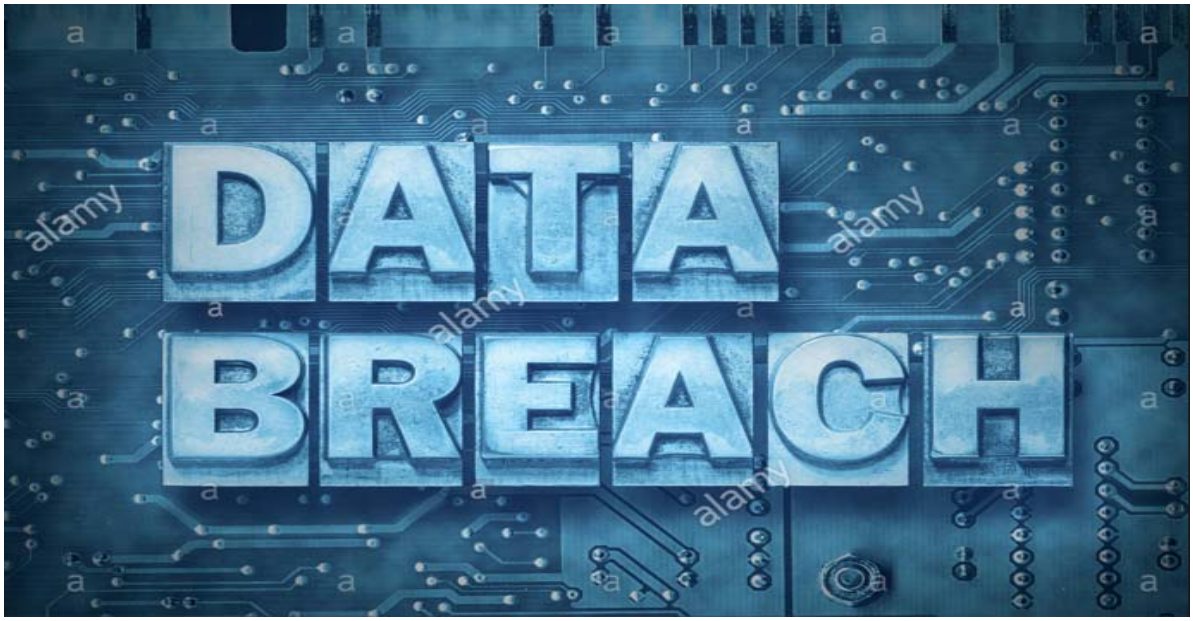
STUDIO TECNICO LEGALE

CORBELLINI

Studio AG.I.COM. S.r.l.



GUIDA ALLA GESTIONE DEL DATA BREACH

PER IL TITOLARE DEL TRATTAMENTO

Schema di procedura per la gestione delle ipotesi di violazione dei dati personali (data breach) ai sensi del Regolamento UE 2016/679 (G.D.P.R.).

MODELLO REV. 1.0

INTRODUZIONE

LA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Una violazione dei dati personali (c.d. *data breach*) può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali ed immateriali alle persone fisiche coinvolte.

Alcuni esempi che possiamo fare di questi danni sono: la perdita del controllo dei dati personali che li riguardano o la limitazione dei loro diritti, casi di discriminazione, furto o usurpazione d'identità, perdite finanziarie connesse alla sottrazione delle credenziali dell'home banking, decifratura non autorizzata delle forme di pseudonimizzazione attuate, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale e d'ufficio o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

IL CONTENUTO DI QUESTA GUIDA

La presente guida si prefigge lo scopo di indicare, al Titolare del trattamento dei dati, le opportune modalità di gestione del *data breach*, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016 (Considerando n. 85,86,87,88 ed Artt. 33 e 34) e nella *Guidelines on personal data breach notification under Regulation 2016/679 – article 29 data protection working party*.

