POLYCY DATA BREACH
ai sensi dell'Articolo 33 del GDPR

FINALITA' E AMBITO DI APPLICAZIONE

Fornire procedure e linee guida da seguire in casi di Data Breach secondo gli obblighi imposti dal Regolamento Europeo 2016/679

Destinatari

Al fine di garantire la tutela e i diritti degli interessati, la presente Policy è messa a disposizione e deve essere osservata dai seguenti soggetti:

- Titolari del trattamento
- Responsabile della Protezione Dati (DPO)
- Dirigenti designati e lavoratori ncaricati al trattamento del titolare per le sole finalità e con le modalità connesse alle loro responsabilità e mansioni lavorative
- Responsabili esterni del titolare per le sole finalità e con le modalità alle loro responsabilità e obbligazioni contrattuali

COMITATO DI CRISI

Per la gestione e la mitigazione e risoluzione di tutti gli adempimenti derivanti dal Regolamento Europeo in materia di Data Breach , il Titolare del trattamento ha individuato un comitato di crisi composto da:

Dirigente incaricato

Responsabile settore IT

Data Protection officer

DATA BREACH

Qualsiasi atto, volontario o involontario, interno o esterno, che comporti la distruzione, il danneggiamento, la perdita, la modifica, la rivelazione, l'accesso non autorizzato, o il trattamento illecito ~~o senza autorizzazione di Dati Personali trasmessi, conservati o comunque elaborati dal Titolare~~ costituisce un Data Breach.

OBBLIGHI DEL TITOLARE IN CASO DI DATA BREACH

Il Titolare del trattamento è tenuto a notificare al Garante per la Protezione dei Dati personali il Data Breach senza ritardo e cmq entro 72 ore dal momento in cui ne viene a conoscenza a meno che tale evento non costituisca un rischio per i diritti e le libertà delle persone fisiche

Il Titolare del trattamento è considerato ***consapevole*** del Data Breach a partire dal momento in cui vi sia un ragionevole grado di certezza riguardo al fatto che l'incidente si sia verificato e che i dati personali siano stati compromessi. Inoltre, il Titolare del trattamento è considerato ***consapevole*** del Data Breach nel momento in cui ne vengono a conoscenza i Responsabili del trattamento. Pertanto, il Titolare del Trattamento deve implementare opportune misure di sicurezza tali da obbligare ciascun Responsabile del trattamento a comunicare anche il solo sospetto di occorrenza di un evento qualificabile come Data Breach. Il Titolare del trattamento deve rendere noto a chiunque tratti, a qualsiasi titolo, i propri Dati Personali l ' obbligo di segnalare immediatamente qualsiasi Data Breach tramite casella di posta elettronica certificata.

VALUTAZIONE

A seguito della segnalazione di un Data Breach, il Titolare del trattamento è tenuto ad effettuare una valutazione circa la possibilità che da questo derivi un rischio per i diritti e le libertà degli Interessati.Il rischio in questione esiste se dalla violazione possono derivare danni fisici, materiali o immateriali, agli interessati, quali perdita del controllo dei Dati personali, limitazione di diritti, discriminazione, furto o usurpazione di identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei Dati Personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica. Inoltre, particolare attenzione dovrà essere posta in caso di Data Breach che coinvolga Dati Particolari o Dati relativi alla salute. Nella valutazione, il Titolare del trattamento deve tenere conto della probabilità del rischio e della sua gravità basandosi su:

- Tipo di violazione: la gravità del rischio può essere diversa a seconda che venga violata la confidenzialità dei dati, la loro disponibilità, o l' integrità di questi.
- Tipo di dati oggetto del Data Breach: più i dati sono "sensibili"- e quindi appartenenti a categorie particolari di dati personali – più alto sarà il rischio per gli interessati.
- Facilità con la quale l'Interessato può essere identificato: in alcuni casi, infatti, a seguito di una violazione, tale attività può risultare particolarmente semplice .
- Gravità delle conseguenze per gli Interessati: a seconda della natura dei dati violati, le conseguenze possono essere particolarmente serie.
- Caratteristiche peculiari degli interessati: alcune categorie di soggetti, ad esempio i bambini, rischiano di essere maggiormente esposti in caso di violazione.

- Ogni altra informazione utile per proteggere i diritti e le libertà degli Interessati.

Nel caso in cui entro le 72 ore dalla scoperta del Data Breach il Titolare del trattamento non sia in possesso di tutte le informazioni sopra indicate, dovrà darne esplicita comunicazione all' Autorità Garante, concordando con questa le modalità e i termini per integrare le informazioni.

