UNIVERSITÀ POLITECNICA DELLE MARCHE

DII Dipartimento di Ingegneria dell'Informazione

unimc

Gestione Data Breach: implicazioni operative e riflessioni sul campo

Loredana Cantarini

Università Politecnica delle Marche

Divisione Qualità Processi e Protezione Dati

l.cantarini@univpm.it

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Sommario

1 Introduzione - Contesto

1. Introduzione – Contesto normativo

Perché la scelta di questo tema?

Data Breach: tema quanto mai attuale che ha assunto un'importanza crescente negli ultimi anni.

- Le statistiche mostrano come il **2021** sia stato un anno particolarmente difficile sul fronte della cybersecurity e della protezione dei dati personali, tanto che nel 2021 **le notifiche di data breach** al Garante sono **aumentate più del 50%** rispetto al 2020.

1. Introduzione – Contesto normativo
Qualche numero

Anno 2021: **n. 2071 notifiche al Garante**

soggetti pubblici (50,5%) – soggetti privati (49,5%)

In particolare, **nel settore pubblico**, le violazioni dei dati personali hanno riguardato soprattutto comuni, istituti scolastici e strutture sanitarie (Asl, Aziende ospedaliere, Policlinici e Irccs);

nel **settore privato**, sono stati invece coinvolti sia piccole e medie imprese e professionisti, sia grandi società del settore delle telecomunicazioni, energetico, bancario e dei servizi.

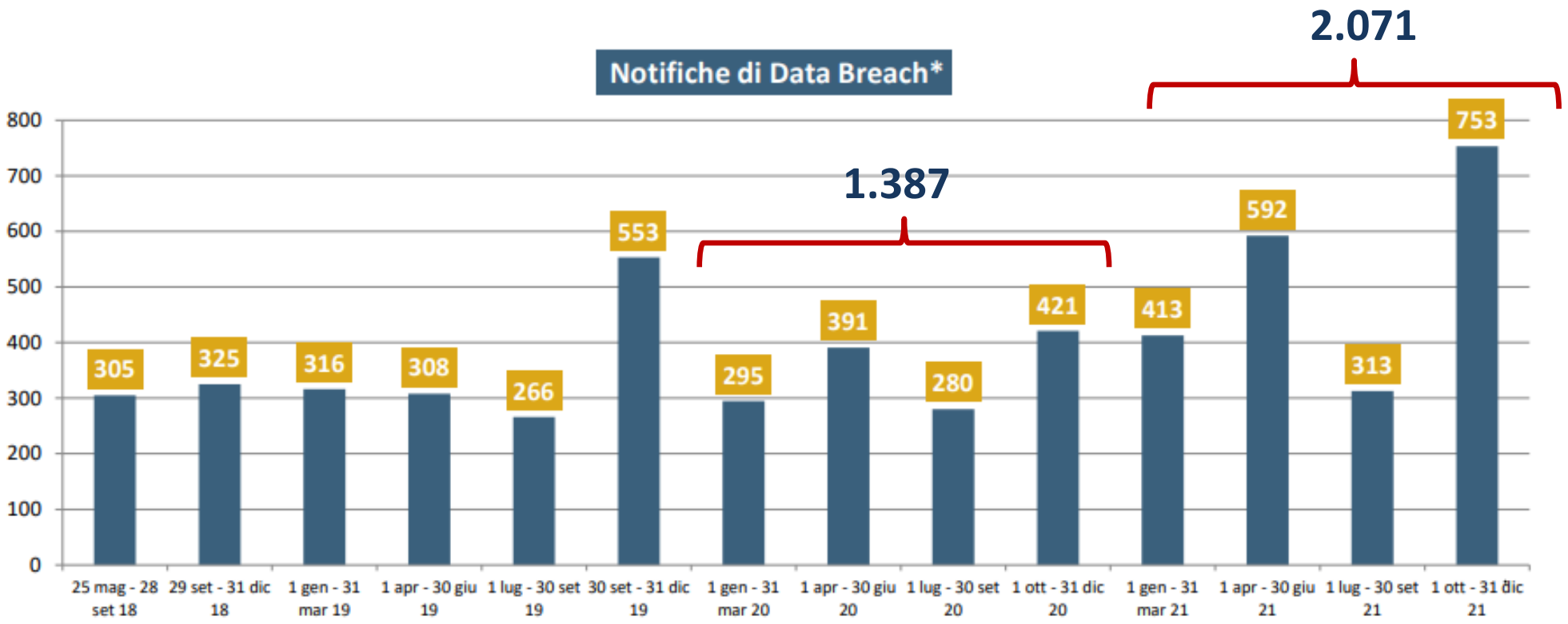
Fonte: Relazione 2022 del Garante per la Protezione dei Dati personali sull'attività svolta nel 2021, Roma 7 luglio 2022