In questo documento si sintetizzano le regole per garantire il rispetto dei principi esposti e la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione del *data breach*, sotto i diversi aspetti relativi a:

- modalità di segnalazione al Titolare da parte di chi venga a conoscenza della violazione

- modalità e profili di segnalazione all'Autorità Garante

- valutazione dell'evento accaduto

- eventuale comunicazione agli interessati

DEFINIZIONI

Al fine di una più ampia leggibilità della guida, si ritiene utile inserire le principali definizioni con riferimento agli articoli del G.D.P.R. di riferimento:

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 (art. 4, punto 1).

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 (art. 4, punto 2).

INTRODUZIONE

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6).

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 (art. 4, punto 7).

Data Protection Officer: la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).

Autorizzato al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 4, punto 10).

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 (art. 4, punto 8).

Violazione dei dati personali (c.d. Data breach):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 (art. 4, punto 12)

PREMESSA

Nelle prossime pagine troverà le procedure specifiche di gestione, che comunque Le chiedo di condividere con me nel caso in cui si verificasse uno dei casi che configurano un data breach.

Ho trovato utile suddividere le procedure a seconda che la violazione avvenga

- **All'interno della struttura** (quindi all'interno degli uffici e degli organi di pertinenza del Titolare)

- **All'esterno della struttura** (cioè presso un soggetto terzo, come ad esempio il gestore di un sistema in cloud a cui ci si sia affidati in forza di un contratto, che è stato designato quale "Responsabile esterno del trattamento", e che comunichi che si è verificata, presso di lui, una violazione dei dati.

Luca Corbellini
Data Protection Officer

GESTIONE DEL DATA BREACH INTERNO

È necessario che il Titolare del trattamento dia notizia, a tutti i dipendenti autorizzati al trattamento dei dati, mediante idonea circolare o formazione specifica, della presente procedura.

LA PROCEDURA

Ogni operatore autorizzato a trattare i dati personali, qualora venga a conoscenza di un potenziale caso di *data breach*, avvisa tempestivamente il Titolare del trattamento.

Quest'ultimo, valutato l'evento, se confermate le preoccupazioni di potenziale *data breach*, lo segnala tempestivamente al Data Protection Officer tramite e-mail da inviare a dpo@agicomstudio.it.

Ai fini di una corretta classificazione dell'episodio, il D.P.O. utilizzerà lo schema di scenario di *data breach*, allegato alla presente guida.

Pertanto, sulla scorta delle determinazioni raggiunte, il D.P.O. predispone l'eventuale comunicazione all'Autorità Garante, a firma del titolare, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.

Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi).

La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del D.P.O.

LA COMUNICAZIONE DELLA VIOLAZIONE AGLI INTERESSATI

Nel caso in cui dal *data breach* possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Il Titolare del trattamento predispone l'eventuale comunicazione agli interessati da inviarsi nei tempi e nei modi che lo stesso, anche attraverso la funzione consulenziale del D.P.O., individuerà come più opportuna come specificato nell'art. 34 del G.D.P.R. e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

La comunicazione deve comprendere almeno:

• nome e recapiti del DPO;

• le probabili conseguenze della violazione dei dati;

• eventuali misure adottate dal titolare per porre rimedio o attenuare l'infrazione.

L'adeguatezza di una comunicazione è determinata non solo dal contenuto del messaggio, ma anche dalle modalità di effettuazione. Le linee guida, sulla base dell'art. 34, ricordano che devono sempre essere privilegiate modalità di comunicazione diretta con i soggetti interessati (quali email, SMS etc.).

GESTIONE DEL DATA BREACH ESTERNO

LA PROCEDURA

Ogniqualvolta il Titolare del trattamento si trovi ad affidare il trattamento di dati ad un soggetto terzo/responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di *data breach* sia inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di *data breach*.

Ad ogni responsabile del trattamento deve essere comunicato il contatto del D.P.O. al quale effettuare la predetta segnalazione tramite l'indirizzo e-mail dpo@agicomstudio.it.

