COME ASSICURARE LA CONFORMITA' IT, DIMINUENDO IL RISCHIO DI SANZIONI E DISPORRE UN SISTEMA DI CONTROLLO ADEGUATO

Webinar in collaborazione con

GRUPPOIMPERIALI

MEGA
SEE THE BIGGER PICTURE

Associazione Italiana Internal Auditors

28 Settembre 2021

COME AFFRONTARE LA CONFORMITA' IT, DIMINUENDO IL RISCHIO DI SANZIONI, E DISPORRE UN SISTEMA DI CONTROLLO ADEGUATO

ANDREA CAPPELLETTI

Revenue & Business Development Manager - AIIA

Associazione Italiana Internal Auditors

GRUPPOIMPERIALI

MEGA
SEE THE BIGGER PICTURE

INTERVENGONO:

ALBERTO DIARI
Director
MEGA International

ANNA IRACE
Coordinatrice Area Compliance
Gruppo Imperiali

ELISA PASSANTE
Solution Manager
MEGA International

FRANCESCO BLAFO
Service Partner
MEGA International

AVV. DIEGO CORDUA
Gruppo Imperiali

AVV. LUCREZIA D'AVENIA
Gruppo Imperiali

MEGA
SEE THE BIGGER PICTURE

GRUPPOIMPERIALI

Associazione Italiana Internal Auditors

COME AFFRONTARE LA CONFORMITA' IT E DISPORRE UN SISTEMA DI CONTROLLO ADEGUATO
Sfide e strategie

ALBERTO DIARI
MEGA International
adiari@mega.com

Associazione Italiana Internal Auditors

GRUPPOIMPERIALI

MEGA
SEE THE BIGGER PICTURE

IT COMPLIANCE

Aumento delle violazioni di sicurezza informatica e anche dei costi:

- Aumento del numero di attacchi informatici a causa della digitalizzazione del business e della pandemia: es (lavoro da remoto)
- Le leggi sulla privacy come la GDPR possono significare multe ingenti per le organizzazioni che subiscono violazioni della sicurezza informatica, senza considerare anche i costi non finanziari come i danni alla reputazione

La Compliance IT è diventata una priorità assoluta in tutte le organizzazioni fino alla C-suite:

- La motivazione principale è che quasi ogni azienda si basa su una combinazione di risorse digitali alimentate da dati. Quindi, questi dati devono essere adeguatamente gestiti, archiviati e protetti, e il mancato rispetto di questa regola porta a multe normative, copertura mediatica negativa e perdita di fatturato
- Gli attacchi informatici sempre più sofisticati. Questi includono ingegneria sociale, malware e ransomware

MEGA
SEE THE BIGGER PICTURE

GRUPPOIMPERIALI

Associazione Italiana Internal Auditors

LA TEMPESTA PERFETTA PORTA UNA NUOVA SERIE DI SFIDE

L'aumento del crimine informatico

- Garantire la sicurezza IT
- Evitare interruzioni operative
- Proteggere i dati aziendali
- Evitare danni finanziari e di reputazionali

Nuove normative e regolamentazioni

- Assicurare la conformità agli standard normativi
- Gestire la complessità e il cambiamento normativo
- Evitare danni finanziari e reputazionali

La nascita di un nuovo comportamento lavorativo

- Sostenere la digitalizzazione del business
- Gestire la generalizzazione del lavoro a distanza
- Abbracciare in modo sicuro IoT, IA, Analytics, ...

UN'ORGANIZZAZIONE SOTTO ATTACCO INFORMATICO

L'Aumento del Cybercrime

$ 1Trn (1% World GDP)

Costo globale del cybercrime nel 2020

30 000

Numero di cyber-attacchi quotidiani solo negli Stati Uniti (+800% : Fonte FBI)

