PMPI Solutions

Target GDPR

Un percorso di adeguamento al Regolamento Europeo della Privacy e alla sua gestione dinamica

GDPR - *General Data Protection Regulation – Regolamento UE 2016/679*

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il nuovo Regolamento sulla protezione dei dati personali e la libera circolazione dei dati personali, che avrà piena applicazione a decorrere dal **25 maggio 2018**, il cosiddetto (**GDPR**, *General Data Protection Regulation- Regolamento UE **2016/679**).*

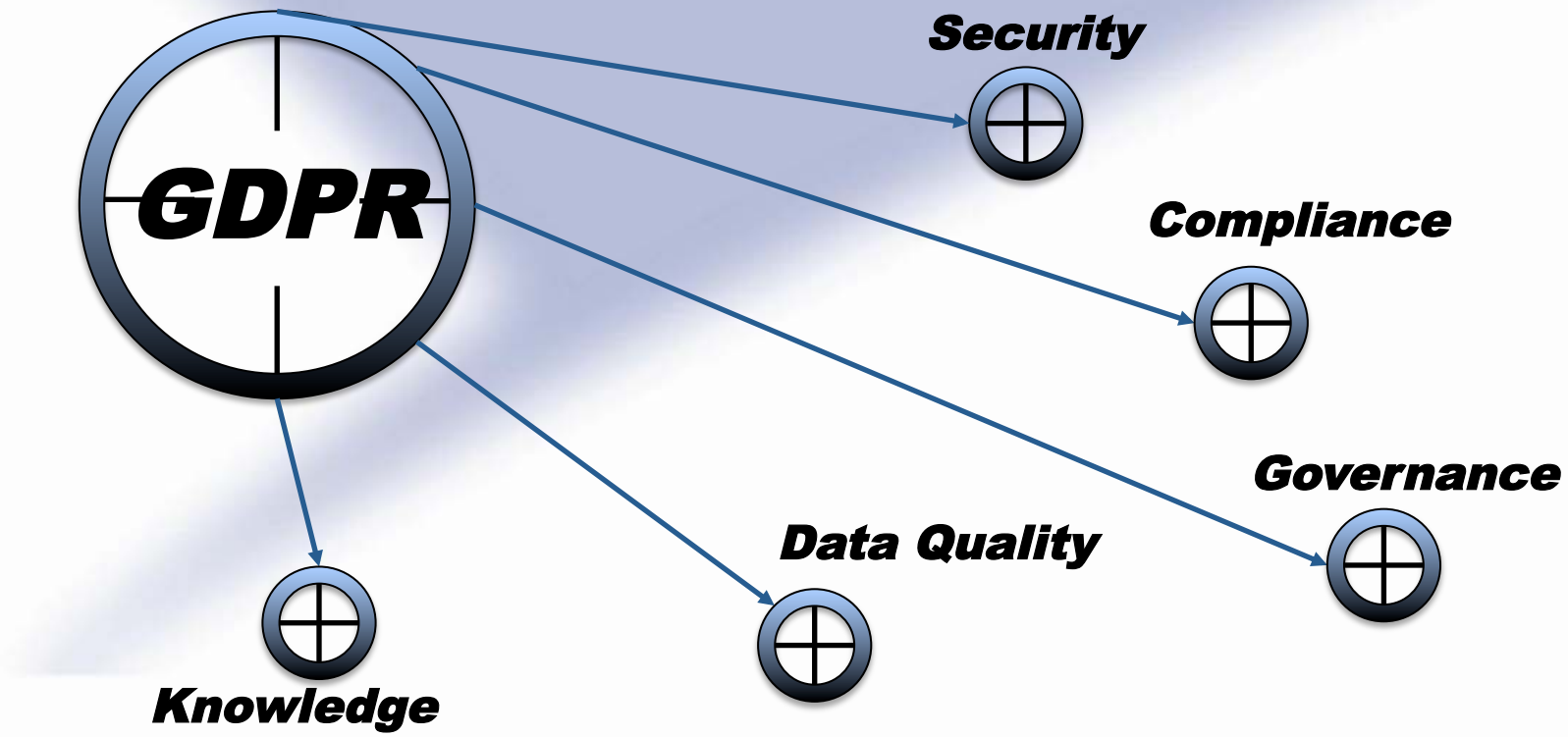
Il Regolamento abroga la Direttiva 95/46/CE, attuata in Italia prima con la legge 675/96 e successivamente con il Codice Privacy del 2003 (D.Lgs. 196/2003), e si applicherà direttamente in tutti gli Stati Membri senza necessità di un intervento legislativo dei medesimi a tal fine.

