PROCEDURA INTERNA PER LAGESTIONE DEL DATA BREACH

ai sensi del GDPR 2016/679, delle linee guida del WP29 e delle indicazioni fornite dal Garante per la protezione dei dati personali

Sommario

1. Premessa introduttiva

Ascla Società Cooperativa Impresa Sociale *(anche solo "ASCLA" "Titolare" "Ente"* quale Titolare del Trattamento, e nei casi di cui all'art. 26 del GDPR quale contitolare, ai sensi del Regolamento europeo n. 2016/679 (da qui in avanti GDPR), è tenuta a garantire la sicurezza dei dati personali trattati nell'ambito delle proprie attività e ad agire prontamente in caso di violazione dei dati stessi (come definito al punto 3).

L'Ente di formazione ASCLA pianifica emette in atto procedure idonee a rilevare e limitare tempestivamente gli effetti di una violazione, valutare il rischio per le persone fisiche e stabilire se sia necessario o meno notificare la violazione all'autorità di controllo competente e comunicarla alle persone fisiche interessate, ove necessario.

2. Scopo della procedura

Il presente documento ha lo scopo di indicare a tutti i soggetti che operano presso ASCLA le modalità di gestione di una violazione, anche solo potenzialmente ***data breach***, ovvero di un episodio di violazione di dati personali, nel rispetto dei principi e delle disposizioni contenute nel GDPR.

Il presente documento è messo a disposizione di tutto il personale e i collaboratori dell'Ente, attraverso comunicazione e la pubblicazione nella pagina istituzionale.

La procedura sintetizza le regole per gestire nel migliore dei modi una *violazione dei dati/data breach*, alla luce degli artt. 33 e 34 del GDPR e delle Linee Guida sotto i diversi aspetti relativi a:

- Modalità e profili di segnalazione al Titolare;
- Valutazione dell'evento accaduto;
- Modalitàeprofilidisegnalazioneall'autoritàGaranteperlaprotezionedeidatipersonali(daquiinavantiGarantePrivacy);
- Eventuale comunicazione agli interessati.

3. Violazione dei dati personali

Una violazione dei dati personali (o *data breach*), ovvero 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 (art. 4, punto 12 del GDPR) può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Il *data breach*, o "violazione dei dati personali" nella traduzione italiana, è un concetto estremamente ampio. Esso include certamente eventi in cui l'intervento malevolo di terzi è manifesto, ma comprende anche una serie di ipotesi riconducibili all'inosservanza di norme sulla sicurezza da parte del Titolare del trattamento. Tendenzialmente, il concetto di data breach viene a essere equiparato a quello di rilevante discontinuità nel normale funzionamento di un sistema informatico.

Rientra nella categoria dei *data breach* anche un incidente sulla sicurezza dal quale deriva una perdita di disponibilità dei dati non permanente, ma circoscritta a un limitato periodo temporale, ad esempio la perdita di accesso temporanea ai dati, in quanto potrebbe comunque comportare un significativo impatto sui diritti e le libertà degli individui, come ad esempio un blackout elettrico che impedisca all'interessato di accedere ai propri dati.

Anche la violazione che comporta una perdita temporanea di disponibilità dovrebbe essere documentata (così come nel caso di perdita o distruzione permanente di dati personali). L'indisponibilità di un dato personale causata dalla manutenzione programmata del sistema in corso non può essere considerata una "violazione della sicurezza" ai sensi del GDPR.

Le violazioni di dati personali possono essere ricondotte a una serie di eventi, tra cui:

- ***Divulgazione di dati personali a soggetti non autorizzati;***
- ***Perdita o furto di documenti o strumenti nei quali sono memorizzati dati personali;***
- ***Perdita o furto di documenti cartacei contenenti dati personali;***
- ***Infedeltà aziendale (ad esempio, data breach causata da una persona interna che, avendo autorizzazione ad accedere ai dati, ne produce una copia per fini non consentiti);***
- ***Accesso abusivo (ad esempio, data breach causata da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);***
- ***Casi di pirateria informatica (usurpazione delle credenziali di accesso, phishing, ransomware);***
- ***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 (ad esempio, forzatura di porte o finestre, distanze di sicurezza o armadi contenenti archivi con informazioni riservate);***
- ***Smarrimento di PC portatili, dispositivi o attrezzature informatiche aziendali;***
- ***Invio di e-mail contenenti dati personali e/o particolari a un destinatario errato o erroneo.***

Per gestire tali *data breach*, occorre seguire le disposizioni di seguito descritte.

