COMITATO REGIONALE PER LA GESTIONE VENATORIA

PROCEDURA PER LA GESTONE DELLE VIOLAZIONI DI DATI PERSONALI

(Data Breach)

Regolamento (UE) 2016/679 relativo alla protezione dei dati personali

DATA CREAZIONE: 15 maggio 2025

Sommario

1. La Mappa delle Responsabilità

La tabella seguente elenca le figure chiave del processo di gestione delle violazioni e ne descrive caratteristiche e compiti.

	Figura	Nominativo	Compito assegnato
A	Addetti al trattamento dei dati personali 	*Tutti gli addetti al trattamento*	Sono le persone che effettuano i trattamenti dei dati personali all'interno dell'organizzazione e che devono segnalare eventuali violazioni ricevute all'incaricato alla gestione delle Violazioni.
B	Incaricato alla Gestione delle Violazioni 	*PAOLO TRIPODI*	È la persona individuata all'interno dell'organizzazione a ricevere e gestire le segnalazioni di violazione e attuare la procedura. Attiva l'Amministratore di Sistema e informa l'Amministratore Delegato e il Referente interno della Privacy.
C	Amministratore di Sistema 		È la persona che gestisce e manutiene l'impianto di elaborazione e/o sue componenti: basi di dati reti, apparati di sicurezza e software.
D	Referente interno della Privacy 	*PAOLO TRIPODI*	Sovraintende le operazioni di gestione della privacy comprese eventuali violazioni di dati personali.
E	Amministratore Delegato 	*SERGIO GRANGE*	È il legale rappresentante del Titolare del trattamento (che è l'organizzazione) ed effettua la comunicazione al garante dell'eventuale violazione.
F	DPO 	ENRICO CAPIRONE (ISIMPLY)	Il responsabile della protezione dei dati (DPO), se designato, ha il compito di: a) informare e fornire consulenza al Titolare del trattamento e ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento e dalle altre disposizioni relative alla protezione dei dati; b) sorvegliare l'osservanza del regolamento, di altre disposizioni relative alla protezione dei dati e delle politiche del Titolare sul trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento; d) cooperare con l'autorità di controllo; e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

G	Responsabili esterni 	Tutti i responsabili esterni	Sono le persone fisiche o giuridiche, le autorità pubbliche, i servizi o altri organismi che tratta dati personali per conto del Titolare del trattamento.

2. Il Sistema di Rilevazione

Nel caso di rilevazione e/o di sospetto di violazione qualsiasi addetto al trattamento o l'Amministratore di sistema devono inviare una mail all'Incaricato alla gestione delle violazioni il quale deve prendere in carico quanto ricevuto compilando il **Modulo gestione segnalazione** (Allegato 1) compilato.

Ricevuta la segnalazione, l'Incaricato alla gestione delle violazioni attiva la procedura di gestione della violazione.
Le segnalazioni devono essere tempestivamente comunicate all'Incaricato alla gestione delle Violazioni non oltre 12 ore dalla conoscenza della violazione, all'indirizzo mail ufficiosegreteria@comitatovenatorio.vda.it
La presa in carico di tutte le segnalazioni è di responsabilità dell'Incaricato alla gestione delle violazioni che provvederà a gestirle coinvolgendo le altre funzioni interessate secondo quanto specificato nella presente procedura.

La segnalazione potrebbe arrivare anche da un **soggetto esterno**:

- Interessato
- Responsabile esterno
- Organi di Polizia
- Autorità di Controllo
- altro

Per la segnalazione da soggetto esterno sono disponibili sul sito i dati di contatto del Titolare, del DPO e il canale a cui inviare eventuali violazioni.

3. La Procedura per la gestione delle violazioni

Nella tabella di seguito viene analizzata la procedura per la gestione delle violazioni con l'indicazione dei soggetti coinvolti, le azioni da intraprendere e le modalità operative da seguire.