Tale Regolamento s'inserisce all'interno di quello che, insieme alla Direttiva Europea 2016/680, è stato definito il "***Pacchetto europeo protezione dati***".

Il Regolamento introduce, tra l'altro, anche una serie di obblighi per le imprese che trattano dati personali, in un'ottica di maggiore tutela per gli interessati. Vanno in questa direzione due degli elementi fondanti del regolamento: l'obbligo di protezione dei dati fin dalla progettazione (Privacy by Design) e quello di protezione per impostazione predefinita (Privacy by Default).

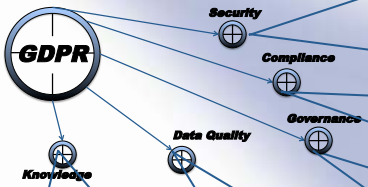
Un'opportunità non solo un obbligo

L'usuale percezione dell'entrata in vigore di una nuova normativa è quella di un "appesantimento" della gestione consueta nelle organizzazioni, sia pubbliche che private.
Tuttavia nel caso nel nuovo Regolamento Europeo della Privacy, la richiesta conformità entro il 25 Maggio 2018 si deve vedere come un'opportunità da sfruttare per traguardare in un unico progetto più obiettivi.



Molteplici obiettivi, un unico progetto

L'adeguamento al GDPR infatti, consente di traguardare all'interno di un unico progetto molteplici obiettivi:



Security

L'opportunità di implementare un **sistema di protezione delle informazioni** resiliente e ad alta dinamicità

Compliance

Percorrere una strada strutturata di adeguamento al Regolamento Europeo ed un sistema di monitoraggio continuo

Knowledge

L'opportunità di acquisire una conoscenza approfondita del proprio sistema di gestione delle informazioni

Data Quality

L'opportunità di "ripulire" i propri sistemi da informazioni ridondanti e non propriamente gestite

Governance

L'opportunità di gestire con sicurezza il proprio sistema di protezione dei dati garantendo un gestione integrata degli incidenti (data breach, manipolazione dei dati, uso non corretto, etc.)

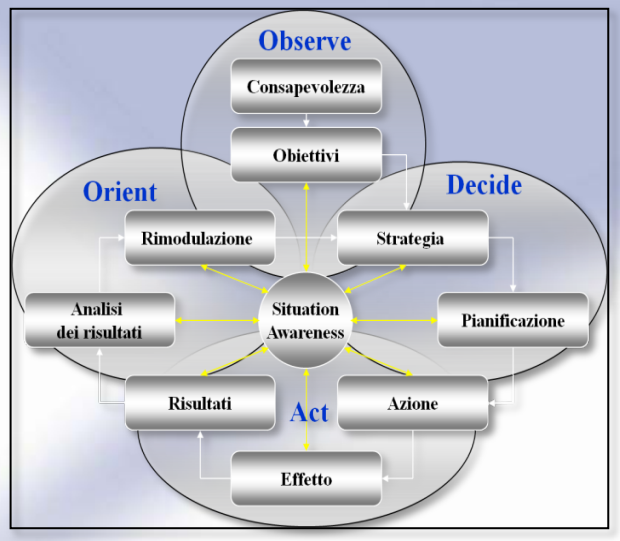
Il Progetto

Il Progetto intende guidare l'Azienda nel processo di adeguamento al GDPR mediante l'utilizzo di modelli operativi tendenti alla ***Governance*** dei processi di gestione sicura delle informazioni.(CoBIT)
In tale ottica si opera affinché siano realizzati in conformità al suddetto Regolamento:

- Classificazione dei Dati Personali;
- Classificazione dei Trattamenti effettuati;
- Valutazione del rispetto dei Principi Privacy;
- Progettazione nel rispetto della Privacy by Design e Privacy by Default
- Definizione delle misure di sicurezza applicabili;
- Adozione di Codici di Condotta Privacy;
- Valutazione d'impatto (DPIA - Data Protection Impact Assessment)
- Registro dei trattamenti effettuati;
- Redazione delle nomine dei Responsabili del Trattamento Dati;
- Redazione di informativa privacy e consenso privacy;
- Redazione di procedure per la violazione dei dati personali (Data Breach);
- Redazione di procedure per l'esercizio dei Diritti dell'Interessato;
- Adempimento degli obblighi privacy in materia di Profilazione;
- Software selection (eventuale) per la scelta degli elementi applicativi in grado di supportare la conformità.

