GIOIELLERIA GATTOPARDO

DI LENNY ARTALE

PROCEDURA

PER **LAGESTIONE** DELLE **VIOLAZIONI**

DEI DATI PERSONALI.

(Data Breach)

Sommario

1. INTRODUZIONE

La normativa contenuta nel Regolamento UE 2016/679 si propone di tutelare la riservatezza dei dati personali, per evitare che un uso non corretto di essi possa danneggiare o ledere le libertà fondamentali e la dignità personale di ognuno.

In particolare i dati trattati dalla **Gioielleria Gattopardo di Lenny Artale** il cui campo d'attività riguarda la vendita di carburanti e lubrificanti, garantendo prodotti, servizi e consegne, sono le informazioni personali (es. dati anagrafici, recapito, codice fiscale, ecc.) e sensibili indispensabili per l'erogazione e la gestione delle prestazioni richieste e previste dall'oggetto sociale.

La **Gioielleria Gattopardo di Lenny Artale** si impegna a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).

In tal senso la **Gioielleria Gattopardo di Lenny Artale** ha redatto la presente procedura al fine di garantire, secondo un processo standardizzato, le azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali e per poter riscontrare, nei tempi e nei modi previsti dalla normativa europea, l'Autorità Garante e/o gli interessati.

2. SCOPO

Questo documento descrive le modalità operative adottate dalla Fioielleria Gattopardo di

Lenny Artale al fine di garantire la gestione, in maniera standardizzata e nel rispetto di quanto previsto dall'art. 33 del GDPR sulle violazioni dei dati personali.

Nello specifico si è definito un flusso procedurale per la gestione delle violazioni dei dati personali trattati dalla Gioielleria Gattopardo di Lenny Artale, che si integra con le procedure già adottate dalla stessa in materia di protezione dei dati personali

3. CAMPO DI APPLICAZIONE

Il presente documento determina i processi di gestione delle violazioni di dati personali che possono accadere per un ampio numero di ragioni che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di

stanze di sicurezza o archivi, contenenti informazioni riservate);

- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

4. DEFINIZIONI

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 (art. 4, punto 1).

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 (art. 4, punto 2).

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6).

Titolare del trattamento: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, punto 7).

Violazione dei dati personali (c.d. **Data breach**): 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 (art. 4, punto 12).

5. DESCRIZIONE DELLE ATTIVITÀ

Nel presente paragrafo sono descritte le modalità operative adottate dalla "**Gioielleria Gattopardo di Lenny Artale** " per assicurare all'interessato l'esercizio dei propri diritti e si applicano a tutti i trattamenti definiti nel "**Registro delle attività di trattamento**", secondo l'informativa fornita all'interessato e nel rispetto di quanto previsto dal GDPR.

5.1. Segnalazioni di potenziale violazione

Le violazioni di dati personali sono gestite dal Titolare del trattamento.

5.2. Monitoraggio degli eventi di potenziale violazione

L'individuazione di potenziali violazioni dei dati personali avviene, oltre che per segnalazione diretta da parte degli attori coinvolti, anche a seguito di attività di monitoraggio degli eventi che possono arrecare violazioni dei dati, sia digitale ed automatizzata che cartacea.

Il monitoraggio viene effettuato tramite il controllo delle attività di trattamento definite nel Registro dei trattamenti, in particolare per quei trattamenti che sono stati valutati con rischio non trascurabile in fase di valutazione d'impatto.

Le attività di monitoraggio si possono suddividere in due tipologie:

a. **Il monitoraggio degli eventi di natura *Software.***

- Tale monitoraggio include l'insieme delle attività di controllo finalizzate al rilevamento degli eventi tracciati dai sistemi informatici.

Tali eventi relativi ai sistemi ICT sono monitorati e gestiti dall'Amministratore di Sistema, ove previsto, che è responsabile della sicurezza operativa dei sistemi ICT aziendali.

In caso di rilievo di **concreta, sospetta e/o avvenuta violazione** dei dati personali relativi ai sistemi ICT aziendali, l'Amministratore di Sistema deve immediatamente informare dell'accaduto il Titolare del trattamento, mediante la compilazione dell'Allegato A - Modulo di comunicazione interna di Data Breach da inviare a mezzo pec all'indirizzo pec: artalelenny@pec.it

b. **Il monitoraggio dei luoghi fisici del trattamento e dell'archiviazione di dati personali.**

- I luoghi fisici preposti al trattamento di informazioni personali sensibili, con particolare riferimento agli eventuali archivi cartacei, devono essere controllati periodicamente dal personale incaricato al trattamento, e dai Responsabili interni i quali assumono la responsabilità dei trattamenti dagli stessi effettuati.

