Procedura: cosa fare in caso di
"DATA BREACH"
Ossia, in caso si verifichi una VIOLAZIONE DI DATI PERSONALI

In integrazione delle procedure adottate dal Titolare del trattamento in materia di protezione dei dati personali, ai sensi della normativa vigente, si adotta la procedura seguente, da seguire qualora vi fosse un cd "*data breach*".

1. Premessa.

Ai sensi del Regolamento Europeo 2016/679 (di seguito "il GDPR"), il Titolare del trattamento di dati personali è tenuto a garantire la sicurezza dei dati personali da esso trattati e ad adottare idonee misure di sicurezza di tipo tecnico e organizzativo. Infatti, ogni Titolare deve poter dimostrare di aver adottato tali misure di sicurezza al fine garantire la protezione dei dati personali fin dall'inizio del trattamento *(privacy by design*) per impostazione predefinita (*privacy by default*). Qualora, nonostante l'adozione di tali misure, dovesse verificarsi una violazione dei dati personali all'interno della propria struttura, il Titolare del Trattamento deve tenere determinati comportamenti, fra cui la notifica di quanto avvenuto all'Autorità Garante per la protezione dei dati (di seguito "Garante Privacy").
Il presente documento è volto a chiarire al Titolare del Trattamento cosa è ad esso richiesto dalla normativa in caso di violazione di dati personali e a dare spunti su come sia possibile, con piccoli accorgimenti, evitare il verificarsi di tali violazioni di dati personali. Inoltre, alla fine della trattazione, si troveranno allegati due documenti:
- modello di comunicazione da inviare agli interessati;
- registro delle violazioni su cui riportare le azioni intraprese e/o le eventuali cause di esoneri.

2. Cosa si intende con "data breach"?

Troviamo una definizione di *data breach* nell'art.4 GDPR, il quale indica che si tratta di qualunque "*violazione di sicurezza che comporti 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.

Dunque, una violazione di dati personali può accadere sia accidentalmente che di proposito: i dati personali subiscono un trattamento non voluto dal Titolare, non preventivato e che le misure di sicurezza adottate non hanno potuto evitare. Questo può avvenire sia a causa di comportamenti dolosi di terzi che a seguito di un semplice errore da parte di una persona autorizzata al trattamento degli stessi.
Esempi di *data breach*: perdita o furto di documenti cartacei e/o digitali, casi di pirateria informatica, invio di una comunicazione riservata a persone diverse dai destinatari (sia per errore che per gesto volontario), divulgazione di dati confidenziali a persone non autorizzate, ecc.

3. Cosa deve fare il Titolare del trattamento in caso di data breach?

Il titolare del trattamento ha l'obbligo innanzitutto di prendere coscienza e di **documentare** l'avvenuta violazione, le circostanze che hanno causato tale violazione, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Il GDPR stabilisce che, qualora vi sia un rischio per i diritti e le libertà personali degli interessati, il *data breach* va comunicato al Garante Privacy. Quando vi sia **alta probabilità** di rischio dei diritti e delle libertà personali, la violazione vada comunicata, oltre che al Garante Privacy, anche agli interessati. La valutazione relativa alla sussistenza della

"*alta probabilità di rischio dei diritti e delle libertà personali*" è rimessa alla valutazione del Titolare del trattamento. Questo riflette il generale senso di responsabilizzazione che il GDPR vuole infondere nel Titolare del trattamento, al fine di porre in essere azioni frutto di ragionamento.

> ***Esempi concreti di data breach:***
>
> *Pensiamo, ad esempio, a un invio di una comunicazione e-mail inviata in C/C da parte di una struttura sanitaria o da un ente erogatore di mutui a tutti i propri utenti – i quali possono così prendere visione di tutti gli indirizzi e-mail degli altri utenti. In tal caso siamo in presenza di un tale "alto rischio": tutti gli utenti possono vedere gli indirizzi e-mail degli altri utenti e, in questo modo, sapere che la persona è anch'essa utente della struttura sanitaria o ha acceso un mutuo presso la struttura in questione. Si ricorda a tal fine che anche l'indirizzo e-mail è un dato personale.*
>
> *Un ulteriore caso di data breach si ha qualora vi sia la perdita o il furto di un supporto, sia cartaceo (un raccoglitore) che informatico (ad esempio un notebook o un cellulare aziendale) su cui sono conservati dati personali (magari anche sensibili) di clienti.*
>
> *Nel mondo scolastico si può pensare alla documentazione relativa a PEI e PDP che va persa, erroneamente eliminata in modo non rimediabile o la cui riservatezza viene violata.*
>
> *Rientra nella concezione di data breach anche il caso di infedeltà aziendale, qualora ad esempio un dipendente - soggetto autorizzato al trattamento di determinati dati personali - ne faccia una copia che poi diffonda al pubblico, ad esempio su qualche Social Network.*
>
> *Si può inoltre far riferimento a un attacco informatico, per cui i dati personali detenuti dal Titolare del trattamento nel sistema informatico aziendale vengano distrutti o sottratti intenzionalmente.*