FASE	TITOLO ATTIVITA'	DESCRIZIONE ATTIVITA'
1	**ACQUISIZIONE DELLA SEGNALAZIONE** 	Ricevimento della segnalazione e comunicazione a: 1. Segnalatore (ricevimento di conferma presa in carico); 2. Amministratore di sistema; 3. Referente interno della Privacy; 4. Amministratore Delegato.
2	**GESTIONE TECNICA DELLA VIOLAZIONE** 	Analisi della segnalazione: 1. Raccolta informazioni; 2. Analisi tecnica della violazione; 3. Definizione dei soggetti coinvolti; 4. Accertamento dell'effettiva sussistenza del data breach.
3	**VALUTAZIONE** 	Valutazione circa la natura dei dati che sono stati violati e della tipologia di eventi che si sono verificati per determinare se si è in presenza di una situazione che presenti rischi per i diritti delle persone fisiche e quindi decidere se: 1. notificare al Garante per la Protezione dei Dati Personali; 2. segnalare agli organi di Polizia.
4	**NOTIFICA AL GARANTE** 	(*eventuale*) Comunicazione al Garante utilizzando la specifica procedura attraverso il sito web dell'Autorità.
5	**SEGNALAZIONE A ORGANI POLIZIA** 	(*eventuale*) Comunicazione agli organi di polizia

6	**COMUNICAZIONE AGLI INTERESSATI** 	(*ove possibile*) Comunicazione agli interessati dell'avvenuta violazione e delle misure di mitigazione del danno messe in atto.
7	**REGISTRAZIONE DELLA VIOLAZIONE** 	Registrazione sul Registro delle Violazioni della violazione o della presunta violazione gestita.

FASE 1 - ACQUSIZIONE DELLA SEGNALAZIONE		
Chi?	**Che cosa?**	**Come?**
Incaricato alla Gestione delle Violazioni 	– Raccolta della segnalazione – Analisi preliminare della segnalazione e compilazione della scheda evento	Ricezione della segnalazione e compilazione del **Modulo gestione segnalazione** (Allegato 1) contenente tutte le informazioni raccolte: – data evento anomalo; – data presunta di avvenuta violazione; – data e ora in cui si è avuto conoscenza della violazione; – fonte segnalazione; – tipologia violazione e di informazioni coinvolte; – descrizione evento anomalo; – numero interessati coinvolti; – quantità di dati personali di cui si presume una violazione; – indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di device mobili; – sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione; – informazione di contatti del segnalatore/i (mail e telefono).
Incaricato alla Gestione delle Violazioni 	Informazione della presa in carico della segnalazione al segnalatore	Invio al segnalatore di una mail di presa in carico della segnalazione di violazione con i dati registrati.

Incaricato alla Gestione delle Violazioni 	Informazione della segnalazione e dell'attivazione della procedura di gestione all'amministratore di sistema	Invio mail all'Amministratore di sistema per informare circa l'attivazione e presa in carico della segnalazione di violazione e attivazione della procedura di gestione
Incaricato alla Gestione delle Violazioni 	Informazione della segnalazione e dell'attivazione della procedura di gestione agli organi apicali dell'organizzazione	Invio mail di informazione di presa in carico della segnalazione di violazione a: – Referente interno della Privacy – Amministratore Delegato

FASE 2 - GESTIONE TECNICA		
Chi?	**Che cosa?**	**Come?**
Incaricato alla Gestione delle Violazioni 	Attivazione del Gruppo di Lavoro	L'incaricato alla gestione delle violazioni contatta e attiva l'Amministratore di Sistema ed eventuali altre figure (addetti interni e/o responsabili esterni) necessarie all'analisi tecnica della segnalazione di violazione. Il **Modulo gestione segnalazione** (Allegato 1) viene riutilizzato e aggiornato, se necessario, nella prima parte, per la più approfondita valutazione di primo livello descritta di seguito.
Incaricato alla Gestione delle Violazioni + Gruppo di Lavoro 	Analisi preliminare e valutazione di primo livello della segnalazione	Il gruppo di lavoro attivato effettua una prima valutazione della segnalazione per confermare o meno che si tratti di una violazione. Obiettivo dell'analisi di primo livello è quello di verificare che la segnalazione non sia un "falso positivo". Nel caso venga accertato che si tratta di violazione su dati personali, l'Incaricato alla Gestione delle Violazioni, responsabile dell'analisi di primo livello, con la collaborazione degli uffici coinvolti dalla violazione, recupera le informazioni di dettaglio sull'evento necessarie alle analisi di secondo livello, e le riporta aggiornando **Modulo gestione segnalazione** (Allegato 1).

