Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

APPROVATO CON
DELIBERAZIONE N. 759 DEL 20/07/2021

GESTIONE DEL DATA BREACH
Procedura da applicare in caso di violazione di dati personali (artt. 33 e 34 GDPR)

Versione	V. 2.0
Data	20/07/2021
Approvazione (data/firma)	20/07/2021
Scadenza	---

ABBREVIAZIONI 2
DEFINIZIONI 2
RIFERIMENTI NORMATIVI 3
A. DATA BREACH 4
B. PROCESSO DI DATA BREACH NOTIFICATION 5
1. ACQUISIZIONE DELLA NOTIZIA E INFORMAZIONE AL TITOLARE DEL TRATTAMENTO 5
2. ANALISI TECNICA DELL'EVENTO 6
3. VALUTAZIONE DELLA GRAVITÀ DELL'EVENTO 7
4. NOTIFICA AL GARANTE DELLA PRIVACY 7
5. ALTRE SEGNALAZIONI DOVUTE 10
6. COMUNICAZIONE AGLI INTERESSATI 10
7. INSERIMENTO DELL'EVENTO NEL REGISTRO DELLE VIOLAZIONI 12
8. MIGLIORAMENTO 12
ALLEGATO 1 – SOGGETTI PREPOSTI A GESTIRE LE VIOLAZIONI 13
ALLEGATO 2 - MATRICE ASSEGNAZIONE RESPONSABILITÀ 14
ALLEGATO 3 – IMPIEGO DEL REGISTRO DELLE VIOLAZIONI 15
ALLEGATO 4 - TABELLA DELLA VALUTAZIONE DEL RISCHIO PER LE LIBERTÀ DEGLI INDIVIDUI 16
ALLEGATO 5 – MODELLO DI SEGNALAZIONE VIOLAZIONE AL GARANTE PRIVACY 17

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

ABBREVIAZIONI

AgID	Agenzia per l'Italia Digitale
GDPR	General Data Protection Regulation (Reg.(UE) 2016/679)
PA	Pubblica Amministrazione
RPD	Responsabile della Protezione dei Dati
SPID	Sistema Pubblico di IDentità
UE	Unione Europea
WP	Working Party

DEFINIZIONI

Ai fini del presente documento si intende per:

1) «Dati Personali»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «Trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «Titolare»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di Dati Personali;

4) «Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta i Dati Personali per conto del Titolare del Trattamento;

5) «Violazione dei Dati Personali» o anche solo "Violazione": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati;

6) «Data Breach»: 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.

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

RIFERIMENTI NORMATIVI

- Decreto Legislativo 10 agosto 2018 n, 101 "Disposizioni per l'adeguamento della Normativa Nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)"
- Regolamento (UE) 2016/679 del Parlamento Europeo del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in particolare gli articoli 33 (Notifica all'Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento).
- D.Lgs. 196/2003 Codice per la protezione dei dati personali
- Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679.
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015.
- Provvedimento n. 209 del 27 maggio 2021 - Procedura telematica per la notifica di violazioni di dati personali (data breach).
- D.Lgs. 82/2005 Codice dell'Amministrazione Digitale (CAD).
- artt. 331 e 361 del Codice di Procedura Penale (obbligo di denuncia da parte del pubblico ufficiale)
- Decreto 9 gennaio 2008 del ministero degli interni in attuazione della Legge 155/2005 sulle infrastrutture critiche.
- Decreto del Presidente del Consiglio dei Ministri 1 aprile 2008 "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività" previste dall'articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale». G.U. 21 giugno 2008, n. 144.
- Art. 13 del DPCM DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 ottobre 2014 Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese. (14A09376) (GU Serie Generale n.285 del 09-12-2014).
- Decreto Legislativo 18 maggio 2018, n. 65 Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. (18G00092) (GU Serie Generale n.132 del 09-06-2018).

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.

Le Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 precisano la nozione di violazione come di seguito riportata:

Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro ha spiegato che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:

- *"violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzato o accidentale;*
- *"violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;*
- *"violazione della disponibilità", in caso di perdita, accesso o distruzione (accidentali o non autorizzati) di dati personali.*

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Ci si potrebbe chiedere se una perdita temporanea della disponibilità dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. L'articolo 32 del regolamento ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".

Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'articolo 4, punto 12.

Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrebbe essere documentata in conformità all'articolo 33, paragrafo 5. Ciò aiuta il titolare del trattamento a dimostrare l'assunzione di responsabilità all'autorità di controllo, che potrebbe chiedere di consultare tali registrazioni16. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte. Il titolare del trattamento dovrà valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all'articolo 33, il titolare del trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso.

Va notato che, sebbene una perdita di disponibilità dei sistemi del titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il titolare del trattamento consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi.

La mancata notifica può comportare ulteriori accertamenti da parte del Garante poiché può rappresentareun indizio di carenze che, se accertate, possono dar luogo a sanzioni.

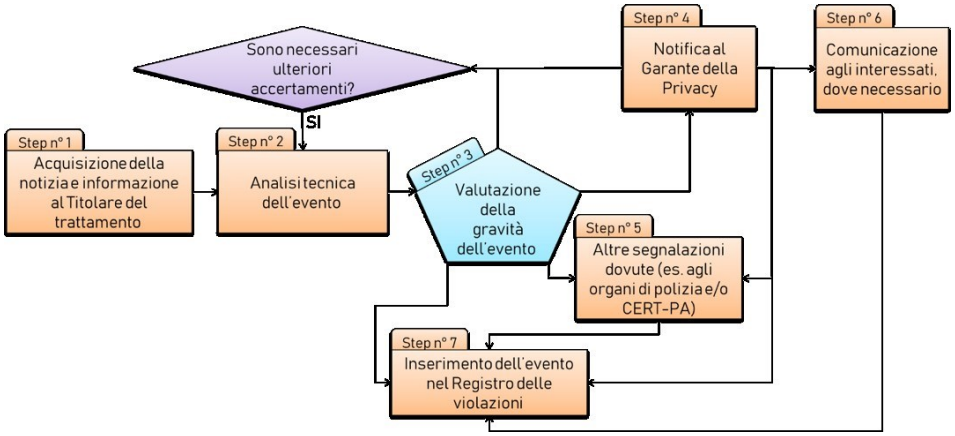
Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

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 (il cui modello è in Allegato 4)

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 passi del processo di notificazione (rappresentati nel relativo schema):

1. Acquisizione della notizia da parte dei soggetti preposti al ricevimento/raccolta della violazione (individuati nell'allegato 1) che provvederanno ad attivare i passi successivi;
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, ove necessario
7. Inserimento dell'evento nel Registro delle Violazioni



1. Acquisizione della notizia e informazione al Titolare del Trattamento

La segnalazione di un Data Breach può essere interna o esterna alla Azienda.

- INTERNAMENTE:
  - Da personale dipendente
  - Da personale convenzionato/stagisti/tirocinanti, ecc.
- ESTERNAMENTE:
  - Da parte degli organi Pubblici (Agid, Polizia, altre Forze dell'Ordine, giornali, ecc.)
  - Da parte del DPO
  - Da parte dei Responsabili (esterni) del trattamento
  - Da parte degli interessati
  - Da parte di ulteriori soggetti.

La segnalazione deve essere inoltrata al Legale rappresentante del Titolare o a chi in quel momento ne fa le veci, mediante:

- Posta elettronica certificata o semplice
- Avvertimento verbale/telefonico 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.

