GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

SME Data

ROMA TRE UNIVERSITÀ DEGLI STUDI
GIURISPRUDENZA
DIPARTIMENTO DI ECCELLENZA 2018-2022

Training Of Trainers

Rischi per i diritti degli interessati: Nozione di "Data Breach" - esempi pratici

Ingg. Fausto Cioffi e Marco Coppotelli

Agenda

Training of Trainers

- **Cos'è un *data breach*?**
- **La gestione di un *data breach***
  - Il rilevamento del *data breach*
  - Il contenimento del *data breach*
  - La valutazione del rischio
  - La notifica del *data breach* al Garante
  - La comunicazione del *data breach* agli interessati
  - La documentazione del *data breach*
- **Il ruolo del responsabile della protezione dei dati**
- **Caso pratico di gestione di un *data breach***
- **Dieci regole per la gestione dei *data breach***
- **Link utili**

Cos'è un data breach? (1)

Training of Trainers

Art. 4, punto 12), del Regolamento

*«**violazione dei dati personali**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati»*

- Una violazione di sicurezza è un qualsiasi evento che può manifestarsi a seguito di un malfunzionamento *hardware* o *software,* di un attacco informatico o di un comportamento umano doloso o accidentale
- Un *data breach* è una violazione di sicurezza che coinvolge dati personali, in seguito al quale il titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali previsti dal Regolamento

Cos'è un *data breach*? (2)

Training of Trainers

Un *data breach* può essere classificato
in base ai tre principi della sicurezza delle informazioni

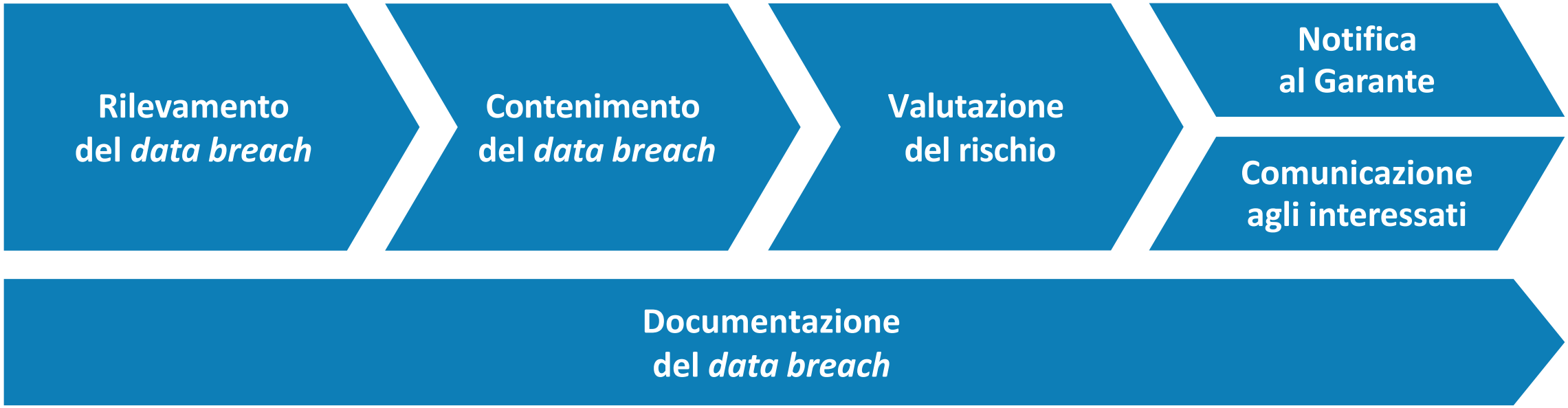
Violazione della disponibilità	Violazione dell'integrità	Violazione della riservatezza
distruzione o perdita non autorizzate di dati personali	*modifica non autorizzata di dati personali*	*divulgazione o accesso non autorizzati a dati personali*

Un *data breach* può anche riguardare contemporaneamente
la riservatezza, l'integrità e la disponibilità dei dati personali,
oppure una combinazione delle stesse

La gestione di un *data breach*

Training of Trainers

Il Regolamento stabilisce una serie di adempimenti che
un titolare del trattamento è chiamato a compiere a seguito di un *data breach*,
anche subordinando i propri interessi economici
e di immagine alla tutela dei dati personali degli interessati