		Nel caso in cui l'evento segnalato risulti essere un falso positivo, si chiude la procedura.
Incaricato alla Gestione delle Violazioni + Gruppo di Lavoro 	Analisi approfondita e valutazione di secondo livello	Per l'analisi di secondo livello viene eventualmente convocato dall'Incaricato alla Gestione delle Violazioni il Gruppo di Gestione della Violazione a cui partecipano: – L'Amministratore di sistema; – Il Responsabile della Protezione dei Dati (DPO) se designato; – Ogni altra figura utile alla gestione della violazione. Obiettivo dell'analisi di secondo livello è identificare la violazione e la categoria di appartenenza (violazione di riservatezza, d'integrità o di disponibilità). In tutti i casi, il Gruppo analizza congiuntamente tutte le informazioni raccolte, classifica l'evento e conclude la compilazione del **Modulo gestione segnalazione** (Allegato 1) per le conseguenti valutazioni. La classificazione viene effettuata con l'ausilio della **Guida per la Valutazione delle Violazioni** La violazione deve essere valutata secondo i livelli di rischio: ☐ NULLO ☐ BASSO ☐ MEDIO ☐ ALTO Il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche anche diverse dall'Interessato a cui si riferiscono i dati, a causa della violazione dei Dati Personali: 1. discriminazioni; 2. furto o usurpazione d'identità; 3. perdite finanziarie; 4. pregiudizio alla reputazione; 5. perdita di riservatezza dei dati personali protetti da segreto professionale; 6. decifratura non autorizzata della pseudonimizzazione;

		7. danno economico o sociale significativo; 8. privazione o limitazione di diritti o libertà; 9. impedito controllo sui dati personali all'interessato; 10. danni fisici, materiali o immateriali alle persone fisiche.
		Il Gruppo deve: ▪ provvedere affinché vengano tempestivamente adottate misure che consentano di minimizzare le conseguenze negative della violazione; ▪ verificare se si può identificare come incidente informatico; ▪ identificare le categorie di persone colpite o potenzialmente a rischio e determinare se rientrano in soggetti sottoposti a particolari tutele (minori, anziani disabili); ▪ Identificare il numero di persone interessate dalla violazione e se numero ridotto, produrre elenco; ▪ individuare eventuali falle nei sistemi di sicurezza.
Incaricato alla Gestione delle Violazioni 	Analisi supplementare	Identificazione di eventuali informazioni aggiuntive rese necessarie a seguito di comunicazione al Garante, o derivanti da precedenti approfondimenti.

FASE 3 – VALUTAZIONE		
Chi?	**Che cosa?**	**Come?**
Incaricato alla gestione delle Violazioni  + Referente interno della Privacy 	Valutazione sull' Impatto agli interessati	Valutare la violazione e identificare l'impatto sulle persone considerando le categorie di dati dei soggetti coinvolti e la quantità di soggetti coinvolti. Valutare le seguenti eventuali condizioni: a. che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;

+ Amministratore Delegato (E) 		b. che si tratti di dati relativi a valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; c. che si tratti di dati di persone fisiche vulnerabili, in particolare minori; d. che il trattamento riguardi una notevole quantità di Dati Personali; e. che il trattamento riguardi un vasto numero di Interessati.
Incaricato alla gestione delle Violazioni  + Referente interno della Privacy  + Amministratore Delegato 	Valutazione necessità di notifica all'Autorità di Controllo e notifica	Valutare la necessità di notifica al Garante e in quante fasi. Redatta la Scheda Violazione Dati, il Gruppo deve valutare le azioni da intraprendere ed avviare la notificazione verso l'Autorità di controllo verificando e validando la documentazione pervenuta dalle precedenti fasi di lavoro. L' Amministratore Delegato notifica la violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la Violazione dei Dati Personali presenti un rischio per i diritti e le libertà delle persone fisiche e dunque sia stato dallo stesso classificato "**NULLO**".
Incaricato alla Gestione delle Violazioni  + Referente interno della Privacy  + Amministratore Delegato	Valutazione necessità di comunicazione a: - interessati - organi di polizia	Valutare le azioni da intraprendere ed avviare la comunicazione verso gli interessati verificando e validando la documentazione pervenuta dalle precedenti fasi di lavoro. Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni: a. sono state messe in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi (sono fatti salvi i casi in cui la violazione della

		sicurezza ha comportato la distruzione o la perdita dei dati personali degli interessati); b. sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche (in tal caso è necessario documentare le misure nella scheda di violazione); c. detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. Il Titolare deve informare gli interessati dell'evento anomalo, in tutti i casi in cui, a norma degli articoli 33 e 34 del Regolamento, il Gruppo valuti che la violazione risulta presentare rischi classificati come "***ALTI***" nell'ultima parte **del Modulo gestione segnalazione (Allegato 1)** per i diritti e le libertà delle persone fisiche.
Incaricato alla gestione delle Violazioni 	Ulteriori verifiche	Valutare se richiedere ulteriori verifiche tecniche.
Incaricato alla gestione delle Violazioni 	Attivazione di eventuali Limitazione del rischio	Attivazione di eventuali contromisure per limitare il rischio di violazione.

FASE 4 – NOTIFICA AL GARANTE		
Chi?	**Che cosa?**	**Come?**
Incaricato alla Gestione delle Violazioni  + Amministratore Delegato 	Notifica	Notifica **entro 72 ore** dalla conoscenza della violazione in capo al Titolare. La notifica deve contenere le seguenti informazioni: ▪ natura della violazione; ▪ categorie e numero indicativo di interessati; ▪ categorie e numero approssimativo di registrazioni dei dati personali in questione; ▪ dati identificativi del contatto del DPO se designato; ▪ altri riferimenti che possono fornire informazioni; ▪ probabili conseguenze della violazione;

		▪ misure adottate per porre rimedio alla violazione. Qualora la notifica all'Autorità di controllo non sia effettuata **entro 72 ore**, va corredata dei motivi del ritardo.

FASE 5 – SEGNALAZIONE ORGANI POLIZIA		
Chi?	**Che cosa?**	**Come?**
Incaricato alla Gestione delle Violazioni  + Amministratore Delegato 	Comunicazione a Organi di Polizia.	In caso di violazione di dati come conseguenza di comportamenti illeciti o fraudolenti, è necessaria la comunicazione agli Organi di Polizia.

FASE 6 – COMUNICAZIONE AGLI INTERESSATI		
Chi?	**Che cosa?**	**Come?**
Incaricato alla Gestione delle Violazioni  + Amministratore Delegato 	Comunicazione della violazione all'interessato	La comunicazione deve essere rivolta all'interessato senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione della violazione, attraverso il canale di comunicazione ritenuto più idoneo. Deve essere effettuata ad opera del Titolare e deve essere intellegibile, concisa, trasparente, e facilmente accessibile; deve essere utilizzato un linguaggio semplice e chiaro adottando, se possibile, la stessa lingua parlata dall'interessato. Rispetto alle modalità della comunicazione si applicano quelle ritenute più idonee dal Gruppo. La comunicazione di Data Breach all'interessato deve contenere le seguenti informazioni: a. data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa; b. natura della violazione dei dati personali; c. nome e i dati di contatto del Responsabile della Protezione dei Dati (se designato) o di altro

		punto di contatto presso cui ottenere più informazioni; d. le probabili conseguenze della violazione dei dati personali; e. una descrizione sintetica delle misure adottate o di cui si propone l'adozione da parte dell'Istituto per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi. Può essere utilizzato il **Modulo – Segnalazione Interessato** (Allegato 2).

FASE 7 – REGISTRAZIONE DELLA VIOLAZIONE		
Chi?	**Che cosa?**	**Come?**
Incaricato alla Gestione delle Violazioni  + Amministratore Delegato 	Registrazione nel Registro delle Violazioni	Nel **Registro delle Violazioni**, l'Incaricato alla Gestione delle Violazioni documenta ogni singolo evento, sia esso, "Falso", "Irrilevante" ovvero "Rilevante"; in quest'ultimi due casi, devono essere indicate nel registro le seguenti informazioni: – Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati; – Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati; – Dove è avvenuta la violazione dei dati; – Modalità di esposizione al rischio; – Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione; – Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati; – Che tipo di dati sono oggetto di violazione; – Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati; – Misure tecniche e organizzative applicate ai dati oggetto di violazione; – La violazione è stata comunicata al Garante; – La violazione è stata comunicata anche agli interessati – Qual è il contenuto della comunicazione resa agli interessati; – Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future.

4. Modulistica

Ad integrazione del presente documento viene fornita la modulistica necessaria per gestire / documentare ogni azione svolta, secondo quanto descritto dalla Procedura operativa.

In particolare, sono parte integrante della procedura i seguenti moduli allegati:

- **Allegato 1**
  Modulo – Gestione segnalazione
  Modello utilizzato dall'Incaricato alla gestione delle Violazioni per la **valutazione di primo livello e integrato con le valutazioni di secondo livello** del Gruppo di Gestione della Violazione**.**

- **Allegato 2**
  Modulo – Segnalazione interessato
  Modello utilizzato dal Gruppo di Gestione della Violazione per la **comunicazione agli interessati**, quando previsto.

- **Allegato 3**
  Guida per la Valutazione delle Violazioni
  Documento che supporta l'Incaricato alla Gestione delle Violazioni nella fase di classificazione degli accadimenti e nella compilazione dell'Allegato 1.

- **Allegato 4**
  Registro delle Violazioni