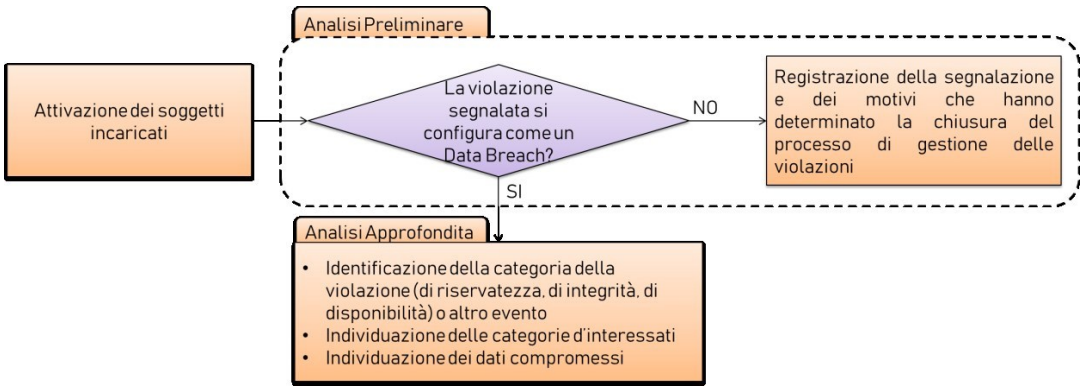
2. Analisi tecnica dell'evento

Il Titolare è responsabile della valutazione e relativa notifica e sarà supportato dai soggetti interni alla Azienda preposti all'analisi tecnica e in particolare il settore dell'Information Technology.
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 Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

Nel corso dell'attività di analisi tecnica è altresì necessario procedere, ove si sia verificato un danno, al contenimento del medesimo

Il contenimento del danno è realizzato operando come di seguito descritto:

- 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 i Clienti, con CERT e con i media,
- Ripristino dei dati, dei sistemi, dell'infrastruttura e delle configurazioni,
- Verifica dei sistemi recuperati.

Tutte le operazioni effettuate devono essere tracciate e riconducibili a specifiche persone, sulla base della matrice allegato 2.

3. Valutazione della gravità dell'evento

Il Titolare è responsabile anche di questa fase, in cui dovrà appurare se l'evento richieda di essere notificato al Garante della Privacy, ovvero se si qualifichi come Data Breach.
Insieme ai soggetti interni di ausilio alla fase di analisi tecnica, il Titolare dovrà:

1. Informare il DPO/RPD
2. 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 della Azienda)
3. Operare una valutazione in ordine alla sussistenza di un rischio per gli interessati e stimare la gravità di questo rischio (vedi tabella in allegato 4);
4. Valutare le azioni rimediali/di mitigazione idonee ad abbattere il rischio entro una soglia di accettabilità;
5. Verificare, successivamente, se sia necessaria una seconda notifica più approfondita, di conseguenza ad un'analisi tecnica supplementare;
6. 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

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.

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

La notifica, in base allo schema predisposto dal Garante Privacy (v. allegato n. 5) può essere:

- "**Preliminare**" quando essa venga effettuata dal Titolare in presenza di informazioni che, pur incomplete, sono tali da far ritenere che si sia verificata una violazione di sicurezza qualificabile come "violazione di dati personali" (o Data Breach) secondo le definizioni di cui in premessa;

- "**Completa**" quando essa venga effettuata dal Titolare all'esito del completamento di tutte le indagini che gli obblighi legali, le buone pratiche, le procedure aziendali, le raccomandazioni del DPO/RPD e l'opportunità del caso gli abbiano suggerito.

- "**Integrativa**" quando essa venga effettuata dal Titolare all'esito di *ulteriori elementi emersi in fase successiva alla notificazione completa*, che comportino la modifica delle circostanze di fatto o delle valutazioni di merito operate con la notifica completa.

Nel caso in cui si proceda a notifica preliminare, la chiusura dell'indagine, in assenza di elementi di fatto che suggeriscano un termine diverso, avviene nel termine ordinatorio di 30 giorni secondo il dettato dell'art.2, comma 2, L. 241/1990.

La notifica, sulla base del Modello reso disponibile on-line dal Garante Privacy (in allegato 5) dovrà contenere i seguenti elementi:

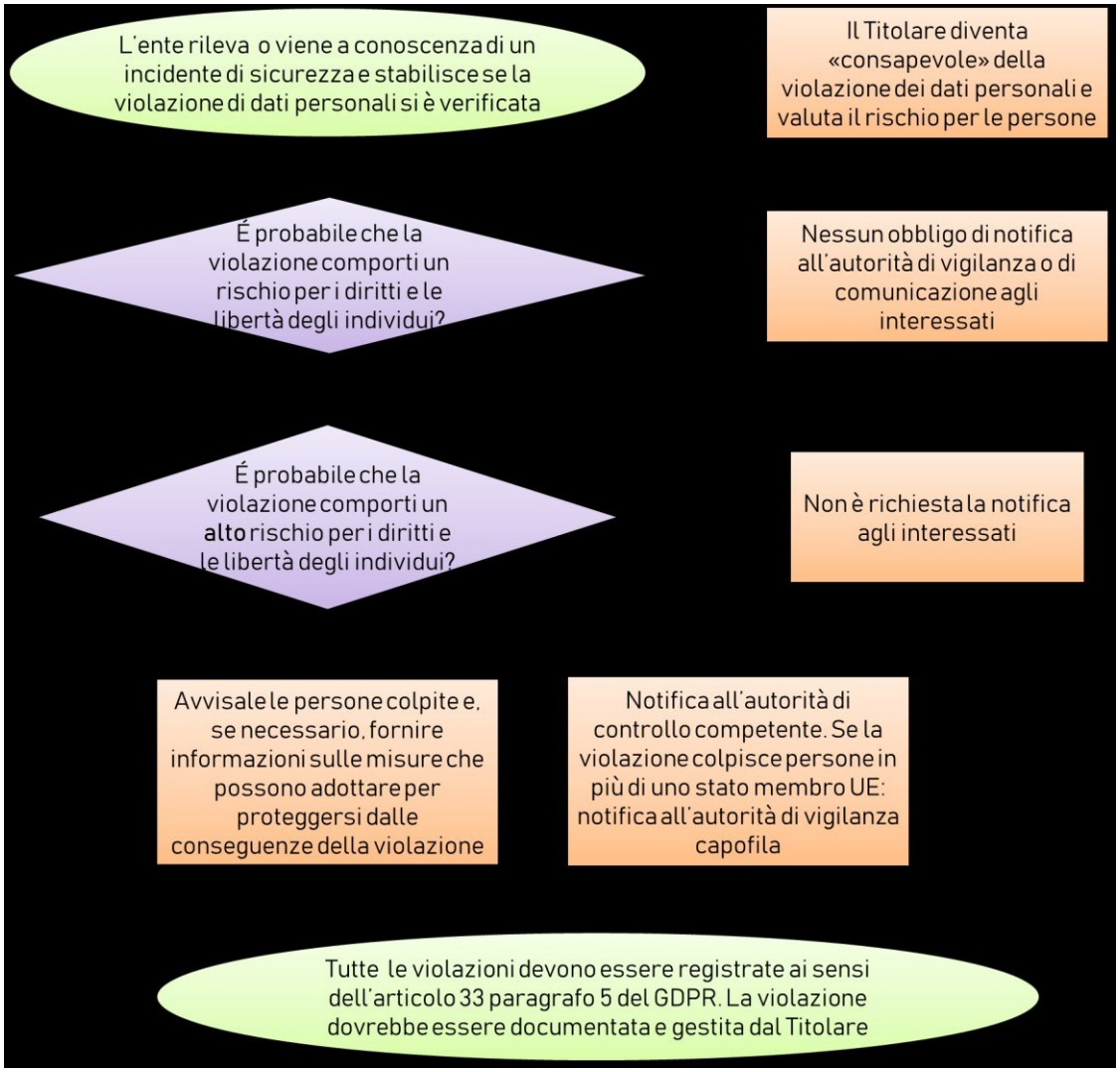
- La descrizione della Violazione dei Dati Personali compresi, ove possibile le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei Dati Personali in questione

