L'ADEGUAMENTO GDPR PER LA CREAZIONE DI VALORE

PROGRAMMA

9.00 Registrazione partecipanti

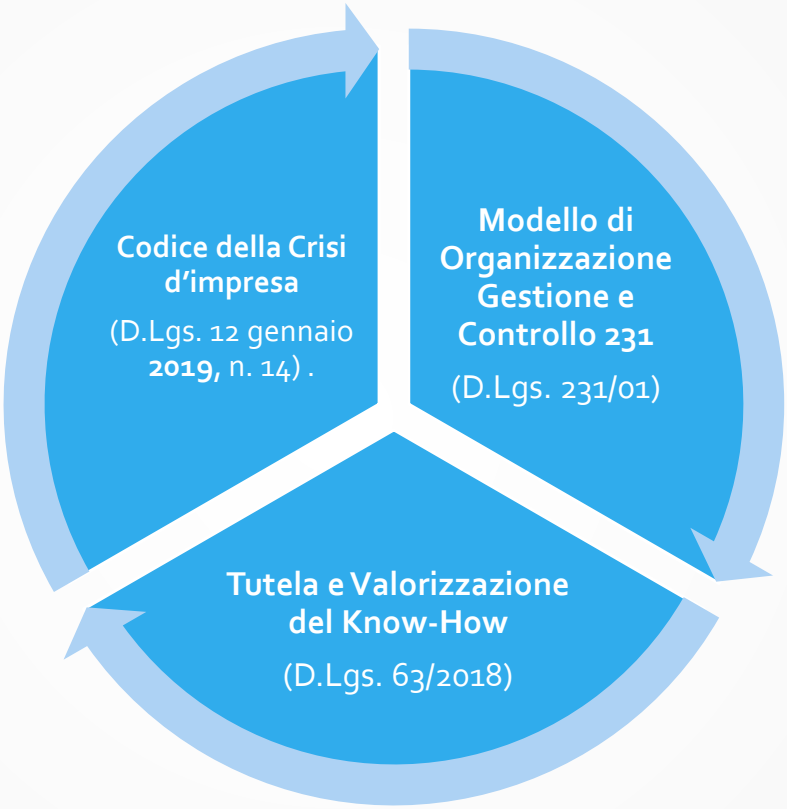
- **Introduzione lavori**
- **Ore 9.30** **Dr.ssa Lina Piccolo** - Vicepresidente delegato Ambiente Sicurezza e Privacy di Confindustria Salerno
- **Interventi**
- **Ore 10.00** **Avv. Riccardo Imperiali di Francavilla - Partner Gruppo Imperiali**
- Aggiornamenti alla normativa di riferimento
- Adeguamento al GDPR: cenni ai principali adempimenti
- **Ore 11.00** **Coffee break**
- **Ore 11.30** **Dr.ssa Anna Irace - Responsabile Compliance - Gruppo Imperiali**
- A che punto siamo? L'importanza di una gap analysis
- Pilastri portanti dell'adeguamento GDPR
- "Procedure organizzative" GDPR:
- Esercizio del diritto di accesso
- Procedura data breach e registro data breach
- Gestione delle Terze parti e audit terze parti
- Il ruolo del DPO e i flussi Informativi

Focus

- Privacy, valorizzazione e tutela del Know how
- **Ore 13.00** **Quesiti**

Pilastri GDPR

Ma non solo…


Codice della Crisi d'impresa
(D.Lgs. 12 gennaio **2019,** n. 14) .
Modello di Organizzazione Gestione e Controllo 231
(D.Lgs. 231/01)
Tutela e Valorizzazione del Know-How
(D.Lgs. 63/2018)

Approccio basato sul rischio»

Il GDPR chiede all'impresa di valutare.

Il nuovo regime introdotto dal GDPR è **basato sul rischio** e questo approccio presuppone una costante **capacità valutativa** ad opera dell'azienda titolare del trattamento dei dati.

L'attenzione collettiva è stata attratta dall'istituzione della valutazione d'impatto (DPIA) ponendo in secondo piano la circostanza **che quasi ogni regola del GDPR presuppone un processo valutativo del titolare**, come dimostra la stessa determinazione del "rischio elevato", presupposto di obbligatorietà della DPIA.

Valutazione continua

In base alla riforma non è più sufficiente limitarsi a rispondere alle prescrizioni di legge ma occorre che l'azienda valuti preventivamente gli impatti che il proprio trattamento possa causare in termini di rischi per gli interessati.

Il concetto di Rischio nel GDPR

Il "rischio" data protection può avere **probabilità e gravità diverse**, in relazione al contesto ed ambito applicativo, alla natura dei dati personali, alla finalità del trattamento.

Il rischio è la probabilità che il trattamento **causi danni fisici, materiali o immateriali, alle persone cui si riferiscono i dati; ciò include la profilazione o il trattamento che potrebbe portare a discriminazione, furto d'identità, danno alla reputazione o inversione della pseudonimizzazione (cioè il passaggio da un'informazione codificata ad una resa nuovamente identificativa**).