La comunicazione deve avvenire senza ingiustificato ritardo, per "ingiustificato ritardo" si considera la notizia pervenuta al titolare al più tardi entro 12 ore dalla presa di conoscenza iniziale da parte del responsabile.

Il D.P.O. effettua una valutazione dell'evento avvalendosi, nel caso, del gruppo privacy del soggetto esterno.

Ai fini di una corretta classificazione dell'episodio il D.P.O. utilizzerà lo schema di scenario di *data breach* allegato alla presente guida.

Pertanto, sulla scorta delle determinazioni raggiunte, il D.P.O. predispone l'eventuale comunicazione all'Autorità Garante, a firma del titolare, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.

Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi)

La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del referente privacy.

NOTIFICA AL GARANTE A CURA DEL RESPONSABILE ESTERNO DEL TRATTAMENTO

Rimane salva la possibilità che sia il responsabile esterno del trattamento ad effettuare una notifica per conto del Titolare del trattamento, se il Titolare del trattamento ha rilasciato specifica autorizzazione al responsabile, all'interno del suddetto contratto. Tale notifica deve essere fatta in conformità con gli articoli 33 e 34 del G.D.P.R..

La responsabilità legale della notifica rimane in capo al Titolare del trattamento.

SCHEMA DI VALUTAZIONE DEGLI SCENARI

IL SISTEMA

Al fine di eseguire la valutazione dell'obbligatorietà o meno della notifica all'Autorità Garante dei data breach e di supportare i soggetti coinvolti nella procedura, vengono illustrati alcuni scenari di possibili violazioni di dati personali.

TIPO DI VIOLAZIONE (BREACH)	DEFINIZIONE	SOGLIA DI SEGNALAZIONE	ESEMPI (segnalazione SI)	CONTROESEMPI (segnalazione NO)
DISTRUZIONE	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	Dati non recuperabili o provenienti da procedure non ripetibili Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi	Guasto non riparabile dell'hard disk contenente uno o più referti che, in violazione al regolamento, erano salvati localmente Incendio di archivio cartaceo Distruzione di documenti originali	Rottura di una chiavetta USB o di un hard disk che non contiene dati personali originali (in unica copia) Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo
PERDITA	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	Dati non recuperabili relativi a più utenti, o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi	Smarrimento di chiavetta USB contenente dati originali Smarrimento di fascicolo cartaceo del personale o dell'utente	Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa

SCHEMA DI VALUTAZIONE DEGLI SCENARI

TIPO DI VIOLAZIONE (BREACH)	DEFINIZIONE	SOGLIA DI SEGNALAZIONE	ESEMPI (segnalazione SI)	CONTROESEMPI (segnalazione NO)
MODIFICA	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	Modifiche sistematiche su più casi Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi	Guasto tecnico che altera parte dei contenuti di un sistema, compromettendo anche i backup Azione involontaria, o fraudolenta, di un utente che porta alla alterazione di dati in modo non tracciato e irreversibile	Guasto tecnico che altera parte dei contenuti di un sistema, rilevato e sanato tramite operazioni di recovery Azione involontaria di un utente che porta alla alterazione di dati tracciata e reversibile Modifica di un documento non ancora validato dal proprio autore.
DIVULGAZIONE NON AUTORIZZATA	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Malfunzionamento del sistema di differenziazione delle credenziali Consegna di un CD con dati di un utente ad altra struttura senza autorizzazione	Un dipendente sul proprio sistema seleziona l'utente Mario Rossi ma interviene sull'utente Luca Bianchi., inserisce i dati e li invia al gestionale. Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati su internet Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.

