

Possibili scenari di "Data Breach"

ESEMPIO	NOTIFICA ALL'AUTORITÀ	COMUNICAZIONE AGLI INTERESSATI	NOTE
<p>Il Titolare conserva il backup di un archivio di dati personali criptati su una chiave USB</p>	NO	NO	<p>Per tutto il tempo in cui i dati sono criptati con uno stato di algoritmi sempre aggiornati, i backup dei dati esistono in un'unica chiave che non è compromessa, e i dati possono essere conservati periodo di tempo corretto, questo non può essere considerato violazione da riportare</p>
<p>Il Titolare gestisce un servizio on line. A seguito di un attacco informatico su quel servizio, i dati personali dei suoi utenti sono stati trafugati. Il Titolare ha utenti in un singolo stato membro</p>	Sì, riferire all'Autorità di controllo se c'è una probabile conseguenza per gli individui	Sì, riferire agli interessati, in base alla natura dei dati personali coinvolti, se la gravità delle probabili conseguenze per gli interessati è alta	
<p>Una breve interruzione di corrente di qualche minuto di durata presso il call center del Titolare che comporta che gli utenti non sono in grado di contattare il Titolare e accedere alla loro documentazione</p>	NO	NO	<p>Questa non è una violazione da notificare, tuttavia è un incidente registrabile secondo l'art. 33 DEL GDPR.</p> <p>Appropriata documentazione sull'evento dovrebbe essere mantenuta dal Titolare</p>

Possibili scenari di “Data Breach”

<p>Un Titolare subisce un attacco informatico <i>ransomware</i> per cui tutti i dati sono decriptati. Non sono disponibili backup e i dati non posso essere recuperati. In fase di investigazione, risulta chiaramente che l'unica caratteristica del <i>ransomware</i> era di decriptare i dati e che non c'era altro <i>malware</i> presente nel sistema.</p>	<p>Sì, riferire all'Autorità di controllo, se ci sono probabili conseguenze per gli individui poiché in questo caso c'è perdita di disponibilità.</p>	<p>Sì, riferire agli individui, in base alla natura dei dati interessati e alla possibile conseguenza della mancanza di disponibilità dei dati, quali possono essere le possibili conseguenze.</p>	<p>Se c'è un <i>backup</i> disponibile e i dati possono essere conservati per un tempo limitato, questo potrebbe non essere riferito all'Autorità di controllo o agli individui poiché non ci sarebbe mancanza definitiva di disponibilità o confidenzialità. Comunque, se l'Autorità di controllo viene a conoscenza di un incidente per altre vie, può considerare un indagine per valutare la bontà l'adempimento rispetto ai più ampi requisiti di sicurezza in base all'art. 32.</p>
<p>Un individuo contatta il call center di una banca per riferire di una violazione di dati. L'individuo ha ricevuto l'estratto conto mensile di qualcun altro. Il Titolare intraprende una piccola indagine (es. che si risolve in 24 ore) e ritiene con ragionevole sicurezza che c'è stata violazione dei dati e che il problema sul sistema può o potrà coinvolgere altri individui.</p>	<p style="text-align: center;">SI</p>	<p style="text-align: center;">Solo agli individui interessati viene notificato se c'è alto rischio ed è chiaro che non riguarda altri.</p>	<p>Se, dopo un'ulteriore indagine si riscontra che l'evento riguarda più interessati, si deve aggiornare l'Autorità di controllo e il Titolare notifica l'evento anche agli altri interessati coinvolti se c'è alto rischio per loro.</p>

Possibili scenari di "Data Breach"

<p>Una mail di <i>direct marketing</i> viene inviata a destinatari nei campi "a" o "cc", consentendo così ad ogni destinatario di vedere l'indirizzo mail di altri destinatari.</p>	<p>Sì, la notifica all'Autorità di controllo può essere obbligatoria se sono coinvolti un gran numero di individui e se sono rivelati <i>dati sensibili</i> (es. nella mailing list di uno psicoterapeuta) o se altri fattori presentano alti rischi (es. la mail contiene le password).</p>	<p>Sì, riferire agli individui in base allo scopo ed al tipo di dati personali coinvolti ed alla gravità delle possibili conseguenze.</p>	<p>La notifica può non essere necessaria se nessun <i>dato sensibile</i> viene rivelato e se viene rivelato solo un minimo numero di indirizzi mail.</p>
<p><u>Hardware</u> Utilizzo di chiavette o dischi USB inappropriati per la sensibilità delle informazioni, uso o trasporto di <i>hardware</i> sensibile per scopi personali, il disco rigido contenente le informazioni viene utilizzato per uno scopo non previsto (ad esempio per trasportare altri dati ad un fornitore, per trasferire altri dati da un database all'altro, ecc.)</p>	<p>Sì, riferire all'Autorità di controllo se c'è una probabile conseguenza per gli individui</p>	<p>Sì, riferire agli interessati, in base alla natura dei dati personali coinvolti, se la gravità delle probabili conseguenze per gli interessati è alta</p>	
<p><u>Hardware</u> Osservazione di uno schermo ad insaputa dell'utilizzatore in un treno, fotografia di uno schermo, geolocalizzazione di un hardware, captazione a distanza di segnali elettromagnetici</p>	<p>Intervento del DPO</p>	<p>Intervento del DPO</p>	

