NATUREDREAM
Riciclo e Smaltimento Rifiuti

GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) AI SENSI DELL'ART. 33 DEL REGOLAMENTO (UE) 679/2016

INDICE

Sommario

1. INFORMAZIONI PRELIMINARI

1.1. Annulla e Sostituisce

Procedura di nuova emissione.

1.2. Motivo dell'emissione/Revisione

Avviare un sistema gestione delle eventuali violazioni dei dati personali al fine di consentire alla Società di effettuare la notifica all'autorità di controllo entro 72 ore dalla scoperta della violazione e agli interessati.

1.3. Definizioni

Ai fini della gestione della documentazione aziendale di NATURE DREAM SRL viene utilizzata la seguente terminologia:

Dato personale: 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 ai sensi dell'art. 4, n. 1, del GDPR;

Dato di categoria particolare: dato personale che, singolarmente o insieme ad altri, sia idoneo a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona ai sensi dell'art. 9, par. 1, del GDPR;

Dati personali relativi a condanne penali o reati: dati relativi alle condanne penali o reati o a connesse misure di sicurezza;

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione ai sensi dell'art. 4, n. 2, del GDPR;

Titolare del trattamento: la Società NATURE DREAM SRL o qualunque suo organo (CDA Consiglio di Amministrazione, PRE Presidente, AD Amministratore Delegato) operante nell'ambito della determinazione delle finalità e dei mezzi di trattamento;

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Amministratore di Sistema: la figura professionale finalizzata alla gestione e alla manutenzione di un

impianto di elaborazione o di sue component;

Addetto al Trattamento: la persona fisica che tratta i dati personali per conto del Titolare;

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali

Interessato: la persona fisica identificata o identificabile direttamente o indirettamente con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, n identificativo on line o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Data Protecion Officer (Responsabile per la Protezione dei Dati): il soggetto designato ai sensi degli artt. 37- 39 del GDPR;

Violazione dei dati personali: 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;

Decreto Legislativo 231/2001 (di seguito "Dlgs 231/2001"): disciplina della responsabilità amministrativa degli enti in base alla quale la società può essere ritenuta responsabile, e conseguentemente sanzionata in relazione a taluni reati commessi o tentati dagli amministratori o dai dipendenti nell'interesse o a vantaggio della Società stessa.

Modello di organizzazione, gestione e controllo ex Dlgs 231/2001 (di seguito "Modello 231"): è il Modello adottato dalla Società atto a prevenire la commissione di reati penali previsti dal D.Lgs 231/2001 Il Modello 231 prevede, tra i vai adempimenti, la predisposizione e attuazione di specifici protocolli di controllo preventivo.

1.4. Rilevanza ai fini del Modello 231

La presente procedura ha rilevanza "specifica" ai fini del Modello 231, in quanto riguarda in modo specifico i processi rilevanti ai fini dell'art. Art. 24-bis. del d.lgs. 231/01 "Delitti informatici e trattamento illecito di dati".

2. SCOPO E CAMPO DI APPLICAZIONE

Definire le responsabilità e le modalità operative per la gestione delle eventuali violazioni dei dati personali ai sensi degli artt. 33 e 34 del Regolamento (UE) n. 679/2016 (GDPR)

3. IDENTIFICAZIONE DELLA FIGURA E DESCRIZIONE DEL PROCESSO

Cosa è una violazione

A titolo esemplificativo e non esaustivo costituiscono *violazione:*

a) l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;

b) il furto o la perdita di dispositivi informatici contenenti dati personali;
c) la deliberata alterazione di dati personali;
d) l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
e) la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
f) la divulgazione non autorizzata dei dati personali.

Conoscenza della violazione

La Società può venire a conoscenza di una possibile violazione dei dati con le seguenti modalità:

- scoperta dagli Addetti al Trattamento o dal Responsabile "interno";
- segnalata da responsabili "esterni";
- segnalata da uno o più interessati;
- altre modalità (es. segnalazione autorità, etc.).

Dal momento in cui viene effettuata la scoperta cominciano a decorrere le 72 ore entro le quali il Titolare deve eventualmente effettuare la notifica al Garante per la Protezione dei Dati Personali.

Segnalazione al Responsabile del Trattamento

L'Addetto al Trattamento che abbia avuto notizia della scoperta della possibile violazione informa immediatamente il Responsabile (ove lo stesso non abbia personalmente scoperto la violazione) o, in sua assenza, il "2° referente" o comunque tutto il personale che, nell'ambito della Società tratta i dati in qualità di "persona designata".

La segnalazione al Responsabile (o ad altro referente indicato) deve essere in forma scritta e riportare:

- quando è stata scoperta la violazione;
- una breve descrizione della violazione.

Attività del Responsabile del Trattamento e del Dpo

Il Responsabile, informato della possibile violazione, convoca ed informa senza indugio il Dpo e l'Amministratore di Sistema.

In tale sede sono valutate le informazioni di cui si è in possesso e si valuta se è necessario effettuare la notifica al Garante e agli interessati e le iniziative più opportune (cosa comunicare, con quale strumento a chi, etc.).