- L'indicazione del nome e i relativi dati di contatto del DPO

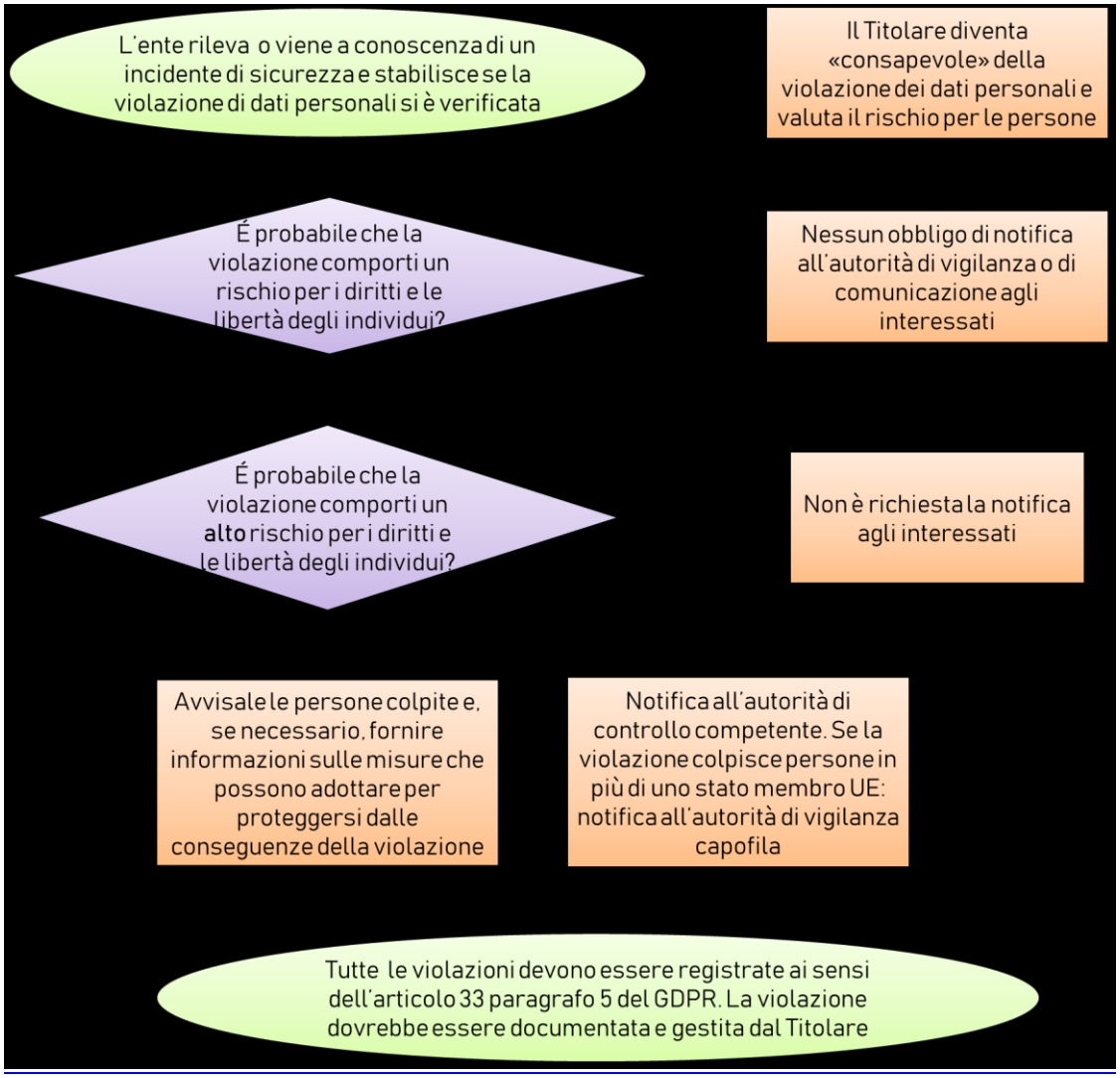
- La descrizione delle probabili conseguenze della Violazione

- 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 (mitigazione).

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012



Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012



Nello specifico, la notifica al Garante sarà effettuata dal Titolare o suo delegato tramite l'utilizzo della procedura disponibile on – line nel sito istituzionale del Garante Privacy, all'indirizzo https://servizi.gpdp.it/databreach/s/ con indicazione del DPO come punto di contatto con il Garante, secondo le istruzioni ivi riportate all'indirizzo https://servizi.gpdp.it/databreach/s/istruzioni.

A seguito di revisione a cura del DPO aziendale, se l'estensione della compromissione è chiara e non si sono verificati episodi analoghi si deve procedere alla notifica all'Autorità. I contenuti della notifica sono specificati dal GDPR e dai documenti citati.

Attenzione: la procedura telematica di notifica prevede l'impiego della firma digitale del legale rappresentante o del suo delegato; la firma digitale può essere sostituita dallo SPID

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

5. Altre segnalazioni dovute

Il Referente Ufficio Privacy, con il supporto dei soggetti indicati in matrice (all. 2), 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);
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).
- il Gestore di Identità Digitale e ad Agid nel caso in cui si individui un uso anomalo di un'identità SPID (Sistema Pubblico di Identità Digitale).

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:

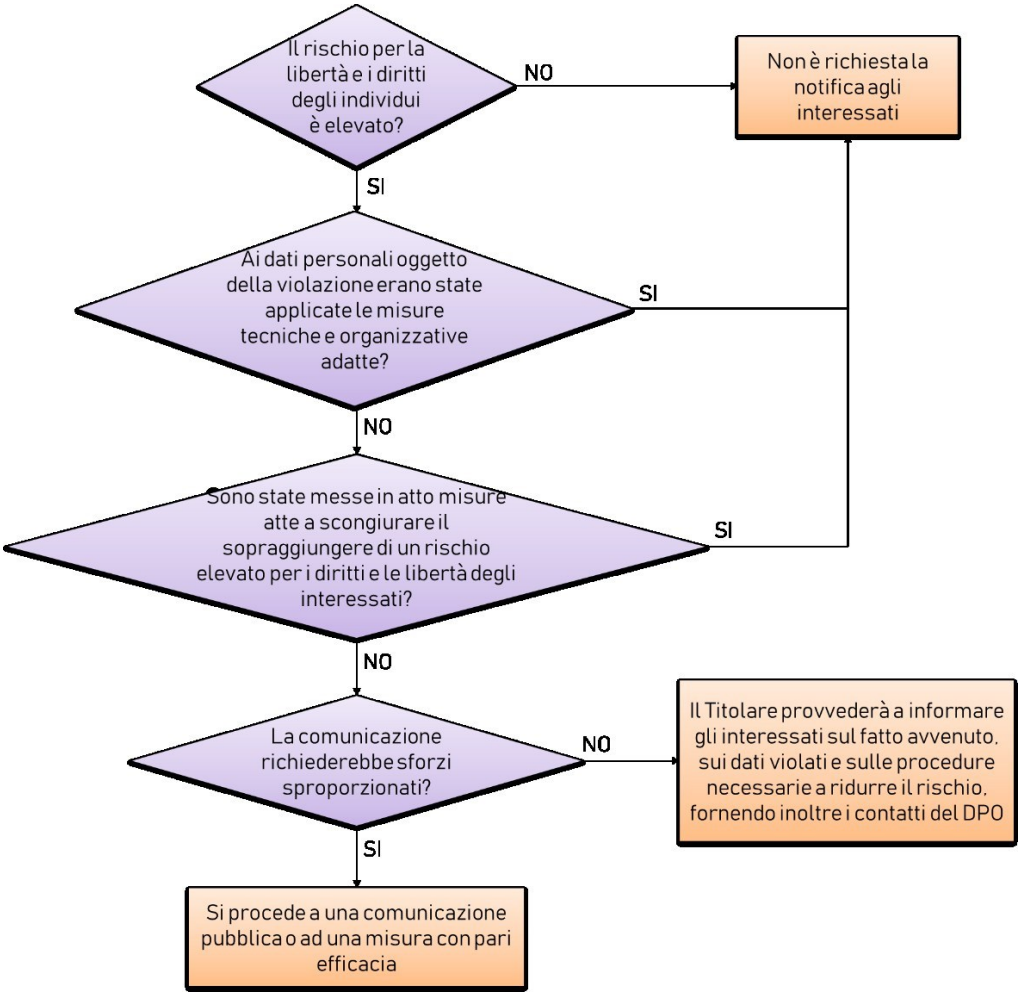
- il Titolare del Trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai Dati Personali oggetto della violazione, in particolare quelle destinate a rendere i Dati Personali incomprensibili a chiunque non sia autorizzato ad accedervi, 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 Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012



