A.S.L. V.C.O.
Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

ALLEGATO A) ALLA DELIBERAZIONE N. 831 DEL 10 AGOSTO 2018

PROCEDURA PROVVISORIA DA SEGUIRE IN CASO DI DATA BREACH

(ART. 33 REGOLAMENTO UE 2016/679 IN MATERIA DI PRIVACY)

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

Indice

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323 5411 0324 4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

A. DATA BREACH

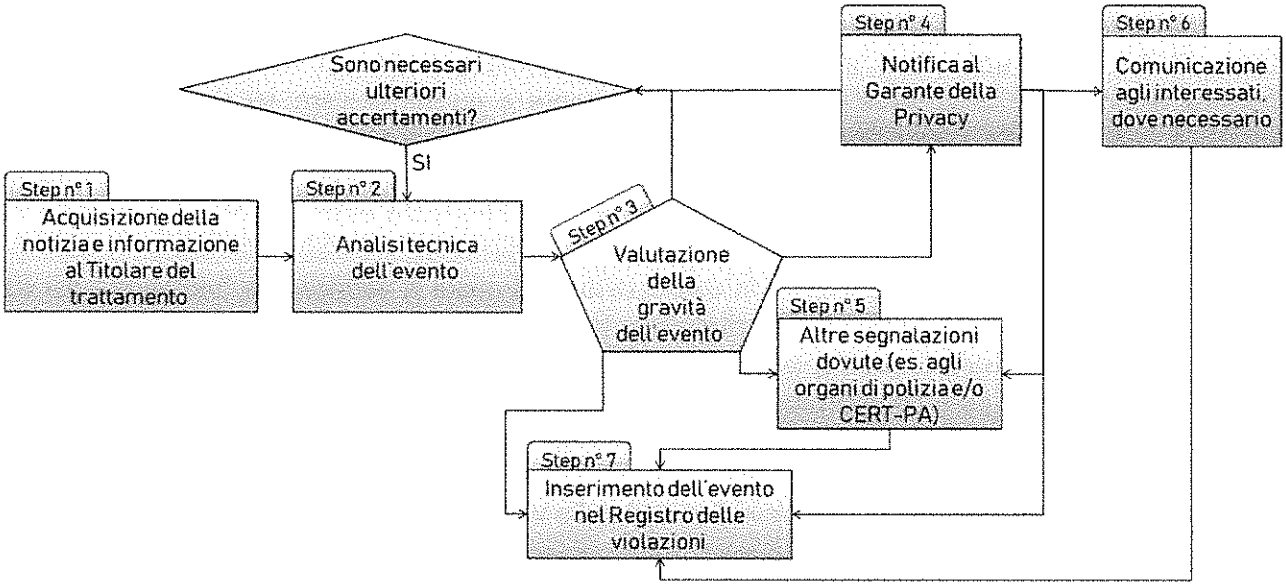
L'art. 33 del GDPR recita che: "In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".
Per "Data Breach" si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali". Nello specifico, si intende una situazione in cui i dati personali, sensibili, protetti o riservati vengono: distrutti, consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato.
La mancata notifica può comportare ulteriori accertamenti da parte del Garante poiché può rappresentare un indizio di carenze che, se accertate, possono dar luogo a sanzioni.
Tutti gli eventi di Data Breach, compresi quelli per cui non sono necessarie le notifiche, devono essere documentati (art. 33 par. 5 del GDPR) su un Registro delle Violazioni.

B. PROCESSO DI DATA BREACH NOTIFICATION

In caso di accertamento di violazione dei sistemi informatici, di involontaria diffusione delle informazioni o di altri eventi che rientrano nella definizione di Data Breach, sarà opportuno seguire i seguenti steps del processo di notificazione (rappresentati nel relativo schema):
1. Acquisizione della notizia e informazione al Titolare del trattamento
2. Analisi tecnica dell'evento
3. Valutazione della gravità dell'evento
4. Notifica al Garante della Privacy
5. Altre segnalazioni dovute
6. Comunicazione agli interessati, dove necessario
7. Inserimento dell'evento nel Registro delle Violazioni

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033



1. Acquisizione della notizia e informazione al Titolare del trattamento

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

• INTERNAMENTE:
o Dal settore dei Sistemi Informativi
o Da altro personale interno