RISCHIO ELEVATO PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE

Qualora dalla valutazione del Titolare del trattamento sia emerso che il rischio per le libertà e i diritti delle persone fisiche è elevato, in aggiunta alla notifica al Garante il Titolare del Trattamento è obbligato a comunicare il Data Breach anche agli Interessati.

La notifica agli interessati, da effettuarsi senza ingiustificato ritardo, dovrà illustrare in maniera chiara e semplice la natura del Data Breach e contenere almeno:

- Il nome e i dati di contatto del Data Protection Officer o di altro punto di contatto presso cui ottenere più informazioni.
- La descrizione delle probabili conseguenze della violazione dei dati personali.
- La descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio al Data Breach e anche, se del caso, per attenuarne i possibili effetti negativi.
- Ulteriori informazioni ritenute di volta in volta opportune dal Titolare del trattamento.

La comunicazione dovrà essere effettuata direttamente ed individualmente agli Interessati, a meno che ciò non rappresenti uno sforzo sproporzionato. Il Titolare del trattamento potrà comunque interpellare all' Autorità Garante per ottenere indicazioni delle modalità più adeguate per la comunicazione dell'evento agli interessati.

LA COMUNICAZIONE AGLI INTERESSATI NON E' NECESSARIA SE IL TITOLARE DEL TRATTAMENTO E' IN GRADO DI DIMOSTRARE IL SODDISFACIMENTO DI ALMENO UNA DELLE SEGUENTI CONDIZIONI:

1. Il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto del Data Breach, in particolare quelle destinate a rendere i dati particolari *incomprensibili* a chiunque non sia autorizzato ad accedervi, quali la *cifratura.*
2. 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.
3. La comunicazione richiederebbe sforzi sproporzionati. In tal caso, si dovrà procedere a una comunicazione pubblica o a una misura simile tramite la quale gli Interessati dovranno essere informati con analoga efficacia

- Numero di individui Interessati: maggiore è il numero di soggetti, maggiori rischiano di essere le implicazioni di un eventuale Data Breach. Anche in questo caso, però, è necessario valutare le singole circostanze, in quanto, in alcuni casi, la violazione può comportare anche gravi rischi per il singolo.
    - Eventuali caratteristiche del titolare del trattamento: anche questo è un elemento da tenere in considerazione, in quanto, a seconda del tipo di attività svolta, la violazione può essere piu o meno grave.

ESITO DELLA VALUTAZIONE E OBBLIGHI PER IL TITOLARE DEL TRATTAMENTO

La valutazione del Titolare del trattamento si conclude con una delle seguenti decisioni.

- Il Data Breach non comporta rischi per le libertà e i diritti degli interessati
- Dal Data Breach possono derivare rischi per i diritti e le libertà degli Interessati
- Il Data Breach presenta un rischio elevato per le libertà e i diritti delle persone fisiche.

NESSUN RISCHIO PER I DIRITTI E LE LIBERTA'

Qualora dalla valutazione del Titolare del trattamento sia emerso che il Data Breach non ha comportato rischi per i diritti e le libertà degli Interessati, il Titolare si limiterà ad aggiornare il Registro dei Data Breach, annotandovi puntualmente gli eventi e le conseguenze del Data Breach, i dati interessati e i provvedimenti adottati per porvi rimedio.

RISCHI PER LA LIBERTA' E I DIRITTI DEGLI INTERESSATI

Qualora dalla valutazione del Titolare del trattamento sia emerso che dal Data Breach possono derivare rischi per le liberta e i diritti degli Interessati, il Titolare del trattamento è obbligato a notificare l 'incidente all' Autorità Garante.

La notifica avverrà entro 72 ore dal momento in cui il Titolare del trattamento è venuto a conoscenza della violazione. Laddove non sia possibile rispettare le tempistiche prescritte, sarà necessario indicare i motivi del ritardo.

Se le circostanze del caso lo richiedono, il Titolare del trattamento può delegare l' attività di notifica del Data Breach al Responsabile del trattamento che sia venuto a conoscenza della violazione.

La notifica del Data Breach all' Autorità Garante dovrà contenere almeno le seguenti informazioni:

- La descrizione della natura delle violazioni dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti dal Data Breach, nonché le categorie e il numero approssimativo di registrazioni dei dati personali
- Il nome e i dati di contatto del Data Protection Officer o di altro punto di contatto presso cui ottenere ulteriori informazioni.
- La descrizione delle probabili conseguenze della violazione dei Dati Personali.
- La descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio al Data Breach o attenuare possibili effetti negativi.

DOCUMENTAZIONE DATA BREACH

Ogni azione intrapresa dal Titolare del trattamento e dal comitato di crisi dalla scoperta del Data Breach sino alla definitiva gestione va documentata.