Il rilevamento del *data breach*

Training of Trainers

Cons. 85 del Regolamento

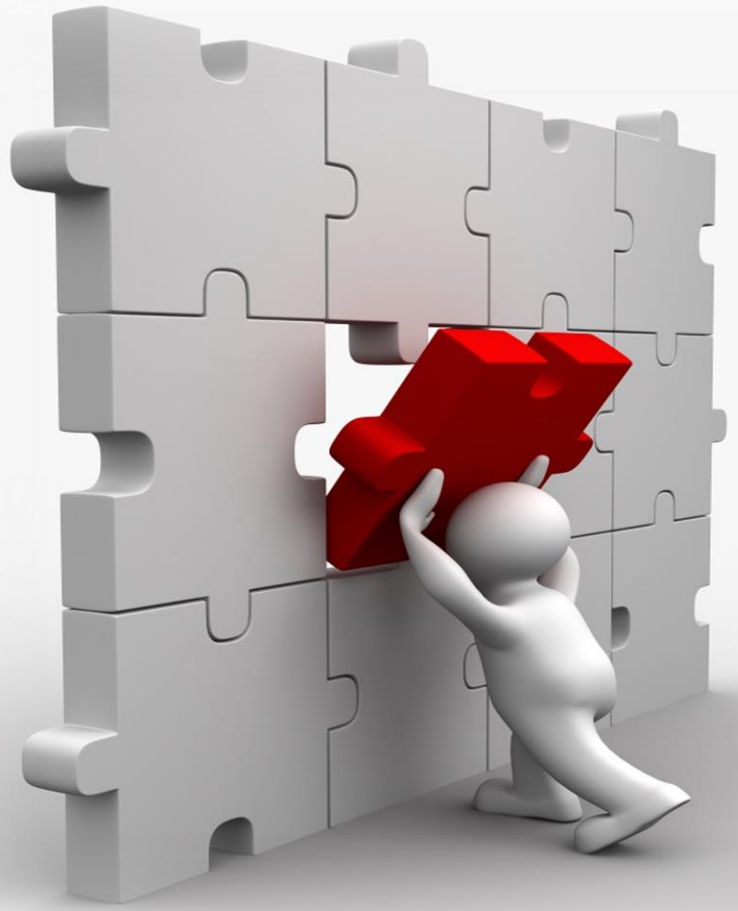
«Una violazione dei dati personali può, ***se non affrontata in modo adeguato e tempestivo****, provocare danni fisici, materiali o immateriali alle persone fisiche* […]*»*

Cons. 87 del Regolamento

«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* […]*»*

- Il Regolamento impone ai titolari e ai responsabili del trattamento di attuare misure tecniche e organizzative necessarie per rilevare immediatamente un *data breach*, ossia per **assicurarsi di venire "a conoscenza" di un *data breach***
- La **capacità di rilevare tempestivamente un *data breach*** è il primo aspetto a cui il titolare del trattamento e il responsabile del trattamento devono rivolgere la loro attenzione

Il contenimento del *data breach*



- Il titolare del trattamento deve predisporre un **piano di risposta agli incidenti di sicurezza**, che gli consenta di rispondere in maniera efficace e ordinata ai *data breach*
- Il piano di risposta agli incidenti di sicurezza dovrebbe essere documentato e dovrebbe includere una lista di **possibili azioni di mitigazione** e una **chiara assegnazione di ruoli e responsabilità**

La valutazione del rischio (1)

Training of Trainers

Cons. 75 del Regolamento

*«I **rischi per i diritti e le libertà delle persone fisiche**, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un **danno fisico, materiale o immateriale** […]»*

Cons. 76 del Regolamento

*«La **probabilità** e la **gravità** del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla **natura**, all'**ambito di applicazione**, al **contesto** e alle **finalità** del trattamento. Il rischio dovrebbe essere considerato in base a una **valutazione oggettiva** mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato»*

I considerando 75 e 76 del Regolamento suggeriscono di valutare il rischio in modo oggettivo, tenendo conto tanto della **probabilità** quanto della **gravità del rischio per i diritti e le libertà delle persone fisiche**

La valutazione del rischio (2)

Training of Trainers

Fattori da considerare nella valutazione del rischio

Le "*Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679*" (WP250 rev.01) individuano alcuni dei fattori da considerare nella valutazione del rischio

Scan me

- **Tipo di violazione**
- **Natura, carattere sensibile e volume dei dati personali**
- **Numero di persone fisiche interessate**
- **Facilità di identificazione delle persone fisiche**
- **Gravità delle conseguenze per le persone fisiche**
- **Caratteristiche particolari dell'interessato**
- **Caratteristiche particolari del titolare del trattamento**

