# POLICY PER LA COMUNICAZIONE DEL *"DATA BREACH"*

La presente policy è stata redatta dal Titolare del Trattamento e disciplina il processo grazie al quale si gestiscono *i data breach* e si redigono i documenti richiesti, in conformità alle vigenti normative in tema di protezione dei dati, ivi incluso, in particolare, il Regolamento UE n. 2016/679.

***

## 1. Definizioni

I termini e le espressioni di seguito indicate assumeranno il significato indicato, che rimarrà il medesimo sia al singolare che al plurale.

"**Autorità**": indica l'Autorità Garante per la Protezione dei dati personali;

***"GDPR"***: identifica il Regolamento UE n. 679 del 27 Aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati personali;

***"Data Breach"***: identifica la violazione di sicurezza che comporta accidentalmente e/o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai sistemi dell'associazione/centro sociale e ai dati personali trasmessi, conservati o comunque trattati;

***"Software"***: espressione di un insieme organizzato e strutturato di istruzioni o simboli capace direttamente o indirettamente di far eseguire o far ottenere una funzione predefinita, un compito o un risultato per mezzo di un sistema di elaborazione elettronica dell'informazione. Il termine *Software* identifica qualsiasi programma per elaboratore, *firmware*, codice sorgente, protocollo, *kit* di sviluppo, libreria, documentazione, *standard*, formato, architettura, linguaggio.

## 2. Durata del processo e modalità di comunicazione

*[Associazione Nazionale Centri Sociali, Comitati Anziani e Orti – Coordinamento [●] ("Ancescao") / centro sociale [●] affiliato Ancescao ("Centro Sociale")]*, in qualità di Titolare del Trattamento, ha l'obbligo di notificare il *data breach* all'Autorità **entro 72 ore** da quando è venuto a conoscenza della violazione, ai sensi dell'art. 33 del GDPR, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora il Titolare del Trattamento, previa consultazione con il responsabile IT, reputi impossibile rispettare tale termine, raccoglie e documenta ogni elemento ed ogni evidenza fattuale tale da giustificare i motivi del ritardo, dandone conoscenza al responsabile IT nonché ai più alti organi dell'associazione/centro sociale.

Tutte le comunicazioni nei confronti dell'Autorità e di responsabili esterni eventualmente coinvolti devono essere compiute in conformità al presente documento e dovranno essere trasmesse mediante posta certificata PEC.

### 3. Inizio della procedura

Qualora il personale designato al trattamento dei dati dovesse accorgersi di una, anche solo presunta, violazione al sistema dell'associazione/centro sociale e/o di un trattamento illecito (anche con strumenti cartacei) dei dati conservati, questi ha l'obbligo di contattare il suo responsabile gerarchico senza ritardi dalla rilevazione della *Data Breach*. A sua volta, il responsabile gerarchico ha il compito di informare i più alti organi dell'associazione/centro sociale ed il responsabile IT del Titolare del Trattamento **entro un'ora** dal momento in cui ha avuto conoscenza dell'avvenuta *Data Breach*.

Qualora il *Data Breach* non fosse avvenuto con strumenti informatici (ad esempio documentazione inviata per errore a mezzo posta, stampa di documenti sospetti, ecc.), la segnalazione dovrà comunque pervenire **entro un'ora** alla dirigenza dell'associazione/centro sociale per attivare con il Responsabile Protezione dei dati (se nominato) le opportune analisi approfondite ed azioni ritenute utili a definire il perimetro della problematica.

**[1h]**

### 4. Identificazione

Una volta venuto a conoscenza della problematica, il responsabile IT ha il compito di porre in essere immediatamente processi idonei a fornire evidenza documentale di quanto accaduto, **entro il termine di 4 ore**. Tale documentazione dovrà essere raccolta (ove possibile) in conformità a idonei processi di *computer forensics* al fine di garantire la identificazione, la raccolta, la conservazione e la eventuale presentazione di eventuali fonti di prova. Tale documentazione dovrà documentare, in particolare gli elementi che dimostrino l'avvenuto *Data Breach*.

La documentazione di ogni singola azione successiva al *Data Breach*, svolta dal responsabile IT, deve risultare necessaria al fine di dimostrare la corretta attuazione di tutte le procedure necessarie volte a cauterizzare la violazione e le conseguenze che ne derivano, come meglio descritto nel paragrafo n. 5.

**[5h]**

### 5. Misure di sicurezza

Una volta individuato il *Data Breach*, il responsabile IT deve mettere immediatamente in atto misure tecniche e organizzative adeguate per limitare le conseguenze dannose derivanti dalla violazione, **entro le 6 ore.**

Per eliminare le cause della violazione, dunque, il responsabile IT dovrà adottare le seguenti misure correttive, se del caso:

- identificare e determinare le cause della violazione;
- interrompere qualsiasi attività che consenta alla violazione di perpetuarsi;
- isolare le fonti da cui proviene la violazione.