SCHEMA DI VALUTAZIONE DEGLI SCENARI

TIPO DI VIOLAZIONE (BREACH)	DEFINIZIONE	SOGLIA DI SEGNALAZIONE	ESEMPI (segnalazione SI)	CONTROESEMPI (segnalazione NO)
ACCESSO NON AUTORIZZATO	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema.	Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi Accesso non autorizzata di un documento non ancora validato dal proprio autore.
INDISPONIBILITA' TEMPORANEA DEL DATO	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	Infezione da ransomware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal backup Cancellazione accidentale dei dati da parte di una persona non autorizzata Perdita della chiave di decrittografia di dati crittografati in modo sicuro irraggiungibilità di un sito di stoccaggio delle cartelle cliniche poste in montagna per isolamento neve	Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso

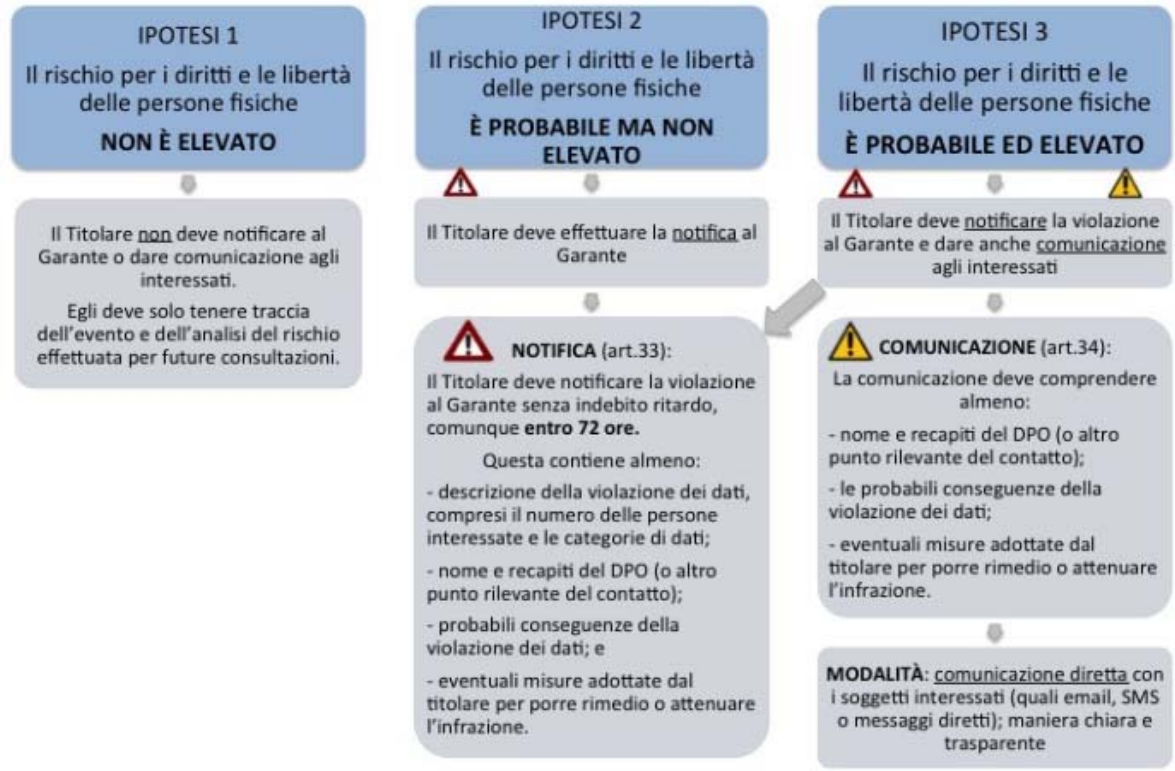
SCHEMA DI VALUTAZIONE DEGLI SCENARI

Un *data breach*, quindi, non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, un incidente (es. un incendio o una calamità naturale), nella semplice perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno), nella sottrazione di documenti con dati personali (es. furto di un notebook di un dipendente).

I casi di *data breach* per le casistiche già descritte si estendono dai dati digitali, ai documenti cartacei o su altri supporti analogici.

La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto/riconducibilità verso l'interessato non è considerato *data breach,* ma è considerato un normale errore procedurale.

