CORSO DI FORMAZIONE PER PROFESSIONISTI DELLA PRIVACY E PRIVACY OFFICERS

Elena Tabet

LA VIOLAZIONE DEI DATI PERSONALI (*Data Breach*)

La violazione dei dati personali

COS'È IL DATA BREACH

(Art. 4 GDPR, definizione 12)
Violazione dei dati personali

«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»

La violazione può essere determinata da accesso abusivo ai sistemi informatici, ovvero da sottrazione o perdita di dati e supporti di memorizzazione.

La violazione dei dati personali

*«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»*

- Ogni DB deve essere considerato come un incidente di sicurezza
- Incidente di sicurezza che riguarda i dati personali trattati
- Violazione comma f dell'art 5 del GDPR

…garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o da danni accidentali («integrità e riservatezza»).

La violazione dei dati personali

Una **violazione dei dati personali** può, se non affrontata in modo adeguato e tempestivo, **provocare danni fisici, materiali o immateriali alle persone fisiche**, ad esempio **perdita del controllo** dei dati personali che li riguardano o **limitazione** dei loro **diritti**, **discriminazione**, **furto** o usurpazione **d'identità**, perdite **finanziarie**, **decifratura** non autorizzata della **pseudonimizzazione**, **pregiudizio** alla reputazione, **perdita** di **riservatezza** dei dati personali protetti da segreto professionale o qualsiasi altro **danno economico** o **sociale** significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il **titolare** del trattamento dovrebbe **notificare** la **violazione** dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro **72 ore** dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo

La violazione dei dati personali

Il **titolare** del trattamento dovrebbe **comunicare all'interessato** la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un **rischio elevato** per i diritti e le libertà della persona fisica, al fine di consentirgli di **prendere** le **precauzioni necessarie**. La comunicazione dovrebbe **descrivere** la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena **ragionevolmente possibile** e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.

La violazione dei dati personali

È opportuno **verificare** se siano state messe in atto tutte le **misure tecnologiche** e **organizzative adeguate** di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato.
È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato.
Siffatta notifica può dar luogo a un intervento **dell'autorità** di **controllo** nell'ambito dei suoi **compiti** e **poteri** previsti dal presente regolamento.

La violazione dei dati personali

Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle **circostanze** di tale **violazione**, ad esempio stabilire se i dati personali fossero o meno protetti con **misure tecniche adeguate** di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.

La violazione dei dati personali

- Concetto preesistente al Regolamento GDPR
- Introdotto nelle norme europee con la Direttiva 136/2009 (*Telecom Package*), applicabile al settore delle comunicazioni elettroniche, che ne prevedeva la futura generalizzazione a tutti gli ambiti
- Il nuovo Regolamento UE estende l'obbligo di notificazione dei *data breach* a qualsiasi settore
  - Autorità di protezione dati nazionale
  - Lead Autorithy
  - Interessato
- Ruolo del Responsabile del trattamento

Considerando

- trattamento dei dati personali degli interessati che si trovano nell'Unione effettuato da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione, quando le attività di trattamento sono connesse all'offerta di beni o servizi indipendentemente dal fatto che vi sia un pagamento correlato.
- l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione possono indicare un'offerta di beni o servizi agli interessati nell'Unione
- la semplice accessibilità del sito web, di un indirizzo di posta elettronica o di altre coordinate di contatto sono insufficienti per accertare tale intenzione

La violazione dei dati personali

- Sanzione ex art 83

- 10 ME – 2% fatturato ww

- Mancata comunicazone/notifica
- Assenza/inadeguatezza di misure di sicurezza adeguate

La violazione dei dati personali

- Principio di responsabilizzazione
  - Titolare e Responsabile devono mettere adeguate misure tecniche e organizzative
  - Ben documentate

- Prevenire la violazione dei dati personali

- Reagire in modo tempestivo

- Comunicare/Notificare

- Obiettivo1: incrementare l'adeguatezza delle misure

- Obiettivo2: proteggere gli individui e i loro dati personali

La violazione dei dati personali

- Confidentiality breach
  - diffusione/accesso accidentale o non autorizzato
- Integrity breach
  - Alterazione accidentale o non autorizzata
- Availability breach
  - Distruzione accidentale o non autorizzata/indisponibilità del dato personale

Obblighi del Titolare

Articolo 33
(Notifica di una violazione dei dati personali all'autorità di controllo)

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.

Attenzione alle clausole da inserire nel contratto fra Titolare e Responsabile

La gestione del data breach

Venire a conoscenza del data breach

La gestione del data breach

Perdita di una chiave USB con dati personali non crittografati

La gestione del data breach

Perdita di una chiave USB con dati personali non crittografati

1. Potrebbe non essere possibile stabilire con certezza se si sia verificata una violazione della riservatezza

2. Sicuramente violazione della disponibilità

3. Venire a conoscenza=sapere della perdita della USB

La gestione del data breach

Qualcuno informa il responsabile del trattamento che ha per errore ricevuto i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata.

