ALLEGATO B
DATA BREACH POLICY

1. INTRODUZIONE

Il nuovo Regolamento Europeo impone agli enti che trattano dati personali l'obbligo di notificare all'Autorità Garante eventuali violazioni delle procedure e dei sistemi di sicurezza dagli stessi all'uopo approntati.
L'unica deroga a tale prescrizione si configura qualora l'ente sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, la predetta violazione non presenti un rischio per i diritti e le libertà delle persone fisiche.
Al contrario, nel caso in cui da tale violazione derivino rischi elevati per i diritti e le libertà delle persone fisiche, l'obbligo di comunicazione si estende anche ai singoli interessati coinvolti.
Timeware S.r.l., per quanto sopra esposto, ha adottato la presente Data Breach Policy per disciplinare le modalità di gestione di eventuali violazioni del proprio sistema di trattamento dei dati.

2. OBBLIGAZIONI GENERALI

In ragione degli obblighi gravanti sul Titolare, i Destinatari sono tenuti a rispettare la presente procedura (i.e. Data Breach Policy).
In particolare:

- ✓ i dipendenti e collaboratori della Società, nello svolgimento delle proprie attività, sono responsabili della comunicazione tempestiva al Data Manager di riferimento di potenziali o attuali violazioni dei Dati personali, nonché di prestare la massima collaborazione nello svolgimento delle attività di verifica e di contenimento delle violazioni in essere;
- ✓ i Responsabili del trattamento dei dati ed ogni altro soggetto terzo che effettua operazioni di trattamento dei dati di cui la Società è Titolare sono tenuti a comunicare tempestivamente al Titolare stesso potenziali violazioni dei Dati personali e fornire tutta l'assistenza necessaria affinché possa adempiere alle obbligazioni previste dalle Leggi sulla protezione dei dati;

3. NORME DI COMPORTAMENTO IN CASO DI DATA BREACH

3.1 Norme di comportamento per i Destinatari

In caso di una violazione di sicurezza che, anche solo potenzialmente, possa apparire idonea a generare un Data Breach, quanto accaduto dovrà essere immediatamente segnalato, non oltre 12 ore dalla conoscenza della violazione da parte del Destinatario ai punti di contatto indicati al paragrafo 5 che segue.
Al fine di coadiuvare il Privacy Officier, nella gestione tempestiva delle attività di notifica della violazione dei Dati personali all'Autorità, il Data Manager di riferimento dovrà prima di tutto

effettuare la segnalazione tramite e-mail contenente l'indicazione degli elementi fondamentali della possibile violazione, con ciò intendendosi:

- una breve descrizione della natura della violazione;
- l'indicazione di categorie e numero approssimativo di dati coinvolti;
- l'indicazione di categorie e numero approssimativo di Interessati coinvolti;
- l'indicazione delle misure adottate per la limitazione delle conseguenze derivanti dalla violazione in essere.

Tale attività potrà essere svolta compilando l'apposito form reperibile sul sito www.timeware.it. Nell'immediatezza dell'evento, il Data Manager di riferimento, coadiuvato dagli autorizzati, dovrà adottare ogni misura idonea a bloccare o, in ogni caso, a limitare le conseguenze derivanti dalla violazione dei Dati personali in essere.

In caso di Data Breach, il Titolare ha l'obbligo, entro 72 ore dal momento in cui ne è venuta a conoscenza, di notificare all'Autorità la violazione. Pertanto, in caso di violazioni di sicurezza anche solo potenziali, i Destinatari sono tenuti a segnalare l'accaduto ai punti di contatto di cui al Paragrafo 5.

3.2 Analisi preliminare ed elaborazione della Scheda evento

Qualora venga segnalata una possibile violazione dei Dati personali, il Privacy Officer, il Data Manager di riferimento, in collaborazione con il Responsabile IT, deve svolgere le necessarie indagini ed avviare un'analisi preliminare provvedendo a compilare la Scheda Evento reperibile sul sito www.timeware.it.
Il Privacy Officer, in collaborazione con il Responsabile IT, è tenuto a comunicare immediatamente al Titolare le risultanze delle anzidette indagini al fine di consentire allo stesso di qualificare correttamente la violazione di sicurezza e valutare la necessità o meno di effettuare la notificazione all'Autorità.
Nel caso in cui la segnalazione effettuata dal Destinatario risulti infondata, il Privacy Officer provvede ad archiviare l'incidente.
In ogni caso, il Privacy Officer è tenuto a dare evidenza del c.d. falso positivo all'interno del Registro dei Data Breach, allegato al presente documento, nella apposita sezione dedicata agli "incidenti infondati".
Nel caso in cui la segnalazione non risulti infondata, il Privacy Officer verifica se la violazione possa comportare un rischio per i diritti e le libertà delle persone fisiche.

3.3 Norme di condotta per il Privacy Officer
3.3.1 Notifica all'Autorità

Caso 1: Nel caso in cui il Privacy Officer valuti che la violazione di sicurezza non sia idonea a rappresentare un rischio elevato per i diritti e le libertà del degli Interessati coinvolti, lo stesso procede, per conto del Titolare, alla registrazione della violazione e all'archiviazione di quanto segnalato avvalendosi del registro allegato al presente documento.

Caso 2: Qualora la violazione possa comportare un rischio per i diritti e le libertà delle persone fisiche, il Titolare, assistito dal Privacy Officer, provvede ad effettuare la notifica all'Autorità nel limite delle 72 ore successive al momento in cui si è avuta consapevolezza dell'avvenuta violazione, nonché alla comunicazione agli Interessati coinvolti secondo le disposizioni di cui al paragrafo 3.3.2 che segue.

