Comune di Dogliani

Ai Sigg.ri Dipenedenti Comunali

Oggetto: PROCEDURA PER LA GESTIONE DI *DATA BREACH* (REGOLAMENTO EUROPEO 679/2016)

Premessa

Il Regolamento Europeo sulla protezione dei dati n. 679/2016 (di seguito "GDPR"), entrato in vigore definitivamente il 25 maggio 2018, introduce l'obbligo di notificare all'autorità di controllo nazionale (Garante Privacy) incidenti sulla sicurezza che comportino la violazione dei dati personali (data breach) e di rendere nota la violazione stessa alle persone fisiche interessate.

La violazione dei dati personali è da intendersi come 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 tale da impedire al titolare del trattamento di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del GDPR.

Il GDPR impone al titolare di disporre le misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati al fine di proteggerli dalle violazioni sopra descritte.

Il presente documento si prefigge lo scopo di indicare le modalità di gestione del *data breach* garantendone la realizzabilità tecnica e la sostenibilità organizzativa.

Al fine di garantirne la massima diffusione interna ed esterna e la massima conoscibilità sulle azioni da intraprendere e sui comportamenti da adottare in caso di *data breach* la presente viene comunicata a tutti i dipendenti dell'Ente e resa disponibile sul sito web istituzionale nella sezione "Amministrazione Trasparente", sottosezione di primo livello "Altri Contenuti", sottosezione di secondo livello "Privacy".

1. Normativa e documenti di riferimento

Regolamento HE 679/2016 ("GDPR")
Dlgs 196/2003 come modificato dal D.Lgs 101/2018;

2. Definizione di violazione dei dati:

2.1 Classificazione delle violazioni:

Le violazioni si classificano nel seguente modo:

- violazione della riservatezza: in caso di divulgazione dei dati personali o accesso agli stessi non v autorizzati o accidentali;
- 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.

La violazione può riguardare la riservatezza, l'integrità, la disponibilità dei dati personali o qualsiasi combinazione delle stesse.

Al fine di adottare le corrette procedure di segnalazione è di fondamentale importanza sapere identificare una violazione, saperne valutare la natura e le potenziali conseguenze negative.
Le violazioni dei dati personali si considerano tali se hanno un reale impatto sulla confidenzialità, integrità o disponibilità dei dati personali degli interessati (cittadini, dipendenti, soggetti terzi ecc).

2.2 Tipologie di violazioni

All'interno della classificazione sopra indicata, quindi, si possono avere le seguenti tipologie di violazione dei dati personali:

- Distruzione: Indisponibilità definitiva di dati personali con impossibilità di ripristino degli stessi. La violazione può essere determinata da una eliminazione logica (es. cancellazione dei dati) oppure fisica (es. rottura dei supporti di memorizzazione) non autorizzata e relativa impossibilità di ripristinare i dati.
- Perdita: Perdita del supporto fisico di memorizzazione dei dati derivante da privazione, sottrazione, smarrimento dei dispositivi contenenti i dati degli interessati oppure dei documenti cartacei. La perdita, può riguardare anche copie od originali dei supporti contenenti i dati personali dei soggetti interessati, ed anche se temporanea può essere potenzialmente dannosa.
- Modifica: Modifiche improprie dei dati degli interessati non autorizzate, effettuate al di fuori dei processi operativi di trattamento dei dati svolti dagli incaricati autorizzati, oppure modifiche con finalità fraudolente eseguite dagli incaricati autorizzati all'accesso.
- Rivelazione: Distribuzione non autorizzata o impropria dei dati personali degli interessati verso terze parti (persone fisiche, persone giuridiche, gruppi di soggetti, pubblico) anche non precisamente identificabili.
- Accesso: Accesso non autorizzato o improprio ai dati degli interessati. Accessi ai dati (anche in sola visualizzazione, sia in caso di accessi logici ai sistemi informatici sia agli archivi cartacei) avvenuti al di fuori dei processi operativi di trattamento dei dati previsti e autorizzati.

2.3 Esempi di eventi che possono generare violazione di dati

Al fine di facilitare l'individuazione di una possibile violazione, vengono di seguito indicati in maniera esemplificativa e non esaustiva, una serie di possibili eventi che potenzialmente possono generare violazioni dei dati personali.