4. Soggetti tenuti all'osservanza della procedura.

La procedura si rivolge a tutti i soggetti che, a qualsiasi titolo, trattano dati personali di competenza di ASCLA e dei suoi contitolari. Questi soggetti includono i lavoratori dipendenti e coloro che, indipendentemente dall'inquadramento contrattuale, abbiano accesso ai dati al fine di garantire l'esecuzione delle prestazioni richieste.

5. Gestione del data breach

Le violazioni di dati personali sono gestite operativamente dalla direzione del Titolare, unitamente al Contitolare, sotto la supervisione del Responsabile della Protezione dei Dati (da qui in avanti DPO). Ogni soggetto autorizzato a trattare dati, qualora venga a conoscenza di un potenziale caso di data breach, è tenuto a informare tempestivamente il Titolare, inviando una pronta comunicazione, anche attraverso le vie brevi, al Presidente e/o al Direttore e/o al DPO. Se necessario, è necessario compilare l'apposito modulo di segnalazione (***MODULO SEGNALAZIONE - DB1***) e inviarlo all'indirizzo di posta elettronica INFO@ASCLA.IT. La segnalazione ricevuta sarà valutata per stabilire il possibile rischio per gli interessati e successivamente annotata nell'apposito registro degli eventi negativi (***REGISTRO EVENTI NEGATIVI***).

Si possono presentare le tre seguenti situazioni:

A. **Improbabilità che la violazione dei dati personali verificatasi presenti un rischio** *per i diritti e le libertà delle persone fisiche: In tal caso, è necessario acquisire la segnalazione e conservarne menzione nel registro, indicando le motivazioni per cui si decide di non procedere con la notifica al Garante.*

B. ***Probabilità che la violazione dei dati personali verificatasi presenti un RISCHIO*** *per i diritti e le libertà delle persone fisiche: In tal caso, è obbligatoria la notifica al Garante. È necessario effettuare la notifica entro 72 ore utilizzando l'apposita procedura telematica disponibile sul portale dei servizi online dell'Autorità, raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/1.*

C. ***Probabilità che la violazione dei dati personali verificatasi presenti un RISCHIO ELEVATO*** *per i diritti e le libertà delle persone fisiche: È necessario procedere immediatamente alla comunicazione agli interessati, oltre alla notifica al Garante Privacy entro 72 ore.*

Al fine di classificare correttamente l'incidente incorso e valutare l'entità del rischio conseguente, il Titolare, congiuntamente al co-titolare e al DPO (se coinvolto), potrà utilizzare il documento allegato alla presente procedura: **SCHEMA DI VALUTAZIONE VIOLAZIONI-DATABREACH (DB3).**

Il criterio determinante per valutare la necessità di avviare una procedura di notifica è la probabilità che la violazione possa porre a rischio (per la notifica all'autorità - Garante Privacy) o a rischio elevato (per la comunicazione anche agli interessati) le libertà e i diritti degli individui.

Appurato il rischio conseguente alla violazione, gli articoli 33 e 34 del GDPR e le linee guida dell'EDPB come aggiornate, indicano al Titolare i termini, le modalità, i contenuti e le deroghe della notifica e della comunicazione di *data breach*.