Il Costo del Cybercrime

$ 4.24M

Costo medio globale della violazione dei dati nel 2021

280 giorni

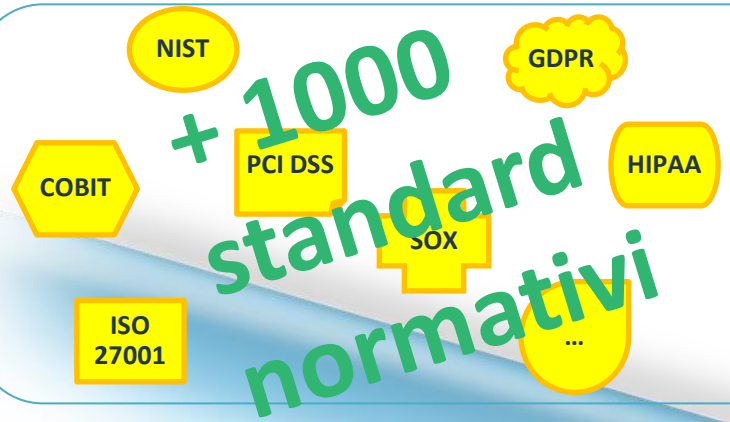
Tempo medio per identificare e contenere una violazione dei dati

2021 Sanzioni GDPR

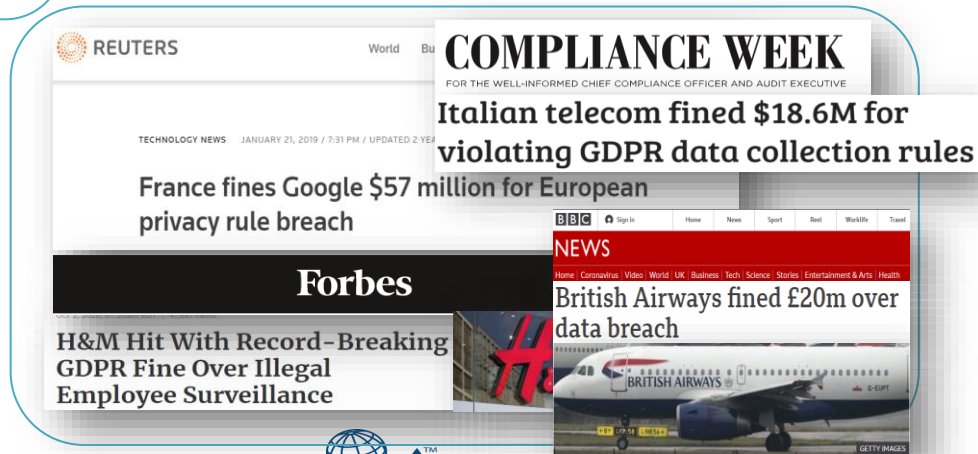
WhatsApp riceve una multa di $267 milioni per violazioni sulla GDPR

Amazon $888M di sanzione per la GDPR

Aumento di Normative e Regolamentazioni



Il Costo delle Regolamentazioni



https://www.cpomagazine.com/data-protection/whatsapps-267-million-gdpr-fine-shows-willingness-of-irish-dpa-to-issue-large-penalties/
https://iapp.org/news/a/tech-company-issued-888m-gdpr-fine/
Ibm.com. 2021. *Cost of a Data Breach Report 2021*. [online] Available at: <https://www.ibm.com/security/data-breach> [Accessed 27 September 2021].

COME L'IT COMPLIANCE PROTEGGE LA VOSTRA AZIENDA

La conformità IT fornisce alle organizzazioni un **approccio strutturato** per garantire la **sicurezza** e la **legalità** delle risorse digitali, migliorando la **resilienza del business**

Un approccio in tre fasi:

Analizzare

Mappare i regolamenti e gli standard di settore rispetto alle risorse IT
Individuare i rischi e i presidi di controllo

Gestire

Raggiungere la conformità IT attraverso la valutazione continua e attuazione dei piani di rimedio

Dimostrare

Dimostrare un'efficace conformità IT al management e alle Autorità

MEGA
SEE THE BIGGER PICTURE

GRUPPOIMPERIALI

Associazione Italiana Internal Auditors

COMPRENDERE I RISCHI NEL CONTESTO DELLE OPERATIONS

Analizzare:

1) Avere una visione **unificata** delle informazioni gestite da IT, Business e Funzioni di controllo
2) Avere un framework completo delle **normative** e dei **rischi di non conformità**
3) Individuare le dipendenze tra le normative e gli elementi della mia organizzazione (**processi, Applicativi, Risorse**)

Gestire:

1) Disporre di strumenti per la **valutazione dei rischi** a cui sono soggetto e il monitoraggio continuo
2) Individuazione delle criticità e condivisione dei **piani di rimedio**