I responsabili esterni eventualmente coinvolti dovranno collaborare per fornire il supporto necessario al personale designato da *[Ancescao/Centro Sociale]*che potrà acquisire le informazioni utili a definire il perimetro del *Data Breach*.

**[11h]**

## 6. Valutazione e relazione all'Autorità

Qualora il Titolare del Trattamento, con il supporto del responsabile IT, stabilisca che il *Data Breach* ha comportato un rischio per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento, sempre con il supporto del responsabile IT, dovrà redigere una relazione da destinarsi all'Autorità (di seguito, la "**Notifica all'Autorità**"), secondo il modello reperibile sul sito *web* della medesima, che comprenda, tra l'altro:

- la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- il nome e i dati di contatto del Responsabile della Protezione dei dati o di altro punto di contatto presso cui l'Autorità potrà ottenere più informazioni;
- l'orario e il luogo in cui è avvenuta la violazione;
- la descrizione dei sistemi informativi interessati;
- la documentazione in possesso atta a identificare e documentare la violazione avvenuta;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate (con relativa documentazione) o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
- se del caso, motivi del ritardo che non consente l'invio della Notifica all'Autorità entro le 72 ore;
- ulteriori elementi, ove richiesto, da altre normative.

## 7. Valutazione e relazione agli interessati

Quando la violazione è suscettibile di presentare un rischio **elevato** per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento, con il supporto del responsabile IT, deve valutare se:

- sono state messe in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai sistemi e ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

Se il Titolare del Trattamento, con il supporto del responsabile IT, ha attuato e garantito che i punti sopracitati siano stati rispettati, il medesimo non ha l'obbligo di dover comunicare all'interessato l'avvenuta violazione (di seguito, la "**Notifica all'Interessato**"). Tale scelta dovrà essere comunque motivata e documentata, con apposita delibera in tal senso dei più alti organi dell'associazione/centro sociale di cui al successivo paragrafo 9.

Nel caso in cui non siano state adottate misure tecniche e organizzative adeguate o misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati, il Titolare del Trattamento, con il supporto del responsabile IT, ha l'obbligo di comunicare la violazione all'interessato senza ingiustificato ritardo.

In particolare, il Titolare del Trattamento, con il supporto del responsabile IT, dovrà redigere il testo della Notifica all'Interessato, contenente la documentazione atta a illustrare l'avvenuta violazione.

Qualora la comunicazione dell'avvenuta violazione nei confronti degli interessati dovesse richiedere sforzi sproporzionati, il Titolare del Trattamento potrà definire contenuti e modalità di una comunicazione pubblica o a una misura simile, tramite la quale gli interessati verranno informati con analoga efficacia.

Gli adempimenti indicati al paragrafo 6 e paragrafo 7 dovranno essere effettuati **entro 24 ore**.

**[35h]**

## 8. Comunicazione agli organi di controllo (ove esistenti) dell'associazione/centro sociale

Una volta stilate la bozza di Notifica all'Autorità e la bozza di Notifica all'Interessato, il Titolare del Trattamento, con il supporto del resposabile IT, deve informare i propri organi di controllo (ad esempio, il Collegio Sindacale), se esistenti, in merito alla valutazione svolta, nonché ai contenuti e alle modalità della Notifica all'Autorità e della Notifica all'Interessato.

Il processo di cui al presente articolo dovrà concludersi **entro le successive 2 ore**.

**[37h]**

## 9. Decisione del Titolare del Trattamento in merito alle notifiche

Spetterà al Titolare del Trattamento, con apposita delibera dei suoi più alti organi, valutare i contenuti della Notifica all'Autorità e la Notifica all'Interessato, valutando altresì l'opportunità della relativa comunicazione all'Autorità e/o agli interessati, nonché le relative tempistiche.

Qualora i più alti organi del Titolare del Trattamento dovessero valutare come non idonee le misure tecniche e organizzative correttive di sicurezza adottate e/o indicare come incomplete le documentazioni relative alla valutazione del *Data Breach*, il responsabile IT riceverà mandato di revisionare, attraverso un processo iterativo, le fasi svolte per apportare le opportune modifiche.

Il processo di cui al presente articolo dovrà concludersi **entro le successive 24 ore.** Di tali operazioni dovrà essere messo a conoscenza il Responsabile della Protezione dei dati (se nominato), che genererà un parere scritto sulla problematica come a Lui sottoposta dai vertici dell'associazione/centro sociale.

**[61h]**

## 10. Invio e notifica all'Autorità e all'Interessato

L'invio della Notifica all'Autorità e della Notifica all'Interessato sono di spettanza del Titolare del Trattamento, il quale è tenuto ed effettuarle in conformità alle linee guida eventualmente offerte dall'Autorità. Il processo di cui al presente articolo dovrà concludersi entro le successive **10 ore**.

**[71h]**