Pertanto, affinché la violazione dei dati personali sia gestita correttamente, è necessario seguire i seguenti step:

1. *Identificazione della violazione e avvio delle azioni correttive per gestire la violazione;*
2. *Indagine su quanto avvenuto e valutazione del rischio per gli interessati con annotazione nell'apposito*

registro;

3. *Eventuale notifica all'Autorità Garante;*
4. *Eventuale comunicazione agli interessati;*
5. *Documentazione della violazione, indipendentemente dall'esito della segnalazione.*

5.1. Identificazione della violazione e avvio delle azioni correttive per gestire la violazione

Rilevata la violazione, si richiede ai responsabili delle aree di competenza del Titolare di porre in essere, se possibile, azioni correttive atte a limitare i danni causati e di comunicare anche attraverso le vie brevi agli apicali, compilando il **MODULO DI SEGNALAZIONE DB1**. Si richiede inoltre di informare i soggetti preposti alla gestione delle violazioni dei dati e di attivare il DPO in base all'urgenza dell'avvenuto incidente.

Soggetti esterni all'ASCLA possono comunque segnalare presunte violazioni di dati personali, di cui siano accidentalmente venuti a conoscenza, utilizzando direttamente il **MODULO-DB1**, messo a disposizione anche online: **MODULO SEGNALAZIONE DB** su **www.ascla.net**.

Qualora la segnalazione provenga da Responsabili del trattamento ex art. 28 del GDPR, ASCLA ricorda che i contratti in essere tra il Titolare e tutti i Responsabili del trattamento individuati prevedono l'obbligo, in capo al Responsabile, di informare tempestivamente il Titolare in caso di violazione.

5.2. Indagine su quanto avvenuto e avvio della valutazione del rischio per gli interessati

Ricevuta la segnalazione, la Direzione, al fine di stabilire se si sia effettivamente verificata un'ipotesi di data breach, procede ad indagini approfondite sull'accaduto, coinvolgendo anche il DPO se necessario. Tale indagine verrà condotta sulla base delle informazioni raccolte nella compilazione del modulo, dal verbale del DPO e dalle dichiarazioni dei soggetti testimoni. Sulla base di tali informazioni, il Titolare, con il coinvolgimento del DPO in base all'urgenza, effettua la prevista valutazione di rischio per i diritti e le libertà degli interessati.

Nel valutare il rischio, verranno considerate le circostanze specifiche della violazione, inclusa la gravità dell'impatto potenziale e la probabilità che tale impatto si verifichi. A tal fine, saranno considerati i seguenti parametri:

a) tipo di violazione,

b) natura e volume dei dati personali violati,

c) facilità di identificazione delle persone fisiche e d) caratteristiche particolari dell'interessato.

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, la direzione coinvolgerà immediatamente il Responsabile del sistema di rete, o il suo delegato in caso di assenza, e le competenti strutture del servizio informatico di ASCLA, tenuto conto anche delle adottate procedure di sicurezza informatica.

A fronte di tale analisi, ASCLA, tramite la direzione, in collaborazione con il DPO, accerterà:

- Se esistono azioni che possano limitare i danni che la violazione potrebbe causare (ad esempio riparazione fisica degli strumenti, utilizzo dei file di backup per recuperare dati persi o danneggiati, isolamento/chiusura di un settore compromesso della rete, cambio dei codici di accesso, ecc.);

- Una volta identificate tali azioni, quali sono le strutture dell'azienda che devono agire per contenere la violazione;
- Denunciare all'Autorità Giudiziaria/Forze di Polizia;
- Se sia necessario notificare la violazione al Garante (ove sia probabile che la violazione presenti rischi per i diritti e le libertà delle persone fisiche);
- Se sia necessario comunicare la violazione anche agli interessati (ove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche).

Qualora la valutazione del rischio dia esito negativo e i soggetti preposti alla gestione dell'incidente non ritengano necessaria la segnalazione all'autorità di controllo, si terrà ugualmente traccia di quanto avvenuto attraverso la compilazione del **REGISTRO DB2**, specificando i motivi per cui non si ritiene di procedere con la segnalazione di Data Breach o se si è ancora in corso di valutazione.