In caso di rilievo di concreta, sospetta e/o avvenuta violazione dei dati personali in particolare relativamente agli archivi cartacei ma anche digitali (ad esempio **smarrimento** o furto di **documenti cartacei o digitali e personal compute**r, ovvero tentativi di **scasso**

alle porte di accesso a alle serrature degli **armadi e cassettiere**, presenza di personale non autorizzato in locali interdetti al pubblico), il Responsabile dell'Area di riferimento a cui afferisce il trattamento, deve immediatamente informare dell'accaduto il Titolare del trattamento mediante la compilazione dell'Allegato A - Modulo di comunicazione interna di Data Breach da inviare a mezzo pec all'indirizzo pec: artalelenny@pec.it

5.3. Modalità operativa di gestione delle violazioni dati personali

La gestione di una violazione dei dati personali è stata standardizzata in un processo suddiviso nelle seguenti quattro fasi:

a. Identificazione e indagine preliminare.
b. Risk assessment e individuazione misure.
c. Notifica all'Autorità Garante.
d. Comunicazione agli interessati.

5.3.1. Identificazione e indagine preliminare

A seguito di ricezione della segnalazione, compilata tramite l'Allegato A, da parte di uno degli attori, il Titolare del trattamento, effettua la registrazione e l'identificazione univoca della segnalazione, quindi effettuerà una valutazione preliminare riguardante la possibile violazione occorsa, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di *Data Breach (violazione)* e se sia necessaria un'indagine più approfondita dell'accaduto e avvierà la fase di *risk assessment* (par. 5.2.2).

Nel caso in cui si individuasse una possibile violazione di dati contenuti in un sistema informatico (ICT), il Titolare inoltrerà la segnalazione all'Amministratore di Sistema per effettuare una istruttoria e le valutazioni di competenza in merito all'accaduto.

Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'Allegato A, quali:

- la data di scoperta della violazione (tempestività);
- il soggetto che è venuto a conoscenza della violazione;
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- la descrizione di eventuali azioni già poste in essere.

5.3.2. Risk assessment e individuazione delle misure

A termine della fase di valutazione preliminare, nel caso si stabilisca che una possibile violazione è effettivamente avvenuta, il Titolare del trattamento:

- adotta le opportune misure correttive e di protezione che possano limitare i danni che la violazione potrebbe causare *(i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso...* ecc.);
- le modalità e le tempistiche di suddette misure, individuando gli attori e i compiti per limitare la violazione;
- le opportune comunicazioni se la violazione ricade nei casi un cui è necessario notificare

all'Autorità Garante per la Protezione dei dati personali *(ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche).*

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Responsabile del Trattamento valuterà la gravità della violazione utilizzando un modello standardizzato, come da Modulo di valutazione del Rischio connesso al Data Breach (Allegato B), secondo le indicazioni di cui all'art. 33 GDPR.

Si precisa che gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio tale da essere *non trascurabile* (*...improbabile che la violazione presenti un rischio...*), l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato.

5.3.3. Notifica all' Autorità Garante competente

Se a seguito delle valutazioni preliminari e del risk assessment effettuato nel rispetto della presente procedura, è stata verificata la necessità di effettuare la notifica della *violazione dei dati,* secondo quanto prescritto dal Regolamento (UE) 2016/679, il Titolare del trattamento della Fioielleria Gattopardo di Lenny Artale, provvederà alla notifica all'Autorità Garante senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza.

5.3.4. Comunicazione agli interessati

Se a seguito delle valutazioni preliminari e del risk assessment, effettuato nel rispetto della presente procedura, è stata valutata la necessità di effettuare la comunicazione della violazione

dei dati a coloro dei cui dati si tratta, in quanto è stato riscontrato un rischio elevato per i diritti e le libertà delle persone fisiche, secondo quanto prescritto dal Regolamento (UE) 2016/679, il Titolare del trattamento provvederà alla comunicazione all'Interessato senza ingiustificato ritardo.

Quanto al contenuto di tale comunicazione, il Titolare del trattamento dovrà:

- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le 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.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento dovrà sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali mail o comunicazioni dirette).

Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

5.3.5. Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di **Data Breach**, ogni qualvolta si verifichi un incidente comunicato dagli attori che partecipano al trattamento la G***ioielleria Gattopardo di Lenny***

Artale sarà tenuta a documentarlo.

Tale documentazione sarà affidata al Responsabile del Trattamento, quest'ultimo provvederà alla tenuta di un apposito Registro dei Data Breach, in cui saranno riportate le seguenti informazioni:

- n. violazione;
- data violazione;
- natura della violazione;
- categoria di interessati;
- categoria di dati personali coinvolti;
- conseguenze della violazione;
- misure adottate;
- notifica all'Autorità Garante Privacy;
- comunicazione agli interessati.

Il Registro dei Data Breach sarà continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

5.5. Diagramma di flusso di gestione delle richieste formali