Pertanto si può essere in presenza di un *data breach* anche nel caso di un evento non compreso nell'elenco di seguito riportato, di contro il verificarsi di uno degli eventi che

seguono non costituisce condizione sufficiente per stabilire l'effettivo *data breach.* Il titolare deve infatti procedere sempre alle opportune valutazioni.

2.3.1 Eventi riguardanti trattamenti elettronici:

a) Eventi accidentali: Eventi anomali determinati da fatti fortuiti che causano la perditadelle caratteristiche di sicurezza dei dati personali dei clienti (confidenzialità, integrità o disponibilità) in caso di trattamenti informatizzati. Rientrano in tali casistiche eventi generati nella gestione dei sistemi ICT (gestiti internamente oppure in outsourcing) quali:

- Esecuzione erronea di comandi e/o procedure per distrazione: ad esempio pubblicazione erronea delle informazioni personali (non di dominio pubblico) su portali web pubblici; erroneo invio di informazioni a enti esterni alla Società, formattazione di dispositivi di memorizzazione, errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi; divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato ecc.
- Rottura delle componenti HW: a titolo di esempio distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e di elettricità, umidità, corto circuito, caduta accidentale, eventi catastrofici/incendi, ecc.
- Malfunzionamenti Software: ad esempio esecuzione di uno script automatico non autorizzato; errori di programmazione che causano output errati, ecc.
- Visibilità errata di dati sul sito web dell'Ente: ad esempio visibilità di dati di altri utenti anche per casi di omonimia.
- Fornitura dati a persona diversa dall'interessato: a titolo di esempio comunicazioni di dati di interessati a destinatari errati; gestione di informazioni avanzate da persone diverse dal Titolare o suo delegato;
- Guasti alla rete: a titolo di esempio caduta delle comunicazioni durante il trasferimento di dati e perdita di dati durante la trasmissione, ecc.

b) Eventi dolosi: eventi dolosi causati da personale interno o soggetti esterni realizzati tramite: accesso non autorizzato ai dati con lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione; compromissione o rivelazione abusiva di credenziali di autenticazione; utilizzo di software malevolo. In tale casistica rientrano gli incidenti di sicurezza ICT che comportano la violazione dei dati personali quali:

- Furto: furto di supporti di memorizzazione e/o elaborazione contenenti dati personali dei clienti;
- Truffa informatica esterna: tutti i casi di frodi realizzate da un soggetto esterno dell'Ente rivolto a procurare a sé o ad altri un profitto o, comunque, un vantaggio in termini economici, pubblicitari, ideologici/politici, qualora tali frodi causino perdita delle caratteristiche di sicurezza dei dati personali dei soggetti interessati (confidenzialità, integrità o disponibilità) trattati dall'ente o da suoi fornitori. Ad esempio: accesso non autorizzato ed illecito alle basi dati dei sistemi contenenti i dati dei soggetti interessati tramite sfruttamento di vulnerabilità dei sistemi;
- appropriazione dei dati di carta di credito; appropriazione (e diffusione) delle credenziali di autenticazione ai servizi dei clienti.
- Truffa informatica interna: tutti i casi di frodi realizzate da personale interno all'Ente che comportano la violazione dei dati personali. Tali eventi possono derivare

dall'utilizzo illecito e/o illegittimo delle informazioni a cui un incaricato del trattamento accede anche se autorizzato.

2.3.2 Eventi riguardanti trattamenti cartacei

a) Eventi accidentali: Eventi anomali causati nell'ambito dei trattamenti non automatizzati effettuati su archivi cartacei dei dati personali dei clienti dell'ente quali:

- Distruzione accidentale di documenti: ad esempio incendio/ allagamento dei locali dove sono presenti archivi cartacei, causati da eventi fortuiti e non dolosi presso le sedi dell'ente e dei locali, degli outsourcers di archiviazione contratti, dei collaboratori cessati dai quali si attende la restituzione della documentazione contrattuale;
- Distruzione per errore di documenti originali, senza eventuale copia, da parte di dipendenti interni, di collaboratori esterni;
- Smarrimento di documenti: ad esempio perdita di documenti contenenti dati dei cittadini, degli outsourcers (es. archiviazione contratti).
- Fornitura involontaria di dati a persona diversa dal contraente: ad esempio invio lettera ad Ente senza mandato, gestione ed evasione reclami/richieste di informazioni avanzate da persone diverse dal titolare della linea non delegato, comunicazione di dati dal subentrato al subentrante e viceversa, invio/visualizzazione di fatture a soggetti diversi dagli autorizzati.

b) Eventi dolosi: Comportamenti dolosi da parte di personale interno o soggetti esterni realizzati, attraverso accessi non autorizzati, nell'ambito di trattamenti effettuati su archivi cartacei di dati personali del Comune quali:

- Distruzione dolosa dei documenti: ad esempio incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati dell'utenza; accesso non autorizzato da parte di terzi ad archivi interni della Società e distruzione volontaria di documenti contenenti dati dell'utenza.
- Accesso non autorizzato: ad esempio accesso non autorizzato da parte di personale interno o soggetti esterni, con lettura e/o copia dei documenti, ad archivi documentali presso le sedi dell'ente, dei collaboratori esterni. Non si verifica violazione se si ha la ragionevole certezza che non vi è stata lettura o copia dei documenti contenenti dati degli interessati.
- Furto (cartacei): Furto da parte di personale interno o soggetti esterni (o non identificati) di documenti cartacei contenenti dati dei soggetti interessati.

3. Notifica della violazione all'autorità di controllo

3.1 Quando è richiesta la notifica

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 la valutazione della violazione non evidenzi rischi per i diritti e le libertà delle persone fisiche.

Il titolare del trattamento viene considerato "a conoscenza" della violazione nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione di dati personali.

Nei casi in cui la violazione non sia evidente e chiara il titolare è tenuto ad attivare tempestivamente le indagini finalizzate a valutare se l'incidente abbia causato una effettiva violazione di dati personali, ad adottare le dovute misure correttive e ad effettuare la notifica, se ritenuta necessaria.

La notifica all'autorità di controllo effettuata oltre le 72 ore, deve essere corredata dai motivi del ritardo.

Ogni singola violazione costituisce un incidente segnalabile con rispettiva notifica; fa eccezione il caso della notifica "cumulativa" da utilizzare in presenza di violazioni multiple riguardanti il medesimo tipo di dati personali violati nel medesimo modo ed in un lasso di tempo relativamente breve.

Contrariamente, diverse violazioni riguardanti tipi diversi di dati personali, violati in maniere diverse, costituiscono separate notifiche per ogni violazione conformemente all'articolo 33.
L'articolo 33, paragrafo 4, afferma che *"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*

Il titolare quindi, a seconda della natura e delle complessità della violazione, può effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente.
In questi casi il titolare provvede tempestivamente (entro le 72 ore) alla notifica all'autorità riservandosi di fornire informazioni supplementari in un secondo momento, si procede pertanto ad una notifica per fasi.

Se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il titolare del trattamento informa l'autorità di controllo.

L'incidente, in questo caso, viene registrato come un evento che non costituisce una violazione.

3.2. Quando non è richiesta la notifica

Quando dalla valutazione risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche il titolare non procede né alla notifica all'autorità di controllo né ad informare la persona interessata.

Nel caso in cui lo stato di assenza di un rischio probabile ai diritti ed alle libertà delle persone fisiche cambi nel corso del tempo si procede alla rivalutazione del rischio al fine di verificare se i nuovi elementi emersi rientrino nell'obbligo di notifica.

4. Contitolari del trattamento

In caso di presenza di contitolari del trattamento, il rispetto agli obblighi di notifica delle violazioni previsti dal GDPR, si fa rinvio agli accordi contrattuali che dovranno obbligatoriamente contenere l'indicazione del titolare responsabile delle violazioni e della eventuale notifica all'autorità di controllo.

5. Responsabile del trattamento

Il responsabile del trattamento svolge un ruolo importante nel consentire al titolare del trattamento di adempiere ai propri obblighi in materia di notifica delle violazioni.

