PROCESSO DI GESTIONE DEL TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento dei dati personali è tenuto a notificare al Garante le violazioni dei dati personali (c.d. Data Breach) che comportano la distruzione, la perdita, la modificazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, in modo accidentale o illecito, conservati o comunque trattati, anche nell'ambito delle comunicazioni elettroniche, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati.

Definizioni

Violazione della Riservatezza: accesso accidentale o abusivo al dato personale.
Violazione dell'Integrità: alterazione accidentale o non autorizzata del dato personale.
Violazione della Disponibilità: perdita o distruzione accidentale o non autorizzata del dato personale.

ACQUISIZIONE DELLA NOTIZIA

OBBLIGO DI REGISTRAZIONE: Il Titolare del Trattamento dovrà documentare nel registro qualsiasi violazione di sicurezza dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma, documentando tutte le informazioni utili ad individuare la violazione e le attività messe in atto per prevenire il verificarsi di eventi analoghi.

La segnalazione di un Data Breach può essere interna o esterna all'azienda.

INTERNAMENTE
- Da personale dipendente;
- Da personale convenzionato/stagisti/tirocinanti, ecc..

ESTERNAMENTE
- Da parte degli Organi Pubblici;
- Da parte dei Responsabili del trattamento;
- Da parte degli interessati;
- Da parte di soggetti terzi.

La segnalazione può essere inoltrata al Titolare per mezzo di
- Posta elettronica;
- Avvertimento verbale o telefonico.

Dal momento in cui il Titolare viene a conoscenza dell'evento, decorre il termine delle 72 ore previsto dalla normativa per l'invio della notifica all'Autorità di controllo.

GESTIONE DELL'EVENTO

In caso di accertamento di una violazione che rientra nella definizione di *Data Breach*, saranno seguite le seguenti procedure per il processo di notificazione:

1. **Analisi dell'evento;**
2. **Valutazione della gravità dell'evento;**
3. **Contenimento del danno;**
4. **Notifica al Garante Privacy;**
5. **Altre segnalazioni dovute;**
6. **Comunicazione agli interessati, dove necessario;**
7. **Azioni correttive specifiche per impedire o comunque limitare il verificarsi di una analoga violazione.**

1. ANALISI DELL'EVENTO

Il Titolare, una volta verificato che l'evento segnalato si configura effettivamente come un "Data Breach", dopo un'analisi preliminare, in base alla tipologia della violazione, dell'analisi tecnica dell'evento, mette in atto tempestivamente misure per il contenimento del danno.
Anche nel caso in cui dall'analisi preliminare emerga che la segnalazione non ha i caratteri del Data Breach, sarà cura del Titolare registrarla nel Registro delle Violazioni.

Durante l'analisi approfondita, verrà effettuato:
- Il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità);
- L'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
- L'identificazione degli interessati;
- Il contenimento del danno.

2. VALUTAZIONE DELLA GRAVITÀ DELL'EVENTO

Il Titolare, appurata la violazione e dopo aver informato il Responsabile per la protezione dei dati, dovrà accertare la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà delle persone.
Nella fase di Valutazione, occorre innanzitutto stabilire se nell'incidente sono coinvolti i dati personali. In caso di risposta positiva occorre valutare l'impatto sugli interessati.
- In caso di una violazione di riservatezza occorre verificare che le misure di sicurezza (es.: pseudonimizzazione o cifratura dei dati) in vigore rendano improbabile l'identificazione degli interessati.
- In caso di perdita di integrità o disponibilità di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati.

Se i rischi per gli interessati sono trascurabili, la procedura può terminare, dopo aver documentato il processo e le scelte operate.
Non si procederà alla notifica della violazione al Garante quando è "improbabile" che la violazione comporti un rischio per i diritti e le libertà delle persone fisiche.
Il giudizio che determina l'improbabilità del rischio deve essere riportato nel Registro delle Violazioni.

