dovrebbero esservi dubbi sulla necessità di tutte e tre le azioni indicate di seguito.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

9.5.3 Caso n. 15: Dati personali inviati per errore tramite posta elettronica

Un elenco dei partecipanti a un corso di inglese giuridico tenuto presso un albergo e della durata di 5 giorni è inviato per errore a 15 partecipanti a un precedente e analogo corso anziché all'albergo. L'elenco contiene nomi, indirizzi di posta elettronica e preferenze alimentari dei 15 partecipanti. Solo due partecipanti hanno indicato le loro preferenze alimentari, dichiarando di essere intolleranti al lattosio. Nessuno dei partecipanti ha un'identità protetta. Il titolare del trattamento scopre l'errore subito dopo l'invio dell'elenco e ne informa i destinatari chiedendo loro di cancellare l'elenco.

Misure in essere e valutazione del rischio

Avrebbero dovuto essere applicate regole rigorose per l'invio di messaggi contenenti dati personali. Occorre prendere in considerazione l'introduzione di meccanismi di controllo supplementari.

I rischi derivanti dalla natura, dalla sensibilità, dal volume e dal contesto dei dati personali sono bassi. I dati personali comprendono dati sensibili sulle preferenze alimentari di due dei partecipanti. Anche se l'informazione relativa all'intolleranza al lattosio è un dato sanitario, il rischio che tali dati siano utilizzati in modo dannoso dovrebbe essere considerato relativamente basso. Mentre nel caso di dati relativi alla salute si presume solitamente che la violazione possa comportare un rischio elevato per l'interessato, nel caso di specie non è possibile individuare il rischio che la violazione comporti danni fisici, materiali o immateriali all'interessato a causa della divulgazione non autorizzata di informazioni sull'intolleranza al lattosio.

Contrariamente ad altre preferenze alimentari, l'intolleranza al lattosio non può di norma essere collegata a convinzioni religiose o filosofiche. Anche la quantità di dati violati e il numero di interessati coinvolti sono molto bassi.

Misure di mitigazione e obblighi

In sintesi, si può affermare che la violazione non ha avuto effetti significativi sugli interessati. Il fatto che il titolare del trattamento abbia contattato immediatamente i destinatari dopo essere venuto a conoscenza dell'errore può essere considerato un fattore di mitigazione.

Se un messaggio di posta elettronica è inviato a un destinatario errato/non autorizzato, si raccomanda al titolare del trattamento di inviare un'e-mail di follow-up, in copia nascosta, ai destinatari non corretti, scusandosi per l'errore, invitando a cancellare l'e-mail inviata erroneamente e informando i destinatari che non hanno il diritto di utilizzare ulteriormente gli indirizzi di posta elettronica loro comunicati.

Alla luce delle circostanze descritte, era improbabile che la violazione dei dati comportasse un rischio per i diritti e le libertà degli interessati, pertanto non si è resa necessaria alcuna notifica all'autorità di controllo o agli interessati. Tuttavia, anche una violazione dei dati di questo tipo deve essere documentata a norma dell'articolo 33, paragrafo 5.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati

✓	X	X

9.5.4 Caso n. 16: Errore nell'invio di corrispondenza postale

Un gruppo assicurativo offre assicurazioni auto. A tal fine, invia per posta aggiornamenti periodici sulle prestazioni assicurative. Oltre al nome e all'indirizzo dell'assicurato, la lettera contiene la targa del veicolo in chiaro, gli importi del premio assicurativo per l'anno in corso e per quello successivo, il chilometraggio annuo approssimativo e la data di nascita dell'assicurato. Non sono inclusi dati sanitari ai sensi dell'articolo 9 del GDPR, né dati relativi ai pagamenti (coordinate bancarie) o dati economici e finanziari.
Le lettere sono imbustate automaticamente. A causa di un errore meccanico, due lettere destinate a contraenti diversi sono inserite in una stessa busta e inviate per posta ordinaria a uno dei due. Il contraente apre la lettera a casa e legge la lettera a lui correttamente indirizzata nonché quella erroneamente consegnata e indirizzata a un diverso contraente.

Misure in essere e valutazione del rischio

La lettera erroneamente consegnata contiene il nome, l'indirizzo, la data di nascita, il numero di immatricolazione in chiaro del veicolo e la classe attribuita per il premio assicurativo dell'anno in corso e dell'anno successivo. Gli effetti sulla persona interessata devono ritenersi di media entità, in quanto sono comunicate a una persona non autorizzata informazioni non accessibili al pubblico, quali la data di nascita o i numeri di immatricolazione in chiaro dei veicoli, nonché i dettagli relativi all'aumento del premio assicurativo.
La probabilità di un uso improprio di questi dati è da valutarsi tra bassa e media. Tuttavia, mentre molti destinatari probabilmente cestineranno la lettera ricevuta per errore, non si può escludere del tutto che, in determinati casi, la lettera sia pubblicata sui social network o che l'assicurato sia contattato.

