Data breach

DECRETO LEGISLATIVO
18 maggio 2018, n. 51

Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

Articolo 25

D.lgs. 18 maggio 2018, n. 51
Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio

Sicurezza del trattamento

1. Il titolare del trattamento e il responsabile del trattamento, tenuto conto delle cognizioni tecniche disponibili, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del grado di rischio per i diritti e le libertà delle persone fisiche, mettono in atto misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio di violazione dei dati.

Articolo 25

Sicurezza del trattamento

D.lgs. 18 maggio 2018, n. 51
Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio

2. Per il trattamento automatizzato il titolare o il responsabile del trattamento, previa valutazione dei rischi, adottano misure volte a:

a) vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);

b) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);

c) impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);

d) impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»);

e) garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);

f) garantire la possibilità di individuare i soggetti ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);

g) garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);

h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);

i) garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);

l) garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

Articolo 25

D.lgs. 18 maggio 2018, n. 51
Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio

Sicurezza del trattamento

1. Salvo quanto previsto dall'articolo 37, comma 6, in caso di violazione di dati personali, il titolare del trattamento notifica la violazione al Garante con le modalità di cui all'articolo 33 del regolamento UE.

2. Se la violazione dei dati personali riguarda dati personali che sono stati trasmessi dal o al titolare del trattamento di un altro Stato membro, le informazioni previste dal citato articolo 33 del regolamento UE sono comunicate, senza ingiustificato ritardo, al titolare del trattamento di tale Stato membro.

IL REGOLAMENTO UE 2016 / 679

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo

REGOLAMENTO UE 2016/679

1. In caso di violazione dei dati personali, il **titolare** del trattamento **notifica la violazione all'autorità di controllo competente a norma dell'articolo 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.**

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo

REGOLAMENTO UE 2016/679

3. La notifica di cui al paragrafo 1 deve almeno:

a) **descrivere la natura della violazione** dei **dati personali** compresi, ove possibile, **le categorie** e il **numero approssimativo di interessati** in questione nonché le categorie e il numero approssimativo di **registrazioni dei dati personali in questione**;

b) comunicare il **nome e i dati di contatto del responsabile della protezione dei dati** o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le **probabili conseguenze della violazione dei dati personali**;

d) descrivere **le misure adottate** o di cui si **propone l'adozione** da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo

REGOLAMENTO UE 2016/679

4. 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.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 33

REGOLAMENTO UE 2016/679

Notifica di una violazione dei dati personali all'autorità di controllo

1. 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 comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 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 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 di cui al paragrafo 1;
c) 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.

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo

REGOLAMENTO UE 2016/679

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Articolo 4

Notifica di una violazione dei dati personali all'autorità di controllo

REGOLAMENTO UE 2016/679

12) «violazione dei dati personali»: 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;

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

GARANTE

COSA È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)?*

Una 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.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Alcuni possibili esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

GARANTE

COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI?

Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia **improbabile** che la violazione dei dati personali comporti un **rischio** per i diritti e le libertà delle persone fisiche.

Il responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare in modo che possa attivarsi.

Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere **accompagnate dai motivi del ritardo.**

Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta** tutte le violazioni dei dati personali, ad esempio predisponendo un apposito registro. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

COME INVIARE LA NOTIFICA AL GARANTE?

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ (VEDI: Provvedimento del 27 maggio 2021).

Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante.

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito **strumento di autovalutazione (self assessment)** che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

LE AZIONI DEL GARANTE

Il Garante può prescrivere misure correttive (v. art. 58, paragrafo 2, del Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare **fino a 10 milioni di Euro** o, nel caso di imprese, **fino al 2% del fatturato totale annuo mondiale**.

www.garanteprivacy.it

garanteprivacy.it

Seguici su

ITA

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Inserire il testo o il doc web

CERCA

I miei diritti

Imprese ed enti

L'Autorità | Temi | Normativa e provvedimenti | News e comunicazione | Amministrazione trasparente

URP e servizi utili

Nello sportello dei servizi è possibile trovare informazioni riguardanti

Modulistica e servizi online

Motore di ricerca FAQ

Reclami e Segnalazioni

CONTATTA L'URP

L'URP (Ufficio Relazioni con il Pubblico) risponde a quesiti e offre informazioni su disposizioni in materia di trattamento e protezione dei dati personali, modalità di tutela (reclami, segnalazioni), richieste di documentazione e materiale informativo.

