Procedura di gestione di una violazione di dati personali

Teleimpianti S.p.A. con sede legale in Via del Tuscolano, 28 - 40128 Bologna (BO) - P.I./C.F. 00550400378, nella persona del suo legale rappresentante *pro tempore*, in qualità di Titolare del trattamento ha adottato la seguente procedura aziendale allo scopo di fornire delle chiare indicazioni in merito alla procedura da adottare nei casi in cui in incidente della sicurezza delle informazioni implichi una violazione dei dati personali (o "*Data Breach*") come prevista e descritta all'interno del Regolamento UE 2016/679 (di seguito anche "Regolamento" o "GDPR").

1. *Definizioni*

Per violazione dei dati personali di intende (art. 4, par.1, n.12, GDPR) la 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.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità dei dati personali. Il Garante Privacy ha fornito un elenco di possibili esempi che configurano una violazione dei dati personali:

- l'accesso o l'ottenimento dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incidenti o altre calamità;
- la divulgazione non autorizzata dei dati personali.

2. *Notifiche*

Teleimpianti S.p.A., in qualità di titolare del trattamento, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui le è venuto a conoscenza, deve notificare la violazione al Garante per la Protezione dei Dati Personali a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica al Garante sia necessaria e sia stata effettuata oltre il termine delle 72 ore, questa deve essere accompagnata dai motivi del ritardo.

Risulta, per tutto quanto sopra esposto, di primaria importanza essere tempestivi nella comunicazione, da parte dei soggetti che trattano dati del titolare del trattamento, di una violazione dei dati personali.

Se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

Il titolare del trattamento, a prescindere dalla notifica al Garante, documenta tutte le violazioni dei dati personali, predisponendo un apposito registro.

La notifica di una violazione di dati personali, quando ne ricorrono i presupposti, deve essere inviata al Garante Privacy tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità.

3. *Tipo di violazioni di dati personali*

Sono oggetto di notifica unicamente le violazioni di dati personali che possono comportare significativi effetti negativi sugli individui, causando danni fisici, materiali o immateriali.

Il Garante Privacy ha fornito in merito alcuni esempi di potenziali danni:

- perdita del controllo sui propri dati personali;
- limitazione di alcuni diritti;
- discriminazione;
- furto d'identità;
- rischio di frode;
- perdita di riservatezza dei dati personali protetti dal segreto professionale;
- perdita finanziaria;
- danno alla reputazione;
- qualsiasi altro significativo svantaggio economico o sociale.

4. *Comunicazione agli interessati*

Nel caso in cui l'esito della valutazione abbia rilevato che la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo (art. 34.1).

La comunicazione deve contenere, con linguaggio semplice e chiaro almeno le seguenti informazioni:

- natura della violazione dei dati personali, ivi comprese le categorie e il numero di interessati nonché il tipo e il numero di record coinvolti
- dati di contatto del responsabile della protezione dei dati
- le probabili conseguenze della violazione
- le misure adottate o da adottare per porre

L'azienda al fine di gestire al meglio le violazioni dei dati ha individuato uno specifico punto di contatto informativo nel rapporto con gli utenti, info@teleimpianti.it

5. Esclusione della comunicazione agli interessati

Non è richiesta la comunicazione all'interessato (GDPR, art. 34.3) se è soddisfatta una delle seguenti condizioni:

- i dati personali sono cifrati;
- successivamente alla violazione è stato possibile adottare misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione richiederebbe sforzi sproporzionati (In tal caso, si procede a una comunicazione pubblica o a una misura simile).

Nel caso in cui non la comunicazione non sia stata ancora effettuata, l'Autorità di controllo può disporne, con propria valutazione, che vi si provveda

6. Gestione della comunicazione del data breach

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato. In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la

stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.

Tutti i soggetti devono attivarsi nella prevenzione, mitigazione di una violazione dei dati nelle fasi di:

- rilevazione e segnalazione della violazione, raccolta delle informazioni
- raccolta informazioni sulla violazione dei dati
- comunicazione della violazione dei dati

7. Rilevazione e segnalazione della violazione

Tutto il personale, collaboratori, fornitori, responsabili, incaricati al trattamento dati, deve comunicare al Legale Rappresentante o il Responsabile IT, non appena se ne ha conoscenza, la violazione dei dati personali utilizzando le vie più brevi (telefonicamente, di persona, via e-mail).

