LICEO STATALE "*Enrico Fermi*" CECINA
LICEO SCIENTIFICO - LICEO SCIENTIFICO Sez. INDIRIZZO SPORTIVO - LICEO CLASSICO - LICEO LINGUISTICO
LICEO DELLE SCIENZE UMANE - LICEO DELLE SCIENZE UMANE opzione ECONOMICO SOCIALE
Via Ambrogi,12 - 57023 Cecina (Li) **- Tel**. 0586/ 681515
Email: lips02000l@istruzione.it **Pec:** lips02000l@pec.istruzione.it **Internet:** www.fermicecina.edu.it
C.F. 80009280498 C.M. LIPS02000L

Procedura di Data Breach

1. Data Breach = Violazione dei dati personali:

"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" (art. 4, n. 12 del Regolamento UE 2016/679.
Le indicazioni della Procedura valgono per qualsiasi tipologia di Dato personale.

2. Gli eventi di Data Breach possono riguardare:
   - sia casi cui è connesso un rischio marginale (es. perdita di una chiavetta USB);
   - che casi più critici di furto o perdita di intere basi dati (es. le banche dati gestite dal Titolare).

Nel caso in cui si verifichi una delle casistiche di seguito riportate, o un analogo scenario, è fondamentale chiedersi se e quale tipo di Dati personali sono coinvolti nell'evento, e, di conseguenza, procedere alla segnalazione.

- furto o smarrimento di laptop, smartphone, tablet del Titolare contenenti Dati personali;
- furto o smarrimento di documenti cartacei contenenti Dati personali;
- furto o smarrimento di dispositivi portatili di archiviazione non criptati, come chiavette USB e hard disk esterni, contenenti Dati personali;
- perdita o modifica irreparabile di archivi contenenti Dati personali in formato cartaceo o digitale (ad esempio, a causa di una errata cancellazione o modifica dai sistemi o dagli archivi digitali del Titolare che non possa essere ripristinata attraverso l'uso di un backup);
- diffusione impropria di Dati personali, per mezzo di:
  - invio di e-mail contenente Dati personali al destinatario errato;
  - invio di e-mail con un file contenente Dati personali allegato erroneamente;

- esportazione fraudolenta o errata di Dati personali dai sistemi del Titolare;
- richiesta di invio di documenti e file contenenti Dati personali da parte di un esterno che si finge fraudolentemente un collega, collaboratore e/o altro soggetto e conseguente invio allo stesso di tali documenti e file;

- segnalazione da parte di un fornitore di un evento di Data Breach sui propri sistemi che ha interessato o potrebbe potenzialmente interessare Dati personali del Titolare del trattamento.

3. Processo di gestione del Data Breach

Al fine di consentire una gestione efficace e tempestiva delle violazioni dei Dati personali, il Titolare del trattamento adotta un processo strutturato per la gestione dei casi di Data Breach che prevede:

- Rilevazione e segnalazione del Data Breach;
- Analisi del Data Breach;
- Risposta e notifica del Data Breach;
- Registrazione del Data Breach.

4. Rilevazione e segnalazione del Data Breach

La rilevazione e segnalazione del Data Breach è un obbligo per tutti i dipendenti e/o collaboratori del Titolare del trattamento.

Nel caso in cui si sia verificato uno degli eventi descritti o in tutti gli altri casi in cui il soggetto che tratta dati personali sia consapevole di altri eventi potenzialmente rischiosi per i documenti e gli archivi, è tenuto a informare immediatamente il Titolare, il quale **provvede – senza indugio** – a darne notizia al responsabile per la protezione dei dati personali (DPO) o al suo Consulente Privacy di fiducia.

Tutti i dati relativi al Data Breach dovranno essere **inseriti nell' apposito registro di Data Breach**.

Al Registro, per ogni singolo incidente di Data Breach, dovranno essere **allegate tutte le comunicazioni** relative all'incidente (ad es. denuncia all'autorità giudiziaria, notifica al Garante Privacy e relativa corrispondenza, comunicazioni agli interessati, etc.).
In tale Registro dovranno essere inseriti tutti gli eventi che determinano o configurano anomalie rispetto alla normale gestione dei sistemi (ad esempio: Virus, perdita di dati, alterazione di dati, attacchi alla rete, furti di credenziali, ecc.).

