Procedura “Gestione delle Violazioni di Dati Personali” – Allegato 3 Fattori da considerare quando si valuta il rischio

Fattori da considerare quando si valuta il rischio

Un “rischio” per i diritti e le libertà per le persone fisiche sussiste, secondo i considerando 75 e 76 del GDPR, se il trattamento può cagionare un danno fisico, materiale o immateriale, agli interessati.
Gli impatti per gli Interessati coinvolti possono essere economici (furto o usurpazione d'identità, perdite finanziarie o ogni altro significativo svantaggio economico) o sociali (discriminazione, umiliazione, danno reputazionale or altro significativo svantaggio sociale). Inoltre, gli Interessati potrebbero diversamente essere altrimenti privati dei loro diritti o del controllo sui loro dati personali.
È importante considerare che l’analisi del rischio derivante da una Violazione richiede una **valutazione caso per caso**.

Il Titolare dovrebbe considerare tanto la gravità dell’impatto sui diritti e sulle libertà delle persone fisiche e quanto la probabilità che tale impatto si verifichi.
Chiaramente, se le conseguenze di una Violazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze si verifichino è maggiore, maggiore è anche il rischio.

La valutazione deve tenere conto dei seguenti fattori:

Fattore di rischio	Descrizione
Tipologie di violazione e circostanze della stessa	Il tipo di violazione verificatosi può influire sul livello di rischio presentato per le persone fisiche. Ad esempio, una violazione della riservatezza che ha portato alla divulgazione di informazioni mediche a soggetti non autorizzati può avere conseguenze meno gravi rispetto a una violazione dell’integrità in cui i dettagli medici di una persona fisica sono stati persi e non sono più disponibili perché la salute o addirittura la vita di questa potrebbe essere a rischio Per valutare la **probabilità** del rischio, è importate considerare anche le modalità e le circostanze della violazione e le possibili intenzioni delle persone non autorizzate all’accesso. Per esempio, in caso di furto di un dispositivo portatile, è necessario valutare se l’obiettivo del ladro fosse il valore economico del bene rubato o i dati memorizzati al suo interno (i computer portatili vengono spesso sottratti per rivendere l’apparecchio, piuttosto che i dati che contengono).
Facilità di identificazione	Influisce sul livello di rischio anche la facilità con cui le persone fisiche possono essere identificate. Se è possibile l’identificazione diretta senza particolari ricerche, il rischio è sensibilmente più elevato rispetto a quello posto da dati pseudonimizzati[1], o dati cifrati che sono incomprensibili a chiunque non sia autorizzato ad accedervi in assenza dell’hash/chiave di decodifica.
Natura e «sensibilità» dei dati personali	Il danno potenziale per gli interessati a seconda della natura dei dati personali coinvolti in una violazione può essere particolarmente grave, soprattutto se la violazione può comportare furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione.

[1] Come precisato dal WP29, una pseudonimizzazione opportunamente implementata (definita all’articolo 4, punto 5, come *“il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile”)* può ridurre la probabilità che le persone fisiche vengano identificate in caso di violazione. Tuttavia, le tecniche di pseudonimizzazione da sole non possono essere considerate sufficienti a rendere i dati incomprensibili.