ASCLA, qualora si trovi ad operare come Responsabile, si impegna a rispettare quanto sopra indicato nei confronti delle controparti che hanno designato loro Responsabile del trattamento in base ai contratti/accordi/convenzioni in essere, stabilendo un tempo massimo per informare il Titolare a partire dal momento della scoperta della violazione, salvo diverso accordo stipulato.

5.3. Eventuale notifica al Garante

Una volta valutata la necessità di effettuare la notifica della violazione dei dati subita, ASCLA, in collaborazione con il DPO, predisporrà la segnalazione e la invierà all'Autorità Garante **senza ingiustificato ritardo** e, comunque, **entro 72 ore** dal momento in cui si è venuti a conoscenza della violazione, cioè da quando si abbia un ragionevole grado di certezza di un avvenuto incidente di sicurezza che riguardi dati personali.

Per l'invio della notifica, verrà utilizzata l'apposita procedura telematica resa disponibile dal Garante sul portale dei servizi online dell'Autorità (https://servizi.gpdp.it/databreach/s/).

ASCLA è tenuto a valutare le circostanze specifiche di ogni effettiva violazione avvenuta. Pertanto, qualora non disponga di tutti gli elementi di dettaglio dell'incidente, è comunque tenuto a effettuare la notifica della violazione al Garante entro 72 ore, con le informazioni in suo possesso, classificando come preliminare la notifica effettuata. Una volta ricostruito il quadro completo della violazione, ASCLA provvederà alla compilazione del medesimo modulo, individuando come integrativa la notifica in essere.

ASCLA, tramite l'ufficio di direzione, curerà l'archiviazione della documentazione riguardante la violazione in modo regolare e puntuale, anche durante il suo sviluppo, così da raccogliere le informazioni necessarie e tutti i dettagli rilevanti, tenute a disposizione dell'Autorità Garante.

Nell'ipotesi in cui la segnalazione sia effettuata oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

La notifica al Garante non includerà i dati personali oggetto di violazione (ad es. i nomi dei soggetti interessati dalla violazione). Viceversa, la notifica, ai sensi dell'art. 33, par. 3, GDPR, indicherà:

- Tipo di notifica: se è preliminare (ASCLA avvia il processo di notifica pur in assenza di un quadro completo della violazione con riserva di effettuare notifica integrativa), completa o integrativa;

- Generalità del soggetto che effettua la notifica e dati dell'ASCLA;
- Riferimenti del soggetto da contattare per ottenere informazioni aggiuntive inerenti la violazione (DPO, Responsabile del trattamento, altri soggetti coinvolti);
- Informazioni di sintesi sulla violazione: indicazioni temporali della violazione, modalità in cui l'ASCLA è venuto a conoscenza dell'incidente, motivi del ritardo della segnalazione;
- Descrizione della violazione: natura della violazione, cause della violazione, categorie di dati personali oggetto di violazione, volume dei dati raccolti, categorie di interessati coinvolti;
- Informazioni di dettaglio sulla violazione: indicazione delle infrastrutture IT coinvolte e la loro ubicazione, misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei sistemi e delle infrastrutture IT coinvolte;
- Probabili conseguenze della violazione dei dati;
- Potenziali effetti negativi per gli interessati;
- Eventuali misure adottate dall'ASCLA per porre rimedio o attenuare l'infrazione e per prevenire simili violazioni future;
- Comunicazione agli interessati;
- Altre informazioni, come comunicazioni ad altre autorità di controllo, organismi di vigilanza o di controllo, all'autorità giudiziaria o di polizia, indicazione dell'appartenenza dei paesi coinvolti allo Spazio Economico Europeo.

5.4. Eventuale comunicazione agli interessati

Accanto agli obblighi di notifica all'autorità di controllo, l'art. 34 GDPR prevede, a carico dei titolari, un obbligo di comunicazione della violazione, senza ingiustificato ritardo, all'interessato per consentirgli di attivarsi a tutela dei propri interessi.

La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione.