Il contratto, o altro atto giuridico, che disciplina il rapporto tra il titolare ed il responsabile del trattamento deve contenere la seguente previsione " *Il responsabile del trattamento assiste 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*
Se il responsabile del trattamento viene a conoscenza di una violazione dei dati personali che sta trattando per conto del titolare del trattamento, deve notificarla al titolare del trattamento senza ingiustificato ritardo e comunque non oltre le 24 ore.

La valutazione del rischio derivante dalla violazione spetta al titolare del trattamento nel momento in cui viene a conoscenza della violazione; in capo al responsabile del trattamento insiste esclusivamente l'obbligo di verificare l'esistenza di una violazione e di notificarla tempestivamente al titolare del trattamento nei tempi sopra indicati.

In considerazione del fatto che ai sensi del GDPR la responsabilità legale della notifica rimane sempre in capo al titolare del trattamento, il responsabile del trattamento può effettuare la notifica della violazione per conto del titolare esclusivamente nel caso in cui quest'ultimo gli abbia conferito apposita autorizzazione e/o nel caso in cui tale modalità sia espressamente prevista negli accordi contrattuali tra i due soggetti.

In caso contrario è fatto obbligo al responsabile del trattamento di informare il titolare, nelle modalità e nei tempi di cui sopra, di ogni potenziale evento di *data breach.*
La segnalazione può essere trasmessa via PEC all'indirizzo protocollo@pec.comune.dogliani.cn.it o vi e-mail all'indirizzo protocollo@comune.dogliani.cn.it
Delle seguenti prescrizioni è fatta apposita menzione nel contratto, o altro atto giuridico, che disciplina il rapporto tra il titolare ed il responsabile del trattamento.

6. Responsabile della protezione dati (RPD)

Il Responsabile della Protezione dati (di seguito "RPD") fornisce consulenza e informazioni al titolare del trattamento e/o al responsabile del trattamento in merito alla valutazione della necessità di notificare una violazione. L'RPD coopera inoltre con l'autorità di controllo e funge da punto di contatto per l'autorità di controllo e per gli eventuali interessati.

Il RPD viene informato tempestivamente dell'esistenza di una violazione e viene coinvolto nell'intera gestione delle violazioni, nonché nel processo di notifica.

Il RPD, quindi, svolge un ruolo di assistenza nella prevenzione delle violazioni, fornisce consulenza e monitora il rispetto delle norme durante il processo di gestione della violazione e assiste l'Ente nell'eventualità di successive indagini da parte dell'autorità di controllo.

Il RPD, inoltre, su richiesta del titolare del trattamento, esprime pareri in merito alla struttura, all'impostazione, all'amministrazione ed alla conservazione della documentazione relativa al registro delle violazioni.

7. Contenuti della notifica: informazioni obbligatorie da fornire all'autorità di controllo

La notifica all'autorità di controllo deve obbligatoriamente contenere almeno i seguenti elementi:

- descrizione della natura della violazione dei dati personali (compresi, ove possibile, le categorie e il numero degli interessati (persone fisiche i cui dati personali sono stati oggetto di violazione) e le registrazioni dei dati personali in questione (Le categorie di registrazioni dei dati personali fanno riferimento ai diversi tipi di registrazioni di cui il titolare del trattamento può disporre, quali dati sanitari, registri didattici, informazioni sull'assistenza sociale, dettagli finanziari, numeri di conti bancari, numeri di passaporto, ecc.) ;
- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o da adottare 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.

L'impossibilità da parte del titolare di disporre di informazioni precise (ad esempio il numero esatto di interessati coinvolti) non costituisce un ostacolo alla notifica tempestiva delle violazioni; in questo caso la comunicazione deve contenere un'approssimazione sul numero di persone fisiche interessate e di registrazioni dei dati personali coinvolte.

Le informazioni sopra indicate costituiscono il contenuto minimo della notifica, è facoltà del titolare del trattamento, qualora lo ritenga necessario, fornire ulteriori informazioni.

