3 MAGGIO 2018

# Gli strumenti a disposizione delle aziende: Privacy Impact Assessment (PIA) e verifica di adeguamento al GDPR.

VINCENZO DELACQUA

ICIM
Certifichiamo oggi per il domani.

30 ANNI
1988-2018
nel segno di tradizione e innovazione

# Gli strumenti a disposizione delle aziende per ottemperare al GDPR

A. GDPR – regolamento UE 2016/679.

B. Indicazione del Garante per la protezione dei dati personali http://www.garanteprivacy.it/web/guest

C. Gruppo di lavoro ex Articolo 29 http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

D. Lavoro svolto in altri paesi UE (Spagna, Francia (CNIL), Gran Bretagna).

# Cosa fare per iniziare a applicare la GDPR?

Premesso che:

- la maggior parte delle aziende non ha ancora iniziato a interagire con la GDPR, per mancanza dei decreti legge che devono fornire indicazioni sulla via italiana alla protezione dei dati personali;
- la mole delle informazioni attualmente circolanti è tale da scoraggiare molte aziende a iniziare;
- la maggior parte delle aziende gestiscono dati personali comuni e non di tipo sensibile;
- la maggior parte delle aziende italiane ha dimensioni medio-piccole, con strutture organizzative molto snelle e corte;
- da quanto sopra indicato in molti casi non è necessaria la figura del DPO.

**Quale può essere il suggerimento per applicare la GDPR?**

# Cosa fare per iniziare a applicare la GDPR?

Proviamo a definire i passi minimi necessari per raggiungere l'obiettivo di adeguarsi al GDPR.

1. Analisi della situazione attuale (GAP ANALYSIS).
2. Registro delle attività di trattamento dei dati (art. 30 – GDPR). Raccolta, mappatura, priorità dei dati, tracciabilità.
3. Valutazione d'impatto sulla protezioni dei dati (PIA) (art. 35 – GDPR).
4. Definizione delle procedure (esistenti, da integrare, nuove).
5. Rendicontazione delle attività svolte (riesame periodico).

# 1) Analisi della situazione attuale (GAP ANALYSIS)

## Cosa si fa

- Il primo passo è capire quanto si è distanti dai requisiti indicati nel GDPR.
- Per cui la prima operazione è utilizzare lo stesso GDPR come check list e fare una prima valutazione della situazione.
- Da questa analisi emerge sia cosa manca da fare che cosa l'azienda ha già disponibile.
- Inoltre da questa prima analisi emergono anche altre due informazioni, la tipologia dei dati personali che vengono gestiti e la eventuale necessità di un DPO.

# 1) Analisi della situazione attuale (GAP ANALYSIS)

## Esempio

| Articolo | | Domanda | Risposta | Situazione | Gestione |
|---|---|---|---|---|---|
| Articolo 3 Ambito di applicazione territoriale | L'articolo definisce l'ambito territoriale del Regolamento. Il regolamento si applica ai titolari del trattamento e ai responsabili del trattamento dei dati all'interno dell'Unione Europea (UE) e, in determinate circostanze, anche con sede fuori dall'UE | Quando si tratta di elaborare dati personali all'interno dell'UE di soggetti interessati al di fuori dell'UE i requisiti del Regolamento sono soddisfatti? | xx | yyy | aaaa |
| | | Le imprese, esterne alla UE ma parte del gruppo, che si rivolgono a soggetti interessati in Europa con i loro servizi o che controllano il loro comportamento, sono conformi al Regolamento? | xx | yyy | aaaa |

# 1) Analisi della situazione attuale (GAP ANALYSIS)

## Cosa può fare ICIM

- ICIM utilizzando una apposita checklist, può effettuare il **Servizio di GAP ANALYSIS**.
- La durata dell'intervento è relativamente breve con l'impegno da parte dell'azienda di poche persone.
- Viene emesso un verbale che partendo dalla check list fa emergere i punti critici, le mancanze e le necessità che fungono da base di partenza per iniziare a implementare il GDPR.

