ASSOCIAZIONE LA SOGLIA

"Riepilogo" procedura relativa alla notifica di violazione sui dati personali (Data Breach)

PREMESSA

ASSOCIAZIONE LA SOGLIA, in qualità di Titolare del trattamento (di seguito anche "**Titolare del trattamento**"), è tenuta ai sensi del Regolamento Europeo 2016/679 (di seguito anche "**GDPR**") a mantenere sicuri i dati personali trattati dalla propria struttura e a reagire senza ingiustificato ritardo in caso di violazione dei dati personali (incluse eventuali notifica all'Autorità Garante competente ed eventuali comunicazioni agli interessati).
È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'azienda, che permettano, altresì di rispettare gli adempimenti previsti dalla normativa europea, nei tempi e modi ivi previsti (es. notificazione all'autorità garante e/o comunicazione agli interessati).

SCOPO

Lo scopo di questa procedura è di fornire un flusso di gestione delle violazioni dei dati personali trattati **ASSOCIAZIONE LA SOGLIA.** Questo documento integra le procedure in essere presso il Titolare del trattamento ai sensi del GDPR e degli ulteriori provvedimenti in materia di protezione dei dati personali.

COS'È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Una violazione di dati personali è ogni violazione di sicurezza che comporti 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 dal Titolare del trattamento.

Le violazioni di dati personali possono accadere per un ampio numero di ragioni, che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale: ad esempio, data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico;
- accesso abusivo: ad esempio, data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite;
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (i.e. forzatura di porte o finestre di stanze di sicurezza o archivi contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

AMBITO DI APPLICAZIONE E DESTINATARI

Questa procedura è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento (meglio descritti al punto 5 della presente procedura) ovvero:

- nonché a coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (di seguito genericamente denominati DESTINATARI INTERNI);
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dal DESTINATARIO INTERNO che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR (di seguito genericamente denominati DESTINATARI ESTERNI).

ALLEGATO A – MODULO DI COMUNICAZIONE INTERNA DI DATA BREACH

Da compilare a cura dei Destinatari e da inviare al Titolare del Trattamento LA SOGLIA, al seguente indirizzo lasoglia@lasoglia.it.

Comunicazione di Data Breach	Note
Data scoperta incidente:	
Data dell'incidente:	
Nome cognome e dati di contatto (indirizzo e-mail, numero telefonico) della persona che compila il presente modulo. In caso di destinatario esterno indicare anche la ragione sociale:	
Luogo dell'incidente (se in Italia o all'estero e specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili):	
Breve descrizione dell'incidente (con precisazione della natura della violazione: violazione della riservatezza; violazione della disponibilità; violazione dell'integrità):	
Breve descrizione della/e banca/che dati oggetto dell'incidente e della tipologia di dati coinvolti (es. dati personali comuni; categorie particolari di dati, tra cui origine razziale o etnica, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale; dati relativi a condanne penali e reati):	
Categorie (es. lavoratori; clienti; fornitori; utenti sito web) e numero approssimativo di interessati coinvolti nell'incidente e numero approssimativo di registrazioni dei dati personali coinvolti:	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta dell'incidente:	
Nome e cognome del Destinatario che ha compilato il presente allegato:	
data:	