Processo di valutazione dei rischi riferito ai trattamenti

La valutazione **dei rischi sui diritti e le libertà degli interessati**, conseguenti all'effettuazione di specifici trattamenti, si distingue in **due principali tipologie:**

La **valutazione preliminare**
La **valutazione d'impatto** o DPIA.

Il **processo di valutazione dei rischi** relativi ai trattamenti **si compone di distinte fasi** che hanno l'obiettivo di identificare e minimizzare i rischi impattanti i diritti e le libertà fondamentali degli interessati, incoraggiando sistemi di protezione adeguati ed efficaci.

I ° FASE - Valutazione prima

Prima della DPIA occorre effettuare **una precisa valutazione detta "preliminare".** La valutazione viene detta "preliminare" per due motivi:

- in quanto essa **precede la valutazione d'impatto**, la quale diventa obbligatoria solo se la valutazione precedente attesta la presenza di un rischio elevato nel trattamento considerato
- perché tale valutazione deve essere effettuata **prima che il trattamento sia realizzato**, in quanto il legislatore persegue l'obiettivo di utilizzare i dati personali in contesti a rischio contenuto.

Pertanto, il binomio valutazione preliminare / DPIA consente di:

1. individuare i trattamenti a potenziale rischio elevato
2. mitigare il rischio "elevato" sino a soglie contenute.

Oggetto di valutazione preliminare e di DPIA (Data Protection Impact Analysis)

Si è detto che la valutazione preliminare precede ed è condizione essenziale della DPIA; nel senso che la DPIA può ritenersi obbligatoria solo se, in precedenza, il rischio connesso ad un determinato trattamento sia stato valutato (o si sarebbe dovuto valutare) di **livello elevato** per i diritti e le libertà degli interessati.

Insieme alla distinzione temporale, **le due valutazioni** si differenziano anche per **il loro oggetto**:

- La **valutazione preliminare** deve essere effettuata **su tutti i trattamenti** posti in essere dall'azienda-titolare (al fine di riscontrarne eventualmente il livello elevato del connesso rischio)
- La DPIA riguarda solo quei trattamenti già considerati a **probabile rischio elevato** (riscontrati mediante la valutazione preliminare); nei casi dubbi, tuttavia, le linee guida wp248 rev.01 raccomandano «*di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati*».

Metodologia delle due valutazioni

Sotto il profilo metodologico, è importante che la valutazione preliminare sia impostata in modo agevole in quanto essa deve essere in grado:

- ❑ di scansionare tutti i trattamenti, quindi essa deve poter intervenire anche su ampia scala
- ❑ di completarsi in tempi ragionevolmente rapidi.

Il primo aspetto è di particolare importanza nella fase di messa a norma delle attività aziendali, il secondo assume rilevanza specie nell'attuazione del principio della protezione dei dati fin dalla progettazione ("**by design**").
Di converso, la DPIA deve seguire un metodo ed avere un contenuto minimo, entrambi specificati dalla norma, di maggiore complessità [art. 35(7)].

Elevato rischio? PROCEDO CON DPIA

Considerato che la constatazione della probabilità di un elevato rischio fa **scattare l'obbligo di effettuare la DPIA,** sorge il problema di stabilire **quando un rischio debba considerarsi "elevato"**.

In proposito vengono in aiuto sia il GDPR sia il WPArt29 con un proprio documento di linee guida, il wp248 rev.01 del 4 aprile 2017, come modificato e adottato da ultimo il 4 ottobre 2017.

Il GDPR interviene secondo due direttrici:

- fornendo una **lista di esempi** di trattamenti da considerarsi ad elevato rischio (art. 35.3)
- prevedendo che siano le autorità di controllo a rilasciare ***white list*** e ***black list***, cioè elenchi di trattamenti tipo che comportano rischi elevati ed elenchi di trattamenti per i quali si può escludere la presenza di rischi specifici.

Esempi di "elevato rischio"

Tre sono gli esempi di trattamenti con elevato rischio citati nel GDPR (art. 35):

- una **valutazione sistematica e globale di aspetti personali** relativi a persone fisiche, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o analoghi su dette persone fisiche;
- il **trattamento, su larga scala**, di **dati sensibili o giudiziari**; o
- la **sorveglianza sistematica su larga scala** di una **zona accessibile al pubblico**

Lista del Garante o "black list"

Il GDPR stabilisce che le Autorità pubblichino liste di trattamenti tipici per i quali si ritiene probabile un "elevato rischio" ("**black list**") insieme ad elenchi di trattamenti riguardo ai quali si ritiene di poter escludere questa circostanza ("**white list**").

A fronte del parere espresso dal **Comitato Europeo per la Protezione dei Dati** sul progetto di elenco del Garante italiano (parere 12/2018 del 25/9/2018) quest'ultimo ne ha accolto i rilievi ed ha emesso il provvedimento n. 467 del 18/10/2018 [doc. web n. 9058979] con allegata la **lista definitiva delle tipologie di trattamento a presumibile rischio elevato**.