1. Introduzione - Qualche numero

RGDP

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il bilancio dell'applicazione



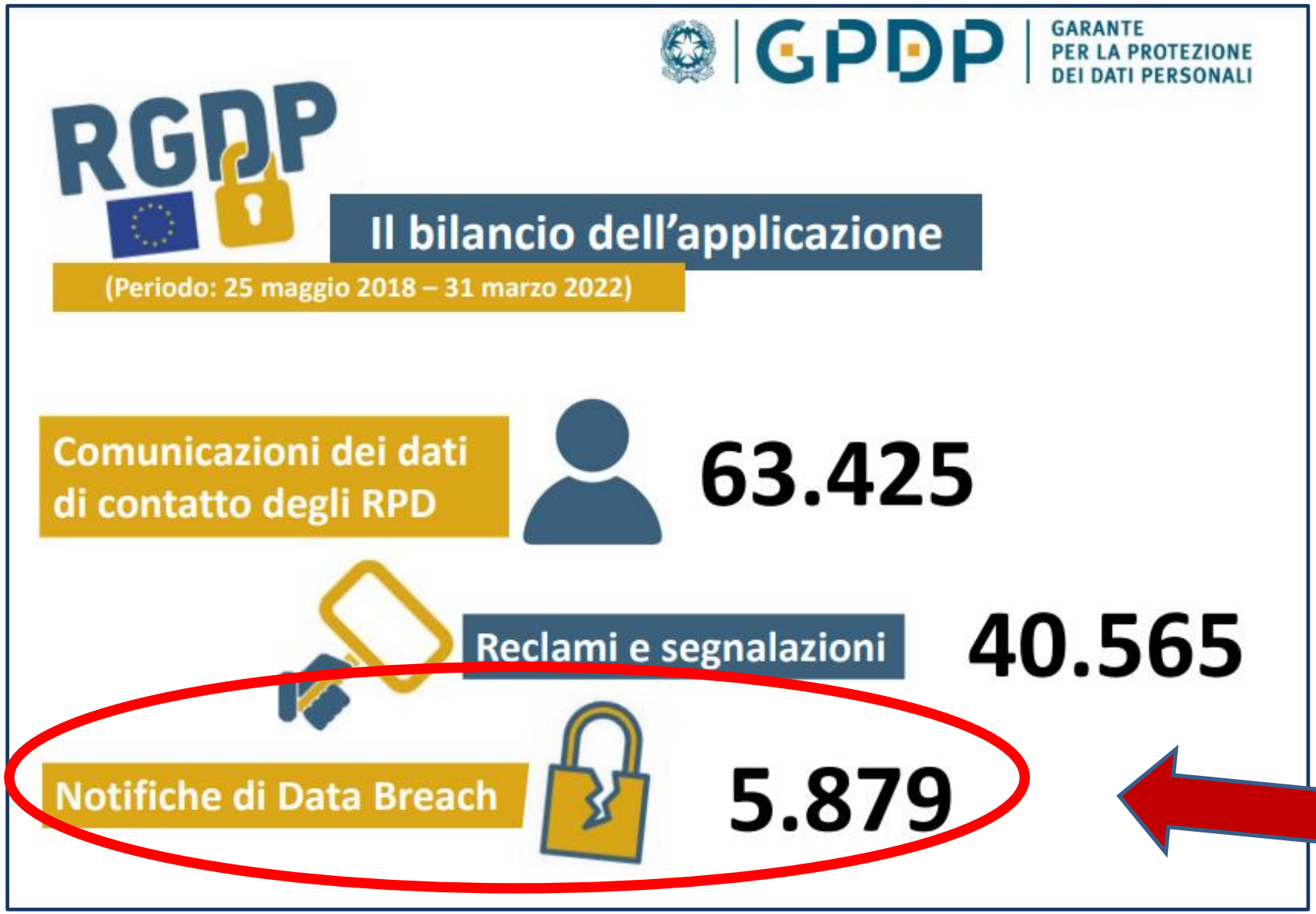
**Il grafico mostra le notifiche di data breach in vari periodi temporali. Il primo periodo considerato copre un arco di 4 mesi (25 maggio-28 settembre 2018), mentre gli altri periodi coprono archi temporali trimestrali.*

