PROCEDURA DI RISPOSTA E COMUNICAZIONE DI UNA VIOLAZIONE DI DATI "DATA BREACH"

Titolare Del Trattamento

D.G. CARPENTERIA S.R.L.
VIA DELLA CORTE BRUCIATA 21 CAP 20043
VANZAGO (MI)
P.iva: 08257680960
PEO: dgcarpenteria@sgcarpenteria.com
PEC: daniferro@legalmail.it
Tel.: 0293180496

Sommario

1. Premessa

Il Titolare, **D.G. CARPENTERIA S.R.L.** in ottemperanza al Regolamento Europeo 2016/679 (di seguito "GDPR"), è obbligato a tutelare la sicurezza dei dati personali trattati nell'ambito delle proprie attività e a rispondere e mitigare immediatamente eventuali violazioni degli stessi dati.
Ciò significa predisporre procedure che definiscano i principi e le azioni generali per gestire con successo la risposta ad una violazione, al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'ente e per poter fornire, nei tempi e nei modi previsti dal GDPR, notifica all'Autorità Garante e riscontro agli interessati.
(E' bene ricordare che le sanzioni previste dal GDPR per omessa notifica di Data Breach all'Autorità di Controllo o omessa comunicazione agli interessati o entrambi gli adempimenti, può comportare l'applicazione in capo all'ente di una sanzione amministrativa pecuniaria fino a 10 milioni di euro o fino al 2% del "fatturato" annuo totale dell'esercizio precedente, anche accompagnata da una misura correttiva ai sensi dell'art. 58 c. 2.)

2. Destinatari

Questa procedura è rivolta a tutti i soggetti (di seguito "Destinatari") che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento quali: dipendenti, collaboratori, dipendenti temporanei, terzi che lavorano e/o agiscono per conto di Titolare **D.G. CARPENTERIA S.R.L.**

Tutti i Destinatari devono essere debitamente informati dell'esistenza della presente procedura.
(È bene ricordarsi di richiamare la violazione di questa procedura nei documenti aziendali che gestiscono comportamenti e provvedimenti disciplinari).

3. Terminologia e Specifiche

Una "**violazione di dati personali**" è "*ogni infrazione alla 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*" e possono consistere in:
- divulgazione di dati confidenziali a persone non autorizzate;
- furto o smarrimento di strumenti su cui sono memorizzati i dati (es: pc portatili, devices, chiavi USB);
- perdita o furto di documenti cartacei;
- infedeltà del dipendente;
- accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite;
- dati/banche dati alterate o distrutte senza autorizzazione;
- virus o altri attacchi al sistema informatico o alla rete;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

Per "**dato personale**" si intende: "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".
In questa procedura si fa riferimento a dati personali presenti su qualsiasi supporto (cartaceo e informatico) conservati o trattati in qualsiasi modo.
Il "**Titolare del Trattamento**" è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.*"
Le violazioni di dati personali sono gestite da **D.G. CARPENTERIA S.R.L.** Titolare del trattamento o da un suo delegato

4. Processo di risposta alle violazioni dei Dati

Il Processo di Risposta alle Violazione dei Dati viene avviato quando un qualsiasi soggetto viene a conoscenza dell'avvenimento di una sospetta / presunta o effettiva violazione dei dati personali. Per la precisione, il soggetto che è a conoscenza dell'incidente dovrà immediatamente informare Referente Interno Privacy o il proprio superiore gerarchico il quale dovrà compiere una valutazione preliminare (eventualmente specificare le modalità) per stabilire se la segnalazione possa essere considerata una violazione di dati personali.
Referente Interno, tiene aggiornata la documentazione, gestisce la compilazione delle varie aree relative al Data Breach si dovrà:
- compilare la segnalazione di un sospetto Data Breach, a fronte di quanto deciso dal gruppo;
- procedere con la compilazione dei vari passaggi (gestione sospetto/chiusura segnalazione/compilazione del Data Breach con ulteriori informazioni) al fine della notifica all'Autorità Garante e/o agli interessati, oppur anche solo per avere una descrizione accurata di quanto avvenuto.