Possibili scenari di "Data Breach"

<p><u>Hardware</u> Tracciatura con un <i>keylogger</i>, rimozione di un componente <i>hardware</i>, connessione di un dispositivo (es. chiave USB) per avviare un sistema operativo o recuperare i dati</p>	Intervento del DPO	Intervento del DPO	
<p><u>Hardware</u> Furto di un <i>laptop</i> in una camera d'albergo, furto di un telefono cellulare professionale da parte di un borseggiatore, recupero di materiale o supporti da rottamare, perdita di un supporto di memorizzazione elettronico, non cancellazione di dati da materiale o supporti venduti o ceduti a terzi</p>	Intervento del DPO	Intervento del DPO	
<p><u>Software</u> Ricerca di contenuti, incrocio di dati illegittimo, elevazione di privilegi, cancellazione di tracce, invio di spam dal sistema di messaggistica, messa fuori uso della rete</p>	Intervento del DPO	Intervento del DPO	
<p><u>Software</u> Scansione di indirizzi e porte di rete, raccolta di dati di configurazione, studio del codice sorgente per determinare errori sfruttabili, test delle risposte del database a <i>query</i> dannose</p>	Intervento del DPO	Intervento del DPO	

Possibili scenari di “Data Breach”

<p><u>Software</u> Tracciatura con un <i>keylogger</i>, contagio da codice dannoso, installazione di uno strumento di controllo remoto, sostituzione di un componente con un altro durante un aggiornamento, un'operazione di manutenzione o un'installazione (parti del codice o dell'applicazione sono installati o sostituiti)</p>	Intervento del DPO	Intervento del DPO	
<p><u>Rete di dati</u> Intercettazione di flussi di dati sulla rete <i>Ethernet</i>, acquisizione di dati su una rete <i>wireless</i></p>	Intervento del DPO	Intervento del DPO	
<p><u>Persone</u> Divulgazione involontaria durante la conversazione, ascolto delle conversazioni in una sala riunioni con apparecchiature di amplificazione</p>	Intervento del DPO	Intervento del DPO	
<p><u>Persone</u> Influenza (<i>phishing</i>, ingegneria sociale, corruzione), pressione (ricatto, molestie morali)</p>	Intervento del DPO	Intervento del DPO	
<p><u>Persone</u> Assunzione di dipendenti, cambio di incarico, acquisizione di tutta o parte dell'organizzazione</p>	Intervento del DPO	Intervento del DPO	
<p><u>Documenti cartacei</u> Lettura, fotocopia, fotografia</p>	Intervento del DPO	Intervento del DPO	

Possibili scenari di "Data Breach"

<u>Documenti cartacei</u> Furto di documentazione negli uffici, furto di posta nella cassetta postale, recupero di documenti gettati nei rifiuti	Intervento del DPO	Intervento del DPO	
<u>Trasmissione di documenti cartacei</u> Lettura di libri firma in circolazione, riproduzione di documenti in transito	Intervento del DPO	Intervento del DPO	
<u>Hardware</u> Aggiunta di hardware incompatibile che determina un malfunzionamento, rimozione dell'hardware essenziale per il corretto funzionamento di un'applicazione	Intervento del DPO	Intervento del DPO	
<u>Software</u> Modifiche non desiderate in un <i>database</i> , cancellazione di file utili per il corretto funzionamento, errore di manipolazione che porta alla modifica dei dati	Intervento del DPO	Intervento del DPO	
<u>Software</u> Errore durante l'aggiornamento, la configurazione o la manutenzione, contagio da codice malevolo, sostituzione di un componente con un altro	Intervento del DPO	Intervento del DPO	

Possibili scenari di "Data Breach"

