Regolamento UE 2016/679, GDPR: Data Breach - adempimenti

Laura Marengo

Unione Industriale Torino

Laura Marengo Ufficio Legale Unione Industriale Torino

Dati Personali

- **GDPR: art.4 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

Che cos'è una violazione di dati personali, Data Breach?

- GDPR art. 4 12)

«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»

Violazione dei dati personali – data breach

- **RISERVATEZZA**: divulgazione o accesso non autorizzato ai dati personali (accidentale o per negligenza o intenzionale)
- **DISPONIBILITA'**: perdita di dati personali o della possibilità di accesso ad essi (accidentale o per negligenza o intenzionale)
- **INTEGRITA'**: alterazione di dati personali (accidentale o per negligenza o intenzionale)

Sicurezza dei dati

- **Fisica** *(locali, armadi, stampanti, ...)*

- **Logica/organizzativa** *(policy aziendali, accordi di riservatezza, incarichi al trattamento dei dati, istruzioni, formazione...)*

- **Informatica** *(cyber security)*

Sicurezza del trattamento, art. 32 GDPR: misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio à responsabilizzazione del Titolare (accountability)

Esempi di data breach «informatici»
Linee guida WP29

- Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati.

- Un titolare del trattamento subisce un attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati.

- Una società di *hosting* di siti web che funge da responsabile del trattamento individua un errore nel codice che controlla l'autorizzazione dell'utente. A causa di tale vizio, qualsiasi utente può accedere ai dettagli dell'account di qualsiasi altro utente.

- Perdita o furto di un dispositivo contenente dati personali

Quadro normativo Data Breach

- Art. 33 GDPR Notifica di una violazione dei dati personali all'autorità di controllo
- Art. 34 GDPR Comunicazione di una violazione dei dati personali all'interessato
- GDPR Considerando 85, 86, 87 e 88
- Linee Guida Gruppo di lavoro art.29 Garanti europei
- *Obbligo di notifica al Garante era già presente per: settore comunicazioni elettroniche, biometria, dati sanitari inseriti in Dossier e dati comunicati fra PA.*

Notifica al Garante, art. 33 GDPR

- Titolare del trattamento: notifica al Garante violazione dei dati personali 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 *(responsabilizzazione del titolare)*

- Se la notifica non è effettuata entro le 72 ore à deve essere corredata dei motivi del ritardo

