FASE DI SEGNALAZIONE

INCIDENTE ESTERNO/INTERNO

- Modifica erronea di un database;
- Smarrimento/distruzione chiavetta USB, telefonino aziendale o altro strumento contenente dati personali;
- invio errato a terzo non autorizzato;
- smarrimento/distruzione di documentazione cartacea/digitale
- malware che crittografa una cartella di rete
- allagamenti o incendi e conseguente perdita dati
- attacchi informatici di varia natura

AL REFERENTE PRIVACY (*Maria Raffaella Scorrano*)

MEDIANTE MODULO "**ALLEGATO1"** (Modello di segnalazione e gestione di Data Breach)

INVIATO ALL'INDIRIZZO E-MAIL ***nopm010005@istruzione.it***

GESTIONE SEGNALAZIONE DA PARTE DEL RESPONSABILE

PROTOCOLLARE LA SEGNALAZIONE

AVVISARE TEMPESTIVAMENTE DS prof.ssa Maria Motta

INIZIO DECORSO 72H

FASE DI VALUTAZIONE

Soggetti

DIRIGENTE SCOLASTICO (*prof.ssa Maria Motta)*

RESPONSABILE PROTEZIONE DATI (DPO/RPD) (*Avv. Martina Marchetti*)

RESPONSABILI DEL TRATTAMENTO EX ART. 28 GDPR (es. Amministratore sistema/responsabile IT) (*Fabio Iacovino*)

Contenuto

ANALISI PRELIMINARE: SI È VERIFICATA LESIONE DI:

- RISERVATEZZA
- INTEGRITA'
- DISPONIBILITA'

DEI DATI PERSONALI

NO

ARCHIVIAZIONE PROCEDURA - REGISTRAZIONE

Il Titolare deve documentare qualsiasi violazione dei dati personali

SI

ANALISI APPROFONDITA:

- Che lesione si è verificata?
- Sono rimaste coinvolte categorie di soggetti vulnerabili (minori, anziani, malati ecc)?
- Numero interessati coinvolti
- Indicazione di eventuali analisi ulteriori (per polizia, magistratura ecc)

DETTAGLI VALUTAZIONE

Vedi Guida Procedura data breach

valutazione RISCHIO considerando GRAVITA' e PROBABILITA'

FASE DI COMUNICAZIONE A TERZI (eventuale)

NOTIFICA GARANTE

- Da fare quando è **probabile** che la **violazione presenti rischi per i diritti e le libertà** delle persone fisiche
- **Entro 72 ore** dalla protocollazione mediante **ALLEGATO 2**
- **Contenuto e modalità invio** vedi Procedura Data Breach

DENUNCIA POLIZIA POSTALE

È obbligatoria quando la violazione dei dati sia **conseguenza** di **comportamenti illeciti o fraudolenti.**
Per alcuni data breach è possibile effettuarla tramite http://www.commissariatodips.it/.

COMUNICAZIONE CERT PA (OGGI CSIRT Italia)

- Va fatta In caso di **incidente informatico**
- occorreinviare il documento di autoverifica e la segnalazione dell'incidente:
- PEC: cert-pa@pcert.agid.gov.it
  PEO: cert-pa@cert-pa.it;

COMUNICAZIONE INTERTESSATI

- Va fatta quando si verifica un **rischio ELEVATO** per i diritti e le libertà delle persone
- Va fatta **senza ingiustificato ritardo** fisiche
- Esclusioni, contenuto e modalità vedi GDB