Dimostrare:

1) **Comunicare** internamente
2) **Dimostrare** efficacemente le attività svolte

Associazione Italiana Internal Auditors

COME AFFRONTARE LA CONFORMITA' IT, DIMINUENDO IL RISCHIO DI SANZIONI, E DISPORRE UN SISTEMA DI CONTROLLO ADEGUATO

La quadratura del cerchio tra misure tecniche e organizzative

ANNA IRACE
Gruppo Imperiali
anna.irace@imperiali.com

Associazione Italiana Internal Auditors

GRUPPOIMPERIALI

MEGA
SEE THE BIGGER PICTURE

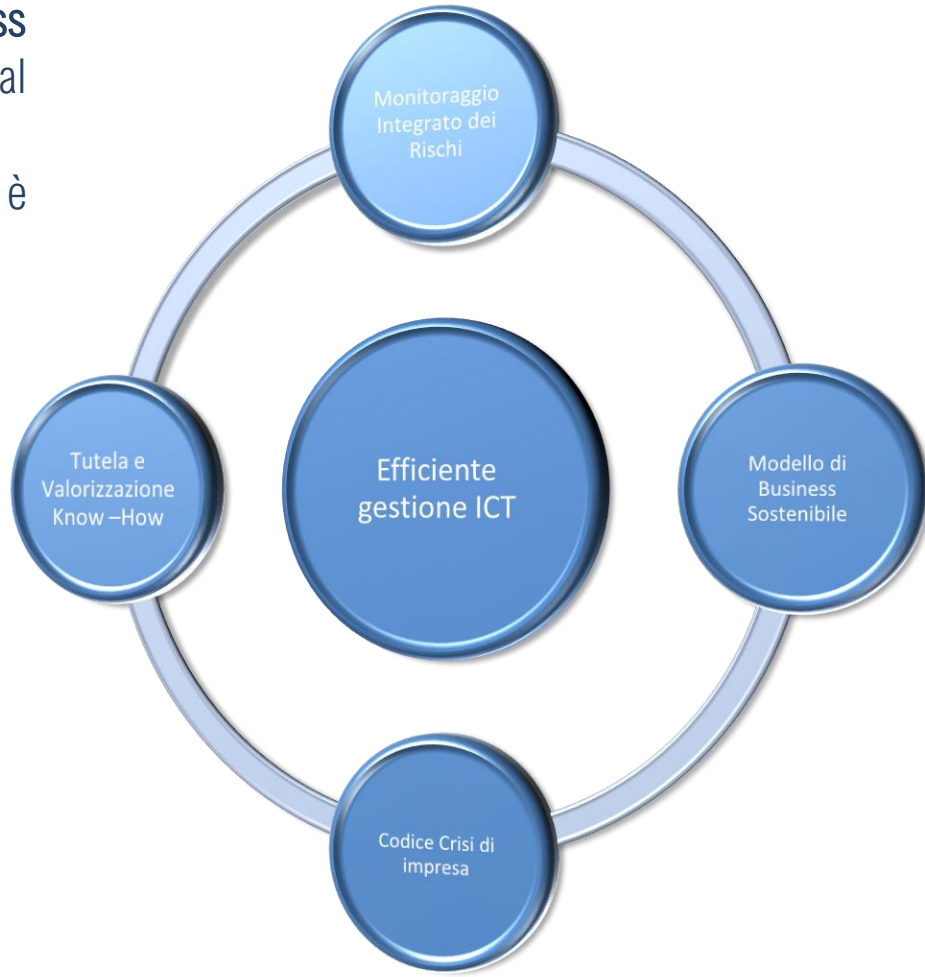
LA QUADRATURA DEL CERCHIO TRA MISURE TECNICHE E ORGANIZZATIVE

La compliance IT è parte integrante dei processi aziendali oggi indispensabile per consentire l'implementazione in modo strutturato, efficace ed organico di **un modello di business sostenibile,** consentendo all'imprenditore di poter adempiere alle diverse normative in base al **principio di accountability -** «filo rosso» che unisce diverse normative (GDPR, 231, 262 etc).
Con l'aiuto dei nostri esperti, il tentativo è di illustrare come la compliance del sistema IT è indispensabile per assicurare:

