PROCEDURA DATA BREACH

1. SCOPO

Lo scopo del presente disciplinare interno è di definire la procedura per la segnalazione e la gestione di una possibile breccia nella sicurezza (Data Breach) di dati personali in affidamento.

2. APPLICABILITA'

La presente procedura si applica a tutto il personale alle dipendenze o funzionalmente dipendente del Titolare.

Il Regolamento Europeo per la Protezione dei Dati Personali (GDPR) con l'articolo 33, ha introdotto l'obbligo generalizzato, in capo al **Titolare del trattamento** di notifica di data breach al Garante della Protezione dei Dati Personali competente a norma dell'art. 55 GDPR e seguenti.

Con l'articolo 34 lo stesso Regolamento, quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, obbliga il **Titolare del trattamento** a comunicare la violazione all'interessato senza ingiustificato ritardo, utilizzando un linguaggio semplice e chiaro.

Per questi motivi, tutto il personale soggetto al presente disciplinare è tenuto a comunicare al Titolare ogni possibile situazione di data breach in cui incorra inviando una email al seguente indirizzo: fim_brescia@cisl.it e avvisandolo telefonicamente al cellulare.

La mail va inviata in copia anche al DPO all'indirizzo: dpo.fim.brescia@cisl.it

Tale missiva dovrà essere inviata senza ritardi ingiustificati e dovrà contenere i dati richiesti nella presente procedura.

3. DEFINIZIONI

COSA È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)?	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. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. Alcuni possibili esempi: ▪ l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;

- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

4. PROCEDURA PER IL PERSONALE

In caso di possibile situazione di Data Breach il personale del Titolare dovrà tempestivamente:

1. inviare una email a fim_brescia@cisl.it mettendo in copia dpo.fim.brescia@cisl.it
2. avvisare telefonicamente il Titolare al cellulare
3 . in caso di mancata risposta telefonica, stampare la mail iniziale e conservarla

4.1 CONTENUTO MAIL DI SEGNALAZIONE

La mail di segnalazione dovrà contenere almeno i seguenti dati

- Descrizione accurata di quanto accaduto
- Sottosistemi coinvolti
- Tempistiche di ogni singolo fatto rilevato
- Dimensione numerica dei dati coinvolti (stima)
- Dimensione qualitativa dei dati coinvolti (stima)
- Se il fatto sia terminato o ancora in atto
- Personale interno coinvolto
- Contromisura prese
- Contromisure ancora da prendere

- Possibili rischi per gli interessati
- Riferimenti di persone utili alla gestione del data breach

5. PROCEDURA PER IL TITOLARE E PER IL DPO

In caso di possibile situazione di Data Breach occorsa su segnalazione o su diretta conoscenza il Titolare dovrà:

1. Dare riscontro alla eventuale segnalazione tramite email
2. Convocare nel più breve tempo possibile, e comunque entro le 24 ore successive alla segnalazione, il DPO per valutare la segnalazione
3. In seguito alle valutazioni fatte il Titolare convoca i Responsabili delle funzioni interessate al possibile Data Breach nel più breve tempo possibile
4. Attivare le procedure per minimizzare gli effetti possibili della violazione (se la violazione interessa la funzione IT, attivare le relative procedure in capo al Responsabile dei Servizi Informativi)
5. Anche utilizzando la procedura https://servizi.gpdp.it/databreach/s/self-assessment valutare se sussistano le condizioni per la notifica della violazione al Garante per la Protezione dei Dati Personali e per l'eventuale comunicazione agli interessati
6. Se sussistono le condizioni previste dall'articolo 33 del GDPR (sussistenza di rischio per le libertà e i diritti dell'interessato), il DPO comunica al Garante per la Protezione dei Dati Personali opportuna notifica entro le 72 ore successive alla segnalazione iniziale
7. Se sussistono le condizioni previste dall'articolo 34 del GDPR (sussistenza di elevato rischio per le libertà e i diritti dell'interessato), il DPO comunica agli interessati l'avvenuta violazione nel minor tempo possibile e salvo I casi previsti al comma 3 articolo 34 del GDPR

Per approvazione del Titolare