8. Comunicazione all'interessato

Ai sensi dell'articolo 34, paragrafo 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".*

8.1 Contenuto della comunicazione

La comunicazione di una violazione agli interessati deve avvenire senza ingiustificato ritardo e, deve descrivere con un linguaggio semplice, chiaro e trasparente la natura della violazione dei dati personali e deve contenere obbligatoriamente i seguenti contenuti minimi:

- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

8.2 Modalità della comunicazione

La violazione va comunicata direttamente agli interessati coinvolti.

Nel caso la comunicazione diretta non risulta percorribile si procede ad una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c); la misura più efficace, valutata la fattispecie concreta, viene stabilita dal titolare.

Il titolare, può contattare l'autorità di controllo per chiedere indicazioni ed orientamenti in merito all'opportunità di informare gli interessati sulla violazione ai sensi dell'articolo 34, ma anche sui messaggi appropriati da inviare loro e sul modo più opportuno per contattarli. Qualora il titolare non sia in possesso di dati sufficienti per contattare l'interessato procede ad informarlo non appena sia ragionevolmente possibile (ad esempio può accadere che il titolare entra in possesso di dati necessari per contattare l'interessato nel momento in cui lo stesso esercita il proprio diritto di accesso ai dati ai sensi dell'articolo 15).

8.3 Quando la comunicazione non deve essere effettuata

La comunicazione agli interessati in caso di violazione dei dati non deve essere effettuata, ai sensi dell'articolo 34 paragrafo 3, se si verifica una delle seguenti tre condizioni:

- Il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione tali rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (es. cifratura);
- Subito dopo la violazione il titolare ha adottato una serie di misure che rendano improbabile l'elevato rischio posto ai diritti e alle libertà delle persone fisiche (es. l'immediata azione nei confronti del soggetto che ha avuto accesso ai dati personali in modo da inibirne qualsiasi utilizzo);
- Contattare gli interessati richiede uno sforzo sproporzionato. In tale circostanza il titolare provvede ad effettuare una comunicazione pubblica o individua una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace.

Seppure la violazione inizialmente non rilevi necessità di una comunicazione all'interessato per l'assenza di rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe nel tempo subire delle variazioni, pertanto il titolare rivaluta il rischio e provvede all'eventuale comunicazione nelle modalità di cui sopra.

8.4 Quando la comunicazione va sempre effettuata

Il titolare provvede in qualunque caso alla comunicazione nel caso in cui questa venga richiesta direttamente all'autorità di controllo al fine di evitare da parte della stessa l'esercizio dei poteri sanzionatori.

9. Valutazione del rischio

Non appena il titolare del trattamento viene a conoscenza di una violazione oltre a mettere in campo tutte le azioni necessarie a contenere l'incidente, valuta anche il rischio che potrebbe derivarne.

Il rischio viene valutato in base a criteri oggettivi; i Considerando 75 e 76 del Regolamento UE 2016/679 stabiliscono che la valutazione deve tenere conto della probabilità e della gravità del rischio per i diritti e le libertà degli interessati.

La valutazione del rischio per i diritti e le libertà delle persone fisiche a seguito di una violazione esamina il rischio in maniera diversa rispetto alla valutazione d'impatto sulla protezione dei dati (DPIA). La valutazione di impatto prende in considerazione infatti un evento ipotetico; nel caso invece di una violazione effettiva, l'evento si è già verificato, quindi l'attenzione va concentrata esclusivamente sul rischio risultante dell'impatto di tale violazione sulle persone fisiche.

La valutazione viene effettuata tenendo conto dei seguenti criteri:

- Tipo di violazione: valutare se la violazione può influire sul livello di rischio per persone fisiche;
- Natura, carattere sensibile e volume dei dati personali: valutare il carattere, il tipo ed il volume dei dati violati.
- Facilità di identificazione delle persone fisiche: valutare la facilità con cui un soggetto che può accedere a dati personali compromessi riesce a identificare persone specifiche o ad abbinare i dati con altre informazioni per identificare persone fisiche.
- Gravità delle conseguenze per le persone fisiche: valutare il grado di gravità del danno potenziale che la violazione potrebbe creare alle persone.
- Caratteristiche particolari dell'interessato: valutare attentamente se la violazione riguardi dati personali relativi a minori o ad altre persone fisiche vulnerabili che possono essere soggette a un rischio più elevato di danno.
- Caratteristiche particolari del titolare del trattamento di dati: valutare la natura e il ruolo del titolare del trattamento e delle sue attività che possono influire sul livello di rischio per le persone fisiche in seguito a una violazione.
- Numero di persone fisiche interessate : valutare il numero di persone fisiche coinvolte nella violazione.

