PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

artt. 4, n. 12, 33 e 34 Regolamento (UE) 2016/679

La presente procedura disciplina la segnalazione, valutazione, gestione e documentazione di ogni violazione, anche solo sospetta, di dati personali trattati dagli Istituti Paritari Filippin.

1. Che cos'è un data breach

È una violazione di sicurezza che comporta, accidentalmente o illecitamente, distruzione, perdita, modifica, divulgazione non autorizzata o accesso a dati personali. Può riguardare dati digitali o cartacei.

- invio di e-mail o documenti al destinatario errato;
- smarrimento o furto di PC, smartphone, chiavette, fascicoli o verifiche;
- accesso non autorizzato a registro elettronico, Microsoft 365, Segreteria Digitale o altri sistemi;
- credenziali compromesse, malware, attacchi informatici o cancellazione/alterazione di dati;
- pubblicazione o condivisione indebita di dati, fotografie, dati sanitari o altre informazioni riservate;
- inserimento o esposizione non autorizzata di dati personali in strumenti di IA, compreso Microsoft Copilot;
- accesso improprio a dati relativi a mensa/CIBOS, trasporti, personale, videosorveglianza o altri servizi dell'Istituto.

2. A chi si applica

A docenti, personale ATA, collaboratori, consulenti e a ogni soggetto che tratti dati per conto degli Istituti Filippin. I Responsabili esterni ex art. 28 GDPR devono segnalare le violazioni secondo i tempi e le modalità previsti dal contratto e, comunque, senza ingiustificato ritardo.

3. Cosa deve fare chi rileva o sospetta una violazione

- segnalare immediatamente l'evento al referente interno individuato dall'Istituto utilizzando il Modulo A o, in urgenza, con comunicazione immediata seguita dal modulo;
- non cancellare messaggi, log, file o altre evidenze utili;
- non contattare autonomamente il Garante, gli interessati, la stampa o soggetti esterni, salvo specifica autorizzazione;
- adottare soltanto le prime misure urgenti di contenimento per cui si è autorizzati (es. disconnettere un dispositivo compromesso, richiamare un'e-mail ove possibile, cambiare una password compromessa), informandone subito l'Istituto.

4. Flusso di gestione

Fase 1 – Presa in carico: Il Titolare o il referente delegato registra la segnalazione, verifica i fatti e coinvolge tempestivamente DPO e referente IT quando necessario.

Via S. Giacomo, 4
31017 Pieve del Grappa (TV)
Tel. 0423 932000 - Fax. 0423 932939
www.filippin.it - segreteria@filippin.it

Fase 2 – **Contenimento e valutazione**: Sono individuati dati, interessati, sistemi coinvolti, cause, conseguenze, misure già adottate e ulteriori azioni di contenimento. La valutazione è documentata nel Modulo B.

Fase 3 – **Notifica al Garante**: Se la violazione può presentare un rischio per i diritti e le libertà delle persone fisiche, il Titolare provvede alla notifica al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Se la notifica avviene oltre 72 ore, ne sono indicate le ragioni.

Fase 4 – **Comunicazione agli interessati**: Se la violazione è suscettibile di presentare un rischio elevato, il Titolare comunica la violazione agli interessati senza ingiustificato ritardo, salvo le eccezioni previste dall'art. 34 GDPR.

Fase 5 – **Registro e chiusura**: Ogni violazione è documentata nel Registro Data Breach, anche quando non viene notificata al Garante. Sono registrati fatti, effetti, valutazione e misure correttive.

5. Criteri essenziali di valutazione

- tipo di violazione: riservatezza, integrità e/o disponibilità;
- natura, sensibilità e volume dei dati;
- numero e caratteristiche degli interessati, con particolare attenzione a minori e persone vulnerabili;
- facilità di identificazione e possibili conseguenze: discriminazione, furto d'identità, danni economici, reputazionali, sociali o perdita di riservatezza;
- efficacia di cifratura, autenticazione, backup e altre misure di protezione;
- possibilità di recuperare i dati, contenere l'evento e prevenire ulteriori accessi.

6. Ruoli

La decisione sulla notifica al Garante e sulla comunicazione agli interessati compete al Titolare del trattamento, con il supporto del DPO e, per gli aspetti tecnici, dei referenti IT. Il DPO svolge funzione di consulenza e sorveglianza; non sostituisce il Titolare nelle decisioni.

7. Documenti collegati

- Allegato A – Segnalazione interna di possibile Data Breach;
- Allegato B – Scheda di valutazione e decisione;
- Allegato C – Registro delle violazioni di dati personali;
- Registro dei trattamenti, informative, lettere di autorizzazione, policy di sicurezza e Regolamento per l'uso dell'IA degli Istituti Filippin.

Via S. Giacomo, 4
31017 Pieve del Grappa (TV)
Tel. 0423 932000 - Fax. 0423 932939
www.filippin.it - segreteria@filippin.it