Criteri di determinazione dell'elevato rischio

In parallelo alla pubblicazione delle liste dei trattamenti a rischio elevato, le linee guida wp248 rev.01 indicano i criteri atti ad accertare la sussistenza di un rischio elevato. Si tratta di criteri di valutazione che vanno essi stessi giudicati con ponderazione, evitando applicazioni acritiche.

Nel tentativo di fornire dei principi orientativi, il gruppo di lavoro evidenzia che **la concomitante presenza di due o più di tali criteri è sintomo di rischio elevato** sebbene non possa escludersi che in determinate circostanze la presenza anche di uno solo di tali criteri possa rendere obbligatoria la DPIA.

Questa osservazione lascia ad intendere nuovamente che **l'esercizio valutativo è comunque un compito proprio del titolare del trattamento.**

9 Criteri per determinare il rischio elevato (Linee Guida wp 248 rev.01)

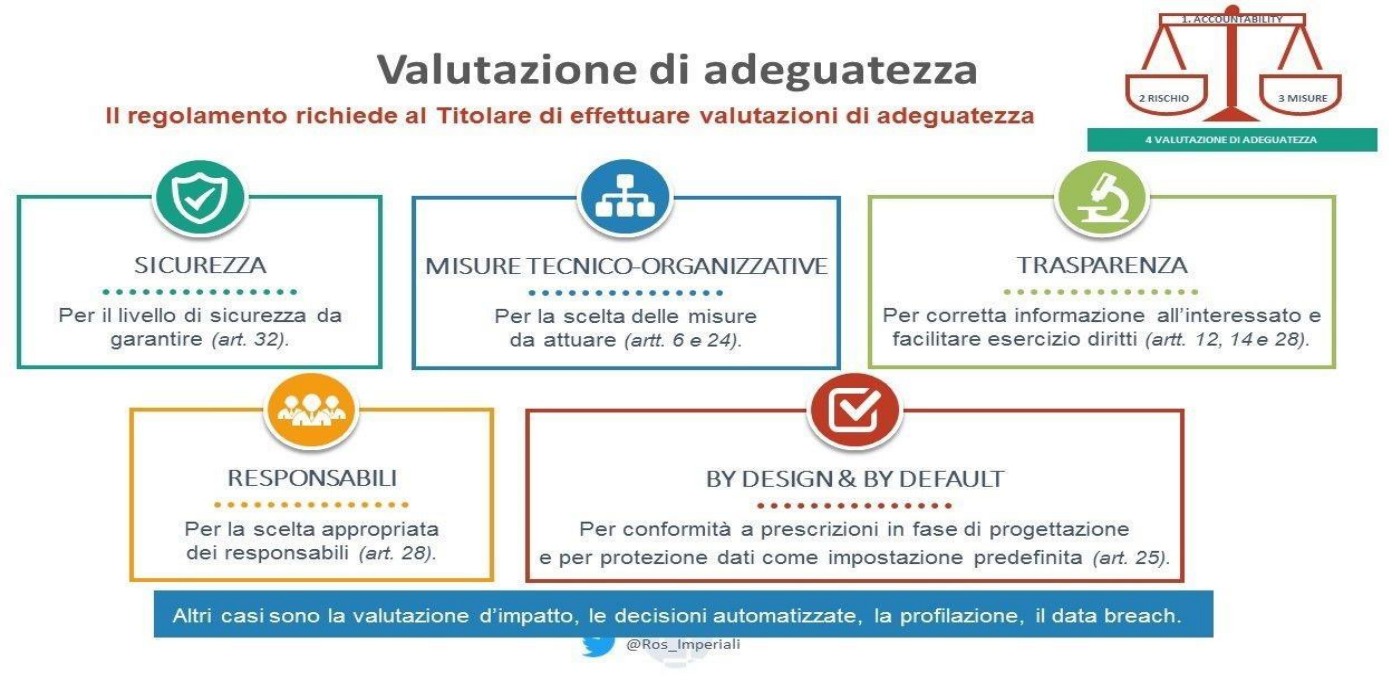
I 9 criteri per determinare il rischio "elevato"

L'utilizzo corretto di questi criteri, secondo il suggerimento del Gruppo, porta a ritenere che quando nella circostanza oggetto di esame **ne risultano presenti due o più, la sussistenza di un "rischio elevato" ai diritti ed alle libertà degli individui risulta probabile**. Pur nella constatazione che possono esservi situazioni in cui la presenza anche di uno solo dei criteri elencati faccia ritenere probabile l'esistenza di un rischio elevato, il principio generale è quello per cui quanto più numerosi sono i criteri di cui si trova riscontro nel trattamento esaminato, tanto maggiore è la probabilità di un rischio elevato a diritti e libertà delle persone. Infine, il principio va interpretato anche "a contrariis" nel senso che se, nonostante la presenza di uno o più di tali criteri, il titolare decida in ultima analisi di non realizzare una valutazione d'impatto sulla protezione dei dati, in tali casi lo stesso deve giustificare e **documentare i motivi che lo hanno spinto a non effettuare una DPIA**, nonché includere/registrare i punti di vista del DPO, se designato.