<p><u>Rete di dati</u> Attacco "man-in-the-middle" per modificare o aggiungere dati al traffico di rete; <i>replay attack</i> (rinvio di dati intercettati)</p>	Intervento del DPO	Intervento del DPO	
<p><u>Documenti cartacei</u> Modifica dei numeri in un documento, sostituzione di un documento con un falso</p>	Intervento del DPO	Intervento del DPO	
<p><u>Trasmissione di documenti cartacei</u> Modifica di una nota all'insaputa dell'estensore, sostituzione di un libro firma con un altro, invio multiplo di lettere contraddittorie</p>	Intervento del DPO	Intervento del DPO	
<p><u>Hardware</u> Archiviazione di file personali, utilizzo per scopi personali</p>	Intervento del DPO	Intervento del DPO	
<p><u>Hardware</u> Unità di memoria piena, interruzione di corrente, sfruttamento eccessivo delle capacità di elaborazione, surriscaldamento, eccessiva temperatura, attacco "Denial of Service"</p>	Intervento del DPO	Intervento del DPO	
<p><u>Hardware</u> Aggiunta di hardware incompatibile che porta ad un malfunzionamento, rimozione di un componente necessario per il funzionamento del sistema</p>	Intervento del DPO	Intervento del DPO	

Possibili scenari di "Data Breach"

<p><u>Hardware</u> Inondazioni, incendi, atti vandalici, degradazione dovuta all'usura naturale, malfunzionamento di un dispositivo di memorizzazione</p>	Intervento del DPO	Intervento del DPO	
<p><u>Hardware</u> Furto di un <i>laptop</i>, perdita di un telefono cellulare, rottamazione di un supporto o di attrezzature, dischi sottodimensionati che portano ad una moltiplicazione di supporti e alla perdita di alcuni di loro</p>	Intervento del DPO	Intervento del DPO	
<p><u>Software</u> Cancellazione di dati, utilizzo di software contraffatto o copiato, errore dell'operatore che porta alla cancellazione dei dati</p>	Intervento del DPO	Intervento del DPO	
<p><u>Software</u> Superamento del dimensionamento del database, inserimento di dati al di fuori dei valori previsti, attacco "<i>Denial of Service</i>"</p>	Intervento del DPO	Intervento del DPO	
<p><u>Software</u> Errore durante l'aggiornamento, la configurazione o la manutenzione, contagio da codice malevolo, sostituzione di un componente con un altro</p>	Intervento del DPO	Intervento del DPO	

Possibili scenari di "Data Breach"

<u>Software</u> Cancellazione di un programma in esecuzione o di codice sorgente, virus, <i>malware</i> "bomba logica"	Intervento del DPO	Intervento del DPO	
<u>Software</u> Non rinnovo della licenza software utilizzata per accedere ai dati, interruzione degli aggiornamenti di sicurezza da parte del produttore, fallimento del produttore, corruzione del modulo di archiviazione contenente i numeri di licenza	Intervento del DPO	Intervento del DPO	
<u>Rete di dati</u> Riduzione della larghezza di banda, <i>download</i> non autorizzato, interruzione dell'accesso a Internet	Intervento del DPO	Intervento del DPO	
<u>Rete di dati</u> Interruzione del cablaggio, scarsa ricezione della rete Wi-Fi, ossidazione dei cavi	Intervento del DPO	Intervento del DPO	
<u>Persone</u> Decesso, pensionamento, cambio di incarico, fine del contratto o licenziamento, acquisizione di tutta o parte dell'organizzazione	Intervento del DPO	Intervento del DPO	

Possibili scenari di "Data Breach"

<u>Documenti cartacei</u> Cancellazione graduale nel tempo, cancellazione volontaria di parti di un testo, riutilizzo di documenti per prendere appunti estranei al trattamento, uso di quaderni per fare qualcos'altro	Intervento del DPO	Intervento del DPO	
<u>Documenti cartacei</u> Invecchiamento di documenti archiviati, bruciatura di documenti durante un incendio	Intervento del DPO	Intervento del DPO	
<u>Documenti cartacei</u> Furto di documenti, perdita di documenti durante un trasloco, smaltimento	Intervento del DPO	Intervento del DPO	
<u>Trasmissione di documenti cartacei</u> Sovraccarico dei servizi postali, sovraccarico di un processo di convalida	Intervento del DPO	Intervento del DPO	
<u>Trasmissione di documenti cartacei</u> Taglio del flusso a seguito di una riorganizzazione, blocco della posta a causa di uno sciopero	Intervento del DPO	Intervento del DPO	
<u>Trasmissione di documenti cartacei</u> Modifica delle modalità di spedizione, riassegnazione di uffici o locali, riorganizzazione della spedizione di documenti cartacei, cambio della lingua utilizzata	Intervento del DPO	Intervento del DPO	

Possibili scenari di "Data Breach"

<u>Trasmissione di documenti cartacei</u> Riorganizzazione che elimina un processo, scomparsa di un corriere di documenti, perdita delle poste	Intervento del DPO	Intervento del DPO	
---	--------------------	--------------------	--