Necessaria, inoltre la tenuta del REGISTRO DATA BREACH, ossia la documentazione di tutte le violazioni di dati personali analizzate (notificate o meno), nonché tenere traccia di tutte le decisioni del gruppo di lavoro principale.
Poiché questi documenti potrebbero essere esaminati dalle autorità di controllo, devono essere scritti in modo preciso e accurato per garantire la tracciabilità e la responsabilizzazione.

(Tutta la documentazione relativa all'area data breach (registri, allegati segnalazioni, allegati all'analisi di un sospetto data breach) possono essere archiviati all'interno in modo tale da averla sempre a disposizione in caso di controllo).

6. Iter da seguire

6.1: Identificazione e indagine preliminare

Il Referente Interno Privacy dovrà assegnare un livello di urgenza alla violazione e condurre una valutazione preliminare circa la notizia di sospetto Data Breach occorso, per stabilire se si tratti effettivamente di una violazione di dati personali e se si renda necessaria un'indagine più approfondita dell'accaduto, procedendo con il risk assessment.

6.2: Contenimento, recovery e risk assessment

Una volta stabilita la presenza di un Data Breach, Referente Interno Privacy, dovrà stabilire:
- se possano essere intraprese azioni che possano limitare i danni;
- quali siano i soggetti che debbano agire per contenere la violazione;
- se sia necessario notificare la violazione all'Autorità Garante (ossia nel caso in cui "non sia improbabile" che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

(Fare riferimento a "Linee guida in materia di notifica delle violazioni di dati personali (Data breach notification) – WP250" adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017 – versione emendata e adottata il 6 febbraio 2018.)

6.3: Eventuale notifica all'Autorità Garante

Una volta accertata la necessità di notificare la violazione di dati all'Autorità Garante, l'ente dovrà provvedervi, senza ingiustificato ritardo e, ove possibile entro 72 ore dall'avvenuta conoscenza.
Pertanto, Referente Interno Privacy, individuerà l'Autorità di Controllo competente ed elaborerà il documento di notifica da inviare, che dovrà includere le seguenti informazioni:
- una descrizione della natura della violazione;
- le categorie dei dati personali in questione;
- il numero approssimativo degli interessati;
- il nome e le informazioni di contatto del Responsabile del Gruppo di Risposta alle Violazioni dei Dati / Responsabile della Protezione dei Dati;
- le conseguenze della violazione dei dati personali;
- le misure adottate per gestire la violazione dei dati personali;
- qualsiasi informazione relativa alla violazione dei dati.

(Queste informazioni, vengono richieste durante la compilazione della fase 3 della Gestione di un Data breach).

6.4: Eventuale comunicazione agli interessati

La comunicazione all'interessato dell'avvenuto Data Breach è da intendersi come un vero e proprio diritto dell'interessato. Questa consiste nell'atto con il quale il Titolare del trattamento porta a conoscenza dell'interessato il verificarsi di una violazione di dati personali con rischio elevato per i diritti e le libertà delle persone fisiche coinvolte (gravi anomalie incorse nel trattamento).
A ciò consegue che il Referente Interno Privacy dovrà valutare se la violazione dei dati personali possa effettivamente comportare un rischio elevato per i diritti e le libertà dei soggetti coinvolti. In caso affermativo dovrà procedere alle dovute comunicazioni senza ritardo.
La comunicazione deve contenere:
- il nome e le informazioni di contatto del Responsabile del Gruppo di Risposta alle Violazioni dei Dati / Responsabile della Protezione dei Dati;
- le conseguenze della violazione dei dati personali;
- le misure adottate per gestire la 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 alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.
Se, per esempio a causa del numero di interessati, la comunicazione dovesse richiedere sforzi sproporzionati, Referente Interno Privacy 1dovrà identificare la modalità più appropriata per garantire che i soggetti interessati siano informati, anche attraverso l'utilizzo di canali pubblicamente disponibili.

7. Validità e gestione del documento
Questo documento è valido a partire dal **1 SETTEMBRE 2025**
Il responsabile per questo documento è inserire Referente Interno Privacy il quale deve controllare e, se necessario, aggiornare il documento con frequenza almeno annuale.
(Verificare la correttezza delle informazioni relativamente al soggetto che è responsabile della revisione di questo documento e sull'effettivo periodo di revisione, come da protocolli interni).

Data: 01/05/ 2025

Titolare: **D.G. CARPENTERIA S.R.L.**