# 2) Registro delle attività di trattamento dei dati (art. 30 – GDPR). Raccolta, mappatura, priorità dei dati, tracciabilità

## Cosa si fa

L’art. 30 del GDPR indica che il titolare o il responsabile del trattamento devono tenere un registro delle attività di trattamento svolte sotto la "propria responsabilità".
Questo Registro contiene almeno le seguenti informazioni:

a. Il nome e i dati di contatto del titolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati

    ***CHI*** *effettua concretamente l’attività di trattamento (Organigramma per la GDPR).*

# 2) Registro delle attività di trattamento dei dati (art. 30 – GDPR). Raccolta, mappatura, priorità dei dati, tracciabilità

## Cosa si fa

b. Le finalità del trattamento

***PERCHÉ*** *i dati sono gestiti (raccolti, elaborati, divulgati, conservati, cancellati),*

***DOVE*** *i dati vengono raccolti e custoditi,*

***QUANDO*** *i dati vengono raccolti.*

c. Una descrizione delle categorie di interessati e delle categorie di dati personali;

***QUALI*** *categorie di dati vengono trattati, da chi e i rischi correlati per ciascuna categoria di dati.*

# 2) Registro delle attività di trattamento dei dati (art. 30 – GDPR). Raccolta, mappatura, priorità dei dati, tracciabilità

## Cosa si fa

c. Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali

   ***A CHI** ciascuna categoria di dati è trasferito, consegnato, inviato.*

d. Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate.

f. Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati

   ***COME E QUANDO** i dati devono essere cancellati o anonimizzati.*

# 2) Registro delle attività di trattamento dei dati (art. 30 – GDPR). Raccolta, mappatura, priorità dei dati, tracciabilità

## Cosa si fa

f. Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative

> ***COME*** *garantire la protezione dei dati personali, ridurre al minimo i rischi di accesso non autorizzato e mantenere la tracciabilità del dato.*

Ci aiuta in questo caso l'art. 32 che indica che tenendo conto dello stato dell'arte e dei costi di attuazione, della natura dell'oggetto, del contesto, del rischio e della gravità di ledere i diritti e la libertà delle persone fisiche, si mettono in atto delle misure che comprendono, se del caso:

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 e dei servizi di trattamento;
c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

# 2) Registro delle attività di trattamento dei dati (art. 30 – GDPR). Raccolta, mappatura, priorità dei dati, tracciabilità

## Cosa può fare ICIM

- L’analisi del Registro del trattamento rientra nel **Servizio di GDPR Assessment** che ICIM effettua applicando apposite procedure di verifica.
- Più avanti viene dettagliato l’intervento.

# 3) Valutazione d’impatto sulla protezioni dei dati (PIA) (art. 35 – GDPR)

## Cosa si fa

- L’art 35 cita: "Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".

# 3) Valutazione d’impatto sulla protezioni dei dati (PIA) (art. 35 – GDPR)

## Cosa si fa

**DPIA o PIA (Data Protection Impact Assessment)**.

La **PIA** è una forma di valutazione dei rischi dovuti alla gestione del dato in tutto il suo ciclo di vita. Sempre l’art. 35 oltre a dare una indicazione di quando la PIA è espressamente obbligatoria (ma si suggerisce di applicarla sempre – nota del relatore), fornisce una semplice struttura degli obiettivi della valutazione:

a. Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento,

b. Una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità.

*Descrivendo anche qualsiasi condivisione di informazioni di routine condotta nella gestione dei dati sia all'interno delle dell’azienda che all’esterno.*

# 3) Valutazione d'impatto sulla protezioni dei dati (PIA) (art. 35 – GDPR)

## Cosa si fa

c. Una valutazione dei rischi per i diritti e le libertà degli interessati

*Analizzando i principali rischi potenziali sulla privacy identificati e discutendo dell'impatto sulla privacy complessivo sui singoli individui.*

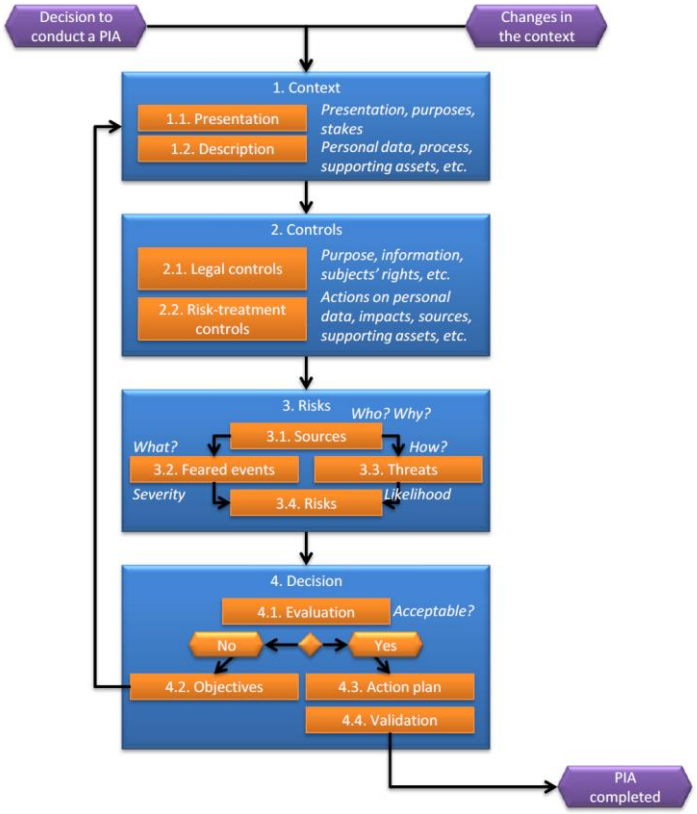
d. Le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

*Identificando la tecnologia utilizzata e fornendo una breve descrizione di come vengono raccolte le informazioni, come viene gestito il back up dei dati, come viene gestita la violazione dei dati e il tracciamento di ogni tipo di attività.*

# 3) Valutazione d'impatto sulla protezioni dei dati (PIA) (art. 35 – GDPR)

## Es.Tratto dal documento del CNIL

- Il CNIL fornisce anche un piccolo Software per poter strutturare una PIA, è un esempio, ma molto valido.



# 3) Valutazione d’impatto sulla protezioni dei dati (PIA) (art. 35 – GDPR)

## Cosa può fare ICIM

- L’analisi della PIA rientra nel **Servizio di GDPR Assessment** che ICIM effettua applicando apposite procedure di verifica.
- Più avanti viene dettagliato l’intervento.

# 4) Definizione delle procedure (esistenti, da integrare, nuove)

## Cosa si fa

L'azienda deve predisporre a fronte del Registro del Trattamento e della PIA uno o più documenti che procedurizzino tutti i processi interni nell'ottica dei requisiti del GDPR, ciò comporta almeno:

a) implementazione di misure tecniche e organizzative secondo il principio *privacy by design* (fase di ideazione e progettazione del trattamento) e *privacy by default* (misure prese come ritorno di problemi e reclami);

b) piani di formazione dei dipendenti;

c) gestione dei reclami dei clienti e della garanzia dell'esercizio dei diritti di cancellazione, accesso, rettifica, opposizione, portabilità e revoca del consenso;

d) ove necessario procedura di notifica delle violazioni all'Autorità competente.

# 4) Definizione delle procedure (esistenti, da integrare, nuove)

## Cosa può fare ICIM

L'analisi completa della conformità al GDPR dell'azienda, rientra nel **Servizio di GDPR Assessment** che ICIM effettua applicando apposite procedure di verifica.

1. Una fase di applicazione e prima valutazione della domanda (verifica documentale da effettuare anche presso l'azienda).
2. Valutazione da parte di ispettori / valutatori esperti che porta a una relazione di valutazione che descrive i punti critici, le mancanze di conformità al GDPR.

La durata dell'intervento è correlata alle caratteristiche della categorie dei dati, alla struttura dei sistemi di gestione e alle dimensioni della azienda con l'impegno da parte dell'azienda del Responsabile e degli Incaricati del trattamento.

Si applicano le norme della serie EN 27000 per la sicurezza dei dati, le EN 31000 per l'analisi dei rischi, le guide PIA di varie nazioni, le guide e le note del Garante, le guide del Article 29 DATA PROTECTION WORKING PARTY e le leggi attualmente in vigore.

# 4) Definizione delle procedure (esistenti, da integrare, nuove)

## Cosa può fare ICIM

- Altro servizio che ICIM eroga è la **FORMAZIONE** sia di primo livello (formazione sul GDPR) che di secondo livello (al Responsabile del trattamento, agli Incaricati del trattamento e a tutte le figure che intercettate dal GDPR).
- Questi corsi sono erogati sia presso la sede ICIM che in house.

