VADEMECUM: Prevenzione e Gestione Data Breach

Nelle Istituzioni Scolastiche

Il presente documento fornisce linee guida essenziali per la gestione dei dati personali, in linea con il Regolamento Generale sulla Protezione dei Dati (GDPR).

1. Definizione di Data Breach

Cos'è la violazione dei dati personali?

Un data breach è una violazione della sicurezza che può avvenire accidentalmente o in modo illecito.

Comporta:

- La distruzione, la perdita, la modifica.
- La divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trattati dall'istituzione scolastica.

2. Prevenzione del Data Breach

Le strategie per minimizzare il rischio di violazione

Le misure preventive si dividono in tre aree fondamentali:

A. Misure Organizzative

- Ruoli e Contatti: Individuare il Responsabile della Protezione dei Dati (DPO) e diffondere i suoi contatti.
- Documentazione: Redigere e aggiornare il Registro delle Attività di Trattamento.
- Formazione: Formare periodicamente tutto il personale scolastico sulle normative GDPR e sulle buone pratiche di sicurezza informatica.
- Principio del Minimo Privilegio: Implementare una politica di accesso ai dati che permetta a ogni utente di accedere solo ai dati strettamente necessari per le proprie mansioni.
- Revisione: Effettuare audit regolari sulla sicurezza dei dati.

B. Misure Tecniche

- Software: Utilizzare software antivirus e firewall sempre aggiornati.
- Autenticazione: Implementare l'autenticazione a più fattori (MFA) per l'accesso ai sistemi informatici.
- Password: Applicare rigorose politiche di gestione delle password (devono essere complesse e cambiate periodicamente).
- Backup: Effettuare backup regolari dei dati critici su supporti protetti e offline.
- Crittografia: Proteggere i dispositivi mobili e le unità di memoria USB con crittografia.
- Controllo: Configurare i sistemi per limitare l'installazione di software non autorizzato e monitorare i log di accesso ai sistemi.

C. Buone Pratiche per il Personale

- Credenziali: Non condividere le credenziali di accesso con altri.
- E-mail e Link: Evitare di aprire e-mail sospette o cliccare su link sconosciuti.
- Dispositivi Personali: Non salvare dati sensibili su dispositivi personali o non protetti.
- Piattaforme Ufficiali: Utilizzare esclusivamente le piattaforme ufficiali per la gestione della didattica e degli alunni.
- Log-out: Scollegare l’account scolastico in uso sui PC una volta finito l’utilizzo della piattaforma.
- Segnalazione: Segnalare immediatamente attività anomale o sospette all'ufficio tecnico o al DPO.

3. Gestione di un Data Breach (La Risposta Immediata)

Procedura per affrontare la violazione

A. Rilevamento e Segnalazione

1. Segnalazione Immediata: Qualsiasi membro del personale che sospetti o scopra una violazione deve segnalarlo immediatamente al Dirigente scolastico e al DPO.
2. Raccolta Informazioni: Il DPO deve raccogliere tutte le informazioni disponibili: natura della violazione, dati compromessi, cause e soggetti coinvolti.
3. Registro Interno: In caso di incidente informatico, deve essere compilata la scheda sull’apposito Registro Incidenti Informatici (come l'Allegato 1).

B. Contenimento e Risoluzione

Le azioni di prima risposta per contenere gli impatti della violazione devono essere intraprese immediatamente:

- Isolamento: Isolare immediatamente i sistemi coinvolti per evitare ulteriore compromissione.
- Disconnessione: Disconnettere eventuali dispositivi infetti o compromessi dalla rete.
- Credenziali: Cambiare immediatamente le credenziali di accesso se compromesse.
- Misure Tecniche: Bloccare gli account compromessi e applicare patch/aggiornamenti di sicurezza.
- Analisi: Effettuare un'analisi forense per determinare l'origine del problema.

4. Notifica e Comunicazione

Obblighi del Titolare (Dirigente Scolastico) e del DPO

A. Notifica al Garante

- Termine: Se il data breach comporta un rischio per i diritti e le libertà degli interessati, l'evento deve essere notificato al Garante per la Protezione dei Dati Personali entro 72 ore tramite apposito portale.
- Eccezione: La notifica non è dovuta se è improbabile che la violazione presenti un rischio per i diritti e le libertà degli Interessati.
- Contenuto: La notifica deve contenere la natura della violazione, le tipologie di dati violati, i contatti del DPO e la descrizione delle misure adottate o in procinto di adozione per mitigare le conseguenze.

B. Notifica agli Interessati

- Rischio Elevato: Se la violazione è suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, occorre informarli senza ritardo.
- Informazioni: Nella comunicazione agli interessati, fornire indicazioni sulle misure di protezione adottate e una descrizione delle misure che l'Istituto intende adottare per porre rimedio alla violazione.

5. Recovery Plan e Azioni Successive

Ripristino e apprendimento dall'incidente

(*SUGGERIMENTO IMMAGINE/ICONA: Icona di un cerchio con una freccia (ciclo di miglioramento) o un "check" verde*)

1. Ripristino Dati: Ripristinare i dati dai backup più recenti ed eseguire test di integrità sui dati ripristinati.

2. Riattivazione: Riattivare i sistemi solo dopo aver verificato la risoluzione della vulnerabilità.
3. Revisione Interna: Redigere un rapporto dettagliato (cause, conseguenze e azioni correttive) da inserire nel registro delle violazioni.
4. Mitigazione/Revisione Sicurezza: Condurre una revisione approfondita delle misure di sicurezza per evitare futuri incidenti.
5. Formazione Continua: Formare il personale su eventuali nuove minacce e protocolli di sicurezza.
6. Monitoraggio: Monitorare costantemente i sistemi per identificare eventuali vulnerabilità residue.

6. Esempi Pratici di Incidenti e Risposte

Per una gestione chiara e rapida, è utile considerare scenari tipici:

Tipo di Incidente (Scenario)	Azioni Immediate	Azioni Successive / Prevenzione Futura
Furto di credenziali di accesso al registro elettronico	Disattivare l'account compromesso; avvisare gli utenti; ripristinare l'accesso con nuove credenziali sicure.	Attivare l'Autenticazione a Più Fattori (MFA); migliorare le politiche di autenticazione; formare il personale su phishing.
Malware che cripta i dati (Ransomware)	Isolare il sistema infetto; identificare il punto di ingresso del malware; avviare il ripristino da backup.	Installare software anti-ransomware; migliorare la protezione delle e-mail; effettuare simulazioni di attacchi informatici.
Erroneo invio di mail contenente dati personali a soggetti non autorizzati	Contattare tempestivamente i destinatari erronei e richiedere la cancellazione del messaggio.	Segnalare l'errore al DPO; valutare il rischio di esposizione; notificare l'incidente se necessario. Implementare controlli automatici sulle e-mail sensibili.