ISTITUTO COMPRENSIVO STATALE N.3 "S. BERNARDINO-BORGO TRENTO"
Via G. Camozzini, 5 – 37126 Verona (VR) tel. 045 8349055/8302762 fax 045 8344488
vric89200e@istruzione.it – www.comprensivo03vr.gov.it

Prot.n. 2657/2018 Bussolengo, 4 ottobre 2018

PROCEDURA GENERALE DATA BREACH

1) **Definizione di data breach di dati personali:** Distruzione e perdita accidentale o illegale, alterazione non autorizzata, diffusione o trasmissione non autorizzata, accesso non autorizzato (incluso ricezione, conservazione o gestione)

Tutti i data breach sono violazioni della sicurezza del dato, però non tutte le violazioni alla sicurezza sono data breach.

2) **Misure di sicurezza minime e misure di sicurezza adeguate:**

Rispettate le misure tecniche di sicurezza (che fanno capo al documento sulle misure minime ICT redatto su indicazioni AGID entro 31/12/2017):

- Inventario dei dispositivi autorizzati e non autorizzati
- Inventario dei software autorizzati e non autorizzati
- Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server
- Valutazione e correzione continua della vulnerabilità
- Uso appropriato dei privilegi di amministratore
- Difese contro i malware
- Copie di sicurezza
- Protezione dei dati

Rispettate le misure fisiche/organizzative/procedurali che si possono individuare nei seguenti punti:

1. Rispetto dei principi generali privacy (raccolta, conservazione, registrazione e comunicazione)
2. Garanzia dei diritti dell'interessato
3. Adozione di un sistema organizzativo privacy (soggetti responsabili e autorizzati al trattamento, corsi di formazione privacy)
4. Analisi dei rischi privacy (DPIA e valutazione d'impatto)
5. Registro dei trattamenti (redazione e gestione)
6. data breach (gestione della notifica e della documentazione)
7. Sistema di gestione privacy (procedure e certificazioni)
8. Trasferimento di dati all'estero

E considerando che l'art. 32 del GDPR menziona misure tecniche ed organizzative adeguate e non più minime.

3) **Identificazione della violazione**

Rispettati i protocolli di sicurezza è possibile individuare la violazione nelle seguenti maniere

1. lettura del log di sistema
2. sopralluoghi fisici nelle scuole da parte del DPO
3. segnalazioni dell'interessato al Titolare/Responsabile del trattamento

4) **Notifica della violazione dei dati personali all'autorità di controllo (art. 33 del GDPR)**

1. Il Titolare/RTD/RPD individua/viene messo al corrente se vi è stato un incidente di sicurezza e stabilisce se sia verificata una violazione dei dati personali
2. Titolare/RTD/RPD valutano il rischio sugli individui
3. Se la violazione non si trasforma in un rischio per i diritti e le libertà dell'interessato non vi è la necessità di notificare l'autorità competente.
4. Permane comunque l'obbligo (art. 33 paragrafo 4) di documentare qualsiasi violazione di dati personali (data evento, tipo evento, dati degli interessati, riferimenti RPD, conseguenze violazione, misure adottate o da adottarsi).
5. Qualora invece vi sia rischio per i diritti e le libertà dell'interessato RPD notifica l'autorità competente senza ingiustificato ritardo e comunque non oltre le 72 ore.
6. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
7. Se inoltre il rischio per i diritti e le libertà è alto anche gli interessati stessi devono essere notificati.

Denominazione istituto	**Violazioni data breach**		
DATA EVENTO	**TIPO DI EVENTO**	**DATI INTERESSATI**	**GESTIONE ***
			Riferimenti RPD **Conseguenze violazione** **Misure adottate o da adottarsi** **Notifica Garante (senza ingiustificato ritardo e, comunque, non oltre 72 ore)**

Dirigente scolastico
Viviana Sette
Documento firmato digitalmente ai sensi del
Codice dell'Amministrazione digitale e normativa connessa