Tale comunicazione all'interessato non è richiesta se:

- Il Titolare del trattamento ritiene che la violazione dei dati personali non presenti un rischio elevato per i diritti e le libertà delle persone fisiche;
- Il Titolare del trattamento ha messo in atto misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;
- Il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- Detta comunicazione richiederebbe sforzi sproporzionati. In tale caso, si procede invece a una comunicazione pubblica o a una misura simile.

Nell'eventualità in cui ASCLA si trovi nell'impossibilità di contattare il soggetto interessato dalla violazione, in quanto non dispone delle informazioni necessarie per riuscire a mettersi in contatto, effettuerà la comunicazione non appena sia ragionevolmente possibile farlo (ad es. qualora il singolo esercitando il proprio diritto di accedere ai dati personali, ai sensi dell'articolo 15 GDPR, fornisca all'ASCLA le informazioni supplementari necessarie per contattarlo).

La comunicazione deve essere distinguibile dalle altre trasmesse agli interessati, in altri termini, la comunicazione deve essere chiara, inequivocabile e richiamare l'attenzione dell'interessato. Pertanto, ASCLA eviterà di trasmettere la comunicazione nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori; solo qualora la segnalazione diretta richieda sforzi sproporzionati, la normativa consente a ASCLA di effettuare una comunicazione pubblica a patto che mantenga lo stesso grado di efficacia conoscitiva del contatto diretto con l'interessato. Così, mentre può ritenersi adeguata la comunicazione fornita attraverso evidenti banner o notifiche disposte sui siti web, non lo sarà se questa sia limitata all'inserimento della notizia in un blog o in una rassegna stampa: l'adeguatezza di una comunicazione è quindi determinata non solo dal contenuto del messaggio, ma anche dalle modalità di effettuazione.

La comunicazione agli interessati, ai sensi dell'art. 34, par. 3, GDPR, comprenderà:

- Una descrizione generale della violazione dei dati (natura della violazione, categorie e numero approssimativo di interessati nonché categorie e numero approssimativo di dati personali coinvolti);
- Nome e dati di contatto del DPO o di altro punto di contatto presso cui ottenere ulteriori informazioni;
- Descrizione delle probabili conseguenze della violazione dei dati;
- Descrizione delle misure adottate o cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali.

5.5. Documentazione della violazione indipendentemente dal suo esito

Indipendentemente dalla valutazione sulla necessità di procedere alla notificazione e/o comunicazione della violazione di data breach, ogni qualvolta si verifichi un incidente, occorre archiviare la documentazione relativa, in virtù di quanto disposto dall'art. 33, par. 5, GDPR, nel rispetto del principio di responsabilizzazione, tenendo l'archivio a disposizione dell'Autorità Garante. ASCLA provvede alla compilazione e all'aggiornamento del REGISTRO.

Nel GDPR non è specificato un periodo di conservazione per tale tipologia di documentazione. Laddove tali registrazioni contengano dati personali, spetta all'ASCLA determinare il periodo di conservazione adeguato, in conformità ai principi applicabili al trattamento dei dati personali, e individuare la corretta base legale per svolgere tale trattamento; tale documentazione potrebbe peraltro risultare idonea prova di conformità alla normativa vigente.

Qualora i "*Data Breach record*" non contengano dati personali, il principio di limitazione della conservazione del GDPR non si applica.

6. Ruolo del DPO

In termini di documentazione delle violazioni, il Titolare del trattamento o il Responsabile del trattamento devono richiedere il parere del proprio DPO in merito alla struttura, all'impostazione e all'amministrazione di tale documentazione. Il DPO svolge un ruolo chiave nell'assistenza alla prevenzione delle violazioni, fornendo

consulenza e monitorando la conformità delle procedure e delle azioni poste in essere, nonché nel corso della notifica all'Autorità Garante durante qualsiasi successiva indagine da parte della stessa. Pertanto, ASCLA informa tempestivamente il proprio DPO dell'esistenza di una violazione, coinvolgendolo durante la gestione delle violazioni e del processo di notifica.