Misure di mitigazione e obblighi

Il titolare del trattamento deve chiedere che, a sue spese, gli sia reinviato il documento originale. Inoltre, dovrebbe informare il destinatario errato del fatto che non può utilizzare in modo improprio le informazioni cui ha avuto accesso.
Probabilmente non sarà mai possibile prevenire del tutto errori di spedizione in una postalizzazione massiva effettuata in forma completamente automatizzata. Tuttavia, se tali errori avvengono con una certa frequenza, è necessario verificare se i dispositivi di imbustamento siano impostate e sottoposte a manutenzione in modo corretto o se vi siano altri problemi di natura sistemica alla base della violazione.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	X

9.5.5 Misure organizzative e tecniche per prevenire/attenuare gli effetti di un'errata postalizzazione

L'applicazione congiunta delle misure indicate di seguito, in funzione delle caratteristiche specifiche del caso, dovrebbe contribuire a ridurre le probabilità del ripetersi di eventi analoghi.

Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione.)

• Definizione di standard specifici — che non lascino spazi all'interpretazione — per l'invio di lettere/e-mail.
• Formazione adeguata del personale sull'invio di lettere/e-mail.
• Quando si inviano messaggi di posta elettronica a più destinatari, questi sono inseriti nel campo "Ccn" per impostazione predefinita.
• Necessità di una conferma supplementare prima di inviare messaggi di posta elettronica a più destinatari senza inserirli nel campo "Ccn".
• Applicazione del principio del doppio livello di controllo.
• Inserimento automatico anziché manuale dei recapiti, con dati estratti da una banca dati disponibile e aggiornata; il sistema di inserimento automatico dovrebbe essere riesaminato periodicamente per verificare eventuali errori nascosti e impostazioni errate.

• Applicazione della funzionalità di invio ritardato (che consente di cancellare/modificare il messaggio entro un determinato periodo di tempo dopo aver premuto il pulsante "Invio").
• Disabilitazione del completamento automatico quando si digitano indirizzi e-mail.
• Sessioni di sensibilizzazione sugli errori più comuni che generano una violazione dei dati personali.
• Sessioni di formazione e manuali sulla gestione di incidenti che generano una violazione dei dati personali, compresa l'indicazione dei soggetti da informare (coinvolgimento del responsabile della protezione dei dati).

9.6 ALTRI CASI — INGEGNERIA SOCIALE (*Social Engineering*)

9.6.1 Caso n. 17: Furto d'identità

Il centro di contatto di un'impresa di telecomunicazioni riceve una telefonata da una persona che si presenta come cliente. Il presunto cliente chiede alla società di modificare l'indirizzo e-mail al quale inviare le informazioni di fatturazione. L'operatore convalida l'identità del cliente chiedendo alcuni dati personali, quali definiti dalle procedure dell'impresa. Il chiamante indica correttamente il codice fiscale e l'indirizzo postale del cliente (perché ha avuto accesso a tali informazioni). Dopo la convalida, l'operatore effettua la modifica richiesta e, successivamente, le informazioni di fatturazione sono inviate al nuovo indirizzo e-mail. La procedura non prevede alcuna notifica al precedente contatto e-mail. Il mese successivo il cliente legittimo contatta la società, chiedendo perché non riceva la fattura al suo indirizzo di posta elettronica, e nega qualsiasi richiesta da parte sua di modificare l'email di contatto. La società si rende conto che le informazioni sono state inviate a un utente illegittimo e annulla la modifica.

Valutazione del rischio, misure di mitigazione e obblighi

Questo caso ben esemplifica l'importanza delle misure preventive. La violazione presenta un elevato livello di rischio, in quanto i dati di fatturazione possono fornire informazioni sulla vita privata dell'interessato (ad esempio, abitudini, contatti) e potrebbero causare danni materiali (ad esempio stalking, rischio per l'integrità fisica). I dati personali ottenuti durante l'attacco possono essere utilizzati anche per facilitare l'acquisizione di account all'interno della specifica organizzazione o per testare ulteriori misure di autenticazione in altre organizzazioni. Tenuto conto di tali rischi, la soglia di "adeguatezza" delle misure di autenticazione dovrebbe essere fissata a un livello elevato in rapporto alla natura dei dati personali cui è possibile accedere una volta effettuata l'autenticazione.
Di conseguenza, sono necessarie sia una notifica all'autorità di controllo sia una comunicazione all'interessato da parte del titolare del trattamento.
È chiaro che il processo di convalida preventiva del cliente necessita di perfezionamenti, alla luce di questo caso. I metodi utilizzati per l'autenticazione non erano sufficienti. La parte malintenzionata è riuscita a finger di essere l'utente legittimo utilizzando informazioni pubblicamente disponibili e altre informazioni cui aveva altrimenti accesso.
Non si raccomanda l'uso di questa forma di autenticazione statica basata su elementi di conoscenza (in cui la risposta non cambia e non ci sono informazioni "segrete", come invece sarebbe nel caso di una password).
L'organizzazione dovrebbe invece utilizzare una forma di autenticazione altamente affidabile quanto alla dimostrazione che l'utente autenticato sia realmente chi afferma di essere, e non altri. L'introduzione di un metodo di autenticazione a più fattori fuori banda risolverebbe il problema, ad esempio per verificare eventuali richieste di variazioni, attraverso l'invio di una richiesta di conferma al precedente indirizzo di contatto; oppure aggiungendo ulteriori domande di controllo e chiedendo informazioni presenti solo sulle fatture precedenti. Spetta al titolare del trattamento decidere quali misure introdurre, in quanto conosce meglio di chiunque altro i dettagli e le esigenze della sua operatività interna.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