10. Registro delle violazioni

E' istituito un registro interno delle violazioni dove vengono annotate sia le violazioni non notificabili che quelle notificabili.

In ossequio al principio di responsabilizzazione di cui all'articolo 5 paragrafo 2, il titolare del trattamento conserva la documentazione di tutte le violazioni come stabilito all'articolo 33, paragrafo 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 ".*

Il registro deve contenere i seguenti dati:

- i dettagli relativi alla violazione (cause, fatti e dati personali interessati);
- gli effetti e le conseguenze della violazione;
- i provvedimenti adottati per porvi rimedio;
- il ragionamento alla base delle decisioni prese in risposta a una violazione (con particolare riferimento alle violazioni non notificate ed alle violazioni notificate con ritardo);

Il titolare conserva la documentazione in conformità dell'articolo 33, paragrafo 5, anche al fine di poter fornire prontamente le prove dall'autorità di controllo in caso di suo intervento.

Il titolare del Trattamento
Comune di Dogliani

Si allega : Modello del Garante perla Protezione dei Dati personali per la notifica delle violazioni dei dati personali (*data breach*)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI – MODELLO DI NOTIFICA AL GARANTE

I titolari di trattamento di dati personali sono tenuti a notificare al Garante le violazioni dei dati personali (*data breach*) che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modificazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, anche nell'ambito delle comunicazioni elettroniche, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati.

La notifica non deve includere i dati personali oggetto di violazione (es. non fornire i nomi dei soggetti interessati dalla violazione).
Si ricorda 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), salvo che il fatto non costituisca più grave reato.

GARANTE
PER LA PROTEZIONE
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)

Tipo di notifica

○ Preliminare[1] ○ Completa ◉ Integrativa [2] rif.

Effettuata ai sensi del ◉ art. 33 RGPD ○ art. 26 d.lgs 51/2018

Sez. A - Dati del soggetto che effettua la notifica

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B - Titolare del trattamento

Denominazione[3]:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Stato:
Indirizzo:
CAP : Città: Provincia:
Telefono:
E-mail:
PEC:

1 Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione con riserva di effettuare una successiva notifica integrativa. E' obbligatoria la compilazione delle sezioni A, B, B1 e C.
2 Il titolare del trattamento integra una precedente notifica (inserire il numero di fascicolo assegnato alla precedente notifica, se noto)
3 Indicare nome e cognome nel caso di persona fisica

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Sez. B1- Dati di contatto per informazioni relative alla violazione

Indicare i riferimenti del soggetto da contattare per ottenere maggiori informazioni circa la violazione

◉ Responsabile della protezione dei dati[4] - prot. n.

○ Altro soggetto[5]

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B2- Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare o responsabile del trattamento[6], rappresentante del titolare non stabilito nell'Ue)

Denominazione[7] *:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile ○ Rappresentante

Denominazione *: ……..……..……..
Codice Fiscale/P.IVA: ……..……..… Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: ……..……..……..
Codice Fiscale/P.IVA: ……..……..… Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: ……..……..……..
Codice Fiscale/P.IVA: ……..……..… Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

[4] Qualora designato, indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD
[5] In assenza di un RPD, indicare i riferimenti di un punto di contatto designato per la notifica in questione
[6] In tale tipologia rientra anche il Responsabile individuato ai sensi art. 28, par. 4
[7] Indicare nome e cognome nel caso di persona fisica

Sez. C - Informazioni di sintesi sulla violazione

1. **Indicare quando è avvenuta la violazione**
   - (•) Il
   - ( ) Dal (la violazione è ancora in corso)
   - ( ) Dal al
   - ( ) In un tempo non ancora determinato

   Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. **Momento in cui il titolare del trattamento è venuto a conoscenza della violazione**
   Data: Ora:

3. **Modalità con la quale il titolare del trattamento è venuto a conoscenza della violazione**
   - ( ) Il titolare è stato informato dal responsabile del trattamento
   - ( ) Altro[8]

4. **In caso di notifica oltre le 72 ore, quali sono i motivi del ritardo?[9]**

5. **Breve descrizione della violazione**

[8] Ad esempio: Segnalazione da parte di un interessato, comunicazione da parte di terzi, ecc.