- ACCEDI AL SERVIZIO TELEMATICO DEDICATO ALLA SEGNALAZIONE DI COMUNICAZIONI INDESIDERATE (TELEMARKETING)
- ACCEDI AL SERVIZIO TELEMATICO DEDICATO ALLA SEGNALAZIONE PER PREVENIRE IL FENOMENO REVENGE PORN
- ACCEDI AL SERVIZIO TELEMATICO DEDICATO AL DATA BREACH
- ACCEDI AL SERVIZIO DI COMUNICAZIONE DEI DATI DI CONTATTO DELL'RPD

Notifica di una violazione dei dati personali (data breach)

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

Auto valutazione per la notifica di una violazione dei dati personali (data breach)

Compilazione della notifica

Istruzioni

Informativa sul trattamento dei dati personali

Pagina informativa - Violazione dei dati personali (data breach)

Fac-simile del modello

Il modello per la notifica della violazione

Notifica di una violazione dei dati personali (data breach)

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

Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali

Questo strumento, a disposizione di ciascun titolare del trattamento di dati personali, consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Mediante alcuni semplici quesiti, il titolare viene guidato nell'assolvimento degli obblighi in materia di «**Notifica di una violazione dei dati personali all'autorità di controllo**» **(art.33** del Regolamento (UE) 2016/679 o art. 26 del D.Lgs. 51/2018) e di «Comunicazione di una violazione dei dati personali all'interessato» (art. 34 del Regolamento (UE) 2016/679 o art. 27 del D.Lgs. 51/2018).

Questo strumento è da considerarsi esclusivamente quale ausilio al processo decisionale del titolare del trattamento e non rappresenta il pronunciamento di questa Autorità sull'applicazione del Regolamento (UE) 2016/679 o del D.Lgs. 51/2018. Le informazioni fornite durante il suo utilizzo non saranno conservate.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il modello di notifica di una violazione dei dati personali

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 Codice in 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 dati personali).

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).

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 questa procedura ***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 legale del 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

- o rappresentante legale
- o 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.

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*] .....

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 per completare il processo di notifica. 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. Il suo contenuto, previa integrazione o modifica, annulla e sostituisce la precedente.

Se la notifica che intendi integrare è stata trasmessa con le precedenti modalità non troverai le informazioni che hai già fornito, e non sarà possibile compilare la sez. C e i punti 2 e 3 della sez. F. 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:

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 che effettua 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'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA).

- o 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)***
- o Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi - ***(Tipologie Enti: Pubbliche Amministrazioni)*** (***IPA www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005***)
- o 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 [1]* ..... Soggetto privo di C.F./P.IVA italiana ☐
Stato* .....
Provincia* ..... Comune* ..... CAP* .....
Indirizzo* .....
Telefono* .....
E-mail[2]* .....
PEC[2]* .....

Articolo 4

definizioni

REGOLAMENTO UE 2016/679

7) «titolare del trattamento»: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Articolo 4

definizioni

REGOLAMENTO UE 2016/679

8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che **tratta dati personali per conto del titolare del trattamento**;

Articolo 28

REGOLAMENTO UE 2016/679

Responsabile del trattamento

1. Qualora un trattamento debba essere effettuato **per conto del titolare** del trattamento, quest'ultimo **ricorre unicamente a responsabili del trattamento** che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

Articolo 28

Responsabile del trattamento

REGOLAMENTO UE 2016/679

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

Articolo 28

Responsabile del trattamento

REGOLAMENTO UE 2016/679

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, **assista il titolare del trattamento** con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) **assista il titolare del trattamento** nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

Articolo 28

Responsabile del trattamento

REGOLAMENTO UE 2016/679

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, **assista il titolare del trattamento** con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) **assista il titolare del trattamento** nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

Articolo 28

Responsabile del trattamento

g) su scelta del titolare del trattamento, cancelli o gli **restituisca tutti i dati personali** dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Articolo 28

Responsabile del trattamento

REGOLAMENTO UE 2016/679

4. **Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento** per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.

…

C1) Rappresentante del titolare del trattamento non stabilito 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, fatti salvi 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

- o a) Compila la sezione
- o 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]* .....

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 protocollo[1*] n.....
  - i cui dati di contatto sono stati già comunicati al Garante, ma al momento non si 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* .....