5. Analisi del Data Breach

A seguito della rilevazione e/o segnalazione, il Titolare, sentito il DPO o il Consulente Privacy, effettua una valutazione al fine di verificare che nell'incidente rilevato siano stati effettivamente violati i Dati personali trattati dal Titolare.

Suddetta analisi è finalizzata alla raccolta ed identificazione delle seguenti informazioni:

- categorie di Interessati cui i Dati personali violati si riferiscono (ad esempio, utenti, dipendenti, fornitori, etc.);
- categorie di Dati personali compromessi (ad esempio, Dati personali, Dati sensibili, Dati giudiziari);

- tipologia di Data Breach: violazione della riservatezza, disponibilità o integrità (ad esempio, accesso non autorizzato, perdita, alterazione, furto, disclosure, distruzione, etc.).

Nell'ambito di tale analisi, il Titolare del trattamento, con il supporto del DPO o del Consulente della Privacy, identifica le azioni di prima risposta da intraprendere nell'immediato per contenere gli impatti della violazione dei Dati personali.

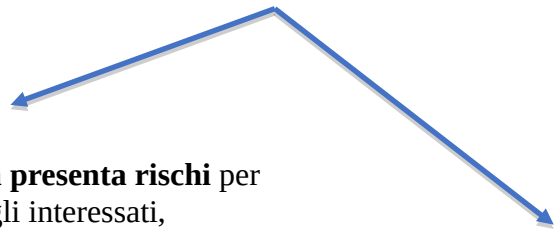
Nell'ambito dell'analisi della violazione, vengono identificate anche le seguenti informazioni:

- identificabilità degli Interessati i cui dati rappresentano l'oggetto della violazione;
- misure di sicurezza tecniche e organizzative che potrebbero aver parzialmente o in toto mitigato gli impatti relativi al Data Breach;
- ritardi nella rilevazione del Data Breach;
- numero di individui interessati.

Sulla base di suddetti parametri, il Titolare del trattamento procede alla **valutazione della gravità** del Data Breach relativamente ai diritti ed alle libertà degli Interessati, a seconda della natura dei Dati personali (ad esempio, Dati Sensibili e/o Giudiziari), delle misure di sicurezza adottate, della tipologia di interessati (ad esempio, minori o altri soggetti vulnerabili).

6. Risposta e notifica del Data Breach

La precedente fase di analisi fornisce al Titolare del trattamento gli strumenti necessari a identificare e valutare le conseguenze negative e gli impatti causati dalla violazione di Dati personali rilevata.



Se il Data Breach **non presenta rischi** per i diritti e le libertà degli interessati, **la notifica all'Autorità Garante non è obbligatoria.** Tale valutazione è condivisa con il DPO o con il Consulente Privacy.

Se è possibile che il Data Breach presenti **rischi** per i diritti e le libertà degli Interessati, il Titolare, con il supporto del DPO e del Consulente Privacy, deve predisporre la **notifica all'Autorità Garante**.

La notifica viene effettuata all'Autorità Garante **entro 72 ore** dal momento in cui il Data Breach è stato rilevato.

Suddetta **notifica** contiene **almeno** le seguenti informazioni:

- natura della violazione dei dati personali (disclosure, perdita, alterazione, accesso non autorizzato, etc.);
- tipologie di Dati personali violati;
- categorie e numero approssimativo di Interessati cui i dati compromessi si riferiscono;
- nome e dati di contatto del DPO se presente, che sarà l'interfaccia per Titolare del trattamento nei confronti dell'Autorità di controllo;
- probabili conseguenze della violazione dei Dati personali;
- descrizione delle misure che il Titolare del trattamento ha adottato o è in procinto di adottare al fine di mitigare le conseguenze del Data Breach;
- ove la stessa non sia presentata entro 48/72 ore dalla rilevazione, i motivi dell'eventuale ritardo nella comunicazione.

Qualora non sia stato possibile fornire contestualmente tutte le informazioni obbligatorie, il Titolare raccoglie quanto prima le informazioni supplementari e provvede a integrare, **senza ritardo**, la notifica già inoltrata all'Autorità di Controllo.

Oltre a notificare il Data Breach all'Autorità Garante, il Titolare è tenuto a valutare **l'esigenza di procedere con la denuncia all'Autorità Giudiziaria competente**, nonché con la notifica del Data Breach, **anche ai soggetti interessati** i cui dati siano stati violati.

Per stabilire se sia necessario provvedere alla notifica agli Interessati, il Titolare del trattamento, di concerto con il DPO o con il Consulente Privacy deve valutare i seguenti fattori:

- il trattamento può comportare discriminazioni, furto d'identità, perdite finanziare, disturbi psicologici, pregiudizio alla reputazione, perdita di riservatezza dei Dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo;
- gli Interessati rischiano di essere privati dei loro diritti, delle libertà o venga loro impedito l'esercizio del controllo sui Dati personali che li riguardano;
- sono trattati Dati personali che rivelano l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;
- in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- sono trattati Dati personali di persone fisiche vulnerabili, in particolare minori;
- il trattamento riguarda una notevole quantità di Dati personali e un vasto numero di Interessati.

La **notifica agli Interessati** deve, pertanto, avvenire nel caso in cui la violazione di Dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, a meno che non sia verificata almeno una delle seguenti condizioni:

- sono state applicate adeguate misure tecniche e organizzative per proteggere i dati prima della violazione, in particolare quelle in grado di renderle non intelligibili per soggetti terzi non autorizzati (ad esempio, misure di cifratura);
- a valle della rilevazione del Data Breach, sono state adottate misure per impedire il concretizzarsi dei rischi per i diritti e le libertà degli Interessati;
- la notifica del Data Breach a tutti gli Interessati singolarmente comporta uno sforzo sproporzionato rispetto al rischio. In tal caso occorrerà comunque procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati possano essere comunque informati con analoga efficacia.

Il Titolare, di concerto con il DPO o il Consulente Privacy valuta di volta in volta, sulla base della tipologia e del numero di Interessati, il canale di comunicazione che appare più opportuno per trasmettere la notifica agli stessi.
In ogni caso la notifica agli Interessati deve contenere almeno:

- nome e dati di contatto del DPO;
- descrizione delle probabili conseguenze della violazione;
- descrizione delle misure adottate o che il Titolare intende adottare per porre rimedio alla violazione e ridurre gli effetti negativi.

7. Data Breach relativo a dati personali trattati in qualità di Responsabile del trattamento

Qualora, a seguito di una segnalazione o nel corso dell'analisi preliminare di cui al precedente paragrafo 4, il Titolare rilevasse che la violazione qualificabile come Data Breach riguarda dati personali di titolarità di un soggetto terzo trattati dal Titolare in qualità di Responsabile del trattamento, procede a informare senza ingiustificato ritardo il soggetto terzo titolare del trattamento.
Nel dettaglio, la comunicazione al soggetto Titolare del trattamento dovrà contenere almeno le seguenti informazioni (oltre a quelle eventualmente richieste dallo stesso soggetto terzo titolare del trattamento):

- descrizione della natura della violazione dei dati personali comprensiva, ove possibile, di informazioni in merito alle categorie e al numero di Interessati nonché alle categorie e al volume approssimativo di dati personali oggetto di violazione;
- nome e dati di contatto del DPO o del Consulente Privacy;
- descrizione delle possibili conseguenze della violazione;
- descrizione di eventuali misure già adottate o di cui si prevede l'adozione per porre rimedio alla violazione di dati personali e per attenuarne i possibili effetti negativi.

La comunicazione, nel testo convalidato dal DPO o dal Consulente Privacy, sarà inviata al soggetto titolare del trattamento entro 48 ore dall'avvenuta rilevazione della violazione o nel minore termine eventualmente indicato dal soggetto titolare del trattamento.