La gestione del data breach

Qualcuno informa il responsabile del trattamento che ha per errore ricevuto i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata.

Il Titolare ne viene immediatamente a conoscenza

La gestione del data breach

Un Titolare rileva che c'è stata una possibile intrusione nella sua rete e rileva che i dati personali presenti sono stati compromessi

La gestione del data breach

Un Titolare rileva che c'è stata una possibile intrusione nella sua rete e rileva che i dati personali presenti sono stati compromessi

Il Titolare ne viene immediatamente a conoscenza

La gestione del data breach

Un hacker contatta il Titolare dicendo di aver hackerato il suo sistema per chiedere un riscatto.

Il Titolare ne viene immediatamente a conoscenza, dopo aver effettuato le verifiche

La gestione dei data breach

CONTENUTO DELLA NOTIFICA DI DATA BREACH

La notifica

a) descrive 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) comunica 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) descrive le probabili conseguenze della violazione dei dati personali;
d) descrive 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.

La gestione dei data breach

CONTENUTO DELLA NOTIFICA DI DATA BREACH

Categorie di interessati

Categorie di dati personali violati

Conseguenze

Misure adottate

La gestione dei data breach

ALTRI ADEMPIMENTI CONNESSI ALLE VIOLAZIONI DEI DATI

- 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 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.

La gestione dei data breach

OBBLIGHI DEL TITOLARE IN CASO DI DATA BREACH

Articolo 34 (Comunicazione di una violazione dei dati personali all'interessato)

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).

La gestione dei data breach

QUANDO NON È RICHIESTA LA COMUNICAZIONE

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;
   c) la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

La gestione dei data breach

VALUTAZIONE DEL GARANTE

- Se il titolare del trattamento non ha ancora comunicato all'interessato la violazione dei dati personali

- l'autorità di controllo valuta la probabilità che la violazione dei dati personali presenti un rischio elevato
  - può richiedere che vi provveda
  - può decidere che una delle condizioni è soddisfatta

La gestione del data breach

a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche

Valutazione del potenziale rischio che potrebbe derivare da una violazione nell'ambito di una DPIA

Valutazione del rischio

- Quando un di trattamento presenta un rischio elevato per i diritti e le libertà delle persone fisiche
  - considerati la natura, l'oggetto, il contesto e le finalità del trattamento
  - prevede in particolare l'uso di nuove tecnologie
- il titolare del trattamento deve effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali
- Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi
- Prima di procedere al trattamento

Rischio - valutazione

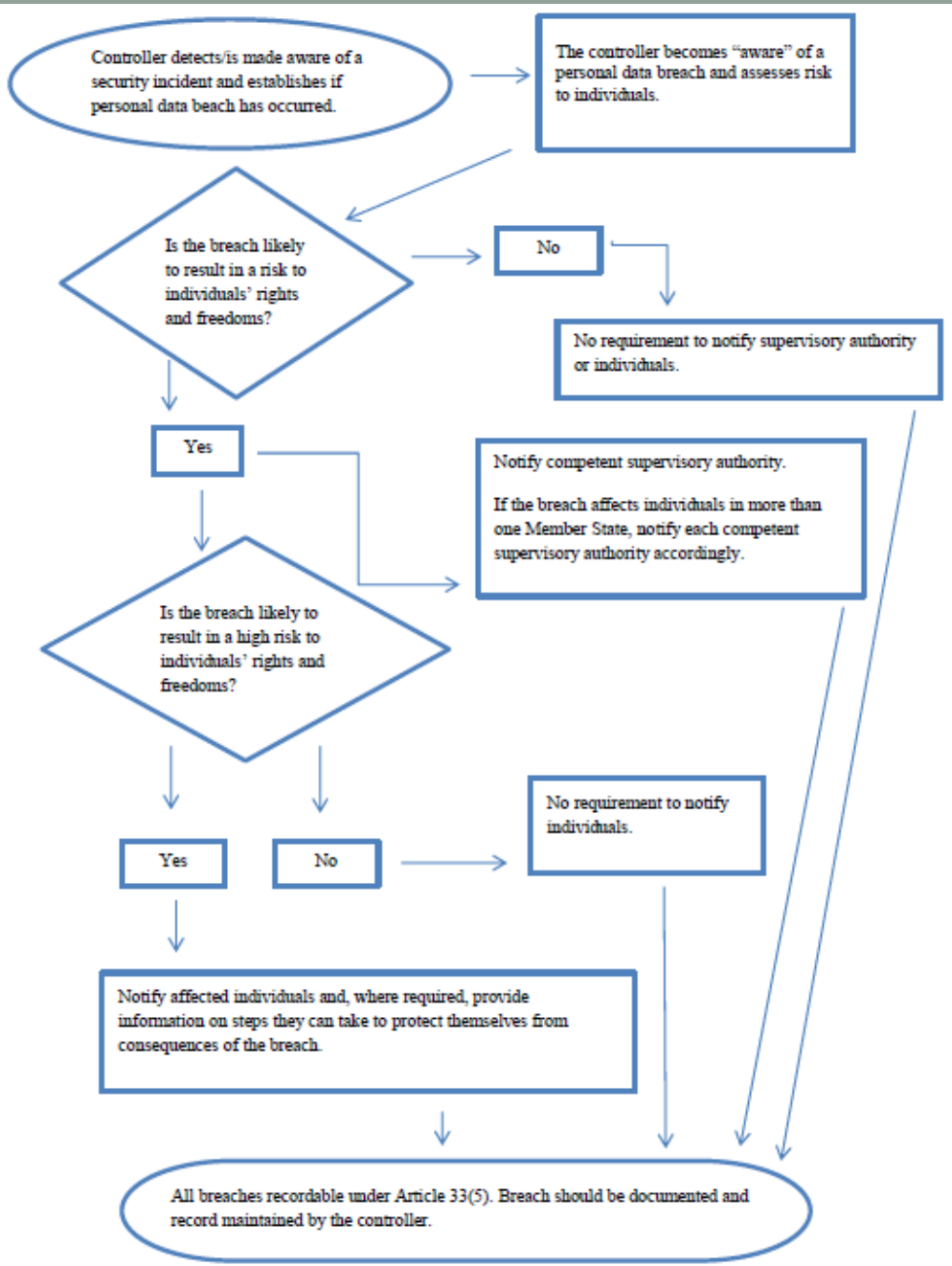
- è la potenzialità che un'azione o un'attività scelta porti a un danno (una perdita o ad un evento indesiderabile)
- non agire è un’azione
- Rischio= P x D
- P= probabilità che un certo evento accada
- D= danno conseguente
- Valutazione del rischio= determinazione quantitativa o qualitativa del rischio associato ad una situazione ben definita e ad una minaccia conosciuta allo scopo di scegliere le adeguate misure di sicurezza
- individuare tutte le circostanze che possono arrecare danno
- stimare la probabilità e gravità del potenziale danno