A valle della decisione di notificare l'Autorità Garante, occorre valutare se è il caso di notificare anche gli interessati. A tale scopo va valutata la gravità del rischio per gli interessati e i loro diritti.

Se il rischio è grave occorre individuare:

- La fattibilità di contattarli singolarmente oppure la necessità di procedere con pubblicazioni su diversi mezzi di comunicazione (sito web, quotidiani, radio, tv)
- le misure di contenimento che gli stessi interessati possano mettere in atto per minimizzare i rischi
- Le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio) come indicato nelle Linee guida elaborate dal Gruppo Art. 29 in materia di trasparenza (WP 260), definite in base alle previsioni del Regolamento (UE) 2016/679.

Anche di queste fasi deve essere prodotta e conservata appropriata documentazione

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

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.
La documentazione dovrà avvenire sull'applicativo "Data Protection Manager" secondo le indicazioni riportate in allegato 4.

8. Miglioramento

Sulla base degli incidenti di sicurezza verificatisi le competenti strutture aziendali, e in particolare il responsabile dell'Information Technology, di concerto con la Direzione Generale, seguirà la metodologia Plan Do Check Act ovvero mettendo in evidenza e documentando le "lezioni apprese" scaturite e sulla base di queste realizzando l'eventuale modifica dell'*Incident Response Plan* e quindi della presente procedura o di altra documentazione di riferimento.

Le azioni previste in questa fase sono:

- Analisi della relazione dettagliata sull'incidente
- Reiterazione del processo di Gestione del rischio informativo
- 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
- Modificare le modalità dei trattamenti coinvolti onde ridurre, fino a escludere, ove possibile, la possibilità del ripetersi dell'evento.
- Revisione del Sistema di Gestione della Privacy
- Revisione delle relazioni con Utenti e Fornitori
- Revisione annuale della procedura.

I soggetti individuati come "Competenti" in base alla tabella in Allegato 1 e tabella RACI in Allegato 2 sono responsabili per la verifica dell'attuazione delle misure di miglioramento individuate.

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

Allegato 1 – SOGGETTI PREPOSTI A GESTIRE LE VIOLAZIONI

Gruppo Gestione operativa Data Breach

	Riceventi	Competenti
Referente Ufficio Privacy[1]	☑	
Direttore S.C. Risk Management		☑
Direttore S.C Sistemi Informativi e Ufficio Flussi		☑
Direttore S.C. Acquisizione e Gestione Logistica Beni e Servizi		☑

Riceventi	Preposti alla ricezione, registrazione e prima analisi delle segnalazioni
Competenti	Predispongono mezzi e strumenti, forniscono consulenza specialistica per le violazioni nell'ambito del dominio di competenza

Identificazione risorse critiche – Ciascuna delle unità indicate identifica una persona delegata allo svolgimento della procedura. In assenza di questi, ciascuna Struttura procede alla sostituzione temporanea, secondo il principio di surrogazione, mediante l'intervento del superiore gerarchico. Il sostituto dei Direttori / Responsabili di Struttura è identificato a norma della Deliberazione n. 540 del 14 maggio 2021

[1] Il Referente Ufficio Privacy è individuato tra il personale in servizio presso la S.S. Legale e Assicurazioni (S.C. Affari Istituzionali-Legali-CNU)

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

Allegato 2 - Matrice Assegnazione Responsabilità

	Segnalante interno[2]	Competenti	Coordinatore Gruppo Privacy	Referente Ufficio Privacy	RPD	Legale rappresentante
Rilevazione incidente	R		A	I		
Acquisizione della notizia			A	R	I	
Analisi tecnica dell'evento	C	R	A	C	C	
Contenimento del danno	C	R	A	C	C	
Valutazione della gravità dell'evento	C	C	R	C	C	A (Se evento significativo)
Notifica al Garante Privacy		C	I	R	C	A
Altre segnalazioni dovute[3]	R	C	C	R		A (Se evento significativo)
Comunicazione agli interessati		C	C	R	C	A (Se evento significativo)
Inserimento dell'evento nel Registro delle Violazioni			A	R	I	
Azioni correttive	R	R	C	C	C	A (Se evento significativo)

Legenda
R Responsabile dell'attività
A Approva e supervisiona
C Consultato
I Informato

I soggetti competenti sulla tipologia della segnalazione possono/debbono avvalersi delle Ditte appaltatrici per il necessario supporto.

[2] Si considera comunque Segnalante Interno il Delegato al Trattamento Dati competente sul trattamento coinvolto nel data breach,
secondo le indicazioni riportate nel Registro delle attività di Trattamento aziendale.
[3] Le altre segnalazioni sono effettuate secondo le deleghe in essere

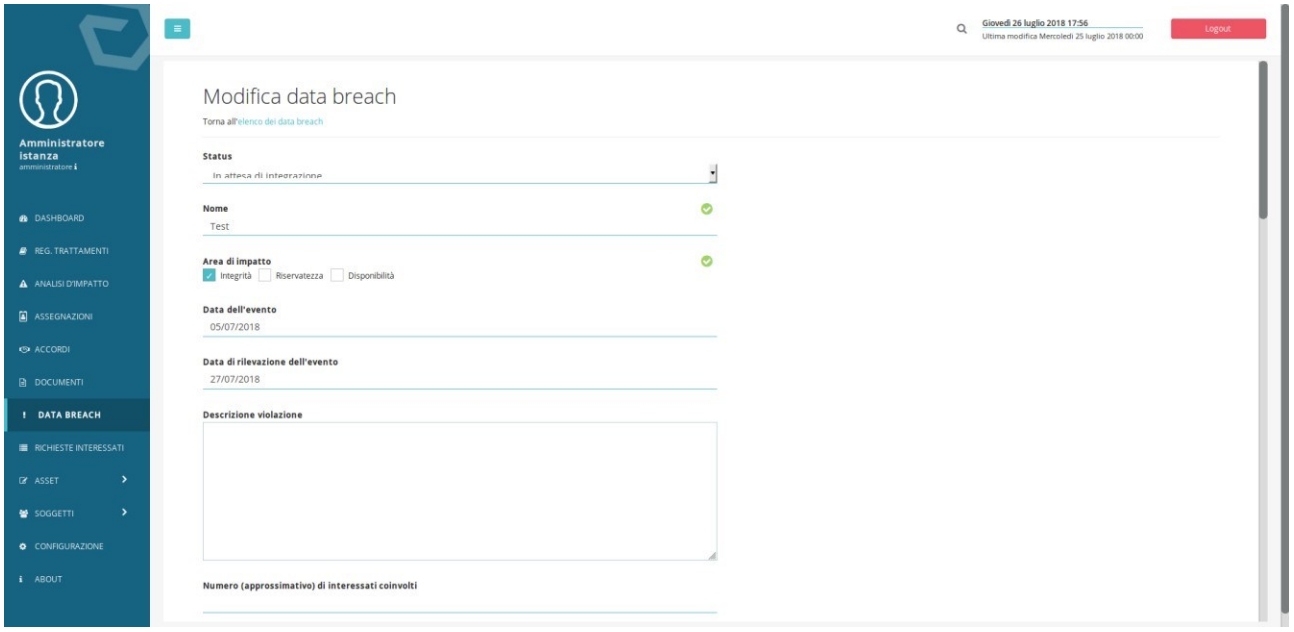
Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

