SISTEMA SANITARIO REGIONALE
ASL VITERBO

REGIONE LAZIO

Procedura di attivazione e gestione di eventuali violazioni di dati personali – Data Breach

Premessa
Il Titolare del trattamento, ai sensi dell'art. 33 del Regolamento UE 2016/679, deve notificare al Garante per la protezione dei dati personali le violazioni di dati personali che presentino un rischio per i diritti e le libertà fondamentali delle persone (cd data breach) di cui venga a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo".
La presente procedura descrive quindi le azioni da attivare e individua le responsabilità di ciascuna attività per garantire al Titolare di poter adempiere a quanto disposto dal nuovo Regolamento UE 2016/679.

Il processo di gestione dello stato di crisi, attivato dalla ricezione di una segnalazione di data breach da parte di uno o più stakeholder dell'amministrazione è stato suddiviso nelle seguenti cinque fasi:

1. **Rilevazione della violazione**
2. **Gestione e Valutazione della violazione**
3. **Notifica al Garante (eventuale)**
4. **Comunicazioni agli Interessati (eventuale)**
5. **Registrazione delle violazioni**

Fase 1 Rilevazione della violazione

In questa fase uno o più soggetti autorizzati inviano, come da istruzione ricevuta, la segnalazione di una possibile violazione della sicurezza con divulgazione o perdita di dati personali alla casella e-mail dpo@asl.vt.it e chiedono conferma telefonando al numero 3387606391, numero di contatto del DPO aziendale.
Il DPO valuta la segnalazione ricevuta e se la comunicazione ricevuta viene stimata come una violazione della sicurezza effettiva la comunica al Titolare del trattamento per l'avvio delle indagini ed attiva la funzione aziendale che si occupa della gestione tecnica per la valutazione dei rischi.

Fase 2 Gestione e Valutazione della violazione

La funzione aziendale che si occupa della gestione tecnica mette in campo quelle azioni che consentano di individuare le eventuali falle di sicurezza e attivando accorgimenti tecnici per ripristinare un livello di sicurezza accettabile.
Effettua quindi una valutazione dei rischi relazionando al DPO aziendale i risultati con l'indicazione dei rischi.
In assenza di rischio il DPO aziendale relaziona al Titolare del trattamento e provvede a chiudere

l'incidente (Fase 5) registrando la violazione, le misure messe in atto dall'amministrazione per ripristinare un alto livello di sicurezza e le eventuali altre azioni messe a piano per evitare che la violazione si ripresenti. Al registro viene allegata la relazione redatta dal DPO aziendale nella quale viene riportata tutta la documentazione prodotta e le motivazioni della mancata notifica al Garante e agli interessati.
In presenza di rischio, informato il Titolare, il DPO aziendale avvia la Fase 3 e in presenza di rischio elevato anche la Fase 4 per la comunicazione agli interessati.

Fase 3 Notifica al Garante (eventuale)

Se la valutazione dei rischi elaborata nella Fase 2 ha rilevato un rischio il DPO aziendale effettua la raccolta delle informazioni per la notifica al Garante, compila il modulo e lo invia al Titolare del trattamento
Il modulo di notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) 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 anche, se del caso, per attenuarne i possibili effetti negativi.

Il Titolare del trattamento effettua la notifica al Garante.

Fase 4 Comunicazioni agli Interessati (eventuale)

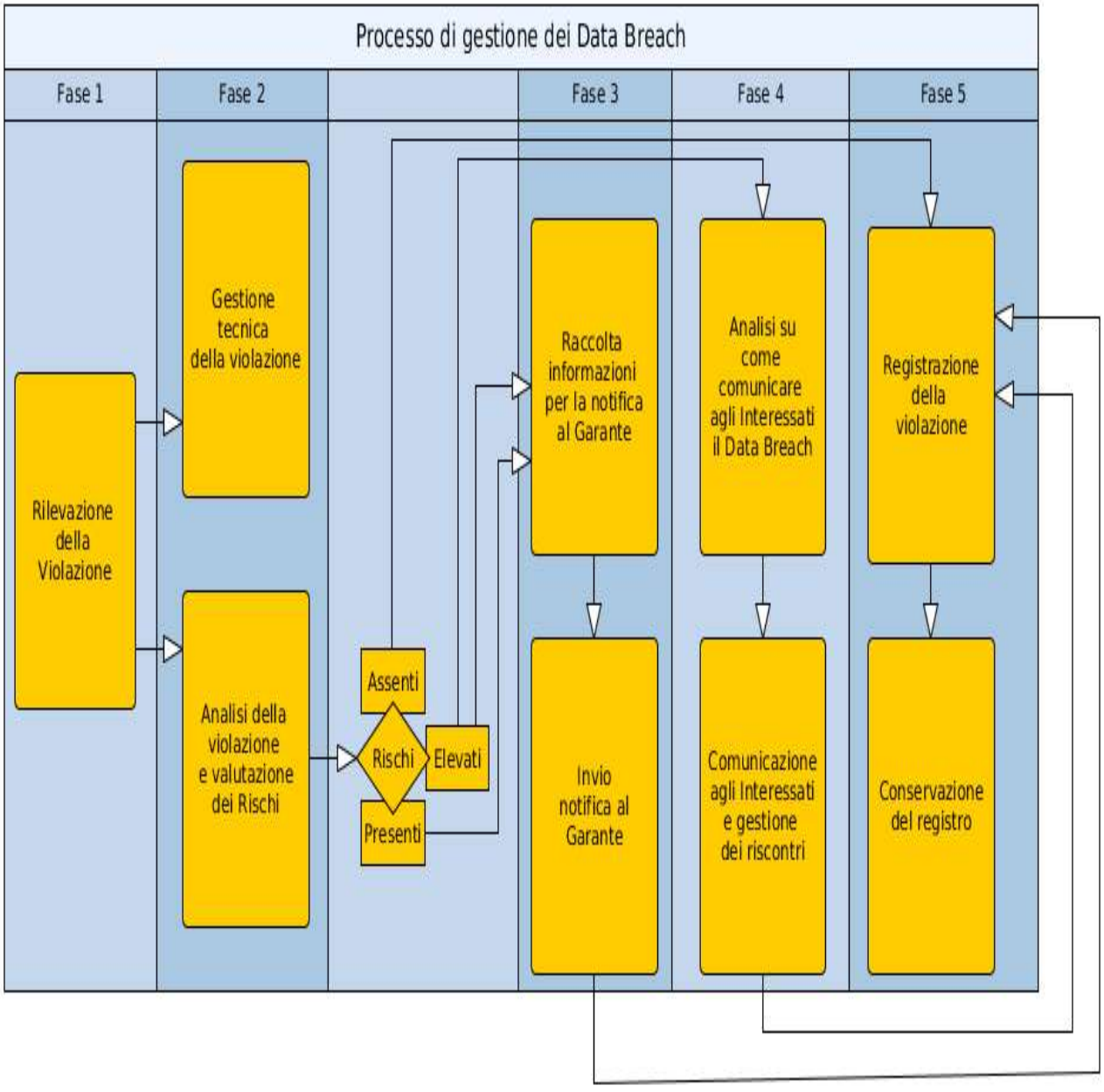
Se la valutazione dei rischi elaborata nella Fase 2 ha rilevato un rischio elevato per i diritti e le libertà delle persone fisiche, dopo alla notifica al Garante, il DPO aziendale elabora un piano di azione che consenta all'amministrazione di comunicare a tutti gli interessati la violazione dei dati. Il piano deve essere autorizzato dal Titolare quindi attivato nel più breve tempo possibile.
La comunicazione deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le seguenti informazioni:

a) il nome e i dati di contatto del responsabile della protezione dei dati (DPO) o di altro punto di contatto presso cui ottenere più informazioni;
b) la descrizione delle probabili conseguenze della violazione dei dati personali;
c) la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora la comunicazione a tutti gli interessati richiedesse sforzi sproporzionati, il DPO aziendale elaborerà il piano di comunicazione prevedendo una comunicazione pubblica o a una misura simile, tramite la quale gli interessati potranno essere informati con analoga efficacia.
Il piano elaborato dal DPO aziendale deve prevedere la ricezione di riscontri dagli interessati per

consentire di verificare che la comunicazione sia stata recepita.
Tutti i riscontri verranno registrati su un apposito registro e conservato per le eventuali verifiche da parte del Titolare o all'autorità di controllo.

Fase 5
Al termine della crisi il DPO aziendale elabora una relazione del data breach riportando tutta la documentazione prodotta nelle diverse fasi, le conseguenze e i provvedimenti adottati per porvi rimedio. Riporta nella relazione l'avvenuta notifica al Garante e agli interessati o le motivazioni della mancata notifica.
Tale documentazione consente all'autorità di controllo di verificare il rispetto delle disposizioni in materia di privacy.
Tutta la documentazione viene quindi indicizzata attraverso il registro delle violazioni che una volta opportunamente firmato dal DPO aziendale e dal Titolare del trattamento viene inviato a conservazione.


Processo di gestione dei Data Breach
Fase 1
Fase 2
Fase 3
Fase 4
Fase 5
Rilevazione della Violazione
Gestione tecnica della violazione
Analisi della violazione e valutazione dei Rischi
Assenti
Rischi
Elevati
Presenti
Raccolta informazioni per la notifica al Garante
Invio notifica al Garante
Analisi su come comunicare agli Interessati il Data Breach
Comunicazione agli Interessati e gestione dei riscontri
Registrazione della violazione
Conservazione del registro