[9] Da compilare solo per notifiche tardive.

6. **Natura della violazione**
   - ☐ a) Perdita di confidenzialità[10]
   - ☐ b) Perdita di integrità[11]
   - ☐ c) Perdita di disponibilità[12]

7. **Causa della violazione**
   - ☐ Azione intenzionale interna
   - ☐ Azione accidentale interna
   - ☐ Azione intenzionale esterna
   - ☐ Azione accidentale esterna
   - ☐ Sconosciuta
   - ☐ Altro (specificare)

8. **Categorie di dati personali oggetto di violazione**
   - ☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
   - ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
   - ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…)
   - ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
   - ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
   - ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
   - ☐ Dati di profilazione
   - ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
   - ☐ Dati di localizzazione
   - ☐ Dati che rivelino l'origine razziale o etnica
   - ☐ Dati che rivelino opinioni politiche
   - ☐ Dati che rivelino convinzioni religiose o filosofiche
   - ☐ Dati che rivelino l'appartenenza sindacale
   - ☐ Dati relativi alla vita sessuale o all'orientamento sessuale
   - ☐ Dati relativi alla salute
   - ☐ Dati genetici
   - ☐ Dati biometrici
   - ☐ Categorie ancora non determinate
   - ☐ Altro

[10] Diffusione/ accesso non autorizzato o accidentale
[11] Modifica non autorizzata o accidentale
[12] Impossibilità di accesso,perdita, distruzione non autorizzata o accidentale

9. Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione[13]

- ◯ N.
- ◯ Circa n.
- ◯ Un numero (ancora) non definito di dati

10. Categorie di interessati coinvolti nella violazione

- ☐ Dipendenti/Consulenti
- ☐ Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
- ☐ Associati,soci, aderenti, simpatizzanti, sostenitori
- ☐ Soggetti che ricoprono cariche sociali
- ☐ Beneficiari o assistiti
- ☐ Pazienti
- ☐ Minori
- ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
- ☐ Categorie ancora non determinate
- ☐ Altro (specificare)

☐ Ulteriori dettagli circa le categorie di interessati

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

- ◯ N. interessati
- ◯ Circa n. interessati
- ◯ Un numero (ancora) sconosciuto di interessati

[13] Ad esempio numero di referti, numero di record di un database, numero di transazioni registrate.

Sez. D - Informazioni di dettaglio sulla violazione

1. **Descrizione dell'incidente di sicurezza alla base della violazione**[14]

2. **Descrizione delle categorie di dati personali oggetto della violazione**[15]

3. **Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione**

4. **Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti**[16]

[14] Segue punto 5, 6 e 7 della sez. C
[15] Segue punto 8 della sez. C
[16] Indicare le misure in essere al momento della violazione

Sez. E - Possibili conseguenze e gravità della violazione

1. Possibili conseguenze della violazione sugli interessati

a) In caso di perdita di confidenzialità: [17]

☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
☐ Altro (specificare)

b) In caso di perdita di integrità:[18]

☐ I dati sono stati modificati e resi inconsistenti
☐ I dati sono stati modificati mantenendo la consistenza
☐ Altro (specificare)

c) In caso di perdita di disponibilità:[19]

☐ Mancato accesso a servizi
☐ Malfunzionamento e difficoltà nell'utilizzo di servizi
☐ Altro (specificare)

Ulteriori considerazioni sulle possibili conseguenze

[17] Da compilare solo nel caso in cui è stata selezionata l'opzione a) del punto 6, Sez. C
[18] Da compilare solo nel caso in cui è stata selezionata l'opzione b) del punto 6, Sez. C
[19] Da compilare solo nel caso in cui è stata selezionata l'opzione c) del punto 6, Sez. C