Allegato 3 – Impiego del Registro delle Violazioni

L'Azienda ha adottato il software "Data Protection Manager", il quale dispone della funzione "Notifica Violazione dei dati – Data Breach" che offre un sistema decentralizzato per la segnalazione delle violazioni di dati. Il sistema è costituito da un Modulo di segnalazione disponibile a tutti gli utenti e da un Registro delle violazioni nel quale confluiscono tutte le segnalazioni. **Il Registro delle violazioni è disponibile solo agli utenti con relativo privilegio applicativo**. Avendo accesso al registro delle violazioni, gli utenti potranno valutare se integrarla con ulteriori dettagli e inoltrare la segnalazione all'autorità di controllo e/o agli interessati.

Il privilegio applicativo sul registro trattamenti è attribuito al Referente dell'Ufficio Privacy e al Coordinatore dell'Ufficio Privacy, nonché, per le funzioni di verifica, al DPO.

Tramite il registro delle notifiche di violazioni (contrassegnato dalla voce di menu Data Breach) è possibile consultare le notifiche generate dagli utenti, modificarle ed integrarle inserendo le informazioni richieste dagli articoli 33 e 34 Regolamento UE 2016/679. In un secondo momento tale integrazione sarà utile ai fini della generazione di un documento che potrà poi essere utilizzato per notificare quella violazione di dati all'autorità di controllo e/o agli interessati.



I campi disponibili nelle singole occorrenze di Data Breach contenute nel registro delle violazioni sono:

- Nome data breach;
- Tipo Data Breach (Disponibilità, Integrità, Riservatezza);
- Data evento + data rilevazione;
- Descrizione violazione;
- Numero (approssimativo) di interessati coinvolti;
- Categorie di interessati coinvolte;
- Categorie di dati coinvolti;
- Descrizione delle possibili conseguenze;
- Misure di sicurezza organizzative e tecniche;

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

- Descrizione misure di sicurezza adottate;
- Descrizione delle misure tecniche ed organizzative adottate per contenere la violazione dei dati e prevenire violazioni future;
- Notifica ed eventuale destinatario della notifica;
- Campo di testo libero per aggiungere ulteriori dettagli sulla notifica.

Tramite il tasto «carica file» posto nella colonna a destra dedicata ai dettagli della violazione, è possibile caricare uno o più file allegandoli ad una possibile o accertata Violazione.

Allegato 4 - Tabella della valutazione del rischio per le libertà degli individui

Livello di impatto/valore	Descrizione
Trascurabile/NA	Gli individui non incontreranno alcun inconveniente nella loro vita personale
Basso/0	Gli individui possono incontrare alcuni inconvenienti, che potranno superare senza problemi (tempo perso a re-imputare informazioni, seccature, irritazioni etc).
Medio/1	Gli individui possono incontrare inconvenienti significativi, che potranno superare con qualche difficoltà (extra costi, negazione di accesso a servizi professionali, paure, incomprensioni, stress, piccoli inconvenienti fisici etc.)
Elevato/2	Gli individui possono andare incontro a conseguenze significative, che potrebbero essere in grado di superare benché con seria difficoltà (appropriazione indebita di fondi, iscrizione in blacklist di istituzioni finanziarie, danni alla proprietà, perdita d'impiego, cauzioni, danni alla salute etc.)
Molto elevato/3	Gli individui possono andare incontro a significative, o anche irreversibili conseguenze, che non potranno superare (incapacità al lavoro, danni psichici o fisici a lungo termine, morte etc.)

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

Allegato 5 – Modello di segnalazione violazione al Garante Privacy

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

Questo servizio *online* per la notifica di una violazione dei dati personali deve essere utilizzato esclusivamente da soggetti (pubbliche amministrazioni, imprese, associazioni, partiti, professionisti, ecc.) che trattano dati personali in qualità di titolari del trattamento.

Per rivolgersi al Garante in qualità di interessato, per lamentare una violazione della disciplina in materia di protezione dei dati personali, occorre inviare una segnalazione (art. 144 del Codicein materia di protezione dei dati personali) che il Garante può valutare anche ai fini dell'emanazione di provvedimenti correttivi, oppure proporre un reclamo (art. 77 del Regolamento (UE) 2016/679 e artt. da 140-*bis* a 143 del Codice in materia di protezione dei datipersonali).

Maggiori informazioni sono disponibili sul sito istituzionale del Garante (https://www.gpdp.it/web/guest/home/diritti/come-agire-per-tutelare-i-tuoi-dati-personali).

Facsimile a titolo dimostrativo non utilizzabile per l'invio della notifica al Garante.

Facsimile a titolo dimostrativo non utilizzabile per l'invio della notifica al Garante.

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

A) Dati del soggetto che effettua la notifica

Il soggetto che effettua la notifica è la persona fisica che, per conto titolare del trattamento, tramite questaprocedura *online* notifica una violazione dei dati personali al Garante, assumendosi la responsabilità circa la veridicità delle informazioni fornite. Pertanto, la notifica dovrà essere effettuata dal rappresentante legaledel titolare del trattamento o da un altro soggetto che agisce su sua delega.

Il sottoscritto Cognome[1*] …….. Nome[1*] ……..
E-mail[2*] ……
nella sua qualità[3] di

- ○ rappresentante legale
- ○ delegato del rappresentante legale

  Cognome[4*] …….. Nome[4*] ……..

notifica la seguente violazione di dati personali e dichiara di aver preso visione dell'informativa sul trattamento dei dati personali e di essere consapevole che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*) o dell'art.44 del d.lgs. 51/2018 (*Falsità in atti e dichiarazioni al Garante*), salvo che il fatto non costituisca più grave reato.

---

[1] Indicare il **Cognome** e il **Nome** del soggetto che effettua la notifica (e che successivamentedovrà apporre la sua firma digitale, conformemente alle istruzioni che riceverà via e-mail).

[2] Indicare un indirizzo **E-mail** valido per la ricezione delle istruzioni per il completamento della procedura di notifica. Nel caso venga indicata una casella PEC, verificare che la stessa sia abilitata alla ricezione di messaggi di posta elettronica ordinaria. Si consiglia, inoltre, di verificare che il messaggio non sia stato spostato automaticamente o per errore nella cartella "spam" o "posta indesiderata.

[3] Indicare se il soggetto che effettua la notifica è il "rappresentante legale" del Titolare del trattamento dati – di cui alla successiva Sez. C - oppure se agisce in **qualità** di "delegato del rappresentante legale.

[4] Qualora la notifica venga effettuata su delega del rappresentante legale è necessario indicare il Cognome ed il Nome del soggetto delegante (il rappresentante legale).

B) Tipo di notifica

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore (**Prima notifica**). Qualora e nella misura in cui il titolare del trattamento non disponga di tutte le informazioni, può fornirle in fasi successive (**Notifica integrativa**) senza ulteriore ingiustificato ritardo (cfr. art. 33, par. 4, del Regolamento).