La notifica all'Autorità 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 Titolare 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.

Qualora e nella misura in cui non sia possibile fornire le anzidette informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

3.3.2 Comunicazione agli Interessati

Nel caso in cui il Data Breach presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Privacy Officer deve assistere il Titolare del trattamento affinché lo stesso comunichi la violazione agli Interessati senza ingiustificato ritardo.

Le comunicazioni agli Interessati devono avvenire mediante il canale di volta in volta ritenuto più idoneo e devono essere effettuate con un linguaggio semplice e chiaro.

La comunicazione agli Interessati deve contenere almeno le seguenti informazioni:

a) La natura della violazione;
b) Il nome e i dati di contatto del Titolare o di altro punto di contatto presso cui ottenere più informazioni;
c) La descrizione delle probabili conseguenze della violazione dei Dati personali;
d) La descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione e anche, se del caso, per attenuare i possibili effetti negativi.

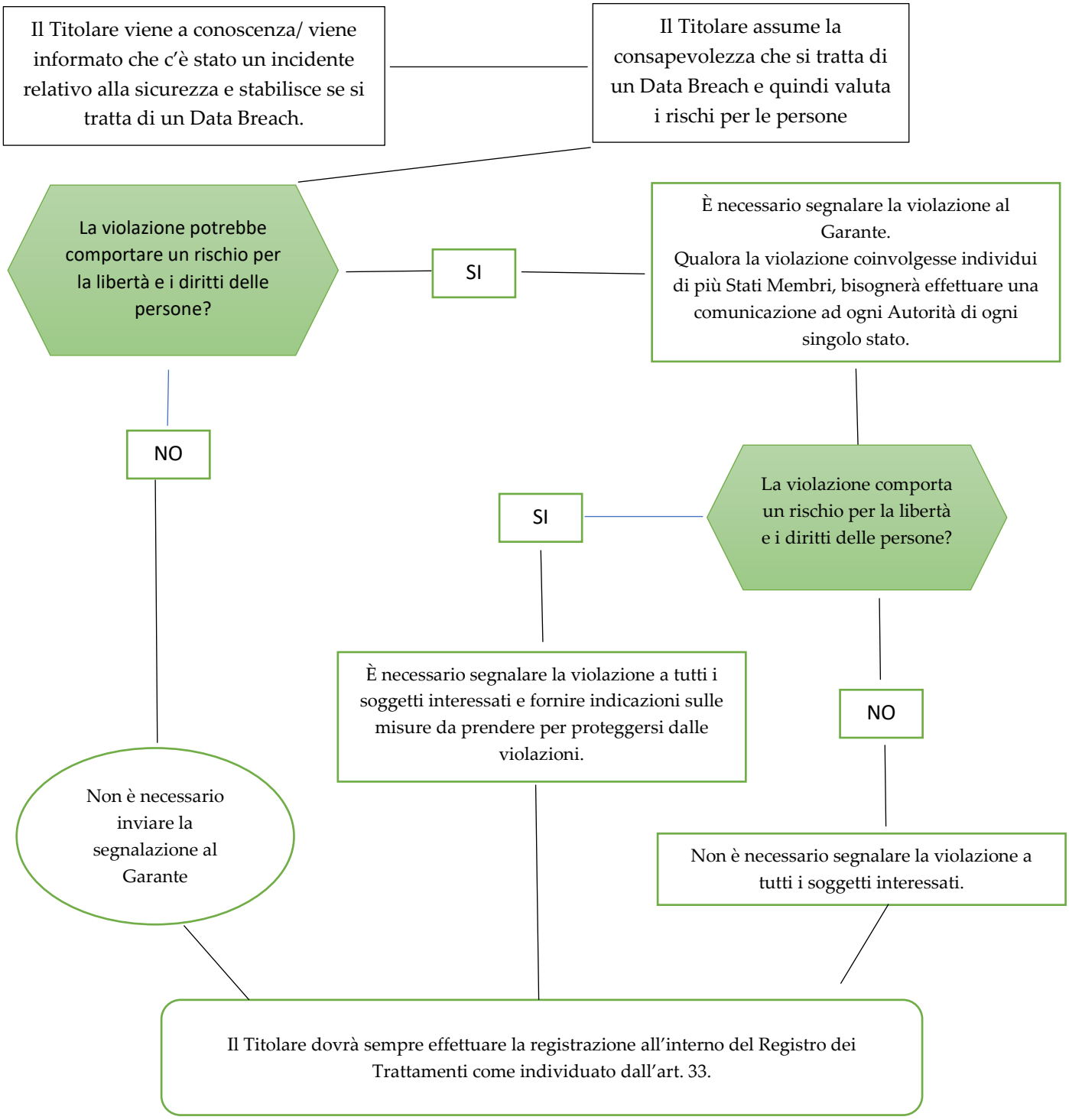
Non è richiesta, al contrario, la comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo 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 personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali, ad esempio, la cifratura;
b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati e 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 Privacy Officer dovrà in ogni caso documentare le violazioni di Dati personali subite, anche se non notificate all'Autorità e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

Anche in caso di notificazione all'Autorità e/o agli interessati il Privacy Officer procede, per conto del Titolare, alla registrazione della violazione avvalendosi del registro di cui al paragrafo 7 che segue.

4. FLOW CHART DATA BREACH POLICY



5. CONTATTI

In caso di presunte violazioni alla sicurezza dei dati personali contattare i seguenti riferimenti:

- Privacy Officer: Massimo Goldaniga
- E-mail: privacy@timeware.it
- Responsabile IT: Angelo Galli
- E-mail: angelo.galli@timeware.it
- Tel.: +39 02 87209260