Laddove tale valutazione dia esisto positivo (e dunque vi sia *alto rischio*) il Titolare del trattamento – oppure, se nominato, il DPO per conto del Titolare - ha l'obbligo di tenere i seguenti comportamenti:

- **notificare l'avvenuta violazione al Garante Privacy** (mediante l'utilizzo del modulo in allegato);
- **comunicare agli interessati la violazione** (è buona prassi spiegare l'accaduto, scusandosi con gli interessati i cui dati personali sono stati oggetto di violazione).

Si specifica che tali comportamenti devono avvenire **entro 72 ore** dalla presa coscienza della violazione.

È importante inoltre sottolineare che un *data breach* di cui risponde il Titolare del trattamento può essere commesso:

- sia dai lavoratori dipendenti o che comunque fanno parte dell'organizzazione interna del Titolare, da esso autorizzati a trattare dati personali;
- sia dai "Responsabili del trattamento" ex art.28

  …se la violazione viene commessa dal Responsabile del trattamento egli deve comunicare al Titolare, senza ingiustificato ritardo dal momento in cui ne viene a conoscenza, qualsiasi violazione dei dati personali. Si raccomanda di inserire un passaggio riguardante tale obbligo nella nomina del Responsabile del trattamento, al fine di assicurarsi la piena comprensione della necessità di effettuare tale comunicazione.

Tutti questi soggetti devono essere informati della presente procedura, al fine di gestire correttamente, in collaborazione con il Titolare del trattamento, una tale evenienza.

PROCEDURA - DATA BREACH

1) PRESA CONSAPEVOLEZZA DELL'AVVENUTA VIOLAZIONE DI DATI PERSONALI

Chiunque, all'interno dell'Istituto comprensivo "Bolzano II – Don Bosco", si accorga dell'avvenuta violazione di dati personali (o abbia il sospetto che possa essere avvenuta) **deve immediatamente allertare il Dirigente Scolastico oppure il DPO.**

2) VALUTAZIONE DEL RISCHIO

La persona competente per la gestione degli aspetti privacy nell'Istituto comprensivo "Bolzano II – Don Bosco", al fine di stabilire se sia effettivamente accaduto un *data breach*, dovrà effettuare delle verifiche, raccogliendo le seguenti informazioni:

- innanzitutto, è necessario definire se effettivamente si è in presenza di un *data breach;*
- secondariamente si deve individuare la data di scoperta della violazione;
- infine, è necessario inquadrare la natura della violazione e dei dati coinvolti (breve descrizione dell'incidente) e il numero approssimativo degli interessati coinvolti nella violazione.

Successivamente alla raccolta di tali informazioni, l'Istituto comprensivo "Bolzano II – Don Bosco" dovrà procedere a valutare il **rischio connesso alla violazione di dati personali** riscontrata.

Vi sono diversi elementi da tenere in debito conto nell'ambito della valutazione del rischio, come ad esempio la facilità con cui potrebbero essere *identificati* gli interessati (per esempio, se i dati sono identificativi - come i dati anagrafici di nome e cognome degli interessati - il rischio è maggiore rispetto a dati non identificativi ed è ancora minore se sono state utilizzate tecniche di crittografia).

Se possibile, bisogna poi valutare le caratteristiche (per esempio, qualora si tratti di minori) e il numero degli individui interessati. Inoltre, in questa valutazione assumono rilevanza anche le caratteristiche del Titolare (per esempio, qualora eserciti un'attività in ambito sanitario, a cui corrisponde il massiccio trattamento - e dunque la violazione - di dati sensibili).

Nella pagina seguente, è riportata una tabella in base alla quale è possibile valutare il rischio connesso a un *data breach*, considerando due variabili: "probabilità" che avvenga una violazione e "gravità" della violazione stessa.