Nel piano di ricognizione delle aree ad elevato rischio potrà risultare utile avvalersi della seguente tabella:

Trattamento considerato	Criterio applicabile
[evidenzia le ragioni per le quali più criteri di quelli evidenziati e selezionati a lato possono coesistere nel progetto/trattamento considerato, giungendo alla conclusione della probabilità di un elevato rischio per i diritti e le libertà delle persone fisiche.].....	❑ Valutazione o assegnazione di punteggio ❑ Processo decisionale automatizzato ❑ Monitoraggio sistematico ❑ Dati sensibili o aventi carattere altamente personale ❑ Trattamento di dati su larga scala ❑ Creazione di corrispondenze o combinazione di insiemi di dati ❑ Dati relativi a interessati vulnerabili ❑ Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative ❑ Trattamento che impedisce l'esercizio di diritti o di avvalersi di un servizio o contratto.

Il concetto di «valutazione di adeguatezza»



DPIA e Rapporti con le terze parti

Il rischio del Titolare è valutato anche tenendo conto delle cd.Terze Parti

Presidio importante è la corretta formalizzazione dei Rapporti con le Terze Parti e Relativi audit

Nell'ambito di servizi che comportano il trasferimento di dati personali ai fornitori

La Società è TITOLARE del trattamento

Valuta l'autonomia del fornitore nel trattamento dei dati trasferiti ai fini della definizione del suo ruolo e sottoscrive con questi uno dei seguenti accordi:

A

Contratto Titolare/Titolare

Il fornitore tratta i dati in modo autonomo.

- Assume il ruolo di **Titolare** del trattamento ex art. 4 c. 7 del GDPR;
- Ha **autonomia** in:

a) verifica conformità del trattamento
b) predisposizione misure tecniche e organizzative
c) responsabilità verso i soggetti interessati

- **Notifica** eventuali violazioni nel trattamento dallo stesso effettuato.

B

Contratto Titolare/Responsabile

Il fornitore tratta i dati in modo non autonomo.

- Assume il ruolo di **Responsabile** del trattamento ex art. 4 c. 8 del GDPR;
- Rispetta le **istruzioni scritte** ricevute dal Titolare;
- Garantisce **competenza** nell'adozione di misure tecniche e organizzative;
- Rispetta obblighi di **collaborazione, informazione e notifica** verso il Titolare;
- Nomina **sub-responsabili** se autorizzato dal Titolare.

VALUTAZIONE D'IMPATTO: CONSULTAZIONE PREVENTIVA

TITOLARE

- ✓ **Se DPIA attesta** che, in assenza di misure, meccanismi, garanzie di riduzione del rischio, **permangono rischi elevati**, ragionevolmente non mitigabili