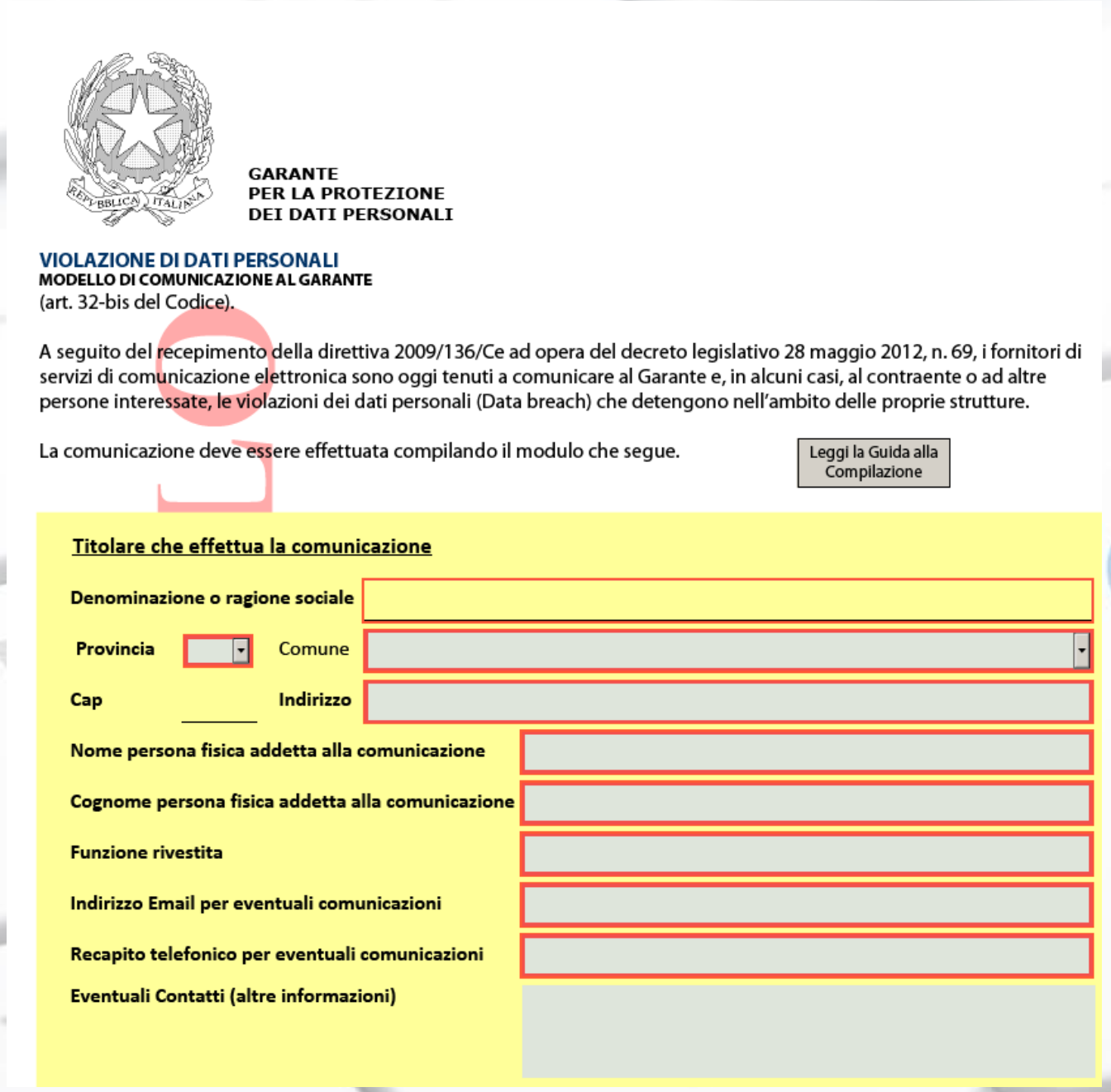
Cosa deve contenere la notifica?

- Descrizione della natura della violazione dei dati, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati in questione

- Il nome e punto di contatto del DPO o di un referente privacy

- Descrizione delle probabili conseguenze della violazione dei dati

- Descrizione delle misure adottate e di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati e anche, se del caso, per attenuarne i possibili effetti negativi



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI
MODELLO DI COMUNICAZIONE AL GARANTE
(art. 32-bis del Codice).

A seguito del recepimento della direttiva 2009/136/Ce ad opera del decreto legislativo 28 maggio 2012, n. 69, i fornitori di servizi di comunicazione elettronica sono oggi tenuti a comunicare al Garante e, in alcuni casi, al contraente o ad altre persone interessate, le violazioni dei dati personali (Data breach) che detengono nell'ambito delle proprie strutture.

La comunicazione deve essere effettuata compilando il modulo che segue.

Leggi la Guida alla Compilazione

Titolare che effettua la comunicazione

Denominazione o ragione sociale

Provincia Comune

Cap **Indirizzo**

Nome persona fisica addetta alla comunicazione

Cognome persona fisica addetta alla comunicazione

Funzione rivestita

Indirizzo Email per eventuali comunicazioni

Recapito telefonico per eventuali comunicazioni

Eventuali Contatti (altre informazioni)

Modello Notifica al Garante

PEC: protocollo@pec.gpdp.it

à Entro 72 ore!