La valutazione del rischio (3)

È PROBABILE CHE CI SIA UN RISCHIO ELEVATO

- Contenimento del *data breach*
- Notifica al Garante
- Comunicazione agli interessati
- Documentazione del *data breach*

È PROBABILE CHE CI SIA UN RISCHIO

- Contenimento del *data breach*
- Notifica al Garante
- Documentazione del *data breach*

È IMPROBABILE CHE CI SIA UN RISCHIO

- Contenimento del *data breach*
- Documentazione del *data breach*

La notifica al Garante (1)

Training of Trainers

Art. 33, par. 1, del Regolamento

«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****»*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

La notifica al Garante (2)

Training of Trainers

Art. 33, par. 3, del Regolamento

«La notifica di cui al paragrafo 1 deve almeno:

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

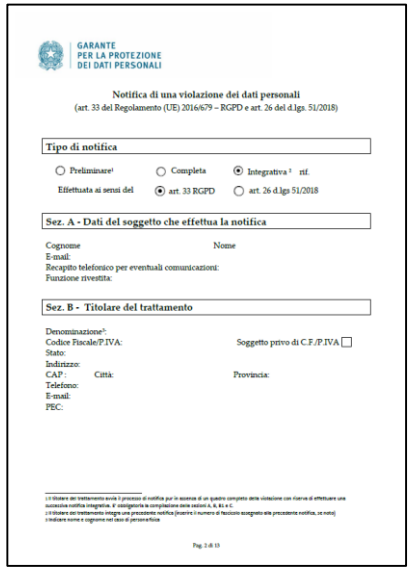
b) *comunicare il **nome** e i **dati di contatto del responsabile della protezione dei dati** o di altro punto di contatto presso cui ottenere più informazioni;*

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

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

Con il Provvedimento n. 157 del 30 luglio 2019, il Garante ha indicato le informazioni da fornire nella notifica di *data breach* ai sensi dell'art. 33 del Regolamento

Scan me


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

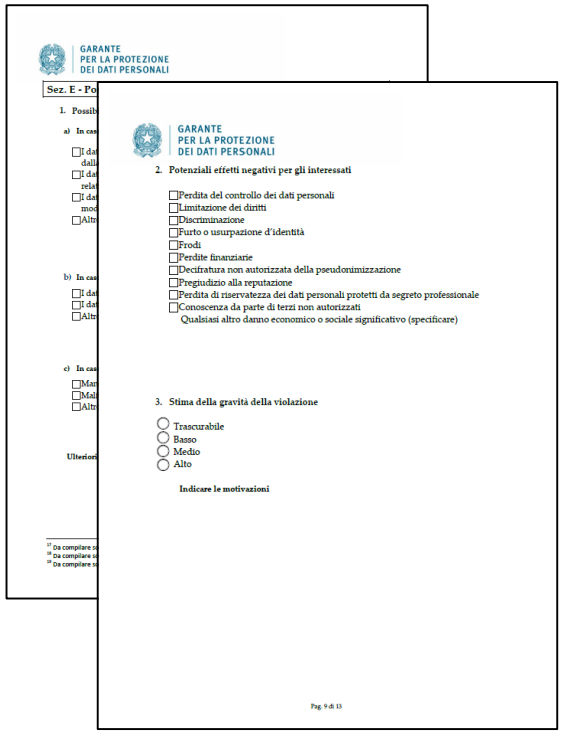
Sez. A - Dati del soggetto che effettua la notifica

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:

La notifica al Garante (3)


GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Sez. E - Po

1. Possib

a) In cas

b) In cas

c) In cas

Ulteriori

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

Pag. 9 di 13

Probabili conseguenze di un *data breach*

- Perdita di controllo sui dati
- Limitazione dei diritti
- Discriminazione
- Furto o usurpazione d'identità
- Perdite finanziarie
- Pregiudizio alla reputazione
- Decifratura non autorizzata della pseudonimizzazione
- Perdita di riservatezza dei dati protetti da segreto professionale
- Qualsiasi altro danno economico o sociale significativo

La notifica al Garante (4)