Consultazione preventiva

GARANTE

- ✓ **Risponde entro 8+6 settimane** al Titolare o Responsabile per iscritto

Assistito su richiesta dal Responsabile

Rif::
(94)
Art. 36

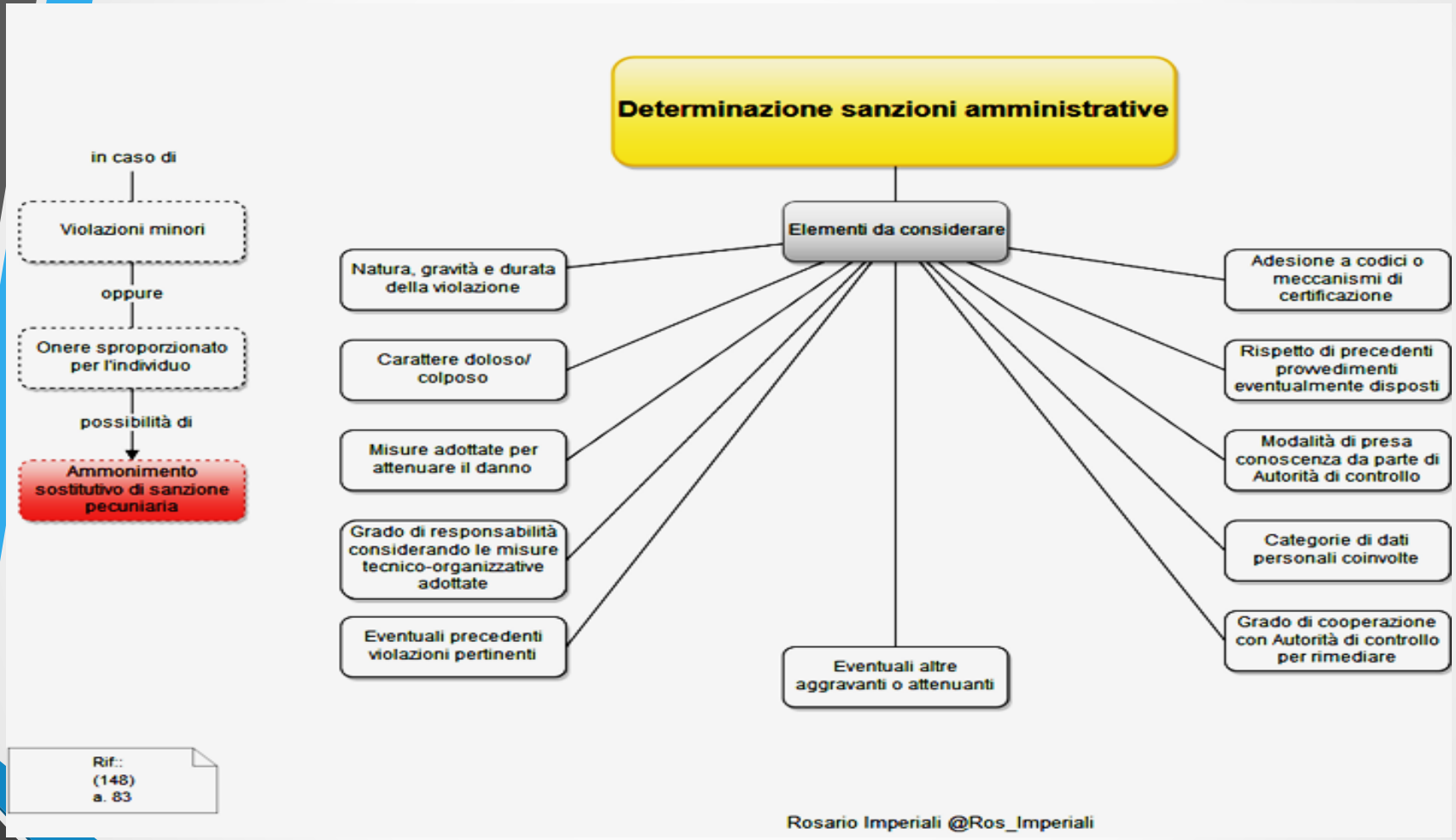
REGIME SANZIONATORIO

Adeguatezza Organizzativa e Sanzioni

L'adeguatezza delle procedure Tecniche Organizzative

Presidio importante anche in caso di Sanzioni

11 criteri per la determinazione della sanzione



11 Criteri per la determinazione delle sanzioni amministrative ex art. 83 c.2 GDPR

Il grado di responsabilità del Titolare o del Responsabile del trattamento tenendo conto delle misure tecniche e organizzative adottate ai sensi degli Artt. 25 e 32 del GDPR

Tale criterio analizza la condotta del Titolare e del Responsabile nel **momento antecedente al verificarsi della violazione e consiste in una valutazione che l'autorità di controllo deve svolgere circa le misure e le politiche adottate** dal Titolare o dal Responsabile del trattamento.

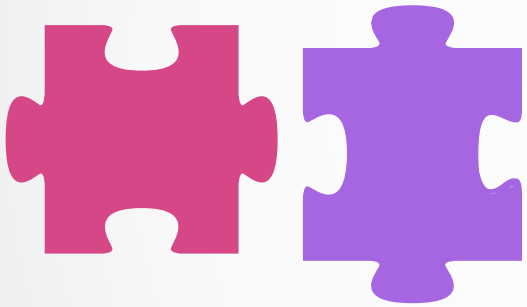
In particolare, in sede di applicazione della sanzione, l'autorità di controllo dovrà tenere conto delle misure tecniche e organizzative che il Titolare ha implementato al fine di garantire il rispetto dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 del GDPR) e la sicurezza dei dati (art. 32 del GDPR) prendendo in considerazione la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Come precisato dal Gruppo di Lavoro Articolo 29 nelle citate Linee Guida tale criterio introduce un **obbligo di mezzi (e non di risultato)**

È importante tenere conto delle norme industriali e dei codici di condotta nel rispettivo campo o professione. I codici di condotta potrebbero fornire un'indicazione delle pratiche comuni nel settore e un'indicazione del livello di conoscenza dei diversi mezzi esistenti per affrontare le tipiche problematiche di sicurezza associate al trattamento.

MISURE TECNICO-ORGANIZZATIVE: ESEMPI E UTILITÀ

Misure Tecniche

Credenziali, Sistema autorizzazione, Cifratura, Antivirus, etc.



Misure Organizzative

Clausole DP, Contratti con Responsabili, Vincoli riservatezza, Istruzioni, Registro

- Sistema di **protezione e reazione alle violazioni** *(data breach)*
- Strumento di **verifica e dimostrazione di conformità**
- Strumento di **riduzione e valutazione del rischio**
- **Modello organizzativo**
- Supporto e facilitazione **all'esercizio del diritti**

PRO per la Gestione dei Diritto degli interessati : Misura organizzativa

E’ utile che la Società, in conformità a quanto richiesto dal Regolamento UE 679/2016, tra le misure organizzative, adotti la Procedura per la gestione dei Diritti dell’Interessato, avente per oggetto l’attività di gestione delle richieste degli interessati che concernono il Trattamento dei Dati Personali della **società**. La Socierà, al fine di rendere consapevoli gli Interessati circa le modalità di esercizio dei loro diritti relativi al trattamento e agevolarli nell’esercizio dei propri diritti, deve ufficializzare in tutte le proprie informative l’attivazione di una casella di posta elettronica dedicata gestita dal coordinatore privacy. – privacy@SOCIETA’.it

Modulo Riscontro Richiesta Interessato / Contenuto della Richiesta

Contenuto Richiesta			
Riportare copia della richiesta ricevuta			
Tipo di Richiesta	Accesso, Rettifica Cancellazione, Oblio, Limitazione, Portabilità, Obiezione	Data Richiesta	GG/MM/AAAA
Richiedente	Nome e Cognome del richiedente	Tipologia Richiedente	Cliente, Dipendente, Fornitore…
Modalità Identificazione Richiedente	Documento d'identità, credenziali, altro	Tipo e N. Documento Identità	(ove necessario)

Modulo Riscontro Richiesta Interessato / Contenuto della Risposta

Contenuto Risposta			
Riportare copia della risposta inviata			
Data Chiusura Richiesta	GG/MM/AAAA	Stato Richiesta	Soddisfatta, Respinta, Obsoleta
Ragione Respingimento Richiesta	In caso di richiesta respinta documentarne le motivazioni.		
Estensione 30 giorni	È stata richiesta un'estensione per la gestione della richiesta? (SI/NO)	Motivazione Richiesta Estensione	In caso di richiesta di estensione per la gestione della richiesta, documentare motivazioni.

Tempistica della Risposta

Il Titolare del trattamento «è tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo, al più tardi «entro un mese» dalla ricezione della Richiesta.

Tenendo in considerazione la complessità ed il numero di richieste, il previsto periodo di un mese può essere esteso di ulteriori due mesi se necessario.

In questo caso il Titolare del trattamento informerà gli Interessati dell'estensione del periodo entro un mese dalla ricezione della Richiesta e li informerà delle motivazioni della estensione.

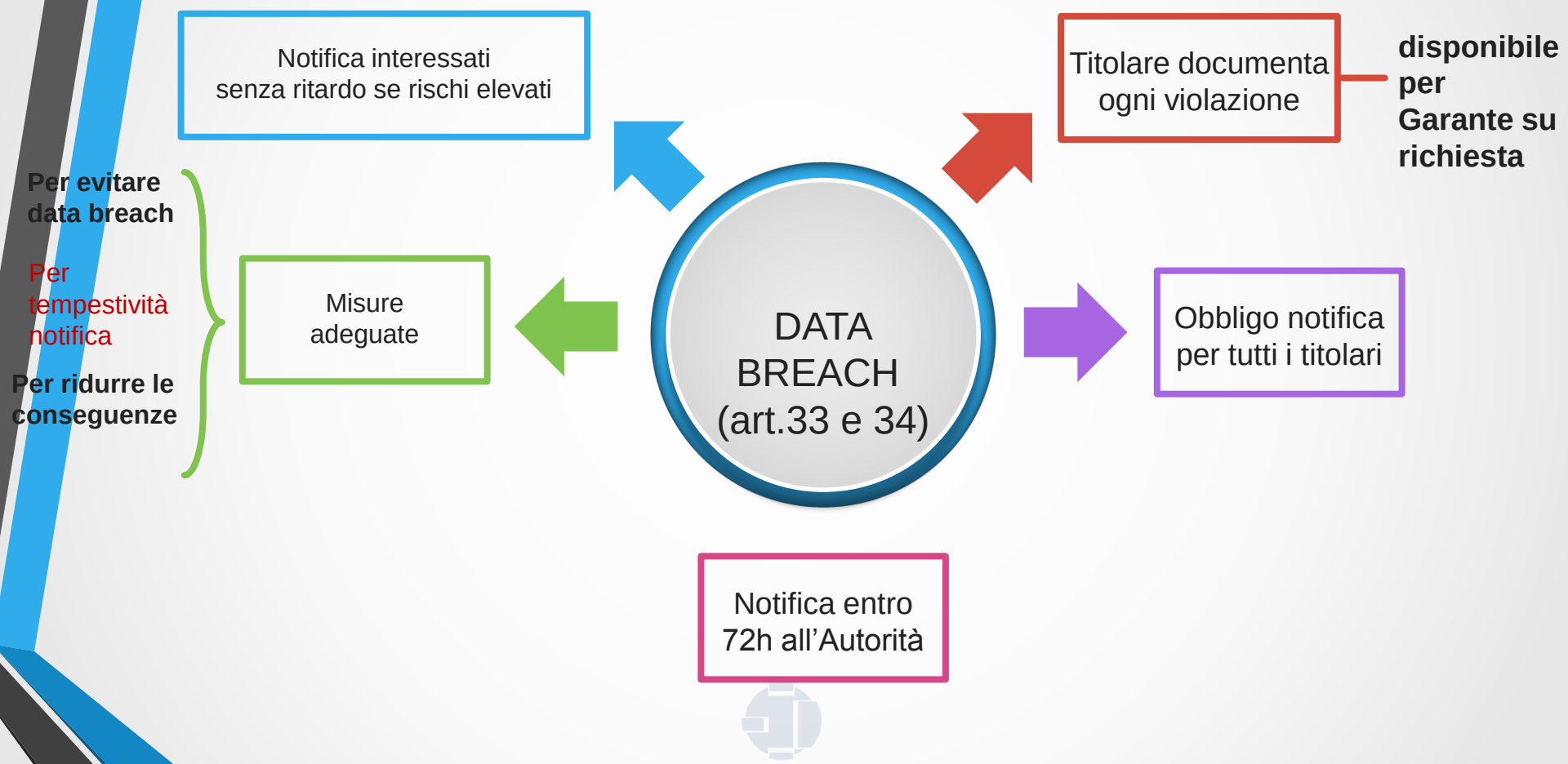
Nel caso la Società non intenda rispondere a una delle richieste di accesso dell'Interessato, il coordinatore privacy informerà l'Interessato, al più tardi entro un mese dalla ricezione della Richiesta, sui motivi per i quali la Richiesta non è stata presa in carico e, contestualmente, lo informerà anche della possibilità di inoltrare un Reclamo all'Autorità di supervisione e di prendere provvedimenti legali.