Fattore di rischio	Descrizione
	Solitamente più i dati sono "sensibili" (cioè comprendono (i) categorie particolari di dati personali[2], (ii) dati relativi a condanne o reati penali, (iii) dati soggetti a obbligo professionale di riservatezza, o (iv) altri dati "sensibili"), maggiore è il rischio di danni per gli interessati derivante dal Data Breach. La divulgazione di dati di carte di credito o numeri di previdenza sociale, che possono consentire il furto d'identità (e quindi comportare danni finanziari) oppure di cartelle cliniche, informazioni sulla posizione o situazione finanziaria della persona fisica (in virtù del carattere intrinsecamente privato dei dati) possono determinare conseguenze rilevanti per l'interessato. Violazioni relative a dati sanitari (cartelle cliniche), documenti di identità o dati finanziari come i dettagli di carte di credito, possono tutte causare danni di per sé, ma se tali dati fossero usati congiuntamente, potrebbero essere utilizzati per effettuare un furto d'identità. Di norma una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale. Tuttavia, anche se si tratta di dati "comuni" o "anagrafici", il rischio potrebbe essere elevato. Ad esempio, è **improbabile** che la divulgazione del nome e dell'indirizzo di una persona fisica in circostanze ordinarie causi un danno sostanziale. Se però sono divulgati il nome e l'indirizzo di un genitore adottivo a un genitore biologico, le conseguenze potrebbero essere molto gravi tanto per il genitore adottivo quanto per il bambino. Se invece i dati contengono identificativi interni dell'Organizzazione o informazioni accessibili al pubblico, il rischio per gli interessati è decisamente inferiore.
Tipologia di Interessati	Se gli interessati sono persone vulnerabili o minori, il rischio può essere considerato più elevato. Se gli interessati sono dipendenti dell'Organizzazione o dei suoi fornitori, il rischio può essere minore, poiché è più semplice ottenere assistenza dai medesimi per l'attenuazione dei rischi.
Quantità di dati e di Interessati	Se la Violazione riguarda un numero significativo di dati personali o di Interessati i rischi possono essere più elevati. Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere in quanto è più **probabile** che un soggetto non autorizzato chi vi accede illegalmente possa utilizzare le informazioni in modo causi impatti negativi per gli Interessati. Tuttavia, una Violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi ed una Violazione avente ad oggetto un numero ridotto di dati personali altamente sensibili può comunque avere un forte impatto sugli interessati.
Caratteristiche del soggetto non autorizzato che ha avuto accesso ai dati	Nel caso di una violazione di riservatezza nel cui ambito i dati personali vengono comunicati a terzi per errore, il rischio per gli interessati può essere maggiore se la divulgazione è esterna, piuttosto che interna all'Organizzazione (p. es. a un dipendente). Difatti, se dati personali vengano inviati accidentalmente all'ufficio sbagliato di un'organizzazione o anche a un fornitore abituale "fidato", il Titolare può chiedere al destinatario di restituire o distruggere in maniera sicura i dati ricevuti. In entrambi i casi, dato che il Titolare ha una relazione continuativa con tali soggetti e può essere a conoscenza delle loro procedure, della loro storia e di altri dettagli pertinenti, può ragionevolmente aspettarsi che non leggeranno o accederanno ai dati inviati per errore e che rispetteranno le istruzioni di restituirli o distruggerli. Anche se i dati fossero stati consultati, il Titolare potrebbe comunque confidare nel fatto che i destinatari non li utilizzeranno, li restituiranno tempestivamente e coopereranno per garantirne il recupero. Il fatto che il destinatario sia "affidabile" può neutralizzare la gravità delle conseguenze della violazione, anche se questo non significa che non si sia comunque verificata una violazione. La **probabilità** che detta violazione presenti un rischio per le persone fisiche verrebbe però meno, quindi non sarebbe più necessaria la notifica all'autorità di controllo o la comunicazione agli interessati.
Caratteristiche particolari del	La natura e il ruolo del Titolare e delle sue attività possono influire sul livello di rischio per le persone fisiche in seguito a una violazione. Ad esempio, nel caso di un ospedale che tratta categorie particolari

[2]Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici e dati relativi alla salute o alla vita sessuale.

Fattore di rischio	Descrizione
Titolare del trattamento	di dati personali, vi è una minaccia maggiore per le persone fisiche nel caso in cui i loro dati personali vengano violati, rispetto a una mailing list di un quotidiano.
Misure di protezione applicate sui dati coinvolti	Se sono stati divulgati dati che sono incomprensibili, ad esempio perché cifrati, il rischio può essere minore. Se sono cifrati, è necessario però valutare se la chiave di decodifica è sicura, in quanto se è stata compromessa assieme ai dati, i vantaggi della cifratura verranno meno e il rischio per gli interessati sarà maggiore. Si noti che la password del laptop non assicura lo stesso grado di protezione della cifratura, in quanto il disco fisso può essere acceduto direttamente collegandolo ad altri dispositivi. Se i dati sono contenuti in un dispositivo, è necessario valutare il grado di difficoltà nell'estrarre i dati dal dispositivo. Ad esempio, se i dati sono contenuti su nastri di backup, è meno probabile che i dati siano acceduti da terzi non autorizzati in quanto l'estrazione è più difficile.