In ultima istanza la scelta spetta la Titolare che in ogni caso deve ricevere per iscritto il parere del DPO. L'eventuale comunicazione della violazione deve esser fatta entro 72 ore dalla scoperta sull'apposito MODELLO DI NOTIFICA AL GARANTE allegato alla presente procedura (All. 2). Ove non sia possibile – sin da subito – avere consapevolezza di tutti gli elementi si provvederà a effettuare una "comunicazione preliminare".

Qualora la violazione sia imputabile a profili informatici di cui all'art. .24-bis. del d.lgs. 231/01, il Responsabile del trattamento dei dati trasmetterà senza indugio un'informativa dettagliata all'OdV.

La notifica deve essere inviata al Garante tramite posta elettronica certificata all'indirizzo **protocollo@pec.gpdp.it** oppure tramite posta elettronica ordinaria all'indirizzo **protocollo@gpdp.it** e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

L'oggetto del messaggio deve contenere obbligatoriamente la dicitura **"NOTIFICA VIOLAZIONE DATI PERSONALI"** e opzionalmente la denominazione del Titolare del trattamento.

Attività successive

Sia in caso di avvenuta notifica sia nel caso in cui non sia stata effettuata le notifica l'incidente dovrà essere annotato nel "registro degli incidenti" (All. 1).

Il Responsabile del trattamento dovrà fornire semestralmente l'estratto aggiornato del registro degli incidenti all'OdV.

In base all'Art. 34 GDPR deve essere predisposta una corretta informazione agli interessati. Il titolare del trattamento deve comunicare la violazione all'interessato senza ingiustificato ritardo, descrivendo con un linguaggio semplice e chiaro la natura della violazione dei dati personali e indicando almeno i dati di contatto del DPO o di altro punto presso cui ottenere più informazioni, le probabili conseguenze della violazione, le misure adottate dal titolare o quelle che adotterà per porre rimedio alla violazione e anche, se del caso, per porre rimedio ai possibili effetti negativi.

Sempre l'art. 34 precisa che qualora la comunicazione richiederebbe sforzi sproporzionati il titolare procede a una comunicazione pubblica, o a una simile misura per informare gli interessati con analoga efficacia.

L'art. 86 del GDPR evidenzia come "la comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o altra autorità competente".

L'Art. 34 conferma che nel caso in cui il titolare non abbia comunicato la violazione dei dati agli interessati, l'Autorità può richiedere che vi provveda.

Le modalità operative della comunicazione del data breach agli interessati e l'adeguatezza della stessa sono state affrontate dal WP29 nelle sopra citate linee guida che specificano come nel "comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard. Ciò contribuisce a rendere la comunicazione della violazione chiara e trasparente".

4. ARCHIVIAZIONE CONSERVAZIONE E ACCESSO ALLA DOCUMENTAZIONE

4.1. Archiviazione e Conservazione

I Documenti sono raccolti in apposite cartelle (fisiche e informatiche) e codificati in modo da essere chiaramente identificabili, prontamente rintracciabili e, se necessario, resi disponibili.
Di seguito si riporta la tabella riepilogativa dei termini e delle responsabilità di conservazione dei documenti citati nella presente Procedura.

TIPO DI DOCUMENTO	CONDIZIONE	CONSERVAZIONE	RESPONSABILITA'
Istruttoria *data breach*	In vigore	Periodo di validità	Responsabile del trattamento/Dpo
	superati	5 anni	
Notifica al Garante	In vigore	Periodo di validità	Responsabile del trattamento/Dpo
	superati	5 anni	
Registro degli incidenti	In vigore	Periodo di validità	Responsabile del trattamento/Dpo
	superati	5 anni	

4.2. Accesso

L'accesso alla documentazione trattata nella presente Procedura è garantito a tutti i componenti degli organi e organismi di governance, ai responsabili e referenti delle funzioni di controllo e a tutti i dipendenti coinvolti dal documento, nonché all'autorità di vigilanza.

5. RIFERIMENTI NORMATIVI INTERNI-ESTERNI

Di seguito si riportano in breve I riferimenti Normativi interni ed esterni di cui la presente procedura ne è espressione.

- Regolamento (UE) 679/2016
- Modello 231
- Codice Etico

6. ALLEGATI

Gli allegati alla presente sono parte integrante del document e costituicono elementi procedurali cui l'azienda deve attenersi.

Allegato 1 – Registro degli incidenti

6.1. Allegato 1 Registro degli incidenti: Modello

Numero Incidente 1

A. Rilevazione dell'incidente

Data

B. Descrizione dell'incidente

Tipo incidente (virus, attacco, alterazione dati, guasto apparati, sottrazione informazioni, blocchi, malfunzionamenti, ecc.)

Sistemi colpiti e/o applicazioni colpite

Funzioni aziendali colpite

L'entità dell'incidente è tale da farlo rientrare nell'attenzione GDPR? SI/NO

Numero Clienti/Utenti oppure Numero Dipendenti colpiti dall'incidente (perdita e/o alterazione dati), ecc.

Tipologia di dati coinvolti

Tipologia di soggetti coinvolti

Note

C. Risoluzione dell'incidente