Adempimenti

- alcune informazioni possono essere fornite in fasi successive senza ingiustificato ritardo, se non è possibile fornirle contestualmente alla notifica

- Registro delle violazioni (allegato al registro dei trattamenti): il titolare documenta qualsiasi violazione dei dati. Tale documentazione consente all'autorità di controllo di verificare il rispetto dell'art. 33 GDPR e delle disposizioni del regolamento europeo à importanza strategica per l'accountability

Comunicazione di una violazione dei dati personali all'interessato, art. 34 GDPR

- Quando la violazione 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

- La comunicazione non è richiesta se è soddisfatta una delle seguenti condizioni:

a) misure tecniche e organizzative adeguate

b) misure atte a scongiurare il sopraggiungere di un rischio elevato per gli interessati

c) detta comunicazione richiederebbe sforzi sproporzionati, in tale caso si procede con una comunicazione pubblica o misura analoga

Il Garante può richiedere che venga effettuata la comunicazione

Comunicazione non necessaria

Non è richiesta la comunicazione se:

a) Il titolare ha messo in atto misure adeguate ai dati oggetto della violazione, es. cifratura;

b) Il titolare adotta successivamente misure atte a scongiurare il rischio elevato per gli interessati

c) La comunicazione richiederebbe sforzi sproporzionati (interessati dalla violazione su larga scala) à comunicazione pubblica

Esempi

- L'indisponibilità, anche solo temporanea, di dati sanitari di pazienti di una clinica potrebbe presentare un rischio per i diritti e le libertà delle persone interessate, poiché, ad es., potrebbe comportare l'annullamento di operazioni o di analisi e mettere a rischio le vite dei pazienti.

- Viceversa, se i sistemi di una società di comunicazione non sono temporaneamente disponibili e tale società non riesce a inviare newsletter, è improbabile che ciò presenti un rischio per i diritti e le libertà delle persone fisiche.

Esempi

- Una violazione che non richiederebbe neanche la notifica al Garante sarebbe la perdita di un dispositivo mobile crittografato in maniera sicura. Se la chiave di cifratura rimane in possesso del titolare del trattamento e non si tratta dell'unica copia dei dati personali, questi ultimi sarebbero inaccessibili a qualsiasi pirata informatico. Ciò significa che è improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati in questione. Ma se in seguito diventa evidente che la chiave di cifratura è stata compromessa o che l'algoritmo è vulnerabile, il rischio per i diritti e le libertà delle persone fisiche cambia e potrebbe quindi essere necessaria la notifica.

Protocollo di risposta al Data Breach: Procedure aziendali

- Adottare una policy aziendale per gestire il data breach
- Formare, educare e sensibilizzare il personale
- Prevedere idonee clausole contrattuali nelle designazione dei Responsabili esterni del trattamento (vigilare)
- E naturalmente, alla base di tutto, rispettare l'art. 32 GDPR **Sicurezza del trattamento**

Data Breach Policy esempio

- Organigramma privacy *(trasparenza e chiarezza dei ruoli)*

- Obbligo di comunicare il DB immediatamente (nel più breve tempo possibile) al Privacy Team o al referente/delegato Privacy o al responsabile IT *(dipende dalle organizzazioni)*

- Valutazione dell'accaduto, conformemente al principio di responsabilizzazione del Titolare *(accountability):*

a) è improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche à Registro delle violazioni

b) entro 72 ore Notifica al Garante

c) eventuale comunicazione agli interessati *(non appena ragionevolmente possibile)*

d) Registro delle violazioni

Data Breach Sanzioni

- GDPR art. 83, p. 4: sanzioni amministrative pecuniarie fino a 10.000.000 EUR o fino al 2% del fatturato mondiale totale annuo se superiore

HELP per le imprese

Informazioni per prevenire gli attacchi e/o per eventualmente valutare la gravità dell'attacco e l'impatto che questo potrebbe avere sui trattamenti dei dati effettuati dall' impresa:

Protocollo Unione Industriale - Polizia Postale

Grazie per l'attenzione

Laura Marengo

Laura Marengo Ufficio Legale Unione Industriale Torino