Il modello operativo

Il modello operativo, è basato su un approccio che abbiamo definito ***EBS – Effects Based Security*** (1) consistente in un sistema altamente dinamico di gestione della sicurezza in presenza di obiettivi in continua ridefinizione al variare delle condizioni nell'ambito del contesto operativo. Ciò consente altresì, con un continuo monitoraggio volto a verificare la conformità delle politiche e dei processi inerenti la sicurezza logica dell'infrastruttura alle leggi e alle regolamentazioni cui l'Organizzazione è soggetta in un ottica di Governance complessiva di tutti i processi di sicurezza delle informazioni.



EBS – Effects Based Security Framework

ISO/IEC 27001

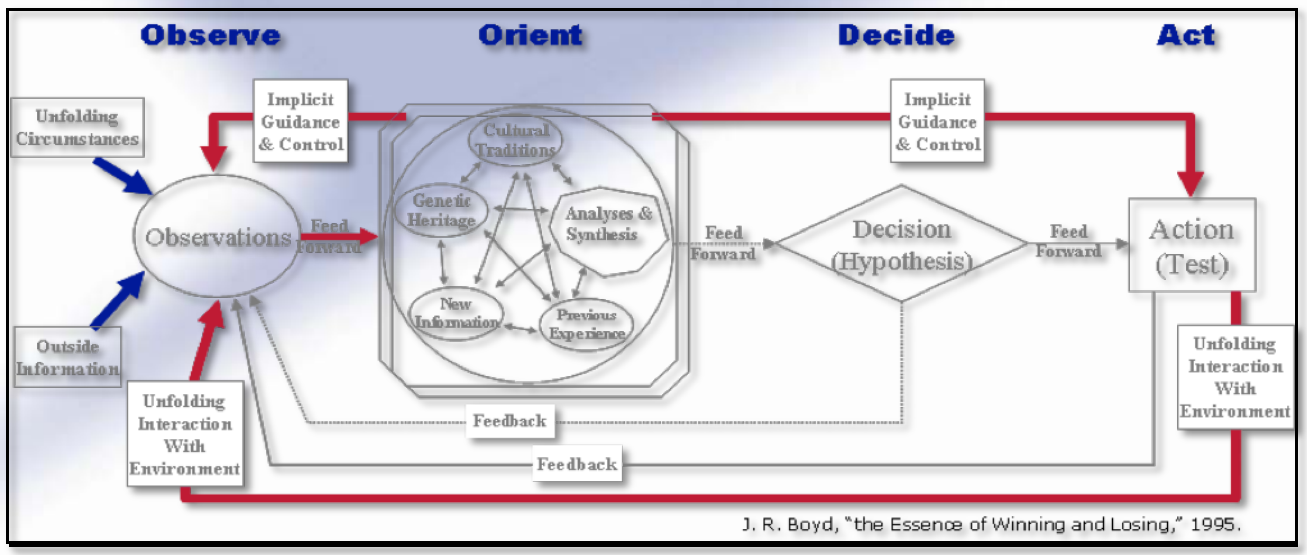
Seguendo inoltre le linee guida dettate dallo standard ***ISO/IEC 27001*** si garantisce un modello di riferimento solido allo scopo di rendere l'applicazione del GDPR ad alta affidabilità.

(1) EBS – Effects Based Security – Ripensare la sicurezza in una realtà complessa – Massimiliano Campita - 2009

La metodologia

Allo scopo di sincronizzare le attività mediante un uso adeguato di specializzazioni, tecniche di ottimizzazione, pianificazione con impiego di processi ciclici secondo lo schema di Boyd (OODA – Observation, Orientation, Decision, Action Loop) riportato nella figura, si rende necessaria una "scomposizione" dell'ambiente operativo in componenti facilmente gestibili.

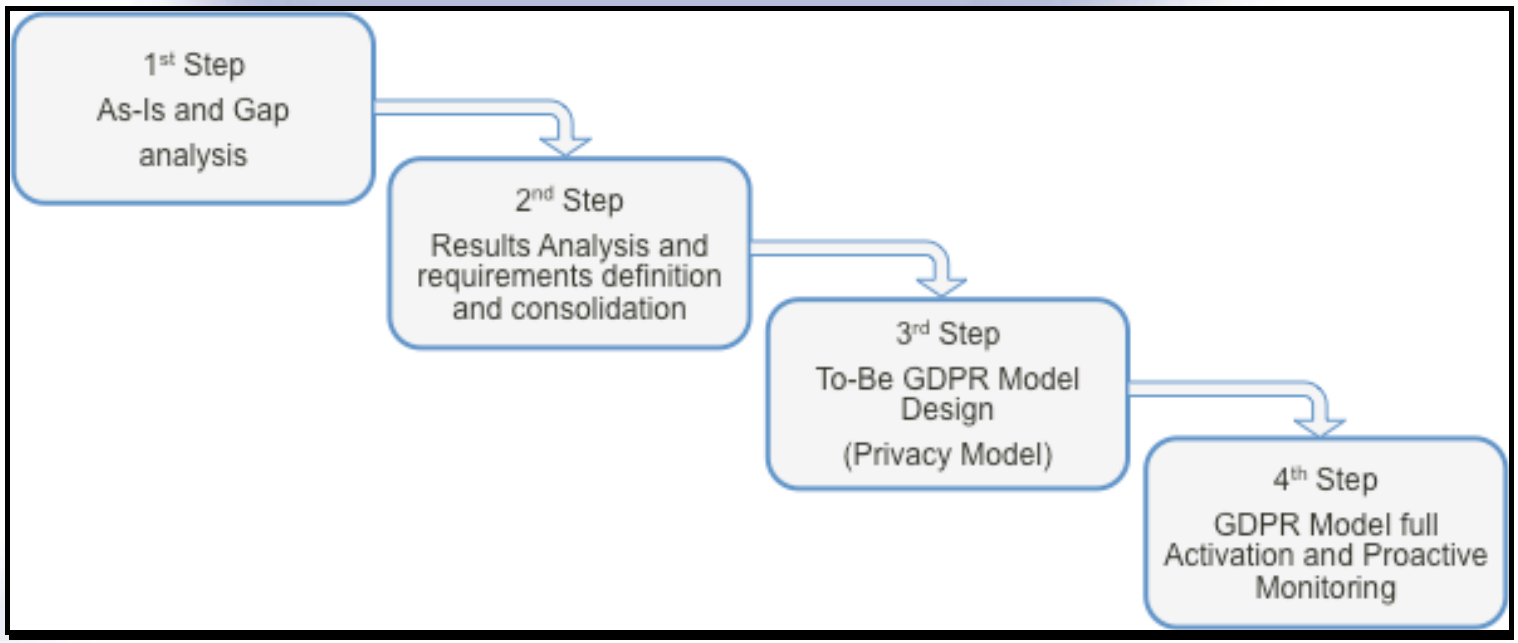
Il tutto con l'obiettivo di implementare misure in grado di godere, pur nella loro rigorosità, di gradi di libertà, che le rendano adeguate a mantenere un livello di controllo dei flussi informativi ed in grado di modulare risposte e deliverable validi in un contesto in continuo divenire e di rischi ed obiettivi chiari e ben definiti (*adaptive response*).



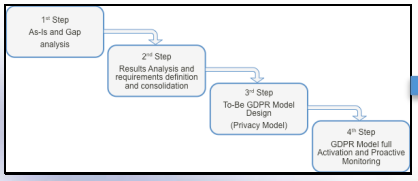
Il percorso di adeguamento al GDPR

Nell'ottica del modello iterativo descritto le attività che vengono svolte interessano ogni elemento delle struttura aziendale e i processi sottesi al trattamento dei dati. Inoltre per poter affrontare il complesso e articolato sistema è indispensabile riferirsi ad un modello di intervento adeguato alle esigenze derivanti dalla definizione degli scenari e dalla conoscenza dei compiti, ruoli e funzioni delle componenti del sistema di protezione.

Questa dunque la rappresentazione grafica delle quattro macro-fasi che compongono il progetto globale di adeguamento al GDPR:



Fasi e strategie



Macro-fase/Step 1 – Osservazione, Ricognizione del contesto e Gap Analysis;
Macro-fase/Step 2 – Analisi Risultati e definizione obiettivi e requisiti;
Macro-fase/Step 3 – Definizione Modello e Impact Analysis (con analisi dei rischi);
Macro-fase/Step 4 – Messa a regime e monitoraggio dinamico.

Tutte le attività che caratterizzano le fasi sopra esposte vengono svolte seguendo la metodologia enunciata e mediante diversificate strategie di approccio come:

- ✧ Un **rapporto continuo e non invasivo** con le risorse competenti e responsabili dei vari processi di trattamento;
- ✧ **L'Analisi continua dei sistemi** informativi a supporto dei processi di trattamento;
- ✧ Un **continuo adeguamento** delle procedure e dei processi di controllo di routine e di escalation;
- ✧ **Supervisione all'inserimento di nuovi sistemi** informatici nel rispetto del concetto di Privacy by design.

PMPI
Solutions

SEC_RITY
is not complete

without
"U"

Servizi per la Sicurezza delle Informazioni