# 5) Rendicontazione delle attività svolte (riesame periodico)

## Cosa si fa

Come in tutti i buoni sistemi di gestione, l'azienda deve adottare e gestire correttamente il Registro dei trattamenti, la PIA e le procedure che gli permettono di assicurare un "ciclo del dato personale", per cui dovrà fornirsi di indicatori che gli permettano di monitorare la situazione di conformità al GDPR e di rendicontare le attività svolte. Tali informazioni dovranno essere tenute sotto stretto controllo da parte del Titolare del trattamento e del Responsabile del trattamento dei dati. Tra questi indicatori si suggerisce di tener sotto controllo:

a. reclami,

b. interventi effettuati a copertura di rischi emersi successivi all'edizione del Registro e della PIA,

c. tempi di notifica delle violazioni all'Autorità competente,

d. idoneità dell'informativa all'interessato,

e. valutazione della raccolta dei consensi liberi specifici resi dagli interessati.

# 5) Rendicontazione delle attività svolte (riesame periodico)

## Cosa può fare ICIM

- Chiaramente se fosse possibile certificare il processo di gestione del ciclo dei dati da parte degli Organismi di certificazione accreditati come indicato da art.42 e art. 43 del GDPR, la fase precedente rientrerebbe nella sorveglianza annuale.

- Purtroppo l'attuale situazione di stallo dei decreti legati al GDPR, non permette di applicare la Certificazione (peraltro caldamente consigliata dalla UE, come si evidenzia in diversi documenti), per cui potrebbe essere fatta richiesta da parte dell'azienda di una "estensione" al **Servizio di GDPR Assessment** che ICIM effettua, da effettuarsi dopo un certo lasso di tempo per permettere la valutazione anche della corretta effettuazione del monitoraggio e della rendicontazione da parte dell'azienda stessa.

# Data Protection Officer

## Cosa fa

Il Data Protection Officer o DPO è una delle novità del Regolamento rispetto ai suoi predecessori descritta dall'art. 37 del GDPR. Sostanzialmente è una figura che nelle aziende, ove è necessario averla, ha una funzione di informazione, consulenza e controllo della gestione del trattamento dei dati, una specie di «RSPP dei dati».

È una figura che dovrà (vedi art. 39 del GDPR):

- conoscere il GDPR e le norme eventualmente applicabili all'azienda nel contesto della privacy;
- informare e sensibilizzare il Titolare del trattamento, il Responsabile del trattamento e gli Incaricati alla corretta applicazione dei trattamenti correlati al Registro e alla PIA;
- monitorare in modo continuativo la situazione;
- cooperare con le Autorità di controllo.

# Data Protection Officer

## Cosa può fare ICIM

Altro servizio che ICIM eroga è la Certificazione del DPO (Data Protecion Officer) a fronte della norma UNI 11697.
Tale certificazione fornisce alla figura professionale una patente di conformità ai requisiti definiti all'art. 37 del GDPR.
L'esame è strutturato in:

- verifica documentale delle caratteristiche del candidato,
- esame scritto (Domande),
- esame scritto (Caso di studio),
- esame orale.

E l'esito positivo comporta l'emissione di un certificato di figura professionale certificata.

# Conclusioni

- I compiti da fare per le aziende che devono adeguarsi al GDPR sono tanti, ma come visto si raggruppano in 4-5 attività che possono comunque essere «gestite».
- L'emissione dei decreti e dei codici di condotta, si spera quanto prima, aiuterà ancor più le aziende a conformarsi ai requisiti indicati nel GDPR.
- Gli stessi decreti e codici di condotta potranno permettere la certificazione volontaria della protezione dei dati che riducendo la responsabilità del Titolare del trattamento e del Responsabile del trattamento, dovrebbe portare anche a una possibile riduzione delle sanzioni, oltre che a una maggior tranquillità nella corretta applicazione del GDPR.

ICIM

Certifichiamo oggi
per il domani.

# Grazie
# per l’attenzione

**www.icim.it**



ICIM

ICIM S.p.A.
Piazza Don Mapelli, 75
20099 Sesto San Giovanni (MI) – Italy
Tel. +39 02 725341
Fax. +39 02 72002098
www.icim.it

ICIM
Certifichiamo oggi per il domani.

1988-2018
30 ANNI
nel segno di tradizione e innovazione