Analisi dei rischi e valutazione d'impatto privacy

- Data protection impact assessment PIA/DPIA
- Elemento chiave del principio di responsabilizzazione (accountability) di titolari e responsabili
  - adozione di comportamenti virtuosi e proattivi
  - dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento
  - documentare le misure e gli accorgimenti adottati
- Il titolare ha l'onere di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali
- In osservanza alle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento

DPIA – quando

- Sempre per i trattamenti che prevedono:
  - una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
  - il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1,
  - il trattamento, su larga scala di dati relativi a condanne penali e a reati;
  - la sorveglianza sistematica su larga scala di una zona accessibile al pubblico
- In casi decisi dall'Autorità, che deve rendere pubblico l' elenco delle tipologie di trattamenti soggetti al requisito della DPIA
- Il titolare deve valutare nuovamente quando variano le condizioni di rischio
- Il titolare può decidere di non predisporre la DPIA:
  - Relazione che giustifica il motivo
  - Comprensiva del parere del DPO


Controller detects/is made aware of a security incident and establishes if personal data beach has occurred.
The controller becomes "aware" of a personal data breach and assesses risk to individuals.
Is the breach likely to result in a risk to individuals' rights and freedoms?
No
No requirement to notify supervisory authority or individuals.
Yes
Notify competent supervisory authority.
If the breach affects individuals in more than one Member State, notify each competent supervisory authority accordingly.
Is the breach likely to result in a high risk to individuals' rights and freedoms?
Yes
No
No requirement to notify individuals.
Notify affected individuals and, where required, provide information on steps they can take to protect themselves from consequences of the breach.
All breaches recordable under Article 33(5). Breach should be documented and record maintained by the controller.

Casi

- Furto di un CD utilizzato per il backup di dati personali criptati
- Furto di dati personali da un sito web che eroga servizi on line
- Interruzione di corrente in un call center, che lo rende indisponibile per una giornata lavorativa
- Attacco tipo ransomware che cifra l'unica copia dei dati di un Titolare
- Attacco tipo ransomware che cifra una copia dei dati di un Titolare
- Alcuni clienti di una banca ricevono l'estratto conto mensile relativo a c/c non intestati a loro

Casi

- Un sito di vendite online subisce un attacco in cui sono rubati nomi utente, password e cronologia degli acquisti che vengono successivamente pubblicati sul web.
- Una società che eroga un servizio di webhosting (in qualità di Responsabile) identifica un errore nel software che controlla i permessi di accesso, tale che ogni utente può accedere ai dettagli dell'account di qualsiasi altro utente.
- Un attacco informatico rende indisponibili i dati dei pazienti di un ospedale per 24 ore
- Un servizio di direct mailing manda messaggi con i riceventi nel campo «A» o «CC»

Grazie

e.tabet@gpdp.it