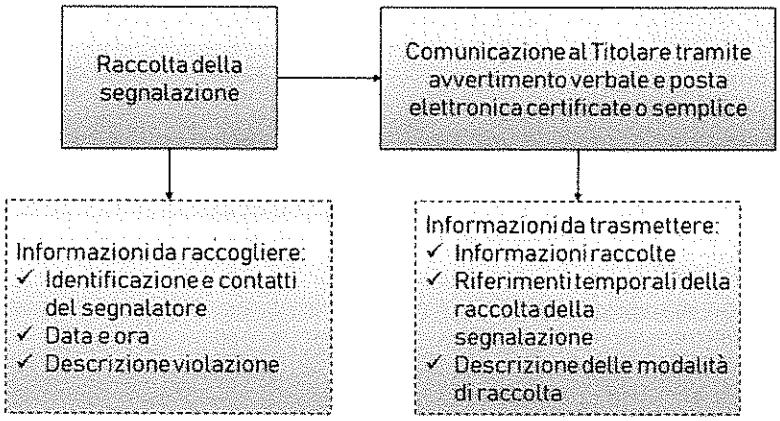
• ESTERNAMENTE:
o Da parte degli organi pubblici (Agid, Polizia, altre forze dell'ordine, giornali, ecc.)
o Da parte di Responsabili esterni al trattamento
o Da parte degli interessati

La segnalazione deve essere inoltrata al Titolare o a chi in quel momento ne fa le veci, mediante:
- Posta elettronica certificata o semplice
- Avvertimento verbale in ogni caso

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

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033



2. Analisi tecnica dell'evento

Il Titolare è responsabile della valutazione e relativa notifica e sarà supportato dai soggetti interni all'Ente preposti all'analisi tecnica, verosimilmente, il settore dei Sistemi Informativi.

Una volta verificato che l'evento segnalato si configuri effettivamente come un "Data Breach" (Analisi Preliminare), verranno svolte tutte le operazioni necessarie a raccogliere gli elementi per una valutazione dell'evento (Analisi Approfondita) ai fini della notifica al Garante della Privacy. È importante sottolineare che, anche nel caso in cui dall'Analisi Preliminare emerga che la segnalazione non ha i caratteri del Data Breach, è necessario registrarla nel Registro delle Violazioni.

Durante l'Analisi Approfondita, dovranno essere accertate le circostanze della violazione, le conseguenze e i relativi rimedi.

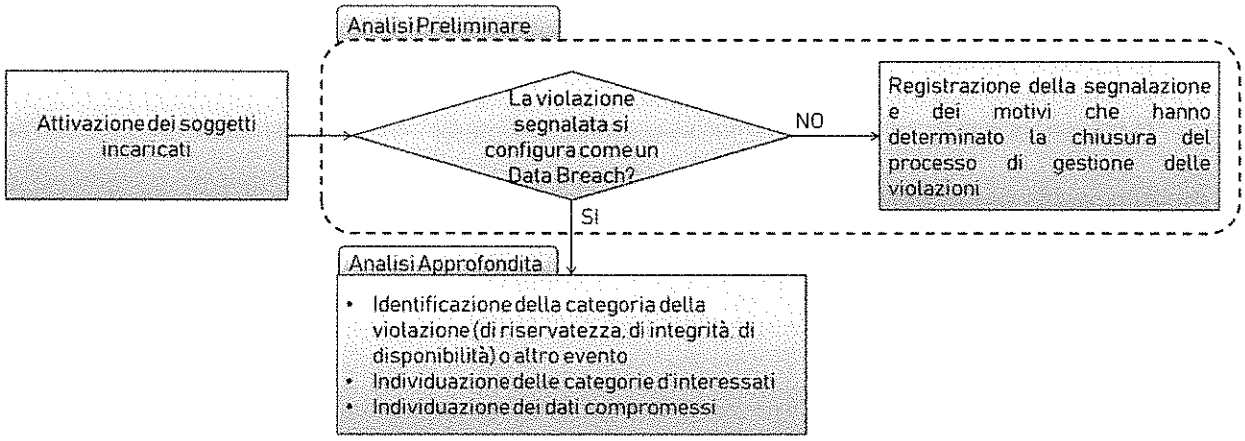
Si precisa che l'art. 33 paragrafo n. 4 del DGPR recita: "Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo". Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni e, anche in caso queste non siano per il momento ritenute esaustive, effettuare la notificazione.