- ❑ **L'implementazione e gestione di modelli organizzativi integrati trasversali ai vari processi favorendo la protezione di valore:**

a) Tutela e valorizzazione del know-how
b) Controllo Integrato dei rischi, protezione del patrimonio aziendale rispetto al rischio di «non conformità»

- ❑ **L'implementazione di un Modello di Business Sostenibile favorendo la creazione di valore efficientando il raggiungimento di obiettivi di business (valorizzare CRM, campagne di fidelizzazione etc.)**



COME ASSICURARE LA CONFORMITA' IT E DISPORRE UN SISTEMA DI CONTROLLO ADEGUATO

…la parola agli esperti…

Associazione Italiana Internal Auditors

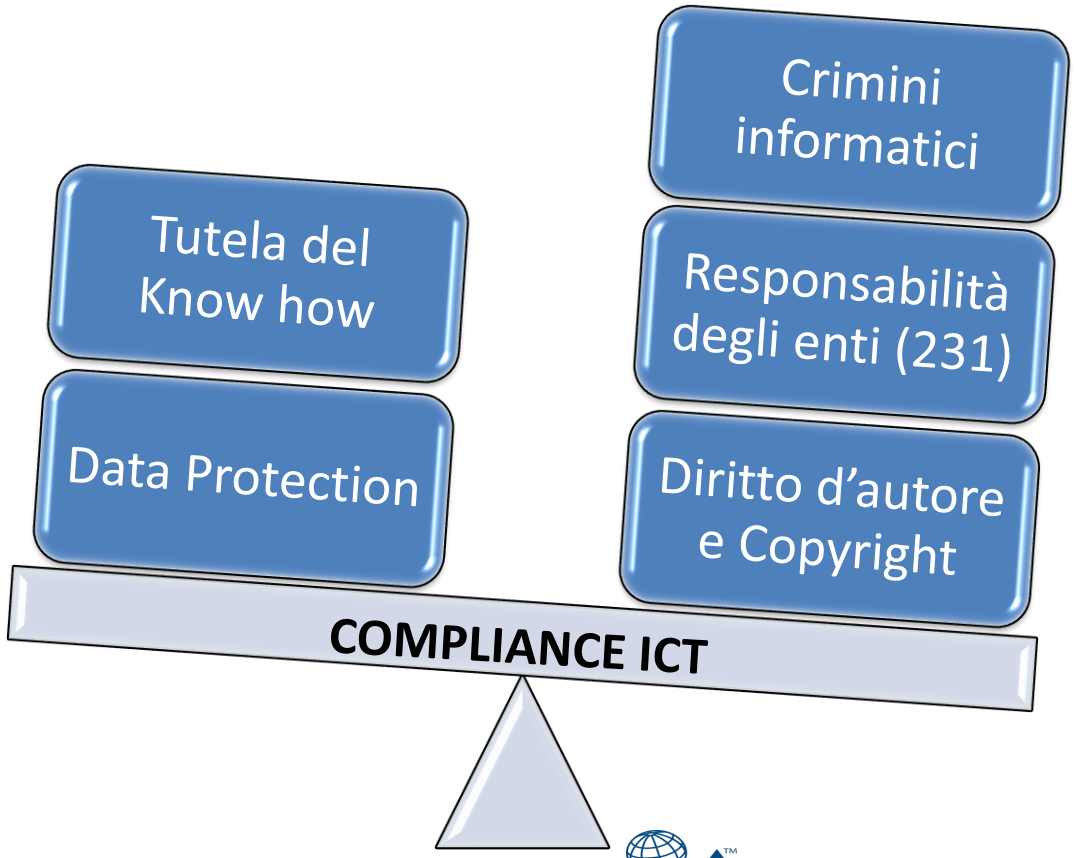
GRUPPOIMPERIALI

MEGA
SEE THE BIGGER PICTURE

LA COMPLIANCE DEI SISTEMI IT COME ELEMENTO CENTRALE PER DIVERSE DISCIPLINE NORMATIVE

la compliance dei sistemi ICT coinvolge diverse discipline normative → a quali standard affidarsi?

1. Ottimizzazione dei controlli su più fronti normativi;
2. Interazione tra organi di controllo (IA – DPO – ODV 231 – Compliance…);
3. Investimenti integrati sul sistema ICT.



NUOVO APPROCCIO ALLA COMPLIANCE INTRODOTTO DAL REGOLAMENTO EU 2016/679

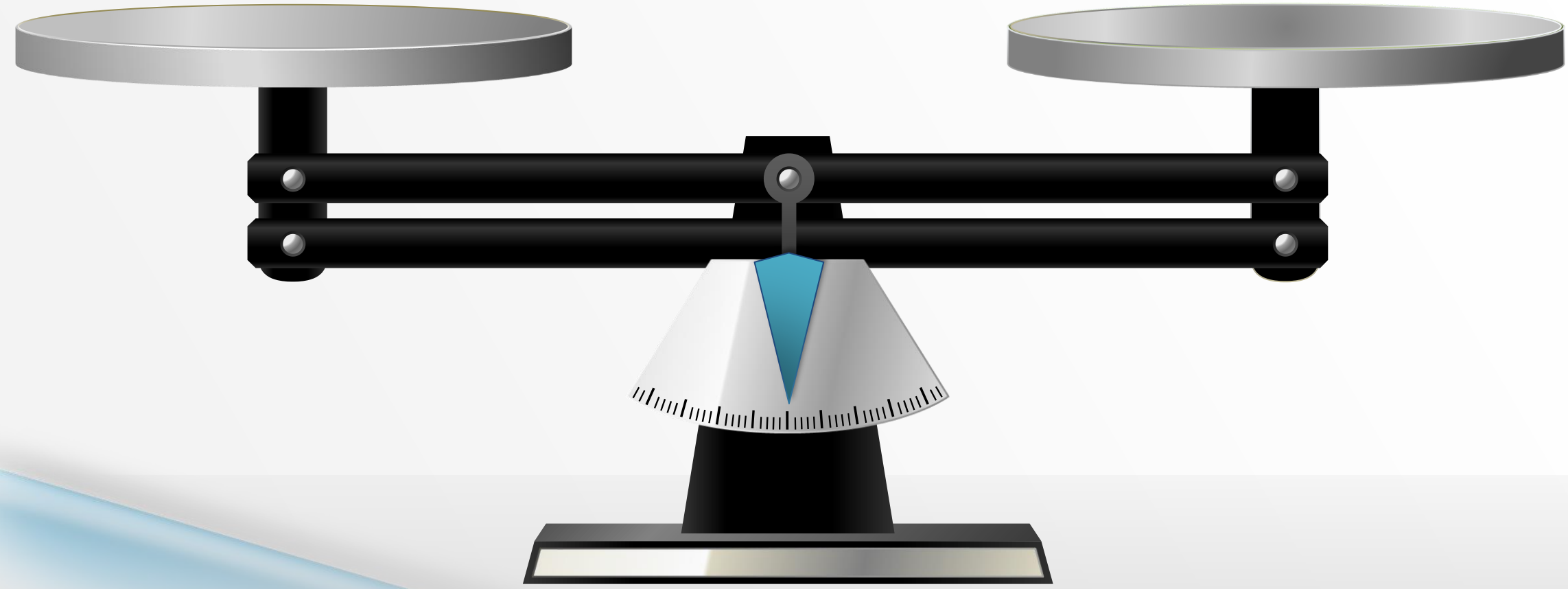
Il Legislatore europeo, con il principio di ***Accountability***- *ossia l´adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l´applicazione del Regolamento*- ha inteso creare uno **strumento flessibile**, in grado di adattarsi a tutte le diverse realtà aziendali (PMI, colossi del web, etc).

Il Legislatore europeo ha adottato un approccio ***«Risk based»*** invece che un classico approccio di tipo prescrittivo.
La scelta delle misure di sicurezza da adottare non sarà dunque rispondente a canoni predeterminati, ma dovrà essere effettuata caso per caso tenendo conto dello stato dell'arte (del grado di avanzamento della tecnologia) e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

I VANTAGGI E GLI SVANTAGGI DEL NUOVO APPROCCIO ALLA COMPLIANCE

flessibilità, uguaglianza, efficacia, autonomia

Valutazione continua, impiego di risorse multidisciplinari, documentazione delle scelte

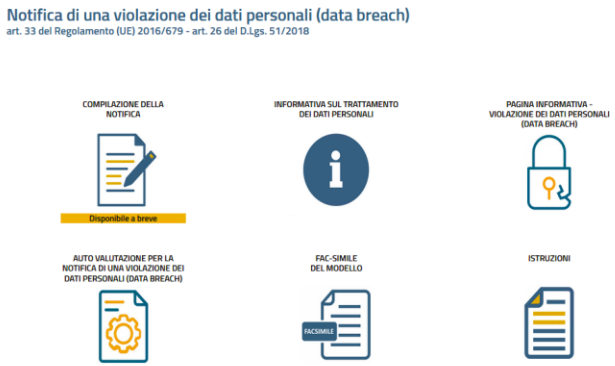


Associazione Italiana Internal Auditors

DATA BREACH: INDIVIDUAZIONE E CORRETTA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

1. Ogni data breach è una violazione di sicurezza, ma non ogni violazione di sicurezza è un data breach;
2. Un data breach può essere doloso, ma anche accidentale;
3. Un data breach può derivare da fattori tecnici e da fattori umani;
4. Non tutti i data breach vanno denunciati alla Polizia Postale;
5. Quando e come effettuare la notifica del data breach al Garante per la Protezione dei Dati Personali;
6. Quando e come effettuare la comunicazione del data breach agli interessati.

Case Studies



[Home - Notifica di una violazione dei dati personali (data breach) (gpdp.it)]

MEGA SEE THE BIGGER PICTURE

GRUPPOIMPERIALI

Associazione Italiana Internal Auditors

LA VALUTAZIONE DEL SISTEMA ICT IN SEDE DI VERIFICA ISPETTIVA DEL GARANTE

1. La verifica delle misure tecnologiche a tutela dei dati personali.
2. Lo standard fornito dallo schema di certificazione INVEO (ISDP10003:2020) e dal Tool.
3. L'importanza della scelta dei fornitori di servizi ICT e dell'adozione di un modello di valutazione del rischio degli stessi; la pianificazione di audit ai fornitori.

Pseudonimizzazione e cifratura dei dati personali
Garanzia di riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento
Ripristino di disponibilità e accesso dei dati personali in caso di incidente fisico o tecnico
Procedura di test – verifica – valutazione regolare dell'efficacia delle misure tecniche ed organizzative per garantire la sicurezza del trattamento
Principali applicazione usate sui sistemi – client server\web application
Misure idonee per accedere a banche dati (username e pwd, strong authentication)
Audit effettuato internamente o presso eventuali responsabili esterni
Eventuali alert implementati su sistemi
Eventuale backup di dati

CASE STUDIES: SANZIONI DEL GARANTE IN TEMA DI MISURE DI SICUREZZA

1. **Whistleblowing**: sanzione per carenza di misure di sicurezza tecniche (cifratura, protocollo di rete sicuro, controllo degli accessi applicativo etc.) *[Ordinanza ingiunzione nei confronti di Aeroporto Guglielmo Marconi di Bologna S.p.a. - 10 giugno 2021 (9685922); Ordinanza ingiunzione nei confronti di aiComply S.r.l. - 10 giugno 2021 (9685947)];*

2. Regolarizzazione dei ruoli DP: «Il rapporto tra titolare e responsabile deve essere regolato da un contratto o da altro atto giuridico, stipulato per iscritto che, oltre a vincolare reciprocamente le due figure, consente al titolare di impartire istruzioni al responsabile e prevede, in dettaglio, quale sia la materia disciplinata, la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare. Il Responsabile del trattamento è, pertanto, legittimato a trattare i dati degli interessati "soltanto su istruzione documentata del titolare " (art. 28, par. 3, lett. a) del Regolamento)». *Ordinanza ingiunzione nei confronti di Roma Capitale - 22 luglio 2021 [9698724]*

COMPRENDERE I RISCHI NEL CONTESTO DELLE OPERATIONS

Un approccio in tre fasi:

Analizzare

Mappare i regolamenti e gli standard di settore rispetto alle risorse IT
Individuare i rischi e i presidi di controllo

Gestire

Raggiungere la conformità IT attraverso la valutazione continua e attuazione dei piani di rimedio

Dimostrare

Dimostrare un'efficace conformità IT al management e alle Autorità

Associazione Italiana Internal Auditors

MEGA
SEE THE BIGGER PICTURE

GRUPPOIMPERIALI

Associazione Italiana Internal Auditors

1. **In fase di selezione di fornitore, la strada più semplice e pratica è affidarsi a delle clausole contrattuali con cui si richiede al fornitore di rispettare determinate misure di sicurezza ritenute accettabili per il titolare. Nella realtà aziendale, in cui sono selezionati numerosi nuovi fornitori ogni mese, come è possibile conciliare la verifica del titolare su tali misure in fase di selezione del fornitore?**

Nelle realtà aziendali più sensibili all'esigenza rappresentata, suggeriamo la predisposizione di un documento di «valutazione preliminare», con il supporto del dipartimento ICT/Cyber security, utilizzando preferibilmente uno standard diffusamente riconosciuto. Tale documento andrebbe strutturato in base ai principali focus (es. disaster recovery, log management, penetration tests, back up, crittografia, etc), sempre con riserva di eventuale audit in corso di contratto.

Una volta ottenute le dovute garanzie sulle misure previste e concordate per il trattamento affidato in outsourcing, queste potranno essere cristallizzate tramite DPA (data processing agreement) ex art. 28 GDPR.

Nella fase successiva di esecuzione del contratto, l'attuazione delle misure concordate potrà essere oggetto di verifica tramite attività di Audit sul fornitore. Nelle realtà più complesse, si consiglia di adottare una procedura interna di gestione di tali verifiche che preveda, partendo da una pianificazione annuale, l'adozione di uno strumento di valutazione della criticità del fornitore, su cui intervenire con appositi piani di remediation.

2. Come si possono monitorare le misure di sicurezza degli applicativi gestiti da fornitore esterno? Tramite certificazioni o altro?

Nel modo più semplice: in fase di selezione del fornitore si consiglia di acquisire e valutare, con il supporto del dipartimento ICT o del consunte esterno in materia, una scheda tecnica dell'applicativo che riporti le misure di sicurezza predisposte, oltre che la prova di eventuali certificazioni rilevanti (es. UNI EN ISO 27001) e di eventuali valutazioni di impatto ex. art. 35 GDPR effettuate sul prodotto dal Fornitore.

Successivamente, in fase di stipula del contratto, si suggerisce di richiedere al fornitore di allegare al DPA ex. art. 28, sottoscritto contestualmente tra le parti, un documento relativo alle misure di sicurezza garantite.

Successivamente, in fase di esecuzione del contratto, sarebbe opportuno sottoporre i fornitori a più alto rischio ad attività di Audit.

3. Come accrescere la "cultura" della cybersec a tutti i livelli dell'organizzazione?

Attraverso misure organizzative quali:

Formazione e sensibilizzazione, possibilmente customizzata e intuitiva, di tutte le risorse aziendali che utilizzano dispositivi ICT;

Elaborazione e diffusione di Policy sull'utilizzo degli strumenti informatici che forniscano indicazioni sui comportamenti da adottare per arginare il rischio di perdite di dati e informazioni (in aggiunta alla Policy, anche le infografiche fornite dal Garante Privacy su malware, phishing etc. possono essere utili);

Elaborazione e diffusione di una Procedura di gestione delle violazioni;

Responsabilizzazione delle risorse apicali nel controllo sull'applicazione delle dette procedure da parte dei sottoposti;

«fail and learn», approfittando di qualsiasi episodio di incident/data breach per creare buone pratiche aziendali

4. Potete gentilmente ripetere il nome del sistema / piattaforma it per la digital governance?

La piattaforma proposta da MEGA per la Digital Governance è HOPEX. Le soluzioni HOPEX collegano business, IT, dati e prospettive di rischio in un'unica piattaforma collaborativa che si integra in tutto l'ecosistema aziendale. Avere una visione integrata di tutto l'ecosistema aziendale permette alle aziende di adattarsi ad un panorama economico in continuo cambiamento ottenendo una migliore comprensione e analisi su come opera l'azienda ed aiuta a prendere le decisioni giuste ed accelerare il valore del business.

Maggiori informazioni sono disponibili sul sito MEGA o contattando uno dei commerciali MEGA.

https://www.cpomagazine.com/data-protection/whatsapps-267-million-gdpr-fine-shows-willingness-of-irish-dpa-to-issue-large-penalties/