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

GARANTE

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 infrastrutture IT coinvolti nella 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, richiedenti asilo)
[ ] 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 di telefono 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 di credito, altro…)
[ ] e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di 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 di identità, passaporto, patente, CNS, altro…)
[ ] i) Dati relativi all'ubicazione
[ ] l) Dati che rivelano l'origine razziale o etnica
[ ] m) Dati che rivelano le opinioni politiche
[ ] n) Dati che rivelano le convinzioni religiose o filosofiche
[ ] o) Dati che rivelano 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

Articolo 4

Notifica di una violazione dei dati personali all'autorità di controllo

REGOLAMENTO UE 2016/679

Ai fini del presente regolamento s'intende per:

1) «**dato personale**»: 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;

13. Numero (anche approssimativo) di registrazioni[6] dei dati personali oggetto di violazione

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

14. Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati

15. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

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'informativa ovvero dalla disciplina di riferimento

[ ] b) I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati

[ ] c) I dati possono essere utilizzati per finalità diverse da quelle previste oppure 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 attenuarne i possibili effetti negativi per gli interessati***

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

I) Valutazione del rischio per gli interessati

Non sono state fornite alcune delle informazioni (es. categorie e numero di interessati, categorie e 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 rischio si 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, come modificate 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 di una 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:*

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

Notifica di una violazione dei dati personali (data breach)

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

DEVI COMUNICARE LA VIOLAZIONE AGLI INTERESSATI COINVOLTI

«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 comunica la violazione all'interessato senza ingiustificato ritardo»*** (cfr. art. 34

Apertura sito esterno in una nuova scheda per l'articolo 34 del Regolamento (UE) 2016/679
, par. 1, del Regolamento (UE) 2016/679 e art. 27 del D.Lgs 51/2018).

La comunicazione di una violazione agli interessati dovrebbe avvenire **"senza ingiustificato ritardo"**, in quanto l'obiettivo principale della stessa consiste nel fornire agli stessi interessati informazioni specifiche sulle misure che questi possono prendere per proteggersi.

A seconda della natura della violazione e del rischio presentato, la tempestività della comunicazione aiuterà le persone (interessati) a prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

CONTENUTO DELLA COMUNICAZIONE

La comunicazione agli interessati coinvolti deve fornire ***«con un linguaggio semplice e chiaro»***(cfr. art. 34

Apertura sito esterno in una nuova scheda per l'articolo 34 del Regolamento (UE) 2016/679
, par. 2, del Regolamento (UE) 2016/679 e art. 27 del D.Lgs 51/2018):

- una descrizione della **natura della violazione**;
- il **nome** e **dati di contatto** del responsabile della protezione dei dati (RPD) o di altro punto di contatto presso cui ottenere più informazioni;
- una descrizione delle **probabili conseguenze della violazione** dei dati personali;
- una descrizione delle **misure adottate** o di cui si propone l'adozione **per porre rimedio alla violazione** e anche, se del caso, **per attenuare i possibili effetti negativi per gli interessati.**

Inoltre, il titolare del trattamento dovrebbe anche fornire **consulenza specifica** alle persone fisiche **sul modo in cui proteggersi** dalle possibili conseguenze negative della violazione. Ad esempio:

- in caso di compromissione delle credenziali di accesso, il titolare dovrebbe fornire anche la raccomandazione di non utilizzare più la password compromessa né una simile nonché di modificare la password utilizzata per l'accesso a qualsiasi altro servizio online qualora coincidente o simile a quella oggetto di violazione;
- in caso di compromissione di dati relativi a conti correnti bancari o strumenti di pagamento (quali carte di credito o debito), il titolare dovrebbe fornire la raccomandazione di monitorare le movimentazioni economiche e/o richiedere supporto al proprio istituto bancario/finanziario.

COME CONTATTARE L'INTERESSATO

La violazione dovrebbe essere comunicata **direttamente** agli interessati coinvolti (ad esempio mediante messaggi di posta elettronica, SMS, comunicazione postale), a meno che ciò richieda uno **sforzo sproporzionato**.

In tal caso, si procede a una **comunicazione pubblica** o a una misura simile (ad esempio banner o notifiche su siti web di primo piano, pubblicità di rilievo sulla stampa) che permetta di informare gli interessati con analoga efficacia (cfr. art. 34, par. 3, lett. c), del Regolamento (UE) 2016/679).

Nel comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che **non devono essere inviati insieme ad altre informazioni**, quali newsletter o messaggi standard. Ciò contribuisce a rendere la comunicazione della violazione chiara e trasparente.

Notifica di una violazione dei dati personali (data breach)

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

DEVI DOCUMENTARE LA VIOLAZIONE

Il titolare del trattamento deve documentare tutte le violazioni dei dati personali che si verificano, indipendentemente dal fatto che una violazione debba o meno essere notificata al Garante.

«Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di verificare il rispetto del presente articolo» (cfr. art. 33

Apertura sito esterno in una nuova scheda per l'articolo 33 del Regolamento (UE) 2016/679
, par. 5, del Regolamento (UE) 2016/679 e art. 26 del D.Lgs 51/2018).

L'obbligo del titolare di documentare tutte le violazioni è collegato al principio di responsabilizzazione (cfr. art. 5

Apertura sito esterno in una nuova scheda per l'articolo 5 del Regolamento (UE) 2016/679
, par. 2, del Regolamento (UE) 2016/679 e art. 3, comma 4, del D.Lgs 51/2018) e agli obblighi del titolare del trattamento responsabilizzazione (cfr. art. 24

Apertura sito esterno in una nuova scheda per l'articolo 24 del Regolamento (UE) 2016/679
del Regolamento (UE) 2016/679 e art. 15 del D.Lgs 51/2018).

Il titolare del trattamento è incoraggiato a creare un registro interno delle violazioni occorse – notificate o meno – e il Garante può chiedere di consultare tale registro.

Oltre ad informazioni quali cause, fatti, dati personali, effetti e conseguenze della violazione, le Linee guida

Apertura sito esterno in una nuova scheda per le Linee guida Notifica violazioni
raccomandano di documentare anche il ragionamento alla base delle decisioni prese in risposta a una violazione, come, ad esempio, il perché una determinata violazione non è stata notificata al Garante.

Se ritieni che la violazione occorsa **non comporti un rischio elevato per gli interessati**, non è obbligatorio effettuare la comunicazione agli interessati.

*«Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, **l'autorità di controllo può richiedere**, dopo aver valutato la probabilità che la violazione dei dati personali presenti un **rischio elevato, che vi provveda** o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta»* (cfr., *par. 4, del Regolamento (UE) 2016/679 e art. 27 del D.Lgs 51/2018).*

1. *La violazione è stata comunicata direttamente agli interessati?*

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

[ ] e1) il titolare ha messo in atto 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 (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

M) Altre informazioni

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

O Sì 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 Sì O No

Note

Il modello di notifica di una violazione dei dati personali

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 interessati in 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	[ ]	[ ]	[ ]

Nel caso in cui la violazione riguardi un servizio affidato all'esterno

È necessario acquisire dal "responsabile del trattamento" (società o professionista a cui è affidato il servizio) tutte le informazioni utili per la compilazione di modello di notifica della violazione al Garante

Fac simile richiesta informazioni al “responsabile” esterno

Codesta società, in qualità di Responsabile del trattamento, a seguito dell’affidamento dei servizi di….. avvenuto con ….., in data xxx ha comunicato per email la possibile violazione del trattamento di dati personali riguardanti gli stessi servizi affidati, in conseguenza della quale, questo ente non risulta in condizione di poterne fruire.

Si precisa, preliminarmente, che sorprende di rilevare che sul sito di codesta società appare una comunicazione dell’xxx che annuncia l’avvenuta violazione, mentre la notizia è stata trasmessa a questo ente, quale titolare del trattamento, soltanto il xxx. Né, in quest’ultima circostanza sono state forniti informazioni utili per comprendere le dimensioni dell’accaduto, le eventuali conseguenze, le misure adottate e le iniziative intraprese, anche con riferimento alle segnalazioni alle autorità competenti.

Questo ente, una volta acquisita la comunicazione ha provveduto a inoltrare al Garante la dovuta segnalazione che tuttavia risulta carente proprio a causa della mancata comunicazione delle informazioni richiesta da parte di codesta società.

Pertanto si riporta di seguito una serie di informazioni che si richiedono allo scopo di potere avere cognizione dell’accaduto e dei rischi connessi, oltre che per fornire al Garante le informazioni richieste dal modello di data breach.

Allo scopo di facilitare la comprensione di quanto richiesto sono riportati, per ogni informazione, i riferimenti relativi al modello predisposto dal Garante.

Informazioni richieste:

F.5: natura della violazione

F.6: causa della violazione

F.7: descrizione della violazione

F.8: Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione

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

H.1 Misure tecniche e organizzative adottate per porre rimedio alla violazione e attenuarne i possibili effetti negativi per gli interessati

H.2 Misure tecniche e organizzative adottate per prevenire simili violazioni future

M.1 La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative1?

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

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

Si rappresenta l’urgenza di avere le informazioni richieste allo scopo di definire la procedura di data breach.