Al fine di schematizzare ancora meglio lo schema del ragionamento prendiamo in prestito, dallo studio legale Delli Ponti, questo diagramma:



LA SEGNALAZIONE AL GARANTE

La segnalazione di un data breach all'Autorità Garante deve contenere alcune informazioni fondamentali. Di seguito le riportiamo per esteso (verificare sul sito del Garante la presenza di modulistica ad hoc):

1. Titolare che effettua la comunicazione:

a. Denominazione o ragione sociale:

b. Sede del titolare:

c. Persona fisica addetta alla comunicazione:

d. Funzione rivestita:

e. Indirizzo email per eventuali comunicazioni:

f. Recapito telefonico per eventuali comunicazioni:

2. Natura della comunicazione:

a. Nuova comunicazione (inserire contatti per eventuali chiarimenti, se diversi da quelli sub 1.):

b. Seguito di precedente comunicazione (inserire numero di riferimento):

b.1. Inserimento ulteriori informazioni sulla precedente comunicazione:

b.2. Ritiro precedente comunicazione (inserire le ragioni del ritiro):

3. Breve descrizione della violazione di dati personali:

4. Quando si è verificata la violazione di dati personali?

a. Il …

b. Tra il ….. e il …..

c. In un tempo non ancora determinato

d. È possibile che sia ancora in corso

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

6. Modalità di esposizione al rischio:

a. tipo di violazione:

a.1. lettura (presumibilmente i dati non sono stati copiati)

a.2. copia (i dati sono ancora presenti sui sistemi del titolare)

a.3. alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

a.4. cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)

a.5. furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)

a.6. altro [specificare]

b. dispositivo oggetto della violazione:

b.1. computer

b.2. dispositivo mobile

b.3. documento cartaceo

b.4. file o parte di un file

b.5. strumento di backup

b.6. rete

b.7. altro [specificare]

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

8. Quante persone sono state colpite dalla violazione di dati personali?

a. [numero esatto] persone

b. Circa [numero] persone

c. Un numero (ancora) sconosciuto di persone

9. Che tipo di dati sono coinvolti nella violazione?

a. Dati anagrafici

b. Numeri di telefono (fisso o mobile)

c. Indirizzi di posta elettronica

d. Dati di accesso e di identificazione (user name, password, customer ID, altro)

e. Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)

f. Altri dati personali (sesso, data di nascita/età, …), dati sensibili e giudiziari

g. Ancora sconosciuto

h. Altro [specificare]

10. Livello di gravità della violazione di dati personali (secondo le valutazioni del titolare):

a. Basso/trascurabile

b. Medio

c. Alto

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

12. La violazione è stata comunicata anche a contraenti (o ad altre persone interessate)?

a. Sì, è stata comunicata il ….

b. No, perché [specificare]

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

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

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

16. La violazione coinvolge contraenti (o altre persone interessate) che si trovano in altri Paesi EU?

a. No

b. Si

17. La comunicazione è stata effettuata alle competenti autorità di altri Paesi EU?

a. No

b. Si [specificare]

IL REGISTRO DEI DATA BREACH

LA NECESSITA' DI DOCUMENTARE

Come accade per tutti i sistemi basati sul concetto di "rischio" e di "valutazione del rischio", la documentazione degli episodi che hanno determinato un danno (violazione dei dati – data breach) è fondamentale al fine di adottare precauzioni (tecniche o comportamentali) che possano scongiurare il verificarsi nuovamente di quell'episodio.