8. Raccolta informazioni sulla violazione dati

Il Legale Rappresentante o il Responsabile IT, appena ricevuta la segnalazione, devono dare precise istruzioni alla persona che li ha contattati affinché questa possa subito procedere alla raccolta delle informazioni, anche indicando dove reperire il modello predisposto a tale scopo

9. Contenuto della notifica

Il contenuto della notifica è indicato espressamente dal GDPR che richiede la descrizione:

- della natura della violazione dei dati personali, categorie, numero di interessati: occorre cioè dettagliare e circostanziare la violazione rilevata (ad esempio quando è avvenuta in termini di data e ora, se sia ancora in corso di svolgimento, dove si è verificata nel caso di smarrimento o furto di dispositivi)
- dell'identità dei riferimenti di contatto (telefonici email)
- delle conseguenze della violazione (possibili danni stimati in termini di probabilità)
- delle misure proposte o adottate dal Titolare del trattamento per porne rimedio.

10. Violazione di dati personali trattati dall'azienda in qualità di responsabile del trattamento

Nel caso in cui l'Azienda abbia sottoscritto contratti/convenzioni che prevedono l'effettuazione di un trattamento di dati personali per conto di altro Titolare e, in virtù di tale rapporto contrattuale, sia stata nominata Responsabile del trattamento, il Legale Rappresentante o il Responsabile IT responsabile della gestione del contratto analizza l'evento e se ritiene possa trattarsi di un incidente di sicurezza, attiva un processo di gestione dell'incidente finalizzato a fornire al Titolare ogni informazione e/o documentazione utile alla predisposizione e trasmissione della notificazione del data breach in base all'accordo sottoscritto tra le parti.

11. Violazione di dati personali trattati in nome e per conto dell'azienda dal responsabile del trattamento

Nel caso in cui il Data Breach si verifichi nell'ambito di un trattamento di dati effettuato, per conto della nostra azienda da un soggetto esterno all'organizzazione, individuato quale Responsabile, si fa riferimento alle clausole contrattuali previsto nell'accordo a responsabile esterno al trattamento.

In base all'accordo sottoscritto tra le parti il Responsabile del trattamento informa tempestivamente il Titolare (Azienda) di ogni violazione dei dati, nonché di ogni situazione anomala o di emergenza che possa compromettere il corretto trattamento e la sicurezza dei dati, al seguente indirizzo mail teleimpianti@pec.teleimpianti.it

Il Legale Rappresentante o il Responsabile IT prende in carico la segnalazione ed effettua una breve indagine finalizzata ad accertare, insieme al Responsabile del trattamento, al Direttore della Struttura e che gestisce il contratto/convenzione, se trattasi di data breach e a valutare il livello di rischio ad esso associato.

Il Responsabile del trattamento è tenuto a collaborare diligentemente con il soggetto competente effettuando un'analisi puntuale e documentata del tipo di violazione, verificando le conseguenze della stessa e indicando la funzione interna alla propria organizzazione che dovrà fornire al Titolare ogni informazione e/o documentazione utile alla predisposizione e trasmissione della notificazione del data breach all'Autorità Garante. Il Responsabile del trattamento deve adoperarsi per ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

12. Data breach e subresponsabile

Quando un responsabile del trattamento ricorra ad un altro responsabile (c.d."sub-responsabile") per l'esecuzione di specifiche attività di trattamento per conto dell'Azienda Titolare, su tale sub-responsabile gravano gli stessi obblighi contenuti nell'accordo sottoscritto tra il Titolare e il responsabile principale, che conserva nei confronti del Titolare l'intera responsabilità.

13. Il registro delle violazioni

Il titolare del trattamento, a prescindere dalla notifica al Garante, documenta tutte le violazioni dei dati personali, ad esempio predisponendo un apposito registro. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

14. Informazione e formazione

L'azienda, in coerenza con il principio di responsabilizzazione, pianifica sessioni di informazione e formazione finalizzate ad illustrare la procedura di Data Breach in termini di ruoli, compiti, responsabilità e sanzioni. Il rispetto della procedura è obbligatorio ed integra i doveri d'ufficio per tutti i soggetti coinvolti (dipendenti e collaboratori a vario titolo).

La procedura avrà la seguente diffusione tramite:

-pubblicazione sulla rete Intranet aziendale, presentazione nei corsi di formazione e momenti informativi;

15. Responsabilità nel caso di violazione della procedura

Il mancato rispetto della presente "Procedura Data Breach" da parte di tutto il personale potrà comportare, nei casi più gravi, conseguenze disciplinari.

16. Modifiche

La procedura sarà costantemente aggiornata alla luce delle modifiche organizzative, tecniche e giuridiche che interverranno in materia.

L'azienda di riserva si riserva di emanare successive istruzioni e circolari di approfondimento in materia.

Data 17/11/2026

Firma_____