9.6.2 Caso n. 18: Esfiltrazione di e-mail

Una catena di ipermercati ha rilevato, 3 mesi dopo la configurazione, che alcuni account di posta elettronica erano stati modificati attraverso la creazione di regole per cui ogni e-mail contenente determinate espressioni (ad esempio "fattura", "pagamento", "bonifico bancario", "autenticazione della carta di credito", "coordinate bancarie") veniva trasferita in una cartella non utilizzata e trasmessa anche a un indirizzo di posta elettronica esterno. Inoltre, a quella data, era già stato commesso un attacco di ingegneria sociale, vale a dire che

l'attaccante, che fingeva di essere un fornitore, aveva modificato le coordinate bancarie di tale fornitore sostituendovi le proprie. Infine, a quella data, erano state inviate diverse fatture false che includevano i nuovi dati relativi alle coordinate bancarie. Il sistema di monitoraggio della piattaforma di posta elettronica aveva segnalato, in ultima istanza, un problema sulle cartelle. La società non è stata in grado di individuare in che modo l'attaccante fosse riuscito ad accedere agli account di posta elettronica, ma ha ritenuto che attraverso un'email infetta fosse avvenuto l'accesso al gruppo di utenti incaricati dei pagamenti.
A seguito della trasmissione di e-mail contenenti determinate parole-chiave, l'attaccante ha ricevuto informazioni su 99 dipendenti: nome e salario riferito a uno specifico mese per 89 soggetti; nome, stato civile, numero di figli, retribuzione, ore di lavoro e altre informazioni sulla retribuzione di 10 dipendenti il cui contratto era terminato. Il titolare ha comunicato la violazione soltanto ai 10 dipendenti appartenenti a quest'ultimo gruppo.

Valutazione del rischio, misure di mitigazione e obblighi

Anche se l'attaccante non mirava probabilmente a raccogliere dati personali, la violazione potrebbe comportare sia un danno materiale (ad esempio, perdite finanziarie) che un danno immateriale (ad esempio furto o usurpazione di identità), e i dati potrebbero essere utilizzati per facilitare altri attacchi (ad esempio phishing); pertanto, la violazione potrebbe comportare un rischio elevato per i diritti e le libertà delle persone fisiche e dovrebbe essere comunicata a tutti i 99 dipendenti e non solo ai 10 dei quali sono state divulgate le retribuzioni.
Una volta venuto a conoscenza della violazione, il titolare del trattamento ha forzato la modifica della password per gli account compromessi, ha bloccato l'invio di e-mail all'account dell'attaccante, ha informato il fornitore del servizio di posta elettronica utilizzato dall'autore dell'attacco in merito alle azioni compiute da quest'ultimo, ha rimosso le regole stabilite dall'attaccante e perfezionato le segnalazioni del sistema di monitoraggio così da generare una segnalazione non appena venga creata una regola automatica. In alternativa, il titolare del trattamento potrebbe eliminare il diritto degli utenti di stabilire regole sull'inoltro dei messaggi di posta elettronica, prevedendo la necessità di un intervento del team del servizio informatico su specifica richiesta, oppure potrebbe introdurre una politica in base alla quale gli utenti dovrebbero verificare e comunicare le regole stabilite sui loro account una volta alla settimana o con maggiore frequenza, nei settori che trattano dati finanziari.
Il fatto che una violazione abbia potuto verificarsi e sfuggire al rilevamento per un periodo così prolungato, e la circostanza per cui, se la violazione fosse proseguita, le tecniche di ingegneria sociale avrebbero consentito di modificare un volume di dati ancora più consistente, evidenziano notevoli criticità nel sistema di sicurezza informatica del titolare del trattamento. Tali criticità dovrebbero essere affrontate senza indugio, ad esempio rivedendo le procedure automatizzate e le verifiche dei cambiamenti, le misure di rilevazione degli incidenti e di risposta agli incidenti. I titolari del trattamento di dati sensibili, informazioni finanziarie, ecc. hanno maggiori responsabilità nel garantire un'adeguata sicurezza dei dati.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

10. ALLEGATI

Allegato 1) fac-simile Data Breach

Allegato 2) istruzioni per la "procedura telematica di notifica"

Allegato 3) Registro del data breach