Tracciabilità delle Istanze

La Società, al fine di assicurare un monitoraggio delle richieste di diritto di accesso dovrà implementare un Registro Istanze Esercizio Diritti GDPR, il cui aggiornamento è affidato al **coordinatore privacy**.

Registro istanze esercizio diritti GDPR							
Data istanza	Canale presentazione istanza	Mittente	Oggetto dell'istanza	Istruttoria - fondatezza istanza	eventuale proroga termini 30 giorni	data chiusura istruttoria	data risposta

DATA BREACH: IN SINTESI



Raccomandazione del Garante

A partire dal 25 maggio 2018, **tutti i titolari** – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'autorità di controllo le **violazioni di dati personali**di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo", ma **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, **la notifica all'autorità** dell'avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del **rischio** per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale **rischio** è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34 quali ad es.

- Il titolare ha messo in atto misure tecniche e organizzative tali da rendere i dati oggetto di violazione incomprensibili a chiunque non sia autorizzato ad accedervi (es. cifratura)

- La comunicazione richiederebbe sforzi sproporzionati. In tal caso il titolare può procedere con una comunicazione pubblica.

Raccomandazione del Garante

Tutti i Titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all´Autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati *(si veda art. 33, paragrafo 5).*

Si raccomanda, pertanto, ai Titolari di trattamento di adottare le misure necessarie **a documentare eventuali violazioni**, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Adeguatezza delle misure nel data breach

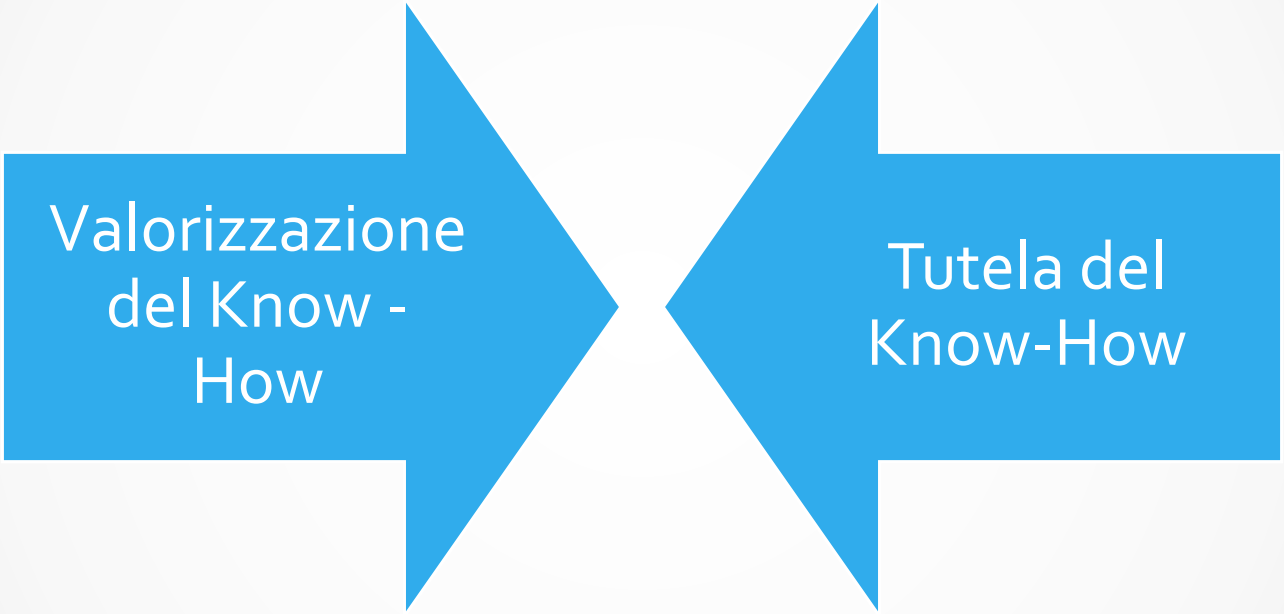
E’ importante dimostrare che la Società, ha adottato il **Registro *Data Breach*** e provveduto all’implementazione della **Procedura «*data breach* e/o violazione dei dati personali»**
Formalizzato il livello d’adeguatezza con approccio basato sul rischio con il Report Art. 32 e Relativi allegati