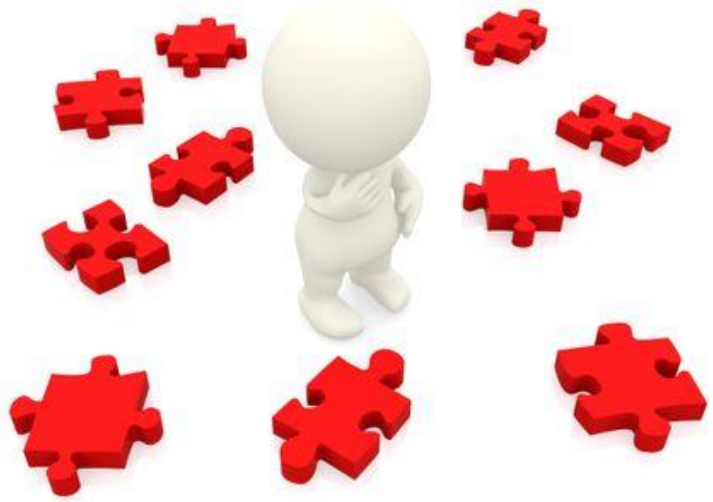
Training of Trainers

Notifica di un *data breach* per fasi

Un titolare del trattamento potrebbe non disporre di tutte le informazioni relative a un *data breach* entro 72 ore dal momento in cui ne è venuto a conoscenza

Art. 33, par. 4, del Regolamento

*«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»*



La comunicazione agli interessati (1)

Training of Trainers

Art. 34, par. 1, del Regolamento

*«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**»*

Cons. 86 del Regolamento

*«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.** […] Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva»*

La comunicazione agli interessati (2)

Training of Trainers

Art. 34, par. 2, del Regolamento

*«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)»*

Cons. 86 del Regolamento

«[…] *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*** […]»

Contenuto della comunicazione

- Descrizione della natura del *data breach*
- Punto di contatto (DPO o altro soggetto)
- Possibili conseguenze della violazione
- Misure adottate, o che si intende adottare, per porre rimedio al *data breach*
- Misure adottate, o che si intende adottare, per attenuare gli effetti negativi del *data breach* per gli interessati
- Indicazioni pratiche sulle misure che gli interessati possono adottare per proteggersi da conseguenze negative

La comunicazione agli interessati (3)

Training of Trainers

L'**obiettivo principale** della comunicazione agli interessati
è quello di fornire loro **informazioni specifiche**
sulle misure che questi possono prendere per proteggersi

Il titolare del trattamento:

- deve individuare il canale di contatto più appropriato per comunicare una violazione agli interessati
- può utilizzare anche diversi canali di contatto, anziché un singolo canale
- deve essere cauto nell'usare un canale di contatto compromesso dalla violazione

La documentazione del *data breach*

Training of Trainers

Art. 33, par. 5, del Regolamento

*«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»*

Contenuto minimo della documentazione

- Dettagli relativi al *data breach*, comprese le cause, il numero e le categorie di interessati, il numero e le categorie di dati personali
- Effetti e conseguenze del *data breach*
- Ragionamenti alla base delle decisioni prese in risposta al *data breach*

Il ruolo del DPO

Training of Trainers

Le “***Linee guida sulla notifica delle violazioni dei dati personali***” indicano alcuni compiti che potrebbero essere assegnati al responsabile della protezione dei dati

Il responsabile della protezione dei dati:

- potrebbe fornire assistenza al titolare del trattamento nella prevenzione e nella gestione dei *data breach*
- potrebbe fornire un parere al titolare del trattamento in merito alla struttura, all’impostazione e alla gestione della documentazione relativa ai *data breach*
- dovrebbe essere informato tempestivamente dell’esistenza di un *data breach*
- dovrebbe essere coinvolto nella gestione dei *data breach* e nel processo di notifica al Garante

Caso pratico di gestione di un *data breach* (1)

Training of Trainers

Valutazione del rischio per i diritti e le libertà degli interessati derivante dal *data breach*

Notifica al Garante e comunicazione agli interessati

Misure tecniche e organizzative per porre rimedio al *data breach*

Misure che avrebbero potuto ridurre il rischio per i diritti e le libertà degli interessati

Caso pratico di gestione di un *data breach* (2)

Training of Trainers

Scenario di riferimento

- Un'Azienda ha realizzato un portale di *e-commerce* a cui sono registrati circa 60.000 utenti
- Un *hacker*, sfruttando una vulnerabilità di tipo *SQL injection*, riesce ad accedere ai dati contenuti nel *database* degli utenti iscritti al servizio
- L'Azienda non si accorge di aver subìto un attacco informatico in quanto non dispone di strumenti per rilevarlo
- Alcune settimane più tardi, l'*hacker* pubblica in rete una parte dei dati che è riuscito a esfiltrare dal *database* del servizio *online*
- Tra i dati oggetto di pubblicazione ci sono il nome, il cognome, l'indirizzo email e la *password* (sotto forma di *hash*) degli utenti
- L'Azienda non ha previsto una scadenza periodica delle *password*
- Le *password* degli utenti sono conservate sotto forma di *hash* MD5

