La sicurezza dei sistemi informatici:
minacce prevedibili e tutele applicabili - data breach e adempimenti del titolare del trattamento

Cosimo Comella, Direttore Dipartimento tecnologie digitali e sicurezza informatica , Autorità Garante per la protezione dei dati personali

Giuseppe D'Agostino, Director PwC Cybersecurity & Privacy

I principali trend e le possibili azioni di rimedio

Il mercato del Cyber Crime

Il Cyber Crime genera profitti maggiori del traffico di droga, con un giro d'affari stimato in più di 3.000 miliardi di dollari

3.000 miliardi $

Stima del volume di affari del cyber crime

Source: Serious & Organized Crime Threat Assessment

In Europa sono presenti più di ***3.600 organizzazioni criminali di Hacker***

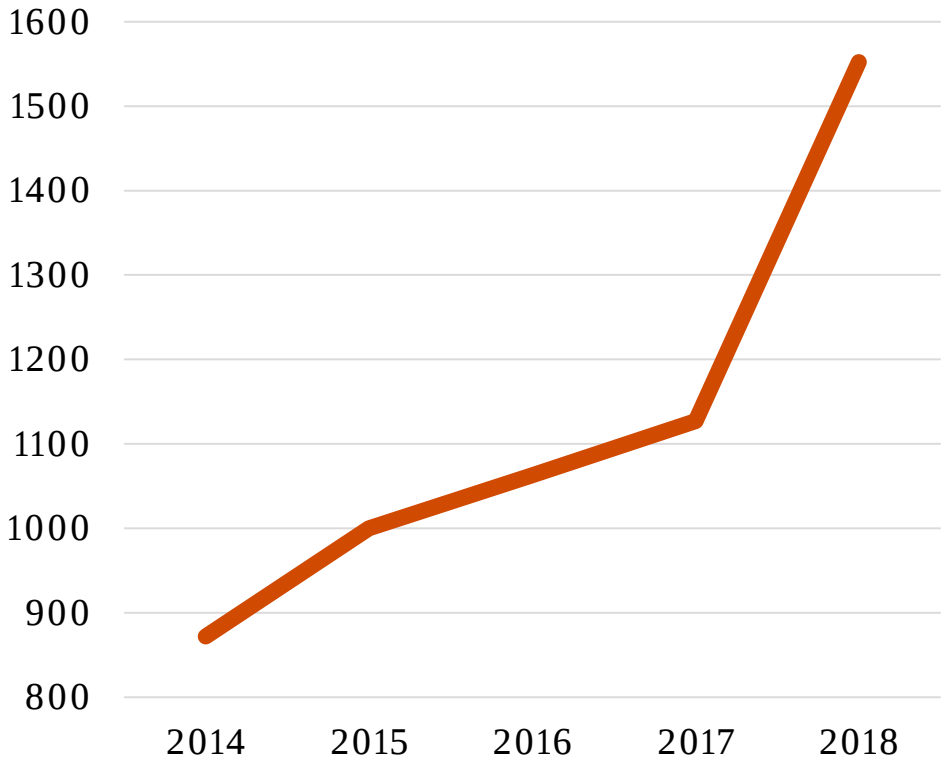
Source: Serious & Organized Crime Threat Assessment

Il crimine organizzato sta cambiando e le aziende si devono adeguare di conseguenza

+ 57% l'aumento di attacchi di Cyber Espionage *dal 2017 al 2018 in Italia*

Source: Rapporto Clusit 2019

Numero di incidenti critici



Source: Rapporto Clusit 2019

Conseguenze di un attacco cyber

È molto complesso quantificare a priori il possibile impatto di incidenti in ambito Cyber Security ma le perdite economiche possono essere rilevanti

YAHOO!

- Nel **2016** Yahoo ha dichiarato di aver subito una **violazione di oltre 3 miliardi di account email.**
- Gli **attacchi sono avvenuti nel 2013 e nel 2014 ma la società ha ammesso l'accaduto solamente nel 2016.**
- Dopo la notizia dei cyberattacchi, Verizon ha rinegoziato l'accordo di acquisizione con Yahoo, **riducendo il prezzo di acquisto di 320 milioni di dollari**.

320 *Milioni di dollari di svalutazione del prezzo di acquisto*

Elevata difficoltà nel valutare il Cyber Risk

EQUIFAX

- Settembre **2017** Equifax subisce una **violazione informatica di 143 milioni di dati di cittadini americani**,
- Equifax **rimandò la comunicazione dell'accaduto per più di 3 mesi**
- Tre suoi dirigenti venderono 1,8 milioni di dollari di azioni.
- A seguito della comunicazione di data breach **il titolo ha perso il 32% del suo valore.**

-32% *Perdita del valore del titolo in borsa*

Evoluzione del contesto

L'introduzione di nuove tecnologie sta espandendo la superfice di attacco delle aziende e richiede un approccio innovativo alla protezione dei dati

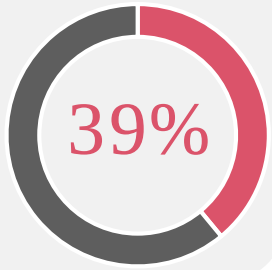
IoT

50 Miliardi

di dispositivi connessi nel 2020

30% Delle aziende dichiara che investirà in **Internet of Things** nei prossimi 12 mesi

Hanno pianificato sufficienti controlli «cyber security» per l'adozione di IoT

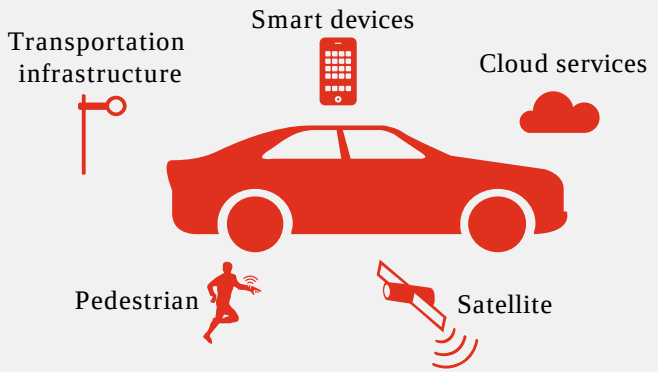


Source: PwC Digital Trust Insights 2018

Connected Car

100% delle nuove auto sarà connesso nel 2022

Superficie di attacco



Source: The 2018 Strategy& Digital Auto Report

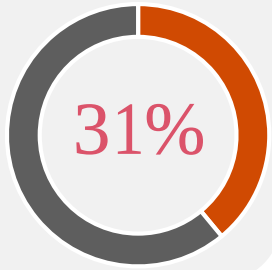
Ai

Hacking

è una delle prime attività in cui l'AI si è dimostrata migliore dell'essere umano

27% Delle aziende dichiara che investirà in **Ai** nei prossimi 12 mesi

Hanno pianificato sufficienti controlli «cyber security» per l'adozione di AI



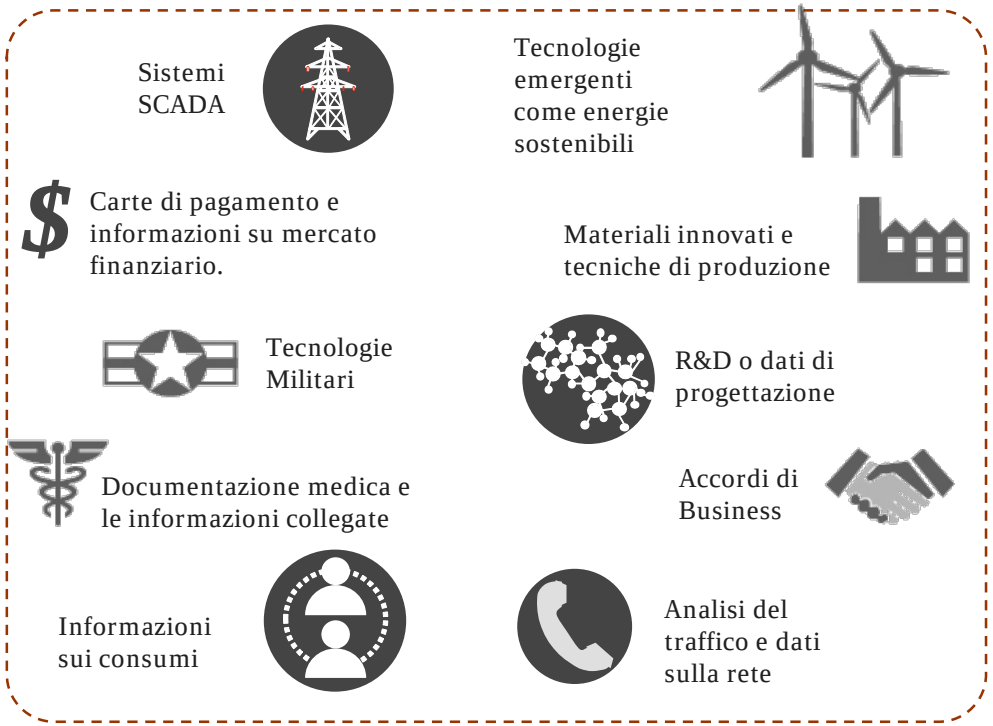
Source: PwC Digital Trust Insights 2018

Minacce e settori a rischio

I dati personali costituiscono uno dei principali target del crimine organizzato in quanto facilmente monetizzabili

Origine delle minacce

Target di attacco



Vettori di attacco

Threat vector	# 2018	'18 vs '17	Trend
Malware	585	31,20%	⇗
Unknown	408	47,30%	⇗
Known / Misconfig.	177	39,40%	⇗
Phishing / Social Eng.	160	56,90%	⇧
Multiple Tech. / APT	98	55,60%	⇧

Source: Rapporto Clusit 2019

Le preoccupazioni dei CEO e il driver di investimento

Il Cyber threat è nella TOP 5 delle priorità dei CEO, le organizzazioni si sentono impreparate e la compliance è il fattore trainante degli investimenti

Source: PwC, 2019 Annual Global CEO Survey

57%

Organizzazioni in Italia reputano prioritario agire in ambito Cyber Security & Data Protection

Source: PwC Digital Trust Insights 2019

COMPLIANCE

1° Fattore trainante di spesa in cyber security in Italia

Source: 2019, Osservatorio Information Security & Privacy, Politecnico di Milano

Come proteggersi

È necessario utilizzare un approccio olistico alla sicurezza, agendo a livello di prevenzione, identificazione e risposta agli incidenti di Cyber Security

Prevention

- Cyber Security Risk Assessment
- Cyber Security Culture
- Strategy & Target Operating Model
- Policy & Procedure
- Security-by-design
- Technical Assessment
- Early Warning
- Red/Blue/Purple Team

Detection

- Log collection & correlation
- User & Endpoint Behaviuor
- Network Monitoring
- Malware Analysis
- APT Detection
- Cyber Security Analytics
- Threat Intelligence
- Threat Hunting

Response

- Cyber Security Incident Management
- Internal & External Communication
- Forensic Investigation
- Recovery Plan

Source: PwC Digital Trust Insights 2019

Security e Privacy by-design e by-default

È fondamentale integrare i principi di sicurezza e privacy all'intero dei programmi di trasformazione aziendale, per esempio nello sviluppo di nuovi servizi e sistemi

91%

delle aziende dichiara di ingaggiare professionisti di privacy e security in progetti di digital transformation e di gestire in maniera proattiva i rischi cyber e privacy nella pianificazione di progetti e budget

53%

delle aziende include una gestione proattiva al rischio già dalle "primissime fasi" del progetto

"

L'adozione di questi principi passa attraverso la **trasformazione culturale** dell'impresa.

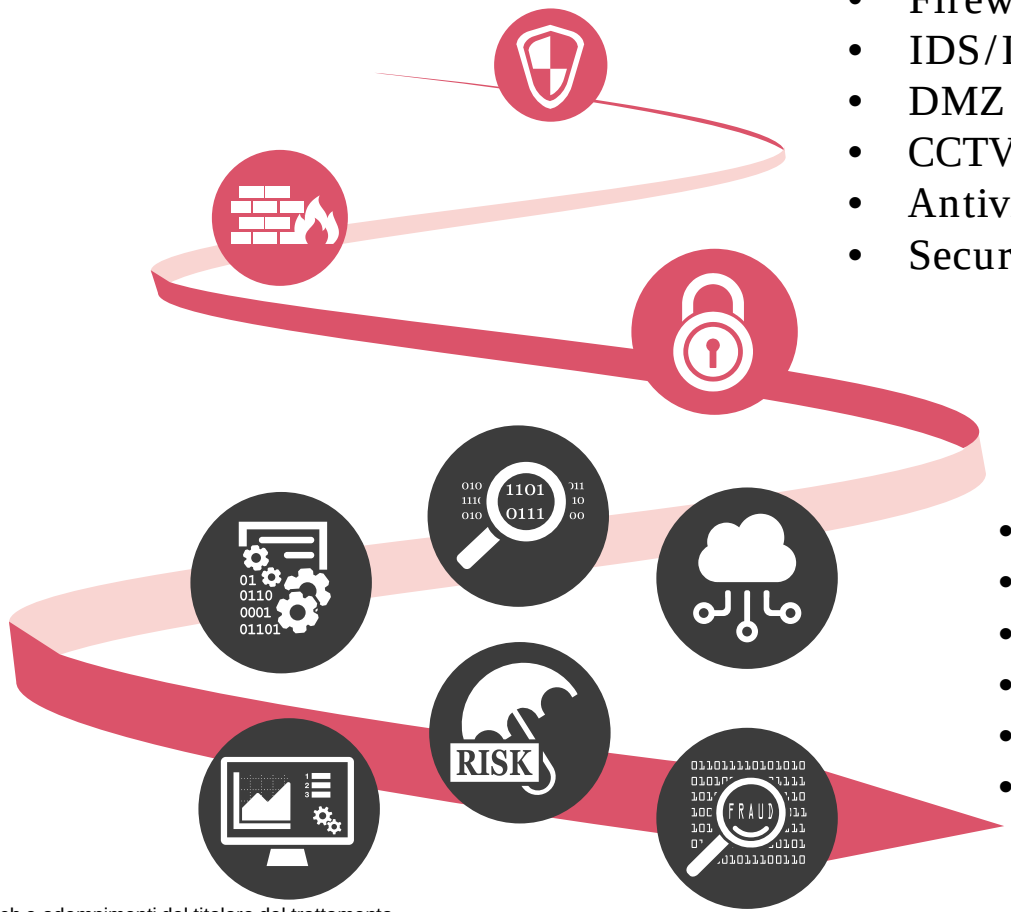
È necessario che le persone da anello debole della catena diventino la **prima linea di difesa**.

Cyber Security Detection & Response

La capacità delle organizzazioni di identificare e rispondere a un data breach sta diventando di vitale importanza, infatti gli investimenti sono sempre più finalizzati a ridurre i tempi di reazione agli incidenti

197 giorni
è il tempo medio per identificare un Data Breach nel 2018

69 giorni
è il tempo medio per contenere un Data Breach nel 2018



- Firewalls
- IDS/IPS
- DMZ
- CCTV
- Antivirus e antispam
- Secure Software Development

- Next Generation Firewalls
- Anti APT
- Managed Detect & Response
- Fraud Detection
- Threat Intelligence
- Purple Team

Source: 2018 IBM - Cost of a Data Breach Study

I data breach nell'era GDPR

L'applicazione del GDPR ha favorito la segnalazione di data breach

375.000+

Organizzazioni hanno nominato un DPO

89.000

Segnalazioni di data Breach

144.000+

Segnalazioni di violazioni dei diritti degli interessati

280.000+

Segnalazioni ricevute dalle Autorità Europee per la protezione dei dati personali

Source: GDPR One Year Anniversary – IAPP, Maggio 2019

Report PwC

PwC Digital Trust Insights Fall 2018

PwC - 22nd Annual Global CEO Survey

Global Economic Crime and Fraud Survey 2018 Summary Italia

Il GDPR: impatto sulla sicurezza

I data breach nell'era GDPR

Dalla reticenza alla trasparenza: un nuovo approccio alla sicurezza

Agenda

- **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 del trattamento**
- **Il ruolo del responsabile della protezione dei dati**
- **I poteri del Garante**
- **Il decalogo della gestione dei *data breach***

Cos'è un *data breach*? (2)

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

Cos'è un *data breach*? (3)

Distruzione non autorizzata	indisponibilità definitiva di dati personali degli interessati con impossibilità di ripristino degli stessi
Perdita	perdita di un supporto fisico di memorizzazione contenente dati personali degli interessati oppure di documenti cartacei
Modifica non autorizzata	modifiche dei dati degli interessati effettuate da incaricati non autorizzati oppure modifiche con finalità fraudolente eseguite dagli incaricati autorizzati
Divulgazione non autorizzata	distribuzione non autorizzata o illecita dei dati personali degli interessati verso terzi anche non precisamente identificabili
Accesso non autorizzato	accesso non autorizzato o improprio ai dati degli interessati oppure accesso ai dati avvenuto al di fuori dei processi di trattamento dei dati previsti e autorizzati

Cos'è un *data breach*? (4)

Cons. 85 del Regolamento

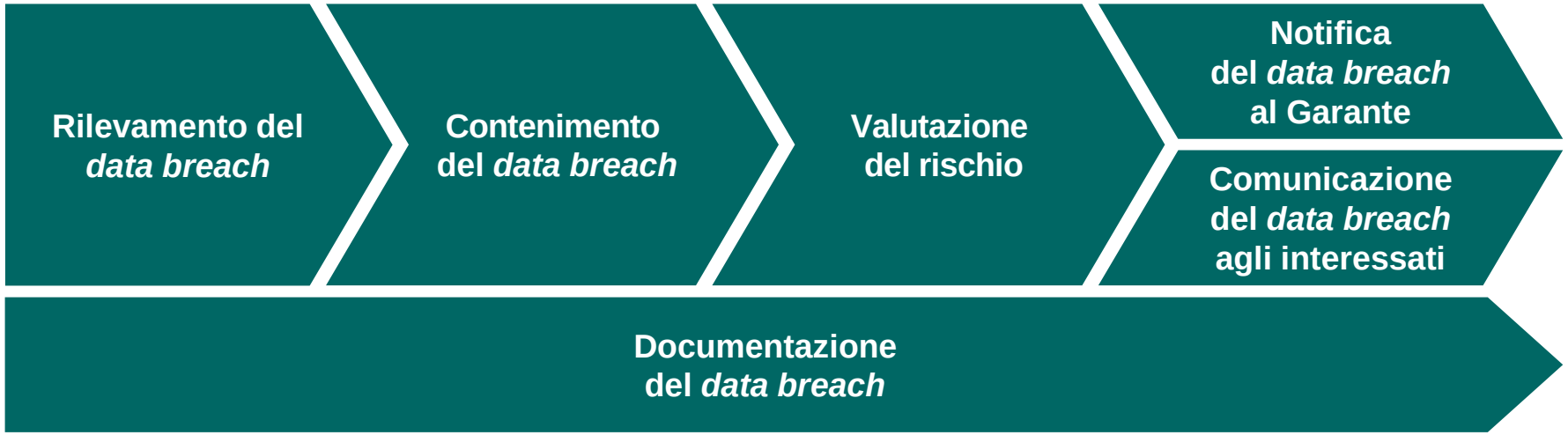
*«Una **violazione** dei dati personali **può**, se non affrontata in modo adeguato e tempestivo, **provocare danni fisici, materiali o immateriali alle persone fisiche**, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione 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* […]»

Possibili conseguenze di un *data breach*

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

La gestione di un *data breach*

- 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
- In caso di *data breach*, il titolare del trattamento deve essere in grado di valutarne la portata e di decidere tempestivamente le misure da adottare per porvi rimedio
- In funzione del rischio derivante da un *data breach*, il titolare del trattamento deve effettuare la notifica al Garante e la comunicazione agli interessati coinvolti



Il rilevamento del *data breach* (1)

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 del trattamento di attuare misure tecniche e organizzative necessarie per rilevare immediatamente un *data breach*, ossia per assicurarsi di venire “a conoscenza” di un eventuale *data breach*
- Il momento in cui un titolare del trattamento può considerarsi “a conoscenza” di un *data breach* dipende molto dalle circostanze in cui lo stesso si verifica
- Il titolare del trattamento dovrebbe dotarsi di procedure interne per poter rilevare un *data breach* in maniera tempestiva
- Non appena venuto “a conoscenza” di un *data breach*, il titolare del trattamento deve stabilire le azioni da intraprendere per far fronte alla violazione

Il rilevamento del *data breach* (2)

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* […]*»*

- 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
- La tardiva reazione a un *data breach* da parte di un titolare del trattamento è spesso causata proprio dall'assenza o dall'inadeguatezza delle procedure di rilevazione dei *data breach*

Il contenimento del *data breach* (1)

- 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 dei ruoli
- Le misure tecniche e organizzative che il titolare del trattamento adotta a seguito di un *data breach* devono avere un duplice obiettivo: quello di contenerlo e quello di attenuare i suoi possibili effetti pregiudizievoli nei confronti degli interessati

Il contenimento del *data breach* (2)

Principali azioni di risposta a un *data breach*

- Rimuovere le cause che hanno determinato il *data breach*
- Identificare e mettere in atto quelle misure volte a attenuare gli effetti negativi del *data breach* per gli interessati
- Ripristinare la normale operatività dei sistemi
- Attivare procedure di *escalation*
- Raccogliere e conservare prove digitali
- Identificare e mettere in atto quelle misure necessarie per evitare che lo stesso *data breach* possa verificarsi di nuovo

La valutazione del rischio (1)

- Gli obblighi di notifica e di comunicazione dei *data breach* introdotti dal Regolamento sono condizionati a una valutazione del rischio effettuata dal titolare del trattamento, in particolare:
  - la notifica di un *data breach* al Garante deve essere effettuata "*a meno che sia improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche*" (art. 33, par. 1, del Regolamento)
  - la comunicazione di un *data breach* agli interessati è necessaria soltanto quanto lo stesso "*è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art. 34, par. 1, del Regolamento)
- Il titolare del trattamento, dopo essere venuto a conoscenza di un *data breach*, non deve solamente contenerlo ma deve valutare anche il rischio che lo stesso presenta
- La valutazione della probabilità e della potenziale gravità di un *data breach* sugli interessati consente al titolare del trattamento di individuare le misure più efficaci per porvi rimedio nonché di avere tutti gli elementi per stabilire se debba essere effettuare la notifica al Garante e, se del caso, agli interessati

La valutazione del rischio (2)

- 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 effettuata a seguito di un *data breach* esamina il rischio in modo differente rispetto alla valutazione d'impatto sulla protezione dei dati (DPIA):
  - la DPIA, nel valutare i rischi di un trattamento, considera anche quelli in caso di *data breach* esaminando in termini generali la probabilità che lo stesso si verifichi e il danno che potrebbe derivarne per le persone fisiche
  - la valutazione del rischio di un *data breach* è esclusivamente incentrata sugli impatti che lo stesso determina sulle persone fisiche

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»*

La valutazione del rischio (3)

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) del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017, fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018, individuano i fattori da considerare nella valutazione del rischio

- **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 (4)

Fattori da considerare nella valutazione del rischio

Tipo di violazione

- Il tipo di *data breach* occorso può influire sul livello di rischio presentato per le persone fisiche

Natura, carattere sensibile e volume dei dati personali

- La natura e il carattere sensibile dei dati personali che sono stati compromessi in un *data breach* sono elementi fondamentali della valutazione del rischio: solitamente più i dati sono sensibili, maggiore è il rischio per gli interessati
- Altro fattore da tenere in considerazione è la quantità dei dati personali oggetto del *data breach*

Numero di persone fisiche interessate

- Un *data breach* può coinvolgere solo pochi interessati oppure diverse migliaia di interessati, se non molti di più. Di solito, maggiore è il numero di interessati, maggiore è l'impatto che il *data breach* può avere

La valutazione del rischio (5)

Fattori da considerare nella valutazione del rischio

Facilità di identificazione delle persone fisiche

- Un fattore importante da considerare è la facilità con cui un soggetto che può accedere a dati personali compromessi riesce a identificare persone fisiche specifiche o ad abbinare i dati con altre informazioni per identificare persone fisiche

Gravità delle conseguenze per le persone fisiche

- A seconda della natura dei dati personali coinvolti in un *data breach*, il danno agli interessati che potrebbe derivarne è particolarmente grave soprattutto se la violazione può comportare un furto di identità, danni fisici o danni alla reputazione

Caratteristiche particolari dell'interessato

- Un *data breach* può riguardare dati personali riferiti a minori o a altre categorie di persone fisiche vulnerabili, che potrebbero essere soggette a un rischio più elevato di danno

Caratteristiche particolari del titolare del trattamento

- Il ruolo del titolare del trattamento e la natura delle attività che svolge possono influire sul livello di rischio presentato da un *data breach*

La valutazione del rischio (6)

È PROBABILE CHE CI SIA RISCHIO ELEVATO

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

È PROBABILE CHE CI SIA UN RISCHIO

- Notifica al Garante
- Documentazione del *data breach*

È IMPROBABILE CHE CI SIA UN RISCHIO

- Documentazione del *data breach*

La notifica del *data breach* al Garante (1)

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**»*

Notifica al Garante

- Il Regolamento impone al titolare del trattamento di notificare un *data breach* senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, ossia dal momento in cui è ragionevolmente certo che si sia verificato un *data breach*
- Il Regolamento chiarisce che, qualora non sia effettuata entro 72 ore, la notifica al Garante deve includere una descrizione dei motivi del ritardo

La notifica del *data breach* al Garante (2)

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**»*

Contenuto della notifica

- Descrizione della natura della violazione
- Numero e categorie di interessati
- Numero e categorie di dati personali
- 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 (inclusa l'eventuale comunicazione del *data breach* agli interessati coinvolti)

La notifica del *data breach* al Garante (3)

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»*

Notifica per fasi

- Un titolare del trattamento non sempre potrebbe disporre di tutte le informazioni relative un *data breach* entro 72 ore dal momento in cui ne è venuto a conoscenza
- Le "*Linee guida sulla notifica delle violazioni dei dati personali*" suggeriscono che, all'atto della notifica iniziale, il titolare del trattamento informi il Garante del fatto che non dispone ancora di tutte le informazioni richieste e che fornirà ulteriori dettagli in un momento successivo
- La notifica al Garante entro le prime 72 ore può consentire al titolare del trattamento per chiedere un parere sulle decisioni in merito alla comunicazione del *data breach* agli interessati
- Se esiste una minaccia concreta per gli interessati (es. furto d'identità), il titolare dovrà agire immediatamente per contenere il *data breach* e comunicarlo agli interessati coinvolti

La notifica del *data breach* al Garante (4)

Art. 33, par. 1, del Regolamento

«[…] *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*** […]»

Casi in cui non è richiesta la notifica al Garante

- Il Regolamento stabilisce che, se è "*improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*", tale *data breach* non è soggetto a notifica al Garante
- Se i dati personali oggetto di un *data breach* sono stati resi incomprensibili attraverso adeguate tecniche crittografiche, una violazione della riservatezza che coinvolga tali dati personali non dovrebbe essere notificata Garante, poiché è improbabile che tale *data breach* possa presentare un rischio per gli interessati

La notifica del *data breach* al Garante (5)

Art. 26, par. 1, del Regolamento

I contitolari del trattamento *«determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento* […]*»*

Nel caso in cui siano previsti contitolari del trattamento, le *Linee guida sulla notifica delle violazioni dei dati personali* raccomandano di determinare le rispettive responsabilità in merito all'osservanza delle disposizioni del Regolamento, comprese quelle relative agli obblighi in tema di notifica e di comunicazione dei *data breach*

La comunicazione del *data breach* agli interessati (1)

Comunicazione agli interessati

- Tempestività della comunicazione agli interessati
- Nei casi indicati nell'allegato B alle "*Linee guida sulla notifica delle violazioni dei dati personali*"

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 del *data breach* agli interessati (2)

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)»*

Contenuto della comunicazione

- Descrizione della natura della violazione
- 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

La comunicazione del *data breach* agli interessati (3)

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

- **Indicazioni pratiche** su come proteggersi da conseguenze negative

Si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard.
Ciò contribuisce a rendere la comunicazione della violazione **chiara e trasparente**

La comunicazione del *data breach* agli interessati (4)

Il titolare del trattamento:

- deve stabilire il canale di contatto più appropriato per comunicare una violazione agli interessati
- deve scegliere un mezzo che massimizzi la possibilità di comunicare correttamente le informazioni a tutte le persone interessate (banner o notifiche su siti web di primo piano, comunicazioni postali e pubblicità di rilievo sulla stampa)
- potrebbe utilizzare diversi metodi di comunicazione, anziché un singolo canale di contatto
- dovrebbe essere cauto nell'usare un canale di contatto compromesso dalla violazione, in quanto tale canale potrebbe essere utilizzato anche da autori di attacchi che si fanno passare per il titolare del trattamento

La comunicazione del *data breach* agli interessati (5)

Casi in cui non va effettuata la comunicazione

Art. 34, par. 3, del Regolamento

«Non è richiesta la comunicazione all'interessato […] *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 di cui al paragrafo 1;*

*c) detta 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»*

Art. 2-*duodecies, c. 2,* del Codice

«[…] l'adempimento degli obblighi di cui agli articoli […] *34 del Regolamento possono, in ogni caso, essere ritardati, limitati o esclusi,* […] *nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, per **salvaguardare l'indipendenza della magistratura e dei procedimenti giudiziari**»*

La documentazione del *data breach* (1)

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»*

- Devono essere documentati tutti i *data breach* che si sono verificati, anche quelli che non sono stati notificati al Garante
- Il titolare definisce metodologia e struttura della documentazione dei *data breach*
- Contenuti minimi:
  - Dettagli relativi alla violazione
  - Cause
  - Dati personali interessati
  - Conseguenze della violazione
  - Provvedimenti adottati

La documentazione del *data breach* (2)

- Documentare le motivazioni per le quali una violazione non è stata notificata (valutazione dei rischi per gli interessati)
- Documentare le motivazioni di una notifica effettuata in ritardo
- Documentare l'eventuale occorrenza di una delle condizioni di cui all'art. 34, par. 3, del Regolamento
- Conservare le prove atte a dimostrare l'avvenuta comunicazione agli interessati
- Il titolare potrebbe richiedere il parere al proprio responsabile della protezione dei dati in merito alla struttura, impostazione e manutenzione della documentazione

Il ruolo del responsabile del trattamento (1)

Art. 28, par. 1, del Regolamento

«Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a ***responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative*** *adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato»*

Art. 28, par. 3, del Regolamento

«I trattamenti da parte di un responsabile del trattamento sono disciplinati ***da un contratto o da altro atto giuridico*** […]. ***Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:*** […]

f) ***assista 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* […]»

Il ruolo del responsabile del trattamento (2)

Art. 33, par. 2, del Regolamento

«Il responsabile del trattamento informa il titolare del trattamento ***senza ingiustificato ritardo*** *dopo essere venuto a conoscenza della violazione»*

Compiti del responsabile del trattamento

- Non deve valutare la probabilità di rischio derivante dalla violazione
- Deve soltanto stabilire se si è verificata una violazione e quindi notificarla al titolare del trattamento

Il contratto tra il titolare del trattamento e il responsabile del trattamento dovrebbe specificare le modalità per il soddisfacimento delle disposizioni di cui all'art. 33, par. 2, del Regolamento

Il ruolo del responsabile della protezione dei dati (1)

Art. 39 del Regolamento

«1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) ***informare e fornire consulenza al titolare del trattamento*** […]

b) ***sorvegliare l'osservanza del presente regolamento****,* […]

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) ***cooperare con l'autorità di controllo****; e*

e) ***fungere da punto di contatto per l'autorità di controllo*** *per questioni connesse al trattamento,* […]

2. Nell'eseguire i propri compiti ***il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento****, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo»*

Compiti del responsabile della protezione dei dati

- Fornire consulenza
- Sorvegliare l'osservanza del regolamento
- Fungere da punto di contatto per il Garante e per gli interessati
- Considerare debitamente i rischi inerenti al trattamento

Data Protection Officer (DPO)

Il ruolo del responsabile della protezione dei dati (2)

Art. 33, par. 3, del Regolamento

«La notifica di cui al paragrafo 1 deve almeno: […]

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 […]*»*

Le "*Linee guida sulla notifica delle violazioni dei dati personali*":

- indicano che il responsabile della protezione dei dati dovrebbe fornire assistenza (al titolare del trattamento) nella prevenzione delle violazioni o nella gestione delle stesse
- raccomandano di informare tempestivamente il responsabile della protezione dei dati dell'esistenza di una violazione e di coinvolgerlo nella gestione delle violazioni e nel processo di notifica

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

I poteri del Garante (1)

Poteri di indagine

Poteri correttivi

Poteri autorizzativi e consultivi

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

I poteri del Garante (2)

I poteri di indagine

Art. 58, par. 1, del Regolamento

*«Ogni autorità di controllo ha tutti **i poteri di indagine** seguenti:*

a) *ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, **di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti**;* […]

e) *ottenere, dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a **tutte le informazioni necessarie** per l'esecuzione dei suoi compiti; e*

f) *ottenere **accesso a tutti i locali** del titolare del trattamento e del responsabile del trattamento, compresi tutti **gli strumenti e mezzi di trattamento dei dati**, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri»*

Art. 157 del Codice

«Nell'ambito dei poteri di cui all'articolo 58 del Regolamento, e per l'espletamento dei propri compiti, il Garante può richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti anche con riferimento al contenuto di banche di dati»

Art. 158, c. 1, del Codice

«Il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali»

I poteri del Garante (3)

I poteri correttivi

Art. 58, par. 2, del Regolamento

*«Ogni autorità di controllo ha tutti i **poteri correttivi** seguenti:* […]

*d) ingiungere al titolare del trattamento o al responsabile del trattamento di **conformare i trattamenti alle disposizioni del presente regolamento**, se del caso, in una determinata maniera ed entro un determinato termine;*

*e) ingiungere al titolare del trattamento **di comunicare all'interessato** una violazione dei dati personali;* […]

*f) imporre una **limitazione provvisoria o definitiva al trattamento**, incluso il divieto di trattamento* […]*»*

Art. 34, par. 4, del Regolamento

*«Nel caso in cui il titolare del trattamento **non abbia ancora comunicato all'interessato la violazione** dei dati personali, **l'autorità di controllo può richiedere**, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, **che vi provveda** o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta»*

I poteri del Garante (4)

Le sanzioni

Art. 58, par. 2, del Regolamento

«Ogni autorità di controllo ha tutti i poteri correttivi seguenti: […]

i) ***infliggere una sanzione amministrativa pecuniaria*** *ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso* […]*»*

Art. 83, par. 4, del Regolamento

«[…] *la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:*

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, ***da 25 a 39****, 42 e 43;*

b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4»

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Il decalogo della gestione dei *data breach* (1)

5 COSE DA FARE

- Quando individui le misure per la sicurezza del trattamento, tieni conto dei rischi che potrebbero derivare da un eventuale *data breach*
- Effettua periodicamente *vulnerability assessment* e *patching* dei sistemi
- Trasforma gli utenti da anello debole della catena a prima linea di difesa, incoraggiandoli a segnalare situazioni anomale
- Documenta tutti i ragionamenti che sono alla base delle decisioni prese in risposta a un *data breach*
- Impara anche dagli errori degli altri

Il decalogo della gestione dei *data breach* (2)

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 tuo *business*, ma piuttosto ai possibili effetti negativi per gli interessati
- Non sottovalutare i rischi presentati 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

Grazie

pwc.com/it