1. Introduzione - Contesto normativo

Qualche numero

Inoltre il **Garante** per la protezione dei dati personali ha **pubblicato** delle **infografiche** in cui vengono **ricapitolati alcuni numeri** che riassumono quello che è stato il costante e progressivo allineamento alla nuova normativa del GDPR.

1. Introduzione - Qualche numero



Fonte: Garante per la protezione dei dati personali

1. Introduzione - Contesto normativo

Data Breach: tema quanto mai attuale,

trasversale e simbiotico tra Autorità nazionali

- Il rispetto del **GDPR** è il presupposto per l'adozione di un **piano di sicurezza informatica**.

Il **legame tra GDPR e cybersecurity** è tale che il 26 gennaio 2022 le due autorità nazionali,
Garante Protezione dei Dati Personali e *Agenzia per la cybersicurezza nazionale*,
hanno sottoscritto **un protocollo di intesa** che include, tra le altre cose,
anche il **monitoraggio congiunto dei data breach** con il Garante
che "provvederà a informare l'Agenzia delle notizie di data breach rilevanti ai fini della cybersicurezza del Paese» e dello sviluppo digitale, per garantire la sicurezza e la resilienza cibernetica
necessarie allo sviluppo digitale del Paese.

1. Introduzione - Contesto normativo

Contesto normativo

- Regolamento europeo in materia di protezione dei dati personali **GDPR 679/2016**
  Artt. 4, 33, 34 - Considerando 85 e 87

- Linee guida **in materia di notifica di violazione dei dati personali** (Gruppo di lavoro 29 - WP29), ai sensi del Regolamento UE 2016/679, adottate il 03 ottobre 2017, rev. 01 del 6 febbraio 2018

- Linee guida sugli **esempi relativi alla notifica** di violazione dei dati personali del 14 gennaio 2021 (EDPB *Comitato europeo per la protezione dei dati)*

- Provvedimento del Garante **sulla notifica delle violazioni dei dati personali** (data breach) - n.209 del 27 maggio 2021, con il quale è stata adottata dal 1° luglio 2021 la nuova procedura telematica per la notifica di violazioni di dati personali.

2

Violazione dei dati personali - data breach

Che cosa è un «data breach»
Tipologie di violazioni dei dati personali

2. Violazione dei dati personali - data breach

Che cosa è un «data breach» ?

è un evento in conseguenza del quale si verifica una "violazione dei dati personali"

- Una **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 GDPR)**

I data breach sono incidenti di sicurezza

2. Violazione dei dati personali - data breach

Gli eventi di data breach possono essere suddivisi in tre macro-categorie:

- violazione di riservatezza: divulgazione o accesso non autorizzato o accidentale ai dati personali;
- violazione di integrità: alterazione non autorizzata o accidentale dei dati personali;
- violazione di disponibilità: perdita accidentale o non autorizzata dell'accesso ai dati o distruzione di dati personali.

2. Violazione dei dati personali - data breach

Una violazione dei dati personali può compromettere la

- riservatezza
- l'integrità
- la disponibilità

del dato personale.

2. Violazione dei dati personali - data breach

Modalità della violazione:

- Accidentale
- In modo illecito o intenzionale

- Interna
- Esterna

Natura della violazione	
Perdita di	**Conseguenze**
Confidenzialità	Diffusione/ accesso non autorizzato o accidentale
Disponibilità	Modifica non autorizzata o accidentale
Integrità	Impossibilità di accesso, perdita, distruzione non autorizzata o accidentale

Causa della violazione		
Interna	intenzionale	accidentale
Esterna	intenzionale	accidentale
Sconosciuta		
Altre cause		

2. Violazione dei dati personali - data breach

Alcune tipologie di violazioni dei dati personali

- **distruzione di dati informatici o documenti cartacei**, intesa come indisponibilità irreversibile di dati con accertata impossibilità di ripristino degli stessi;
- **perdita di dati** conseguente a smarrimento/furto di supporti informatici o di documentazione cartacea;
- **accesso non autorizzato o intrusione a sistemi informatici**, inteso come lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione;
- **modifica non autorizzata di dati**, derivante ad esempio da un'erronea esecuzione di interventi sui sistemi informatici o da interventi umani;
- **rivelazione di dati e documenti a soggetti terzi non legittimati**, anche non identificati, conseguenti ad esempio alla fornitura di informazioni, anche verbali, a persone diverse dal soggetto legittimato.

3 Implicazioni operative

Gestione del data breach

Notifica al Garante e comunicazione agli interessati

3. Implicazioni operative. Gestione del data breach

Cosa fare in caso di violazione dei dati personali

Notifica all'Autorità (art 33 GDPR)

- Il titolare del trattamento **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza, notifica la violazione al Garante, a meno che sia **improbabile** che la violazione dei dati personali comporti **un rischio per i diritti e le libertà delle persone fisiche.**
- Il responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare in modo che possa attivarsi.
- Le notifiche al Garante effettuate **oltre il termine delle 72 ore** devono essere **accompagnate dai motivi del ritardo.**
- Inoltre, se la violazione comporta **un rischio elevato per i diritti delle persone,** il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.
- Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta** tutte le violazioni dei dati personali, ad esempio predisponendo un **apposito registro**. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa

3. Implicazioni operative. Gestione del data breach

Tipo di violazioni notificate al Garante

Vanno notificate le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali. Ciò può includere, ad esempio:

- la perdita del controllo sui propri dati personali
- la limitazione di alcuni diritti, la discriminazione
- il furto d'identità o il rischio di frode
- la perdita di riservatezza dei dati personali protetti dal segreto professionale
- una perdita finanziaria
- un danno alla reputazione
- qualsiasi altro significativo svantaggio economico o sociale.

3. Implicazioni operative. Gestione del data breach

Cosa fare in caso di violazione dei dati personali

Il titolare del trattamento notifica la violazione all'Autorità……

- **Cons. 85** ……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**.

- **Art. 34 GDPR** 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.

3. Implicazioni operative. Gestione del data breach

Misure tecnologiche e organizzative

- **Cons. 87**

  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 de i suoi compiti e poteri previsti dal presente regolamento.

3. Implicazioni operative. Gestione del data breach

Per gestire un data breach dobbiamo essere in grado di:

1. Dimostrare che la violazione presenti/non presenti rischi per i diritti e le libertà delle persone fisiche, nonché la natura e l'entità di tali rischi.

1. Dotarsi di un sistema tecnologico di monitoraggio delle violazioni

2. Organizzare una procedura di data breach che consenta di individuare, di agire per il contenimento e informare tempestivamente l'Autorità di controllo e l'interessato.

3. Implicazioni operative. Gestione del data breach

Fasi del processo di gestione del data breach

- **Fase 1 – Identificazione:** raccogliere tutte le segnalazioni in merito a potenziali data breach.
- **Fase 2 – Valutazione dell'evento:** effettuare una valutazione preliminare delle segnalazioni ricevute mediante la raccolta delle prime informazioni. Analizzare la documentazione e la rilevanza del data breach (Gravità) tramite la stima del potenziale rischio associato ai diritti e libertà delle persone fisiche e, conseguentemente, classificare l'evento. Tale **attività è fondamentale per supportare in modo oggettivo la decisione di notificare o meno il data breach al Garante** ed eventualmente agli interessati coinvolti.
- **Fase 3 – Gestione del Data breach:** effettuare l'analisi dei rimedi e redigere un **Piano di Azione correttivo** con l'obiettivo di mitigare il rischio individuato e predisporre azioni tempestive. Eventualmente redigere le notifiche al Garante e, nel caso fosse necessario, redigere il documento di comunicazione agli interessati.

3. Implicazioni operative. Gestione del data breach

Fasi del processo di gestione del data breach (segue)

- **Fase 4 – Comunicazioni ed esecuzione del Piano di Azione**: Formalizzare la comunicazione al Garante e agli interessati, se necessario. Eseguire il piano di azione correttivo.
- **Fase 5 - Chiusura:** Aggiornare la documentazione e svolgere un esame ex post della gestione del data breach al fine di definire le principali cause dell'evento, le azioni implementate per superare le criticità emerse ed eventuali opportunità di miglioramento dei processi aziendali.

  Aggiornare il **Registro dei data breach**. Se del caso effettuare una valutazione finale delle azioni intraprese e delle risultanze e chiudere l'incidente.

3. Implicazioni operative. Gestione del data breach

Fasi del processo di gestione del data breach (segue)

- È importante ricordare che deve essere dimostrabile **ogni riferimento temporale** sull'incidente e sulla sua gestione, tra cui, il momento in cui il Titolare viene a conoscenza dell'evento, poiché da questo momento decorrono le 72 ore per la notifica al Garante.
- Il momento in cui il Titolare viene a **conoscenza dell'evento viene identificato** come segue:

- nel caso di specifica segnalazione, il giorno in cui la segnalazione è pervenuta al Referente data protection o Reterente It della struttura
- nel caso di alert del sistema, il giorno in cui l'alert è stato rilevato

4 Valutazione del rischio derivante da violazione dei dati personali

Gravità della violazione

Un possibile approccio metodologico

4. Valutazione del rischio da violazione dei dati personali

Gravità della violazione

La **gravità di una violazione** (GV)

è definita come la **stima**

dell'entità del **potenziale impatto**

sugli individui derivante dalla violazione dei dati.

4. Valutazione del rischio da violazione dei dati personali

Gravità della violazione (segue)

Gli **elementi fondamentali** che devono essere presi in considerazione quando si valuta questa gravità sono:

1. Data Processing Context (DPC): **Contesto del trattamento dei dati,** tipo di dati violati adattati al contesto in cui vengono utilizzati
2. Easeof Identification (EI): **Facilità di identificazione** dell'individuo in base ai dati violati
3. Circumstancesof breach (CB): **Circostanze della violazione**, che hanno un'ulteriore influenza sulla gravità della violazione. Affronta le circostanze specifiche della violazione, correlate al tipo di violazione, inclusa principalmente la perdita di sicurezza dei dati violati, nonché qualsiasi intento dannoso coinvolto.

TRE AREE che permettono la valutazione del Data Breach

4. Valutazione del rischio da violazione dei dati personali

Un possibile approccio metodologico

- Una possibile metodologia per **la valutazione della gravità delle violazioni dei dati personali** definita sulla base delle indicazioni fornite dall'**ENISA,** attraverso una **«Scheda di analisi gravità data breach – toolkit»**

Scheda di analisi degli eventi di Data Breach

Ai sensi dell'art.33 comma 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".

4. Valutazione del rischio da violazione dei dati personali

Un possibile approccio metodologico

- Una possibile metodologia per **la valutazione della gravità delle violazioni dei dati personali** definita sulla base delle indicazioni fornite dall'**ENISA, attraverso una «Scheda di analisi gravità data breach – toolkit»**

Toolkit di Valutazione dei rischi derivanti da violazione di dati personali

Gv - Gravità della Violazione

Natura e carattere sensibile dei dati personali			
Categorie di dati personali	**R**	**I**	**D**
Categoria dati trattamento 1 - indentificativi generici	2	2	2
Categoria dati trattamento 2 - sanitari (giuslavoristici)	4	3	3
Categoria dati trattamento 3 - dati identificativi finanziari	3	3	3
Categoria dati trattamento 4 - dati attività lavorativa	3	2	3
	4	**3**	**3**

Caratteristiche particolari dell'interessato	
Categorie di interessati	Vulnerabili
Categoria interessati trattamento 1 - specializzandi	NO
Categoria interessati trattamento 2	NO
Categoria interessati trattamento 3	NO
Categoria interessati trattamento 4	NO
Amplificazione 1	0%
Fascia di età interessati	minori o anziani
Fascia del trattamento 1 - adulti > 18 anni	NO
Fascia del trattamento 2	NO
Fascia del trattamento 3	NO
Fascia del trattamento 4	NO
Amplificazione 2	0%

0
0
0
0
0
0
0
0
0
0

Categorie vulnerabili			
1	2	3	4
10%	15%	20%	20%

Fascie di età vulnerabili			
1	2	3	4
10%	15%	20%	20%

4. Valutazione del rischio da violazione dei dati personali

Un possibile approccio metodologico

Il toolkit «Scheda di analisi gravità data breach» va a calcolare tre dati:

1) la **gravità della violazione** (GV), cioè quando la violazione è grave indipendentemente dalla probabilità;
2) il **Rischio** (R) derivante dalla violazione, tenendo presente anche la perdita della riservatezza, l'integrità, e la disponibilità (RID);
3) **valutazione di rischio fisico (FIM) materiale o immateriale** derivante dalla violazione

Rischio Rid da violazione **Rv= Gv * p** **Gravità della Violazione * probabilità di perdita di RID**

- Questi tre gruppi di valori consentiranno di fare tutte le valutazioni del caso, indipendentemente dal rischio, gravità, piuttosto che i danni dei diritti e le libertà degli interessati.

4. Valutazione del rischio da violazione dei dati personali

Un possibile approccio metodologico

Gravità della Violazione Gv

Rischio RID derivante da violazione $Rv = Gv * p$ Gravità della Violazione * *probabilità di perdita di RID*

Rischio FIM derivante da violazione

Matrice di correlazione del danno			
	R	I	D
Danno fisico	Improbabile	Improbabile	Improbabile
Danno materiale	Improbabile	Probabile	Probabile
Danno immateriale	Improbabile	Probabile	Probabile

Rischio FIMv per gli interessati	
Rischio fisico	Trascurabile
Rischio materiale	Basso
Rischio immateriale	Basso

Conclusione ....

Nella «Relazione 2022 sull'attività svolta nel 2021» presentata a Roma il 7 luglio 2022

Il Presidente del Garante per la Protezione dei Dati Personali, Pasquale Stanzione, si è così espresso:

Di fronte all'alto numero di **attacchi informatici**,
il Garante ha richiamato l'attenzione di pubbliche
amministrazioni e imprese sulla necessità
di investire in sicurezza,
per difendersi, in particolare, dai **ransomware**,
software che prendono "in ostaggio" un dispositivo elettronico
per poi "liberarlo" a fronte del pagamento di somme di denaro.
Una minaccia, questa, che si è particolarmente diffusa
anche nel nostro Paese.

Conclusioni

La protezione dei dati personali costituisce, sempre più, una componente centrale delle democrazie liberali, allorché garantisce che l'innovazione, l'iniziativa economica, l'attività pubblica in ogni campo non violino la dignità della persona.
L'obiettivo è quindi promuovere una civiltà digitale in cui l'innovazione non sia subita dall'uomo, bensì agita, per la promozione dell'umanesimo digitale.

Pasquale Stanzione

Presidente del Garante per la Protezione dei Dati Personali

Relazione 2022 sull'attività svolta nel 2021, Roma 7 luglio 2022

5 Bibliografia

Bibliografia

- **Manuale RPD Programma "T4DATA"** *Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e para pubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea (Regolamento (UE) 2016/679),* luglio 2019
- **EDPB** «Linee guida 01/2021 sugli esempi relativi alla notifica di violazione dei dati», 4 dicembre 2021, Versione 2.0
- **Gruppo di Lavoro art 29** «Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679» Versione emendata e adottata in data 6 febbraio 2018
- **S. Calzolaio**, «*Protezione dei dati personali*», Estratto da DIGESTO delle Discipline Pubblicistiche, Utet Giuridica, Milano 2017

Grazie per l’attenzione!