Nello specifico verrà effettuato, in un tempo consigliabile non superiore a 8-10 ore:

- Il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento
- L'identificazione dei dati violati/distrutti/compromessi
- L'identificazione degli interessati

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033



3. Valutazione della gravità dell'evento

Il Titolare è responsabile anche di questa fase, in cui dovrà appurare se l'evento merita di essere notificato al Garante della Privacy.
Insieme ai soggetti interni di ausilio alla fase di analisi tecnica, il Titolare dovrà:
- Informare il DPO
- Accertare la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà delle persone (cioè quando si è verificata una distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati, sia che questi dati siano trattati all'interno che all'esterno dell'ente)
- Effettuare la notifica al Garante, se necessaria
- Verificare, successivamente, se sia necessaria una seconda notifica più approfondita, di conseguenza ad un'analisi tecnica supplementare
- Effettuare una comunicazione agli organi di polizia, se necessaria

L'art. 33 paragrafo n. 1 chiarisce che non vi è obbligo di notifica della violazione quando è "improbabile" che questa comporti un rischio per i diritti e le libertà delle persone fisiche, ovviamente il giudizio che determina l'improbabilità del rischio deve essere riportato nel Registro delle violazioni.
A questo proposito, il WP29 nelle sue linee guida, precisa che la mancata comunicazione può essere sanzionata ma che nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria.

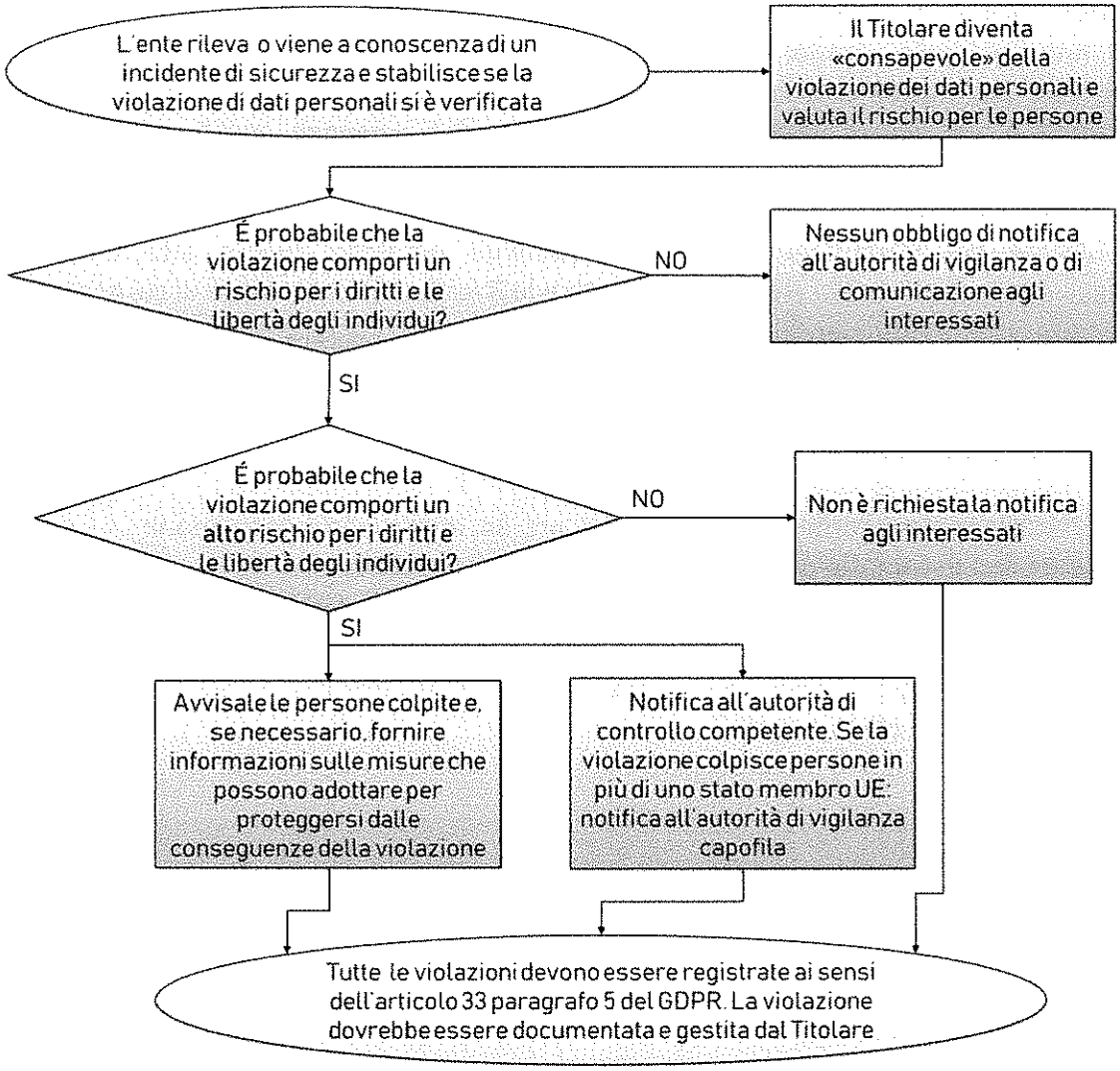
4. Notifica al Garante della Privacy

Come accennato, la notifica di una violazione al Garante è resa obbligatoria dall'art. 33 del GDPR nei casi in cui si verifichi una violazione dei dati personali, a meno che sia improbabile che tale violazione presenti un rischio per i diritti e le libertà delle persone fisiche. La notifica, sulla base del Modello reso disponibile dal Garante Privacy (in allegato) dovrà contenere i seguenti elementi:

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

- La descrizione 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
- L'indicazione del nome e i relativi dati di contatto del DPO
- La descrizione delle probabili conseguenze della violazione
- L'indicazione 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.



Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

5. Altre segnalazioni dovute

Il Titolare dovrà verificare la necessità di informare altri organi quali:
- CERT-PA (in caso di incidenti informatici ai sensi della Circolare Agid n. 2/2017 del 18-04-2017)
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti)

6. Comunicazione agli interessati

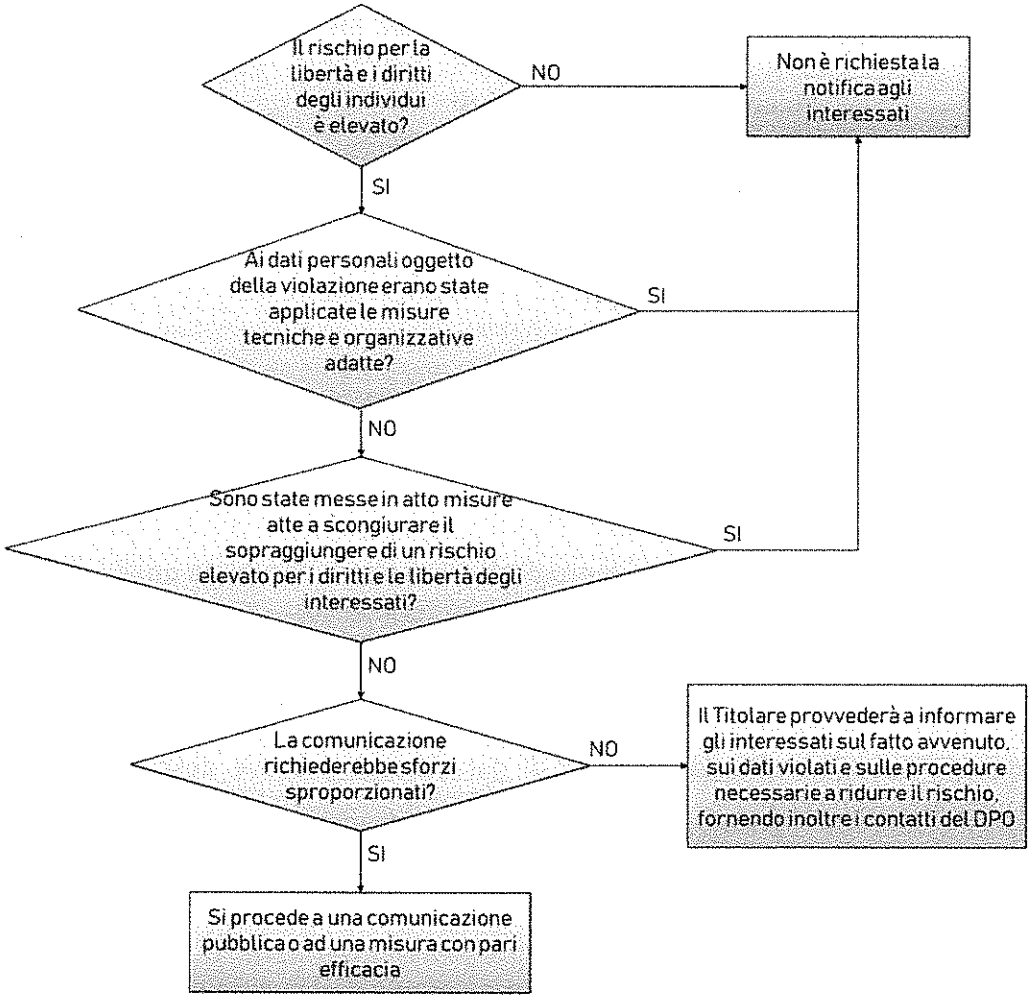
In caso di elevato rischio per la libertà e i diritti degli individui, il Titolare provvederà a informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio.
La comunicazione agli interessati, secondo quanto previsto dal paragrafo n. 3 dell'art. 34 del GDPR, non è richiesta quando:
- 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 la cifratura;
- 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 di cui al paragrafo 1;
- la 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.

La comunicazione deve contenere, ai sensi dell'art. 34, le seguenti informazioni:
- il nome e i dati di contatto del DPO o di altro punto di contatto;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- 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.

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033



7. Inserimento dell'evento nel Registro delle violazioni

L'art. 33 Paragrafo n.5 del GDPR, prescrive al Titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.
Pertanto, tutte le attività indicate sopra, devono essere documentate, tracciabili, ed essere in grado di fornire evidenza nelle sedi competenti.
Tale procedura deve essere diffusa a tutti i soggetti deputati al trattamento dei dati personali che, a diverso titolo, potranno e dovranno essere di ausilio al Titolare del trattamento.
Il DPO dovrà essere informato dal Titolare del trattamento, come indicato sopra, dovrà inoltre configurarsi come punto di contatto delle comunicazioni tra Garante e Titolare.
Nello specifico, la notifica al Garante sarà effettuata dal Titolare tramite PEC e per conoscenza al DPO, con indicazione del DPO come punto di contatto per il Garante.

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

C. ALLEGATO 1 – MODELLO DI NOTIFICA DATA BREACH AL GARANTE PRIVACY

Violazione dei dati personali
Modello di comunicazione al Garante

1. Titolare che effettua la comunicazione:
   a. Denominazione o ragione sociale:
   b. Sede del titolare:
   c. Persona fisica addetta alla comunicazione:
   d. Funzione rivestita:
   e. Indirizzo email per eventuali comunicazioni:
   f. Recapito telefonico per eventuali comunicazioni:

2. Natura della comunicazione:
   a. Nuova comunicazione (inserire contatti per eventuali chiarimenti, se diversi da quelli sub 1.):
   b. Seguito di precedente comunicazione (inserire numero di riferimento):
   b.1. Inserimento ulteriori informazioni sulla precedente comunicazione:
   b.2. Ritiro precedente comunicazione (inserire le ragioni del ritiro):

3. Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione di dati personali ivi trattati:

4. Quando si è verificata la violazione di dati personali?
   a. Il ...
   b. Tra il ..... e il .....
   c. In un tempo non ancora determinato
   d. È possibile che sia ancora in corso

5. Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

6. Modalità di esposizione al rischio:
   a. tipo di violazione:
      a.1. lettura (presumibilmente i dati non sono stati copiati)
      a.2. copia (i dati sono ancora presenti sui sistemi del titolare)
      a.3. alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
      a.4. cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
      a.5. furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
      a.6. altro [specificare]

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

b. dispositivo oggetto della violazione:
   b.1. computer
   b.2. dispositivo mobile
   b.3. documento cartaceo
   b.4. file o parte di un file
   b.5. strumento di backup
   b.6. rete
   b.7. altro (specificare)

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

8. Quante persone sono state colpite dalla violazione di dati personali?
   a. [numero esatto] persone
   b. Circa [numero] persone
   c. Un numero (ancora) sconosciuto di persone

9. Che tipo di dati sono coinvolti nella violazione?
   a. Dati anagrafici
   b. Numeri di telefono (fisso o mobile)
   c. Indirizzi di posta elettronica
   d. Dati di accesso e di identificazione (user name, password, customer ID, altro)
   e. Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
   f. Altri dati personali (sesso, data di nascita/età, ...), dati sensibili e giudiziari
   g. Ancora sconosciuto
   h. Altro [specificare]

10. Livello di gravità della violazione di dati personali (secondo le valutazioni del titolare):
   a. Basso/trascurabile
   b. Medio
   c. Alto
   d. Molto alto

11. Misure tecniche e organizzative applicate ai dati colpiti dalla violazione:

12. La violazione è stata comunicata anche a contraenti (o ad altre persone interessate)?
   a. Sì, è stata comunicata il ....
   b. No, perché [specificare]

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

13.Qual è il contenuto della comunicazione ai contraenti (o alle altre persone interessate)? [riportare il testo della notificazione]

14. Quale canale è utilizzato per la comunicazione ai contraenti (o alle altre persone interessate)?

15. Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

16. La violazione coinvolge contraenti (o altre persone interessate) che si trovano in altri Paesi EU?
    a. No
    b. Si

17. La comunicazione è stata effettuata alle competenti autorità di altri Paesi EU?
    a. No
    b. Si [specificare]