- ✓ **Pseudonimizzazione** e **cifratura** dati personali;
- ✓ **Assicurare continua riservatezza, integrità, disponibilità e resilienza** di sistemi e servizi che trattano i dati personali;
- ✓ **Ripristinare tempestivamente disponibilità e accesso** dei dati in caso di incidente;
- ✓ Procedura per provare, verificare e valutare regolarmente **efficacia misure tecnico-organizzative.**

Alcuni esempi di data breach

- ✓ furto o perdita di dispositivi informatici contenenti dati personali;
- ✓ deliberata alterazione di dati personali;
- ✓ impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- ✓ perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- ✓ divulgazione non autorizzata dei dati personali;
- ✓ accesso o acquisizione dei dati da parte di terzi non autorizzati.

Creazione di Valore



L'adeguamento GDPR base per la tutela del know –how?

Con la pubblicazione sulla Gazzetta Ufficiale del D.lgs. 11 maggio 2018, n. 63, l'Italia ha dato attuazione alla Direttiva UE 2016/943 sulla protezione del know-how e delle informazioni commerciali riservate contro l'acquisizione, l'utilizzo e la divulgazione illeciti degli stessi.

Le due importanti novità introdotte dal D.lgs. 63/2018 consistono, da una parte, in un sostanziale **allargamento della nozione di know-how** contenuta nel CPI (Codice Proprietà Industriale) e, dall'altra, nel **rafforzamento**, quanto a **strumenti** e alla loro applicazione, **della tutela giurisdizionale dello stesso**.

Nuova Nozione di Segreti Commerciali (1/2)

Alla definizione di know-how della Legge n. 129/2004, il decreto legislativo 63/2018 contrappone una differente definizione: nell'art. 1, c. 1, del Codice della proprietà industriale si introduce la **nuova nozione di "segreti commerciali"** che sostituisce quella di "informazioni aziendali riservate" precedentemente prevista nella norma.

Non si tratta di una modifica meramente semantica, in quanto la nuova nozione di know-how trasfusa nella nozione di "segreti commerciali" **comprende,** ma non esaurisce, la categoria delle **esperienze tecnico-industriali, anche commerciali, "riservate" ed estende la protezione anche a tutte le informazioni destinate a non essere divulgate**.

Implementazione di Adeguate Misure Tecniche e Giuridiche

Nel decreto emerge il principio secondo cui **l'autorità giudiziaria** competente a giudicare della sussistenza o meno della violazione del segreto commerciale deve necessariamente valutare se il soggetto il cui diritto si ritiene violato abbia **posto in essere le necessarie e dovute accortezze volte a proteggere il segreto commerciale.**

Sarà importante dimostrate di aver implementato **adeguate «misure tecniche»** (conservazione archivi chiusi, uso di credenziali di autenticazione per l'accesso a cartelle contenenti informazioni riservate etc.), **«misure legali»** (non disclosure agreements, clausole di riservatezza accessori ad altri contratti, ordini di servizio, accordi di non divulgazione etc.) e **«misure organizzative»** (policy per garantire riservatezza informazioni, policy per la classificazione dei dati dal punto di vista del loro valore per l'azienda, protocolli per la tutela della proprietà intellettuale, regolamento interno per la gestione delle informazioni etc.)

SANZIONI PREVISTE DAL SOLO REGOLAMENTO

Organizzazione 2%

Mancata individuazione formale di ruoli e responsabilità nel trattamento dei dati personali

Sicurezza 2%

Mancata adozione di adeguate misure di sicurezza

Informativa e Consenso 4%

Non adempiere agli obblighi sul consenso

Accountability

Omessa DPIA quando richiesta, consultazione preliminare Autorità 2%

Violazione diritti interessati, regole su trasferimenti extra-UE, obblighi Stati Membri, prescrizioni dell'Autorità 4%

2% Sanzione sino a 10 milioni di euro o, in caso di imprese, sino al 2% del fatturato globale annuo

4% Sanzione sino a 20 milioni di euro o, in caso di imprese, sino al 4% del fatturato globale annuo

Grazie

Avv. Riccardo Imperiali di Francavilla

riccardo.imperiali@imperiali.com

Dott.ssa Anna Irace

anna.irace@imperiali.com

Aggiungici su

gruppoimperiali