2. Potenziali effetti negativi per gli interessati

☐ Perdita del controllo dei dati personali
☐ Limitazione dei diritti
☐ Discriminazione
☐ Furto o usurpazione d'identità
☐ Frodi
☐ Perdite finanziarie
☐ Decifratura non autorizzata della pseudonimizzazione
☐ Pregiudizio alla reputazione
☐ Perdita di riservatezza dei dati personali protetti da segreto professionale
☐ Conoscenza da parte di terzi non autorizzati
Qualsiasi altro danno economico o sociale significativo (specificare)

3. Stima della gravità della violazione

○ Trascurabile
○ Basso
○ Medio
○ Alto

Indicare le motivazioni

Sez. F – Misure adottate a seguito della violazione

1. **Misure tecniche e organizzative adottate (o di cui si propone l'adozione[20]) 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) per prevenire simili violazioni future**

[20] Nella descrizione distinguere le misure adottate da quelle in corso di adozione

Sez. G - Comunicazione agli interessati

1. La violazione è stata comunicata agli interessati?

- ◯ Sì, è stata comunicata il
- ◯ No, sarà comunicata il
  in una data da definire
- ◯ No, sono tuttora in corso le dovute valutazioni[21]
- ◉ No e non sarà comunicata perché:

a) il titolare del trattamento ritiene che la violazione dei dati personali non presenti un rischio elevato per i diritti e le libertà delle persone fisiche;
Spiegare le motivazioni

b) 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;

Descrivere le misure applicate

■ c) 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;

Descrivere le misure adottate

d) detta comunicazione richiederebbe sforzi sproporzionati.
Descrivere la modalità (comunicazione pubblica o misura simile) tramite la quale gli interessati sono stati informati

[21] Selezionando questa opzione, il titolare del trattamento si impegna a effettuare una integrazione alla presente notifica

2. **Numero di interessati a cui è stata comunicata la violazione**[22]

   N. interessati

3. **Contenuto della comunicazione agli interessati**

4. **Canale utilizzato per la comunicazione agli interessati**
   - ☐ SMS
   - ☐ Posta cartacea
   - ☐ Posta elettronica
   - ☐ Altro (specificare)

[22] Da compilare solo nel caso in cui al punto 1 venga scelta una delle prime due opzioni.

Sez. H - Altre informazioni

1. **La violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo[23]?**

   ◉ SI (indicare quali):

   ○ NO

2. **La violazione coinvolge interessati di Paesi non appartenenti allo Spazio Economico Europeo?**

   ○ SI (indicare quali):

   ○ NO

3. **La violazione è stata notificata ad altre autorità di controllo[24]?**

   ○ SI (indicare quali):

   ○ NO

4. **La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[25]?**

   ○ SI (indicare quali):

   ○ NO

5. **E' stata effettuata una segnalazione all'autorità giudiziaria o di polizia?**

   ○ SI
   ○ NO

[23] Fanno parte dello Spazio Economico Europeo tutti gli Stati membri della Unione Europea, nonchè l'Islanda, il Liechtenstein e la Norvegia
[24] Autorità di controllo così come definite ex art. 51 del Regolamento (UE) 2016/679
[25] Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Garante per la protezione dei dati personali, in qualità di titolare del trattamento (con sede in Piazza Venezia 11, IT-00187, Roma; Email: protocollo@gpdp.it; PEC: protocollo@pec.gpdp.it; Centralino: +39 06696771), tratterà i dati personali conferiti con il presente modulo, con modalità prevalentemente informatiche e telematiche, per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri attribuiti al Garante dalla disciplina vigente.

Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio e la loro mancata indicazione non consente di ritenere adempiuto il dovere di notificazione della violazione all'autorità di controllo. I dati acquisiti nell'ambito della procedura saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa.

I dati saranno trattati esclusivamente dal personale e da collaboratori del Garante o delle imprese espressamente designate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

Gli interessati hanno il diritto di ottenere dal Garante, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati presso il Garante (Garante per la protezione dei personali - Responsabile della Protezione dei dati personali, Piazza Venezia 11, 00187, Roma, email: rpd@gpdp.it).

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato.