PANETTA & ASSOCIATI

Privacy: sfide e opportunità del mercato digitale e dell'economia dei dati

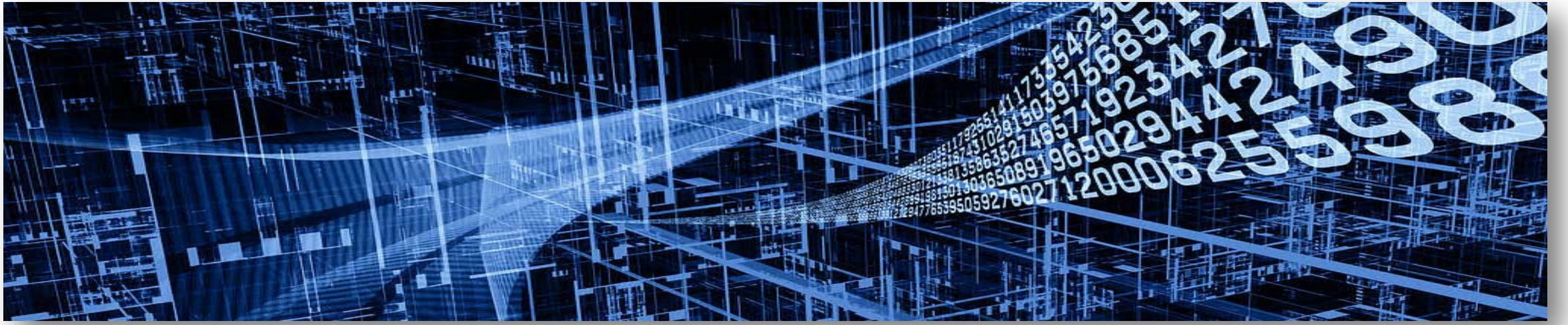
Avv. Lorenzo Cristofaro

Treasury & Finance Forum Day 2018

Castelnuovo del Garda, 21 settembre 2018

IL VALORE DEI DATI E DELLA SICUREZZA

Il reale valore dei dati non è generalmente percepito nella sua interezza, con la conseguenza che i rischi derivanti da eventuali trattamenti illeciti, attacchi o perdite sono spesso sottovalutati dalle aziende.



Non si può più parlare di *privacy* solo come protezione della sfera personale di ognuno di noi, ma bisogna pensare alla tutela e alla sicurezza dei dati anche in quanto patrimonio aziendale, sempre più prezioso e strategico.

I RISCHI PER LA SICUREZZA DEI DATI

Nel periodo considerato dal 2011 al 2017 i costi generati globalmente dalle sole attività cybercriminali sono quintuplicati, passando da circa 100 miliardi di dollari nel 2011 ad oltre 500 miliardi nel 2017.

Ricordiamo, tra i varissimi, il blocco dicentinaia di migliaia di *device* IoT (Satori botnet), gli attacchi basati sui malware WannaCry e NotPetya, i furti per centinaia di milioni di dollari realizzati ai danni di primari istituti bancari compromettendo il sistema SWIFT, i numerosi *data breach* che hanno coinvolto complessivamente miliardi di *account* (es. ThyssenKrupp, Yahoo, Ethiad Airways, KFC) o gli attacchi ad infrastrutture critiche e la diffusione endemica di crimini estorsivi realizzati su larga scala tramite attacchi basati su *ransomware* e *cryptominers*.

Gemalto, Breach Level Index 2017

I RISCHI PER LA SICUREZZA DEI DATI

La maggior parte dei rischi, ad ogni modo, non deriva da interventi esterni all'azienda, ma da inadempimenti o omissioni commesse internamente alla stessa, come ad esempio:

- comunicazione non autorizzata di dati a terzi;
- indebita diffusione o pubblicazione dei dati;
- mancato riscontro alle istanze di esercizio dei diritti;
- definizione di servizi, prodotti e processi inidonei in termini di protezione dei dati;
- trasferimento di dati al di fuori dell'UE in assenza delle necessarie condizioni legali;
- distruzione, perdita o modifica non autorizzata dei dati o accesso indebito agli stessi;
- trattamento in assenza di presupposti giuridici;
- carenza di trasparenza per inidoneità o mancanza di informativa;
- inadeguatezza delle misure di sicurezza adottate.

ALCUNI NUMERI RELATIVI ALLE VIOLAZIONI DELLA SICUREZZA

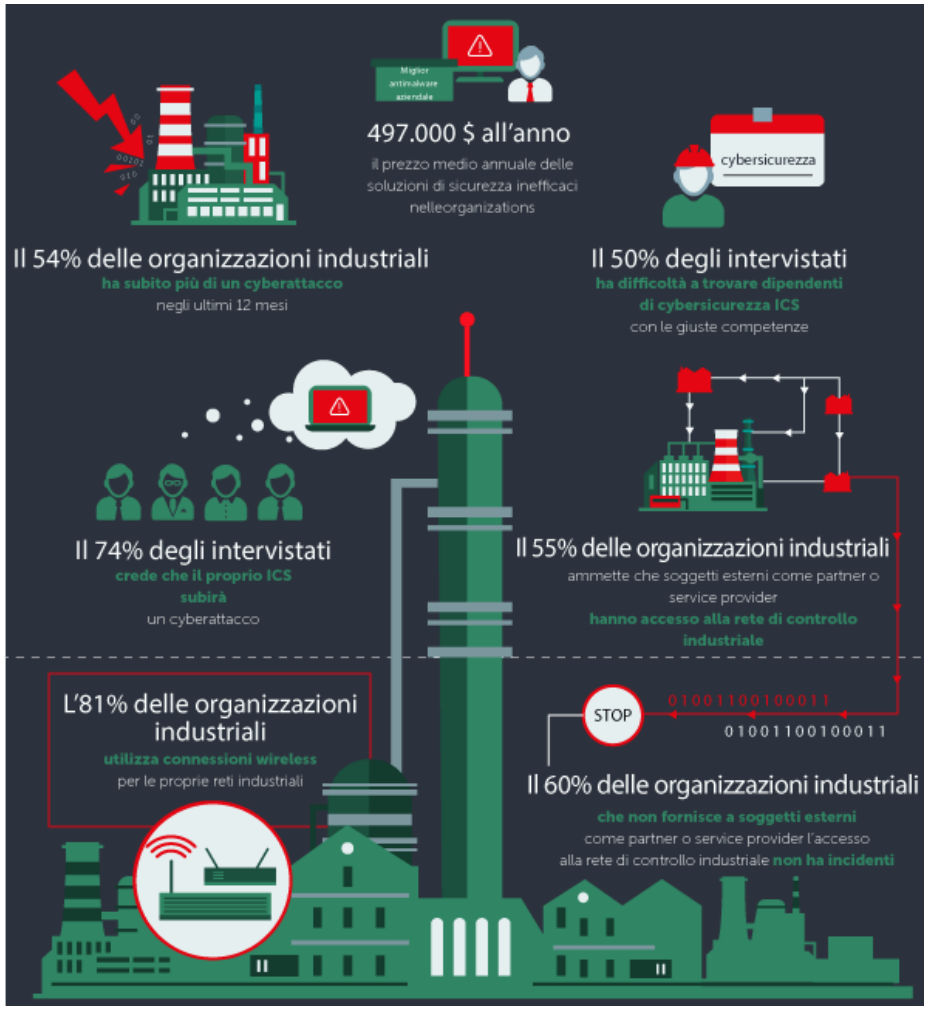
Costo annuale medio per cyberattacchi **€10 mil.**

Crescita annuale media dei costi di cybersicurezza **22,7%**

Numero annuale medio di cyberattacchi **130**

Crescita annuale media del numero dei cyberattacchi **27,4**

Accenture – *Cost of Cybercrime Study* 2017



Kaspersky Industrial Cybersecurity 2017

Il valore delle azioni di società quotate può diminuire, nel periodo successivo ad un serio attacco alla sicurezza, anche del 10%

Lloyd's/Cyence – *Counting the Cost 2017*

IL NUOVO QUADRO NORMATIVO

8 Agosto 2018

D.lgs. 196/2003 riformato

LA CATENA DI FUNZIONI E RESPONSABILITA'

Il primo e fondamentale obiettivo deve essere quello della creazione di una corretta catena di ruoli e responsabilità rispetto a tutti i fornitori di servizi, distributori, agenti, *outsourcer*, partner industriali e commerciali e soggetti esterni a vario titolo coinvolti nell'esecuzione delle attività di *business* e, quindi, nel trattamento di dati e nella gestione della sicurezza.

Security chain

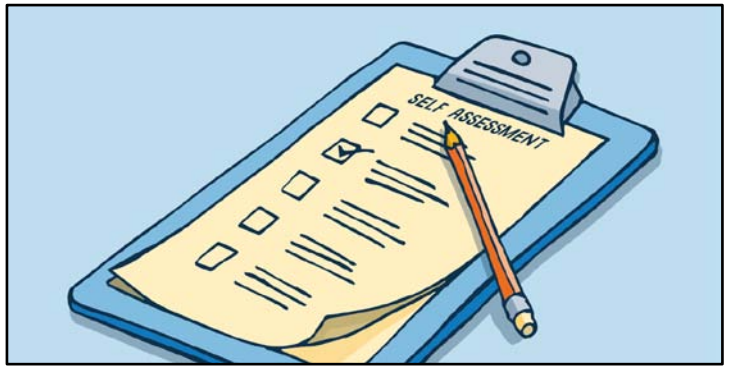
TITOLARE DEL TRATTAMENTO
La persona fisica o giuridica che, da sola o insieme ad altre, raccoglie i dati e detiene il potere di decidere le modalità, le finalità e gli standard di sicurezza del trattamento

RESPONSABILE DEL TRATTAMENTO
La persona fisica o giuridica che tratta dati solo su "delega" scritta del titolare e quindi esclusivamente per conto, nell'interesse e secondo le istruzioni di quest'ultimo

INCARICATO DEL TRATTAMENTO
La persona fisica, operante sotto l'autorità del titolare o del responsabile (es. dipendenti, collaboratori), che svolge materialmente le operazioni di trattamento dei dati

PAROLA D'ORDINE : AUTO-RESPONSABILIZZAZIONE

La principale innovazione introdotta dal GDPR è il rafforzamento del concetto di auto-responsabilizzazione (*accountability*) dell'azienda, la quale dovrà **essere in grado di dimostrare il rispetto degli obblighi imposti dal GDPR**, con particolare riferimento ai principi di (a) **liceità, correttezza e trasparenza dei trattamenti**; (b) **limitazione della finalità dei trattamenti**; (c) **minimizzazione dei dati**; (d) **esattezza ed aggiornamento dei dati**; (e) **limitazione della conservazione dei dati**; (f) **integrità e riservatezza dei dati**.



NIENTE PIU' VERIFICA PRELIMINARE DEL RISPETTO DEGLI OBBLIGHI

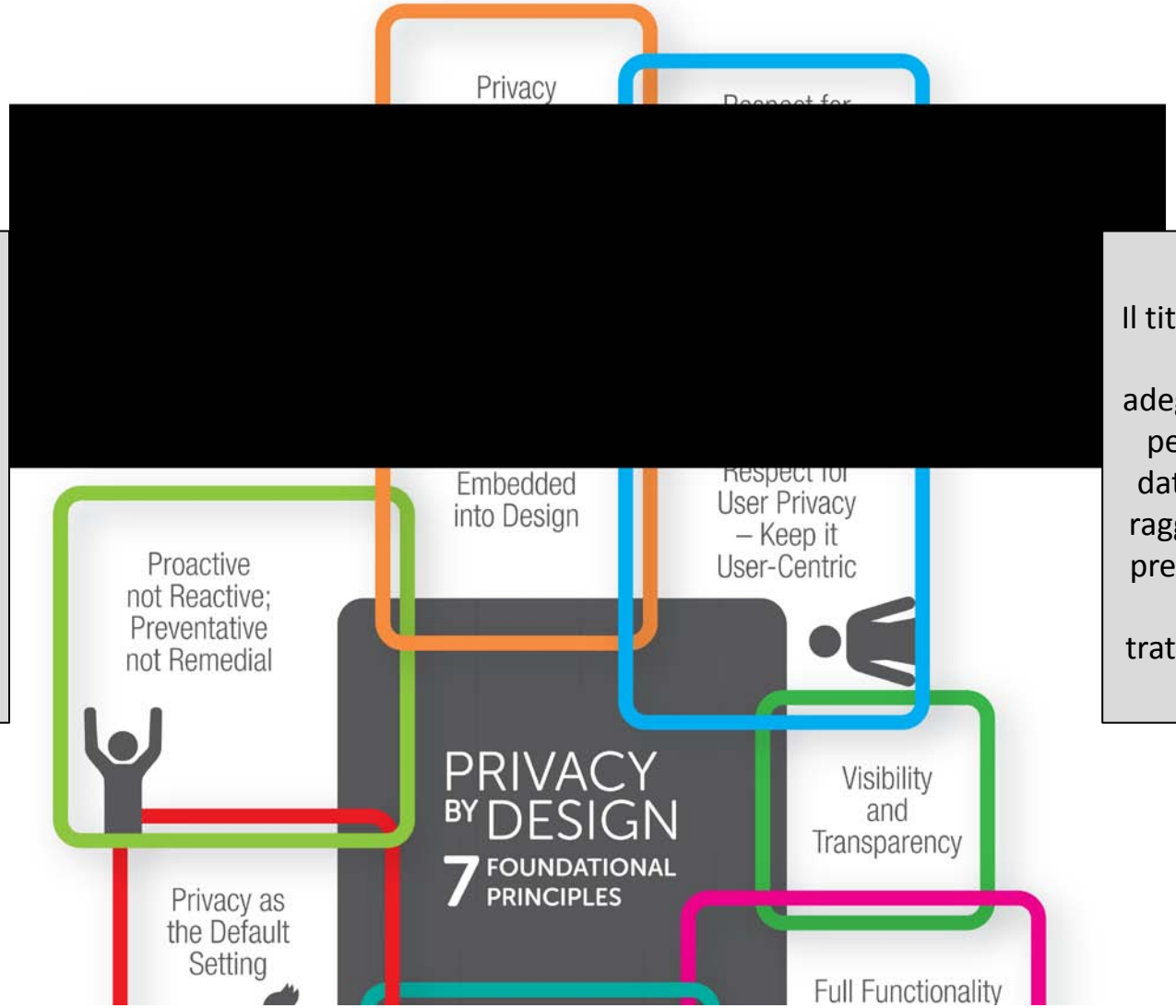
→

AUTOVALUTAZIONE DEI LIVELLI DI SICUREZZA ADOTTATI PER PREVENIRE I RISCHI

NUOVE TECNOLOGIE E SICUREZZA: PRIVACY-BY DESIGN E PRIVACY-BY-DEFAULT

PRIVACY-BY-DESIGN

Tenendo conto dello stato dell'arte, costi di attuazione, natura, ambito di applicazione, contesto, finalità e rischi del trattamento, il titolare, sia al momento di determinare i mezzi del trattamento sia all'atto del relativo svolgimento, adotta misure tecniche e organizzative adeguate a garantire in modo efficace il rispetto i principi di protezione dei dati.



PRIVACY-BY-DEFAULT

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali realmente necessari al raggiungimento delle specifica finalità prefissate, sia in termini di quantità di dati raccolte, che di portata del trattamento, periodo di conservazione ed accessibilità ai dati stessi.

NUOVE TECNOLOGIE: LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Il titolare deve eseguire un'attenta e dettagliata valutazione dell'impatto (*Data Protection Impact Assessment* – "**DPIA**") che i trattamenti che intende svolgere, soprattutto se basati su nuove tecnologie, sono in grado di produrre, quando dagli stessi possono derivare rischi rilevanti per la sicurezza e per i diritti e le libertà delle persone coinvolte.

Elementi minimi della DPIA:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, se applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, con specifica indicazione delle garanzie, misure di sicurezza e meccanismi adottati per garantire la protezione dei dati personali e dimostrare il rispetto del GDPR.

NUOVE TECNOLOGIE: LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

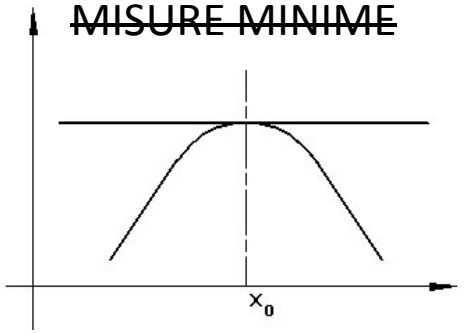
Esattamente nel momento in cui un'azienda innova i propri processi, inventa nuovi servizi o nuove modalità di produzione o di servizio, deve essere presa in considerazione e valutata la protezione dei dati personali, non come una formalità burocratica, ma come una fase strutturale del processo di innovazione, che concorre, insieme ad altre più tradizionali, alla valutazione complessiva sulla sostenibilità del cambiamento.

Si tratta di temi attinenti alla sopravvivenza di tutte le imprese e non prerogative delle grandissime o di alcuni settori. A ben guardare si tratta di aspetti che non riguardano solo la protezione dei flussi informativi, ma anche e soprattutto la sicurezza interna e la tutela dei dati di *business*. Anche per questo nessuna azienda, nemmeno una PMI di produzione che si sente – ed effettivamente è - molto lontana dalle tematiche di privacy e *security*, può chiamarsi fuori e guardare al GDPR come qualcosa che non la riguarda.

LA SICUREZZA IN CONCRETO: QUALI MISURE ADOTTARE?

GDPR: tenendo conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, così come dei rischi per i diritti e le libertà delle persone coinvolte, **occorre mettere in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio**, tra cui ad esempio: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure di sicurezza tecniche e organizzative.

Nel valutare l'adeguatezza del livello di sicurezza, si deve tener conto in particolare dei rischi derivanti dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati.



IL DATA PROTECTION OFFICER (DPO)

Quando va nominato?

Nel caso in cui:

- ✓ il titolare sia un'autorità pubblica o un organismo pubblico (tranne le autorità giurisdizionali nelle loro funzioni);
- ✓ le attività principali del titolare consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- ✓ le attività principali del titolare del consistono nel trattamento, su larga scala, di dati sensibili o giudiziari.

In *outsourcing*

Interno all'azienda

Totale indipendenza

Diretto riporto ai vertici aziendali

In posizioni che non generano conflitti di interessi

Competenza specialistica in materia di sicurezza dei dati

IL DATA PROTECTION OFFICER (DPO)

Con quali funzioni?

Almeno le seguenti:

a) informare e fornire consulenza al titolare e ai dipendenti riguardo agli obblighi di protezione e sicurezza dei dati;
b) vigilare sull'osservanza della normativa e delle policy aziendali in materia;
c) sorvegliare sull'attribuzione di ruoli e responsabilità;
d) vigilare sulla formazione del personale;
e) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
f) cooperare con l'Autorità per la Protezione dei Dati Personali (il "Garante");
g) fungere da punto di contatto per il Garante in relazione ad ogni questione riguardante trattamenti e sicurezza dei dati.

GESTIONE DELLE VIOLAZIONI DELLA SICUREZZA (*DATA BREACH*)

Violazione dei dati personali (*data breach*) nel GDPR: *la violazione della sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati.*

Funzioni maggiormente soggette al rischio di data breach

Cisco – *Annual Cybersecurity Report 2017*

VIOLAZIONI DELLA SICUREZZA: OBBLIGO DI NOTIFICAZIONE

Senza ritardo e non oltre 72 ore dal momento in cui il titolare ne è venuto a conoscenza

Obbligo generale di notificazione delle violazioni di dati personali

Al Garante

A meno che sia improbabile che la violazione possa consistere in un danno agli individui

Agli interessati

Se è probabile che la violazione risulti in un grave rischio ai diritti o alle libertà individuali

Alcuni elementi di mitigazione

- Formazione dei dipendenti;
- Adozione di processi e procedure codificate e collaudate;
- Tempestiva identificazione degli elementi di rischio;
- Gestione delle comunicazioni ufficiali (stampa, istituzioni, interessati, ecc.);
- Capacità di reazione alle emergenze anche fuori orario;
- Ricorso ad un consulente legale specializzato 24/7;
- *Compliance* rispetto a tutte le norme principali del GDPR;
- Adozione di polizze assicurative contro il rischio *data breach;*
- Modalità di ripristino delle funzionalità dei sistemi IT;
- Back-up dei sistemi continuativo e aggiornato;
- *Self-hacking* come strumento di prevenzione e difesa;
- Tutela del dato come *asset* competitivo e leva di sviluppo.

NUOVI E VECCHI DIRITTI

Diritto di Accesso

L'interessato può chiedere in qualsiasi momento al titolare di confermare se sia o meno in corso un trattamento di dati personali che lo riguardano e, in caso positivo, di poter ottenere informazioni a riguardo.

Diritto di Rettifica

L'interessato ha il diritto di ottenere, da parte del titolare, la rettifica di propri dati personali inesatti o la loro integrazione qualora incompleti, senza ingiustificato ritardo.

Diritto alla Cancellazione (all'oblio)

L'interessato ha il diritto di ottenere, da parte del titolare, la cancellazione dei propri dati. Il titolare è tenuto a procedere, senza ingiustificato ritardo, in presenza di terminate ragioni (es. dati non più necessari, revoca del consenso su trattamento dati particolari, ecc.).

Diritto alla Limitazione del trattamento

L'interessato ha il diritto di ottenere la limitazione del trattamento di propri dati personali in presenza di determinate motivazioni (es. contestazione dell'esattezza dei dati, trattamenti ritenuti illeciti, esercizio o difesa di un proprio diritto in sede giudiziaria, esercizio di altri diritti ex GDPR).

Diritto alla Portabilità

L'interessato può chiedere ed ottenere, in un formato strutturato di uso comune e leggibile, i propri dati personali forniti al titolare oppure chiederne il trasferimento. direttamente da titolare a titolare.

Diritto di Opposizione

L'interessato può opporsi al trattamento dei propri dati personali in qualsiasi momento. L'esercizio di tale diritto è maggiormente accentuato nei casi in cui il trattamento sia svincolato dall'esplicito consenso dell'interessato.

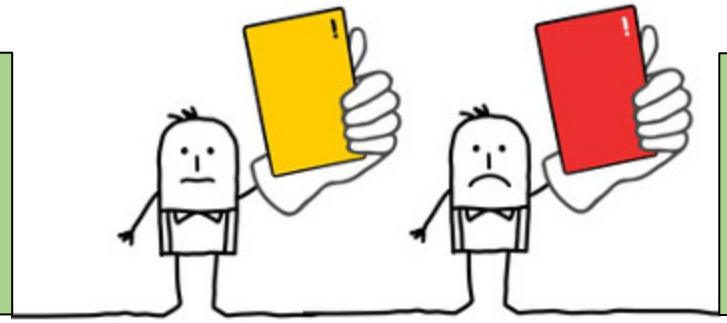
Diritto a non essere sottoposto a processi di decisione automatizzati

Qualora il trattamento venga effettuato. da processi automatici capaci di incidere direttamente sulle libertà e i diritti del soggetto, senza la possibilità di un intervento correttivo dell'uomo, l'interessato ha diritto a non esserne sottoposto.

IL REGIME SANZIONATORIO

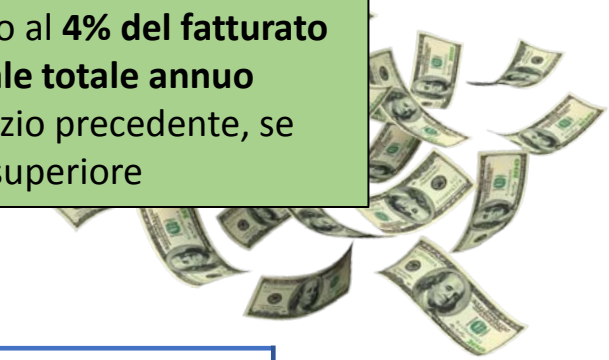
Violazione, tra l'altro, degli obblighi di sicurezza

Fino a **10 milioni di Euro** o, per le imprese, fino al **2% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore



Violazione, tra l'altro, dei diritti e dei principi fondamentali

Fino a **20 milioni di Euro** o, per le imprese, fino al **4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore



Provvedimenti del Garante
Il Garante può esercitare poteri estremamente incisivi, arrivando persino ad inibire il trattamento

Risarcimento del danno
Chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento

Sanzioni penali
Il GDPR ha delegato agli Stati membri il potere di introdurre sanzioni penali o mantenere quelle attualmente applicabili

AFFIDABILITÀ, FIDUCIA E VALORE

Promozione della trasparenza sulle politiche aziendali di trattamento dei dati

Semplificazione delle procedure di esercizio dei diritti individuali

Adesione a codici di condotta e meccanismi di certificazione riconosciuti

Implementazione di misure di sicurezza idonee a prevenire i maggiori rischi identificati

Adozione di procedure aziendali di gestione dei principali adempimenti

GRAZIE DELL'ATTENZIONE

Treasury & Finance Forum Day 2018

PANETTA & ASSOCIATI

STUDIO LEGALE

Avv. Lorenzo Cristofaro – *Counsel*

P&A Studio Legale

Via Arenula 83

Roma – 00186

l.cristofaro@panetta.net