3. CONTENIMENTO DEL DANNO

A seguito dell'analisi, e appurata la violazione, si provvederà, secondo la gravità dell'evento, al contenimento del danno seguendo le procedure di:
- Limitazione degli effetti dell'incidente;
- Raccolta delle prove forensi nel caso sia ipotizzato un reato;
- Determinazione delle azioni possibili di ripristino;
- Valutazione delle eventuali vulnerabilità collegate con l'incidente;
- Individuazione delle azioni di mitigazione delle vulnerabilità individuate;
- Valutazione dei tempi di ripristino;
- Gestione della comunicazione con gli interessati;
- Ripristino dei dati, dei sistemi, dell'infrastruttura e delle configurazioni;
- Verifica dei sistemi recuperati.

4. NOTIFICA AL GARANTE

Nel caso in cui i rischi per l'interessato non siano trascurabili, il Titolare procederà ad inviare, senza ingiustificato ritardo, al Garante per la protezione dei dati una notifica dell'avvenuta violazione.

Qualora gli aspetti della violazione non siano stati chiariti si può attendere fino ad un massimo di 72 ore prima di effettuare una notifica, motivando il ritardo. Alla scadenza delle 72 ore è opportuno fare una comunicazione specificando che sarà oggetto di ulteriori integrazioni.

La comunicazione dovrà riportare i seguenti elementi:

- l'indicazione del nome ed i relativi dati di contatto del DPO;
- tipologia dei dati oggetto di data breach e breve descrizione della violazione;
- data o periodo in cui la violazione dei dati personali trattati si è verificata;
- causa della violazione dei dati;
- modalità di esposizione al rischio - tipo di violazione;
- dispositivo oggetto della violazione;
- sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione;
- persone colpite dalla violazione dei dati personali trattati;
- livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare);
- misure tecniche e organizzative applicate ai dati oggetto di violazione;
- motivazione nel caso in cui gli interessati non vengano informati;
- misure tecnologiche e organizzative assunte per contenere e prevenire violazioni future.

La notifica al Garante sarà effettuata dal Titolare tramite apposita procedura telematica.

5. ALTRE SEGNALAZIONI DOVUTE

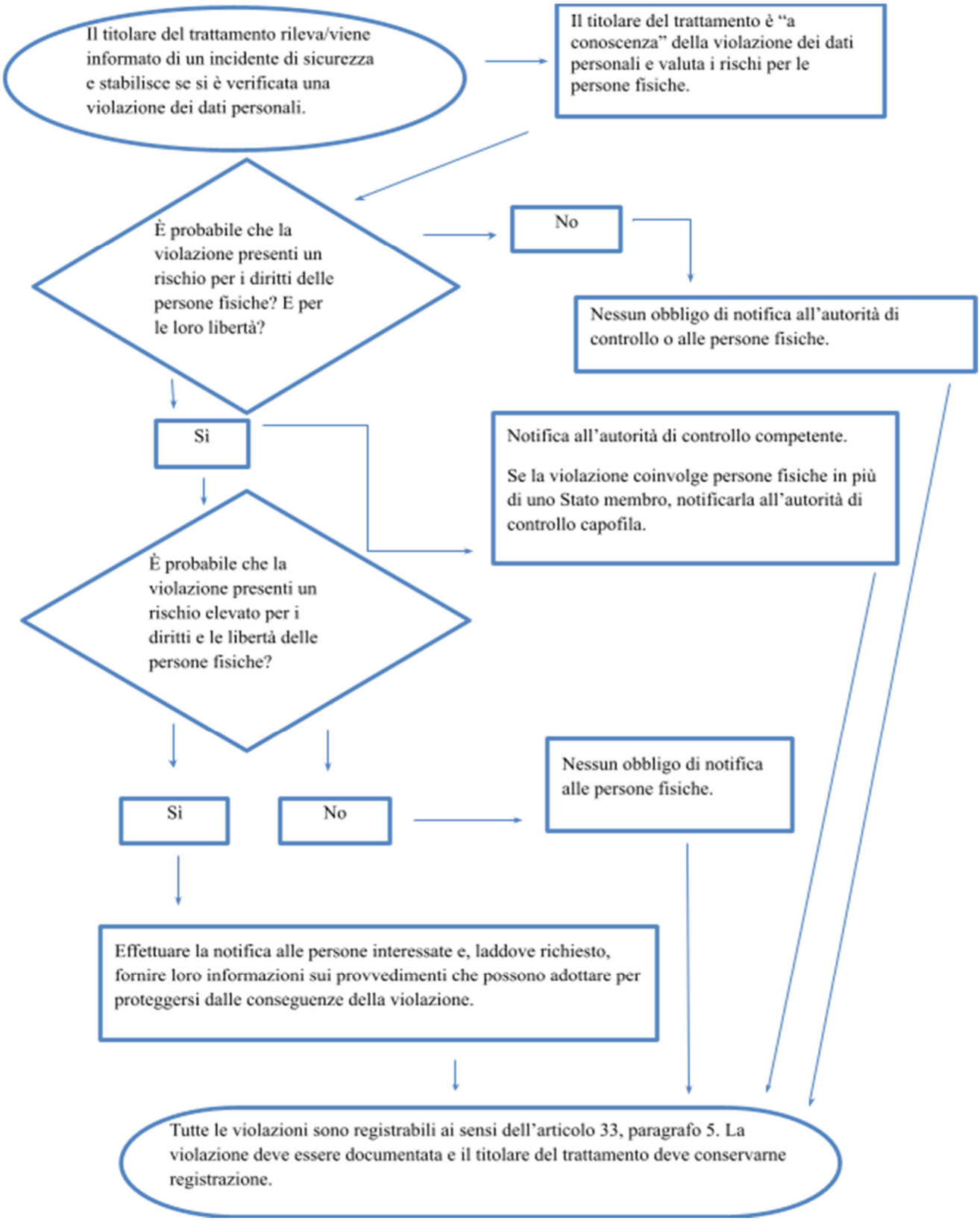
Il Titolare dovrà verificare la necessità di informare altri organi quali Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti) e altri Titolari nel caso in cui agisca come Responsabile o Subresponsabile.

6. COMUNICAZIONE AGLI INTERESSATI

In caso di elevato rischio per la libertà e i diritti degli individui, si provvederà ad informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio.
La comunicazione agli interessati non sarà inoltrata quando le misure di sicurezza messe in atto dal Titolare a tutela dei dati sono idonee a garantire i diritti e le libertà degli interessati.

7. AZIONI CORRETTIVE PER IMPEDIRE O COMUNQUE LIMITARE IL VERIFICARSI DI UNA ANALOGA VIOLAZIONE

Le azioni correttive specifiche per impedire o comunque limitare il verificarsi di una analoga violazione previste in questa fase sono:
- Analisi della relazione dettagliata sull'incidente;
- Eventuale revisione di questo documento (se necessaria) e di eventuali altri documenti collegati (es. Analisi del rischio, Misure di sicurezza);
- Individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi.


Il titolare del trattamento rileva/viene informato di un incidente di sicurezza e stabilisce se si è verificata una violazione dei dati personali.
Il titolare del trattamento è "a conoscenza" della violazione dei dati personali e valuta i rischi per le persone fisiche.
È probabile che la violazione presenti un rischio per i diritti delle persone fisiche? E per le loro libertà?
No
Nessun obbligo di notifica all'autorità di controllo o alle persone fisiche.
Sì
Notifica all'autorità di controllo competente.
Se la violazione coinvolge persone fisiche in più di uno Stato membro, notificarla all'autorità di controllo capofila.
È probabile che la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche?
Sì
No
Nessun obbligo di notifica alle persone fisiche.
Effettuare la notifica alle persone interessate e, laddove richiesto, fornire loro informazioni sui provvedimenti che possono adottare per proteggersi dalle conseguenze della violazione.
Tutte le violazioni sono registrabili ai sensi dell'articolo 33, paragrafo 5. La violazione deve essere documentata e il titolare del trattamento deve conservarne registrazione.