- ○ **Prima notifica**
  - ○ a) Completa
  - ○ b) Preliminare[1]

  La notifica viene effettuata
  - ○ ai sensi dell'art. 33 del RGPD
  - ○ ai sensi dell'art. 26 d.lgs. 51/2018
- ○ **Notifica integrativa**[2]
  - ○ c) fascicolo n.[3*] …… PIN [3*] ……

[1] Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione impegnandosi ad effettuare una successiva notifica integrativa.

[2] Il titolare del trattamento, avvalendosi delle previsioni di cui all'art. 33 par. 4 del Regolamento,integra una precedente notifica.

[3] È necessario inserire il numero del fascicolo ed il relativo PIN. Il numero di **fascicolo** unitamente al PIN sono indicati nella e-mail, indirizzata al soggetto che ha effettuato la prima notifica, con la quale è stata comunicata la corretta conclusione della procedura.

B1) Motivo dell'integrazione

Se procedi con la notifica integrativa per i motivi (a) o (b) troverai le informazioni che hai già fornito con l'ultima notifica e che potrai modificare. La notifica integrativa, ed il suo contenuto, integrerà e sostituirà la precedente notifica.

Se la notifica che intendi integrare è stata trasmessa con le precedenti modalità non troverai le informazioniche hai già fornito. La notifica integrativa, ed il suo contenuto, integrerà e sostituirà la precedente notifica.

1. Si procede all'integrazione per:

- ○ a) Fornire ulteriori informazioni senza completare il processo di notifica
- ○ b) Fornire ulteriori informazioni e completare il processo di notifica
- ○ c) Completare il processo di notifica senza fornire ulteriori informazioni
- ○ d) Annullare una precedente notifica per le seguenti motivazioni:

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

C) Titolare del trattamento

1. Il titolare del trattamento è:

Indicare l'eventuale registro all'interno del quale è censito il Titolare/Responsabile del trattamento cheeffettua la comunicazione. A tal fine si rappresenta che (cfr. DL 19 ottobre 2012, n. 179) tutte le imprese costituite in forma societaria e tutte le imprese individuali iscritte al registro delle imprese o all'albo delle imprese artigiane, nonché tutti i professionisti iscritti ad Ordini o Collegi professionali sono censiti all'interno dell'Indice nazionale dei domicili digitali delle imprese e dei professionisti (INIPEC). Inoltre, tutte le pubbliche amministrazioni (es. scuole, comuni, ecc.) sono iscritte nell'indicedei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA).

- ○ Censito nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti
  (INI-PEC www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale - D.Lgs n. 82/2005)
- ○ Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e deigestori di pubblici servizi - *(Tipologie Enti: Pubbliche Amministrazioni)*
  (*IPA www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005*)
- ○ Non censito in nessuno dei due precedenti indici

2. Dati del Titolare del trattamento

Indicare le informazioni relative al Titolare del trattamento (nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

Denominazione* ……
Codice Fiscale/P.IVA [1]* …… Soggetto privo di C.F./P.IVA italiana ☐
Stato* ……
Provincia* …… Comune* …… CAP* ……
Indirizzo* ……
Telefono* ……
E-mail[2]* ……
PEC[2]* ……

[1] In relazione all'indicazione del Codice Fiscale o Partita IVA si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVAqualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzatoper lo svolgimento dell'attività professionale;
- Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionarela casella "Soggetto Privo di CF/P.IVA".

[2] Per i soggetti che risultano essere censiti in uno degli indici INI-PEC o IPA è **obbligatorio** fornire l'indirizzo PEC, mentre il conferimento dell'indirizzo e-mail è facoltativo. Per i soggetti che non risultano essere censiti in uno dei due citati indici, o che operano in un altro Stato, è obbligatorio fornire un valido indirizzo e-mail, mentre il conferimento della PEC è facoltativo.

C1) – Rappresentante del titolare del trattamento nonstabilito nello Spazio Economico Europeo

Il titolare del trattamento non stabilito nello Spazio Economico Europeo, qualora offra beni o servizi a interessati nello Spazio Economico Europeo, oppure effettui il monitoraggio del loro comportamento (cfr. art. 3, par. 2, del Regolamento), è tenuto, ai sensi dell'art. 27 del Regolamento, a designare per iscritto un rappresentante in uno dei Paesi dello Spazio Economico Europeo in cui si trovano i predetti interessati, fattisalvi i casi in cui il trattamento è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati o dati relativi a condanne penali e reati, ed è improbabile che presenti un rischio per i diritti e le libertà degli interessati, oppure il trattamento è effettuato da autorità o organismi pubblici.

1. Rappresentante del titolare del trattamento

- ○ a) Compila la sezione
- ○ b) Procedi con la notifica senza compilare questa sezione

2. Dati del rappresentante del titolare del trattamento

Denominazione[1*] ……
Codice Fiscale/P.IVA[*] ..... Soggetto privo di C.F./P.IVA italiana ☐
Stato[*] ……
Provincia[*] …… Comune[*] …… CAP[*] ……
Indirizzo[*] ……
Telefono[*] ……
E-mail[2*] ……
PEC[2*] ……

[1] Indicare le informazioni relative al Rappresentante del titolare del trattamento (nel caso di impresa indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).
[2] È obbligatorio fornire almeno un recapito tra E-mail e PEC.

D) Dati di contatto per informazioni relative alla violazione

Il titolare del trattamento deve 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 (cfr. art. 33, par. 3, lett. b), del Regolamento).

- 1) Responsabile della protezione dei dati
  - i cui dati di contatto sono stati già comunicati con la comunicazione prot.[1*]n.……
  - i cui dati di contatto sono stati già comunicati al Garante, ma al momento nonsi dispone[2] del numero di protocollo della relativa comunicazione

    Cognome* ……. Nome* …….
    E-mail* …….
    Recapito telefonico per eventuali comunicazioni* ……..……

- 2) Altro soggetto

  Cognome* ……. Nome* …….
  E-mail* …….
  Recapito telefonico per eventuali comunicazioni* ……..……
  Funzione rivestita* ……..…….

---

[1]Indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD.

[2] Selezionare questa opzione se al momento della compilazione non è possibile reperire il numerodi protocollo assegnato alla comunicazione dei dati di contatto.

E) Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare,responsabile[1])

Denominazione[2*] ……..……..……..
Codice Fiscale[3*] ..... Soggetto privo di C.F./P.IVA ☐
Ruolo O Contitolare O Responsabile

Denominazione[2*] ……
Codice Fiscale[3*] ..... Soggetto privo di C.F./P.IVA ☐
Ruolo O Contitolare O Responsabile

Denominazione[2*] ……
Codice Fiscale[3*] ..... Soggetto privo di C.F./P.IVA ☐
Ruolo O Contitolare O Responsabile

---

[1] In tale tipologia rientra anche l'altro responsabile (c.d. sub-responsabile) di cui all'art. 28, par.2, del RGPD o all'art. 18, comma 2, del d.lgs. 51/2018.

[2] Nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale.

[3] In relazione all'indicazione del Codice Fiscale o Partita IVA si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVAqualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzatoper lo svolgimento dell'attività professionale;

Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionarela casella "Soggetto Privo di CF/P.IVA".

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

F) Informazioni sulla violazione

1. **Momento in cui è avvenuta la violazione**

- a) Il_____/_____/_____
- b) Dal_____/____/_____(la violazione è ancora in corso)
- c) Dal_____/____/_____ al_____/_____/_____
- d) In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. **Modalità con la quale il titolare è venuto a conoscenza della violazione**

- a) Rilevazione da parte del titolare[1]
- b) Comunicazione da parte del responsabile del trattamento
- c) Segnalazione da parte di un interessato
- d) Segnalazione da parte di un soggetto esterno
- e) Notizie stampa
- f) Altro

3. **Momento in cui il titolare è venuto a conoscenza della violazione**

Data …….. **Ora** ……..