L'Art. 33 del G.D.P.R. pone l'attenzione su questa esigenza, il metodo migliore per adempiere a questa regola ma anche per poter comprovare, in caso di ispezione, tale adempimento consiste nella tenuta di un registro dei data breach (già previsto dal Garante con provvedimento 161 del 04 Aprile 2013) che contenga, per ciascun episodio, queste informazioni essenziali:

1. Dettagli relativi alla violazione (cause, luogo, tipologia di dati violati);

2. Effetti e conseguenze della violazione;

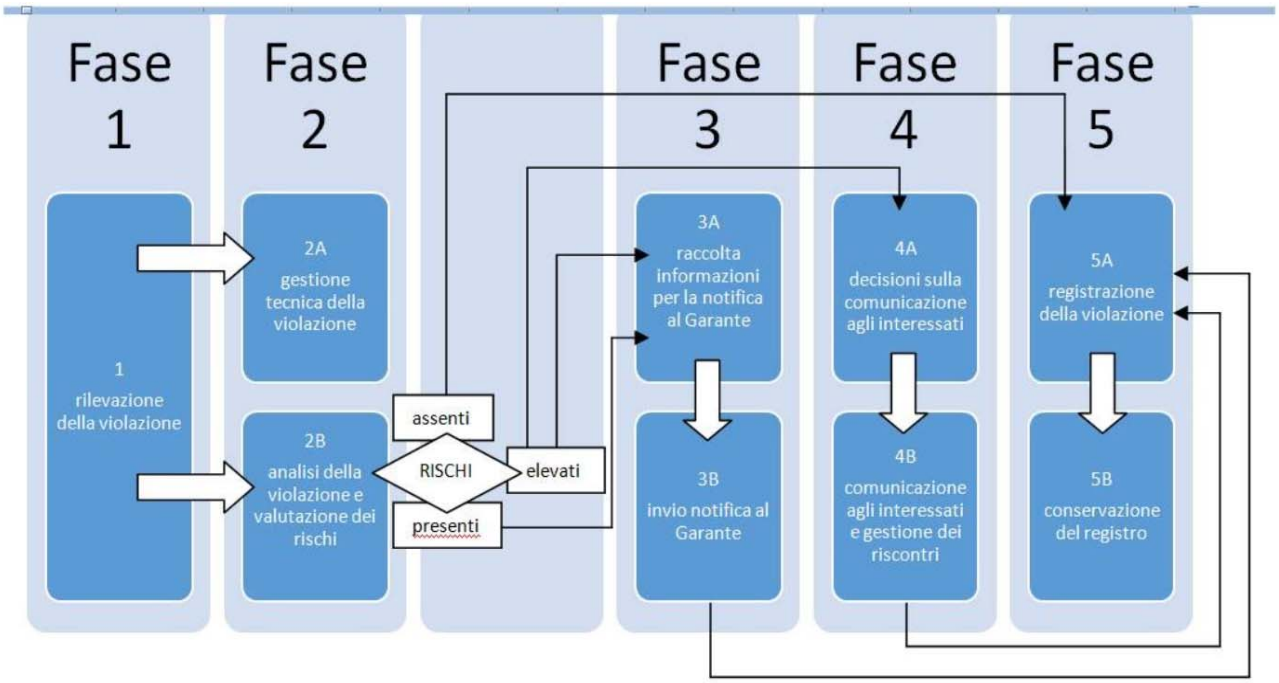
3. Piano di intervento predisposto dal Titolare;

4. Le motivazioni delle decisioni assunte a seguito del data breach nei casi in cui:

a. Il Titolare ha deciso di non procedere alla notifica;

b. Il Titolare ha ritardato nella procedura di notifica;

c. Il Titolare ha deciso di non notificare il data breach agli interessati.



NOTE

CONTATTI

Informazioni di contatto

Per qualsiasi informazione o approfondimento :

LUCA CORBELLINI
DATA PROTECTION OFFICER
SPECIALISTA IN INFORMATICA GIURIDICA

Tel. 02-90601324
Fax 02-700527180
dpo@agicomstudio.it

Informazioni sulla società

Studio AG.I.COM. S.r.l. unipersonale
Via XXV Aprile, 12 – 20070 SAN ZENONE AL LAMBRO (MI)
Tel. 02-90601324
Fax 02-700527180
www.agicomstudio.it

STUDIO TECNICO LEGALE
CORBELLINI
Studio AG.I.COM. S.r.l.