P (Probabilità)						
	4	Molto probabile: avviene nella maggior parte dei casi (probabilità maggiore del 50%)	**4**	**8**	**12**	**16**
	3	Probabile: avviene in una buona parte dei casi (probabilità fra il 20% ed il 50%)	**3**	**6**	**9**	**12**
	2	Poco probabile: può accadere in un certo numero di casi (probabilità fra il 5% ed il 20%)	**2**	**4**	**6**	**8**
	1	Improbabile: è improbabile, accade solo in circostanze eccezionali (probabilità minore del 5%)	**1**	**2**	**3**	**4**
			Nessun impatto sul trattamento dei dati di un servizio erogato internamente o esternamente	Impatto lieve sul trattamento dei dati di uno specifico servizio, come ad esempio: allungamento dei tempi interni di processo; ritardo, disservizio o danno a singolo cliente/utente; mancato adempimento senza risvolti economici	Impatto importante sul trattamento dei dati, come: stallo del processo interno; ritardo, disservizio o danno a più clienti/utenti o a utente/cliente con impatto rilevante sul fatturato; mancato adempimento o inefficienza con risvolti economici	Conseguenze gravissime sul trattamento dei dati, come: blocco dell'erogazione del servizio verso l'esterno; sanzioni; pubblicità dell'evento su siti istituzionali, testate giornalistiche, ecc.; impatto a livello societario ed organizzativo
			1	**2**	**3**	**4**
			G (Gravità)			

A seguito di tale valutazione, il Titolare del trattamento deve decidere comportarsi a seconda del *rischio* derivante dalla violazione dei dati personali:

1. qualora la violazione di dati personali non presenti alcun rischio (**raro**), essa non deve essere comunicata;
2. qualora la violazione di dati personali comporti un rischio, va effettuata la notifica al Garante Privacy;
3. qualora la violazione di dati personali comporti un *rischio elevato per i diritti e le libertà dell'interessato*, si procede inoltre alla comunicazione ai soggetti interessati.

3) LA NOTIFICA AL GARANTE PRIVACY - ENTRO 72 ORE

A seguito della valutazione della necessità di effettuare la notifica della violazione dei dati personali al Garante Privacy, il Titolare del Trattamento deve provvedere a tale notifica, *senza ingiustificato ritardo* e ove possibile entro 72 ore dal momento della scoperta. La notifica al Garante Privacy deve contenere i seguenti elementi:

- la natura della violazione dei dati personali (categorie e numero approssimativo di persone e record di dati in questione);
- il nome e le informazioni di contatto dell'Istituto comprensivo "Bolzano II – Don Bosco";
- il nome e le informazioni di contatto del DPO (laddove applicabile);
- le probabili conseguenze della violazione;
- le misure adottate o da adottare per porre rimedio alla violazione stessa.

Si raccomanda inoltre di mettere in atto adeguate misure per porre rimedio alla violazione e mitigare le conseguenze dell'avvenuta violazione di dati personali.

4) LA COMUNICAZIONE AGLI INTERESSATI (se valutata come necessaria)

Scritta con linguaggio semplice e chiaro, tale comunicazione è volta a informare le persone i cui dati personali sono stati violati dell'avvenuta violazione di dati personali, delle probabili conseguenze, nonché delle misure di sicurezza adottate – o che si stanno adottando. Si indicano inoltre i dati del DPO. La comunicazione agli interessati deve avvenire entro un tempo ragionevole - non vi sono nel Regolamento UE 2016/679 indicazioni *esatte* sulle tempistiche da seguire, come per la notifica al Garante Privacy. Sono privilegiate le modalità di comunicazione diretta agli interessati, ad esempio mediante posta elettronica, in quanto aventi maggiore efficacia conoscitiva.

3) ANNOTAZIONE NEL REGISTRO DELLE VIOLAZIONI

L'avvenuta violazione dovrà inoltre essere annotata da parte del Titolare del Trattamento in un Registro delle violazioni, documentazione volta a tenere traccia delle eventuali violazioni di dati personali avvenute nell'ambito dell'attività di trattamento del Titolare. In questo, oltre a riportare le informazioni contenute nella notifica rivolta al Garante Privacy, il Titolare dovrà riportare le valutazioni e i ragionamenti effettuati in fase di valutazione del rischio, e dare conto delle decisioni prese. Il registro *data breach* dovrà inoltre presentare una struttura tale da garantire l'integrità e l'immodificabilità delle registrazioni in esso contenute.

ALLEGATO 1

Modulo comunicazione di una violazione agli interessati

Gentile Interessato,

siamo venuti a conoscenza che una violazione dei nostri [*elenco dei sistemi interessati dalla violazione: es. sistemi informatici, sistemi di archiviazione cartacea ,..*] ha fatto venir meno ad una o più delle proprietà della sicurezza delle informazioni: riservatezza, disponibilità ed integrità. Abbiamo immediatamente provveduto a notificare tale violazione al Garante Privacy nei modi e nei tempi previsti dal art. 33 del Regolamento UE 2016/679.
Per ridurre il più possibile la gravità e la portata di tale violazione abbiamo incaricato esperti di sicurezza informatica ed esperti legali che parallelamente alle autorità di controllo stanno provvedendo alla mitigazione di questa violazione.

Cos'è una violazione dei dati personali?
L'art. 4 del Regolamento UE 2016/679 definisce la violazione dei dati personali (*data breach*) come una "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Cos'è accaduto:
Descrizione degli eventi che hanno portato alla violazione dei dati personali dell'interessato. Evitare di comunicare informazioni riservate qualora non sia strettamente necessario.

Sono stati coinvolti i seguenti dati personali:
Elenco della tipologia di dati interessati dalla violazione:

- *Dati particolari (es: origine razziale etnica, opinioni politiche, convinzione religiose/filosofiche, appartenenza sindacale, relativi alla salute, relativi alla vita sessuale o all'orientamento sessuale, dati genetici, dati biometrici)*
- *Dati giudiziali (es: condanne penali, reati, connessi misure di sicurezza)*
- *Dati comuni (es: anagrafici, indirizzi postali, indirizzi IP, codici identificativi, conto corrente, carta di credito, valutazioni, ecc.)*

Cosa significa questo per Lei:
Descrizione dei possibili effetti della violazione dei dati sulla persona ed eventualmente breve descrizione delle misure di sicurezza in uso prima dell'incidente.

Come eviteremo in futuro tale problematica:
Al fine di evitare che tale violazione si verifichi nuovamente e di ridurre al minimo l'impatto sui nostri clienti abbiamo attivato le seguenti azioni:

Elencare gli interventi intrapresi e le misure di sicurezza adottate e/o che si adotteranno affinché tale violazione dei dati non si ripeta. É necessario informare l'interessato, ma senza esporre le misure di sicurezza a nuove minacce comunicando informazioni riservate.

Cosa può fare Lei per tutelarsi:
Formulare raccomandazioni per l'interessato intese ad attenuare gli effetti negativi della violazione. Ad esempio:

- *Evitare mail, sms, chiamate sospette*
- *Cambio password presenti nei sistemi*
- *Ecc….*

Nota e contatti:
Tutti gli aggiornamenti futuri in merito a questa violazione della sicurezza possono essere consultati sul nostro sito web all'indirizzo http://www.icbolzano2.it/. Qualsiasi e-mail doveste ricevere su questo incidente di sicurezza deve essere considerata sospetta.
Eventuali richieste o istanze relative all'esercizio dei propri diritti sugli argomenti coperti dal GDPR potranno essere rivolte alla Dirigente scolastica Chiara Nocentini all'indirizzo e-mail Chiara.Nocentini@scuola.alto-adige.it oppure al DPO all'indirizzo e-mail stefano.pastore@reggianiconsulting.it o PEC DPO@PEC.BRENNERCOM.NET.

Cordiali saluti

Firmato digitalmente da:CHIARA NOCENTINI
Limite d'uso:Explicit Text: Questo certificato rispetta le raccomandazioni previste dalla Determinazione Agid N. 121/2019 Explicit Text: Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity
Data:05/01/2021 10:37:57

ALLEGATO 2

Registro delle violazioni

Scheda evento

Numero violazione: 001	
Data evento e ora della violazione anche solo presunta (specificando se è presunta)	
Data e ora in cui si è avuto conoscenza della violazione	
Fonte di segnalazione	
Tipologia dell'evento	
Descrizione dell'evento	
Numero interessati coinvolti	
Numerosità dei dati personali di cui si presume la violazione	
Specificare il tipo di violazione	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	

Si classifica l'evento tra i seguenti casi:

- ☐ *distruzione di dati illecita,*
- ☐ *perdita di dati illecita,*
- ☐ *modifica di dati illecita,*
- ☐ *distruzione di dati accidentale,*
- ☐ *perdita di dati accidentale,*
- ☐ *modifica di dati accidentale,*
- ☐ *divulgazione non autorizzata*
- ☐ *accesso ai dati personali illecito.*

Valutazione del rischio secondo i seguenti livelli di rischio:

- ☐ **NULLO**
- ☐ **BASSO**
- ☐ **MEDIO**
- ☐ **ALTO**

Evento	Conseguenze	Provvedimenti adottati	Notifica all'autorità di controllo	Comunicazione all'interessato