4. **Motivi del ritardo (in caso di notifica oltre le 72 ore)**

5. ***Natura della violazione***

[ ] a) Perdita di riservatezza[2][ ] b) Perdita di integrità[3]
[ ] c) Perdita di disponibilità[4]

6. **Causa della violazione**

[ ] a) Azione intenzionale interna[ ] b) Azione accidentale interna [ ] c) Azione intenzionale esterna[ ] d) Azione accidentale esterna[ ] e) Sconosciuta

[ ] **f)** Non ancora determinata

7. **Descrizione della violazione**[5]

8. ***Descrizione dei sistemi, software, servizi e delle infrastrutture IT coinvoltinella violazione, con indicazione della loro ubicazione***

9. **Misure tecniche e organizzative, in essere al momento della violazione,adottate per garantire la sicurezza dei dati personali coinvolti**

10. Categorie di interessati coinvolti nella violazione

[ ] a) Dipendenti/Consulenti
[ ] b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)[ ] c) Associati, soci, aderenti, simpatizzanti, sostenitori
[ ] d) Soggetti che ricoprono cariche sociali[ ] e) Beneficiari o assistiti
[ ] f) Pazienti[ ]
g) Minori
[ ] h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedentiasilo)
[ ] i) Altro

[ ] l) Categorie ancora non determinate

11. Numero (anche approssimativo) di interessati coinvolti nella violazione

- a) N.....interessati
- b) Circa n.....interessati
- c) Non determinabile
- d) Non ancora determinato

12. Categorie di dati personali oggetto di violazione

[ ] a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita,codice fiscale)
[ ] b) Dati di contatto (indirizzo postale o di posta elettronica, numero ditelefono fisso o mobile)
[ ] c) Dati di accesso e di identificazione (username, password, customer ID,altro…)
[ ] d) Dati di pagamento (numero di conto corrente, dettagli della carta dicredito, altro…)
[ ] e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (datidi traffico, dati relativi alla navigazione internet, altro…)
[ ] f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza[ ] g) Dati di profilazione
[ ] h) Dati relativi a documenti di identificazione/riconoscimento (carta diidentità, passaporto, patente, CNS, altro…)
[ ] i) Dati di localizzazione
[ ] l) Dati che rivelino l'origine razziale o etnici[ ] m) Dati relativi a opinioni politiche
[ ] n) Dati relativi a convinzioni religiose o filosofiche[ ] o) Dati che rivelino l'appartenenza sindacale
[ ] p) Dati relativi alla vita sessuale o all'orientamento sessuale[ ] q) Dati relativi alla salute
[ ] r) Dati genetici

[ ] s) Dati biometrici[ ]
t) Altro

[ ] u) Categorie ancora non determinate

13. **Numero (anche approssimativo) di registrazioni[6] dei dati personalioggetto di violazione**

- a) N. ……..
- b) Circa n. ……..
- c) Non determinabile
- d) Non ancora determinato

14. **Descrizione di dettaglio delle categorie di dati personali oggetto dellaviolazione per ciascuna categoria di interessati**

15. ***Allegati***

[ ] Intendo allegare un documento contenente ulteriori informazioni

1. Es. verifiche interne, monitoraggi, ecc
2. Diffusione/ accesso non autorizzato o accidentale
3. Modifica non autorizzata o accidentale
4. Impossibilità di accesso o distruzione non autorizzata o accidentale
5. Indicare le circostanze in cui si è verificata la violazione e le cause, tecniche o organizzative,che l'hanno determinata
6. Ad esempio numero di fatture, ordini, referti, immagini, record di un database o numero ditransazioni.

G) Probabili conseguenze della violazione

1. *Probabili conseguenze della violazione per gli interessati*

1.1. In caso di perdita di riservatezza:

[ ] a) I dati sono stati divulgati al di fuori di quanto previsto dall'informativaovvero dalla disciplina di riferimento
[ ] b) I dati possono essere correlati, senza sforzo irragionevole, ad altreinformazioni relative agli interessati
[ ] c) I dati possono essere utilizzati per finalità diverse da quelle previsteoppure in modo non lecito
[ ] d) Altro

[ ] e) In corso di valutazione[4]

1.2. In caso di perdita di integrità:

[ ] a) I dati sono stati modificati e resi inconsistenti
[ ] b) I dati sono stati modificati mantenendo la consistenza[ ] c) Altro

[ ] d) In corso di valutazione[4]

1.3. In caso di perdita di disponibilità:

[ ] a) Mancato accesso a servizi
[ ] b) Malfunzionamento e difficoltà nell'utilizzo di servizi[ ] c) Altro

[ ] d) In corso di valutazione[4]

1.4. Ulteriori considerazioni sulle probabili conseguenze

2. Potenziale impatto per gli interessati

[ ] a) Perdita del controllo dei dati personali[ ] b)
Limitazione dei diritti
[ ] c) Discriminazione
[ ] d) Furto o usurpazione d'identità[ ] e)
Frodi
[ ] f) Perdite finanziarie
[ ] g) Decifratura non autorizzata della pseudonimizzazione[ ] h)
Pregiudizio alla reputazione
[ ] i) Perdita di riservatezza dei dati personali protetti da segreto professionale[ ] l) Conoscenza da parte di terzi non autorizzati
[ ] m) Qualsiasi altro danno economico o sociale significativo

[ ] n) Non ancora definito

3. Gravità del potenziale impatto per gli interessati

- a) Trascurabile
- b) Bassa
- c) Media
- d) Alta
- e) Non ancora definita

Motivazioni

4. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

H) Misure adottate a seguito della violazione

1. Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati

2. *Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per prevenire simili violazioni future*

3. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

1. Nella descrizione distinguere le misure adottate da quelle in corso di adozione

I) Valutazione del rischio per gli interessati

Non sono state fornite alcune delle informazioni (es. categorie e numero di interessati, categoriee numero di registrazioni di dati personali, probabili conseguenze della violazione, ecc.) di cui il titolare del trattamento dovrebbe tenere conto nella valutazione del rischio per i diritti e le libertà degli interessati derivante dalla violazione dei dati personali. Pertanto si invita il titolare del trattamento a prestare particolare attenzione nella compilazione della presente sezione, fornendo le motivazioni che lo hanno portato a ritenere che la violazione dei dati personali sia suscettibile, o meno, di presentare un rischio elevato per gli interessati.

Il Regolamento (spec. cons. nn. 75 e 76) suggerisce che, di norma, nella valutazione del rischiosi dovrebbero prendere in considerazione tanto la probabilità quanto la gravità dei rischi per i diritti e le libertà degli interessati e che tali rischi dovrebbero essere determinati in base a una valutazione oggettiva.
Le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017, comemodificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018, individuano i seguenti fattori da considerare – a fronte diuna violazione dei dati personali – nella valutazione del rischio per i diritti e le libertà degli interessati: il tipo di violazione; la natura, il carattere sensibile e il volume dei dati personali; la facilità di identificazione degli interessati; la gravità delle conseguenze per gli interessati; le caratteristiche particolari dell'interessato; le caratteristiche particolari del titolare del trattamento dei dati; nonché il numero di interessati coinvolti.