Caso pratico di gestione di un *data breach* (3)

Training of Trainers

Elementi da considerare per la valutazione del rischio

Tipo di violazione	Violazione della riservatezza dei dati causata da un azione intenzionale esterna
Natura, carattere sensibile e volume dei dati personali	Numero elevato di dati personali, tra cui anche credenziali di autenticazione
Numero di persone fisiche interessate	Numero elevato di interessati
Facilità di identificazione delle persone fisiche	I dati personali violati consentono di risalire facilmente all'identità degli interessati
Conseguenze per le persone fisiche	Perdita di controllo da parte degli interessati sui loro dati personali Furto o usurpazione d'identità

Caso pratico di gestione di un *data breach* (4)

Training of Trainers

Valutazione del rischio

È PROBABILE CHE CI SIA UN RISCHIO ELEVATO

Caso pratico di gestione di un *data breach* (5)

Training of Trainers

Notifica al Garante

- L'Azienda dovrà notificare il *data breach* al Garante entro 72 ore dal momento in cui ne è venuta "a conoscenza"

Comunicazione agli interessati

- L'Azienda dovrà informare gli interessati coinvolti nella violazione inviando una comunicazione che includa anche la raccomandazione di non utilizzare più la *password* compromessa né una simile e di provvedere a modificare le *password* di altri servizi online se coincidenti o simili a quella oggetto di violazione

Caso pratico di gestione di un *data breach* (6)

Training of Trainers

Misure per porre rimedio al *data breach*

- Blocco immediato dell'accesso al servizio coinvolto
- Comunicazione tempestiva agli interessati
- Implementazione di una procedura di *reset* delle *password* oggetto di violazione (le caselle e-mail degli interessati potrebbero essere state violate!)
- Risoluzione della vulnerabilità utilizzata dall'*hacker* e ripristino del servizio

Caso pratico di gestione di un *data breach* (7)

Training of Trainers

Misure che avrebbero potuto ridurre il rischio

- Conservazione sicura delle *password*
- Utilizzo di *password* complesse
- Adozione di meccanismi di *strong authentication*
- Utilizzo di *username* diverse dell'*e-mail*
- *Hardening* e *patching* dei sistemi
- *Logging* degli accessi e delle operazioni
- Utilizzo di sistemi di *security information and event management*

Dieci regole per la gestione di un *data breach* (1)

Training of Trainers

5 COSE DA FARE

- Quando si individuano le misure per la sicurezza di un trattamento, considerare i rischi che potrebbero derivare da un eventuale *data breach*
- Effettuare periodicamente *vulnerability assessment* e *patching* dei sistemi
- Trasformare gli utenti da anello debole della catena a prima linea di difesa, incoraggiandoli a segnalare situazioni anomale
- Documentare tutti i ragionamenti che sono alla base delle decisioni prese in risposta a un *data breach*
- Imparare dagli errori propri e degli altri

Dieci regole per la gestione di un *data breach* (2)

Training of Trainers

5 COSE DA NON FARE

- Non aspettare che si verifichi un *data breach* per predisporre procedure efficaci per gestirlo
- Non notificare al Garante tutti i *data breach*, ma solo quelli che presentano rischi per i diritti e le libertà degli interessati
- Quando si verifica un *data breach* non pensare agli impatti per il *business*, ma piuttosto ai possibili effetti negativi per gli interessati
- Non sottovalutare i rischi derivanti da un *data breach*
- Non vedere la comunicazione di un *data breach* agli interessati come un'ammissione di colpa, ma piuttosto come uno strumento di trasparenza nei loro confronti

Link utili

Training of Trainers

SCAN ME

Portale istituzionale del Garante

Sezione dedicata alle violazioni dei dati personali

https://www.gpdp.it/regolamentoue/databreach

Provvedimenti e interventi del Garante

in materia di violazioni dei dati personali

https://www.gpdp.it/home/ricerca/-/search/tipologia/Data%20breach

SCAN ME

SCAN ME

Registro delle decisioni assunte dalle autorità di controllo UE

in relazione a trattamenti transfrontalieri

https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_it

THANKS!