1. Il titolare del trattamento ritiene[1] che:

- o a) la violazione sia suscettibile di presentare un rischio elevato per i diritti e lelibertà delle persone fisiche
- o b) la violazione non sia suscettibile di presentare un rischio elevato per i dirittie le libertà delle persone fisiche
- o c) siano necessari ulteriori elementi per effettuare la valutazione del rischio peri diritti e le libertà delle persone fisiche

Motivazioni

2. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

L) Comunicazione della violazione agli interessati

Si evidenzia che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto, ai sensi dell'art. 34 del Regolamento, a comunicare la violazione agli interessati coinvolti senza ingiustificato ritardo, a meno che sia soddisfatta una delle condizioni previste dal par. 3 del citatoarticolo.

1. La violazione è stata comunicata direttamente agli interessati?

- o a) Sì, è stata comunicata il_____/____/_____
- o b) No, sarà comunicata entro il_____/____/_____
- o c) No, sono tuttora in corso le dovute valutazioni
- o d) No, perché la violazione non è suscettibile di presentare un rischio elevatoper i diritti e le libertà delle persone fisiche;
- o e) No e non sarà comunicata perché:

[ ] e1) il titolare ha messo in atto le misure tecniche e organizzative adeguatedi protezione e tali misure erano state applicate ai dati personali oggettodella violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (es. cifratura);
Descrivere le misure applicate

[ ] e2) il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
Descrivere le misure adottate

[ ] e3) detta comunicazione richiederebbe sforzi sproporzionati. Il titolare ha proceduto o procederà con una comunicazione pubblica o una misura simile, tramite la quale gli interessati sono o saranno informati con analoga efficacia.
Descrivere la modalità tramite la quale gli interessati sono stati informati

2. Numero di interessati a cui è stata comunicata la violazione

N..... interessati

3. Canale utilizzato per la comunicazione agli interessati

[ ] a) SMS
[ ] b) Posta cartacea
[ ] c) Posta elettronica[ ] d)
Altro

4. Contenuto della comunicazione agli interessati

5. *Allegati*

[ ] Intendo allegare un documento contenente ulteriori informazioni

M) Altre informazioni

1. La violazione è stata notificata ad altri organismi di vigilanza o di controlloin virtù di ulteriori disposizioni normative[1]?

O SI O NO

Indicare a quale organismo e in virtù di quale norma

2. È stata effettuata la segnalazione all'autorità giudiziaria o di polizia?

O SI O NO

Note

1. Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva(UE) 2016/1148 (NIS)

N) Informazioni relative a violazioni transfrontaliere

Un trattamento transfrontaliero (cfr. art. 4, punto 23), del Regolamento) è un trattamento che ha luogo nell'ambito di stabilimenti in più di un Paese dello Spazio Economico Europeo (di cui fanno parte gli Stati membri dell'Unione Europea, nonché l'Islanda, il Liechtenstein e la Norvegia), oppure che ha luogo nell'ambito di un unico stabilimento in un Paese dello Spazio Economico Europeo, ma che può avere impatti significativi sui diritti e sulle libertà di interessatiin più di un Paese dello Spazio Economico Europeo.

1. La violazione riguarda un trattamento transfrontaliero effettuato da un titolare stabilito all'interno dello Spazio Economico Europeo?

- a) Sì
- b) No
- c) Sono tuttora in corso le dovute valutazioni

2. Indicare l'autorità di controllo capofila[1]

- a) Garante per la protezione dei dati personali
- b) Altra autorità di controllo: [Selezionare]
- c) Non si dispone di elementi per individuare l'autorità di controllo capofila

3. Indicare i Paesi dello Spazio Economico Europeo in cui si trovano stabilimenti del titolare, specificando quelli coinvolti nella violazione, o in cui si trovano gli interessati coinvolti nella violazione

	Stabilimenti del titolare	Stabilimenti coinvolti nella violazione	Interessati coinvolti nella violazione
Italia	[ ]	[ ]	[ ]
Austria	[ ]	[ ]	[ ]
Belgio	[ ]	[ ]	[ ]
Bulgaria	[ ]	[ ]	[ ]
Cipro	[ ]	[ ]	[ ]
Croazia	[ ]	[ ]	[ ]
Danimarca	[ ]	[ ]	[ ]
Estonia	[ ]	[ ]	[ ]
Finlandia	[ ]	[ ]	[ ]
Francia	[ ]	[ ]	[ ]
Germania	[ ]	[ ]	[ ]
Grecia	[ ]	[ ]	[ ]
Irlanda	[ ]	[ ]	[ ]
Islanda	[ ]	[ ]	[ ]
Lettonia	[ ]	[ ]	[ ]
Liechtenstein	[ ]	[ ]	[ ]
Lituania	[ ]	[ ]	[ ]

Lussemburgo	[ ]	[ ]	[ ]
Malta	[ ]	[ ]	[ ]
Norvegia	[ ]	[ ]	[ ]
Paesi Bassi	[ ]	[ ]	[ ]
Polonia	[ ]	[ ]	[ ]
Portogallo	[ ]	[ ]	[ ]
Rep. Ceca	[ ]	[ ]	[ ]
Romania	[ ]	[ ]	[ ]
Slovacchia	[ ]	[ ]	[ ]
Slovenia	[ ]	[ ]	[ ]
Spagna	[ ]	[ ]	[ ]
Svezia	[ ]	[ ]	[ ]
Ungheria	[ ]	[ ]	[ ]

4. *Indicare le altre autorità di controllo a cui è stata eventualmente notificatala violazione*

[ ] Austria - Data Protection Authority[ ]
Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection[ ]
Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI) [ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information[ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA) [ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access toInformation
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseaticcity of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedomof Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom ofInformation
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for DataProtection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)

[ ] Islanda - Data Protection Authority[ ]
Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner[ ]
Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)[ ] Rep.
Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing[ ]
Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner
[ ] Spagna - Spanish Agency for Data Protection[ ]
Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata

---

1. L'autorità di controllo dello stabilimento principale in cui ha luogo il trattamento o dellostabilimento unico del titolare del trattamento

O) Informazioni relative a violazioni che riguardano trattamento effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo

Il Regolamento si applica anche al trattamento di dati personali di interessati che si trovano nello Spazio Economico Europeo, effettuato da un titolare del trattamento che non è stabilito nello Spazio Economico Europeo, laddove tale trattamento riguardi: a) l'offerta di beni o la fornitura di servizi a interessati nello Spazio Economico Europeo, oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dello Spazio Economico Europeo (cfr. art. 3, par. 2, del Regolamento)

1. La violazione riguarda un trattamento, a cui si applica il Regolamento, effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo?

- o a) Sì
- o b) No

2. Indicare gli altri Paesi dello Spazio Economico Europeo in cui si trovano gli interessati coinvolti nella violazione

[ ] Austria[ ]
Belgio
[ ] Bulgaria[ ]
Cipro
[ ] Croazia
[ ] Danimarca[ ]
Estonia
[ ] Finlandia[ ]
Francia
[ ] Germania[ ]
Grecia
[ ] Irlanda [ ]
Islanda [ ]
Lettonia
[ ] Liechtenstein[ ]
Lituania
[ ] Lussemburgo[ ]
Malta
[ ] Norvegia
[ ] Paesi Bassi[ ]
Polonia
[ ] Portogallo[ ]
Rep. Ceca [ ]
Romania
[ ] Slovacchia[ ]
Slovenia
[ ] Spagna

[ ] Svezia
[ ] Ungheria

3. Indicare le altre autorità di controllo a cui è stata eventualmente notificatala violazione

[ ] Austria - Data Protection Authority[ ]
Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection[ ]
Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI) [ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information[ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA) [ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access toInformation
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseaticcity of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedomof Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom ofInformation
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for DataProtection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)[ ]
Islanda - Data Protection Authority
[ ] Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner[ ]
Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)[ ] Rep.
Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing[ ]
Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner

[ ] Spagna - Spanish Agency for Data Protection[ ] Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata