MARSH RISK CONSULTING

RISK. DISPUTES. STRATEGY.

Il Regolamento Europeo 679/2016 – General Data Protection Regulation

MARSH

Agenda

Introduzione

Definizioni

Contesto normativo

Framework di Riferimento

Introduzione

Che cosa è il GDPR	Il GENERAL DATA PROTECTION REGULATION (GDPR) rappresenta il nuovo Regolamento Europeo in materia di protezione dei dati per le persone fisiche all'interno dell'Unione Europea.
Quali sono gli obiettivi?	Armonizzare le attività di trattamento dei dati ed assicurare libera circolazione dei dati personali all'interno della UE. Definizione del livello di diritti azionabili, degli obblighi e delle responsabilità dei titolari responsabili del trattamento
A chi si applica?	Il GDPR si applica alle aziende coinvolte nel trattamento dei Dati Personali riguardanti persone fisiche dell'Unione Europea. In casi specifici si applica anche se il titolare del trattamento non è un membro dell'Unione Europea.
Quando entrerà in Vigore?	Il GDPR è già in vigore dal 24 Maggio 2016 e tutti i soggetti a cui si applica la Normativa dovranno recepire il Regolamento entro il 25 Maggio 2018

Introduzione

- **Direttiva** 95/46/CE
- **Direttiva** 2009/136/CE (E-privacy)

- **Regolamento** 679/2016

D.Lgs 196/2003:

- **Codice In Materia Di Protezione Dei Dati Personali** (abrogato in parte)
- **Provvedimenti del Garante**

- Carattere di obbligatorietà
- Direttamente applicabile negli stati membri

Definizioni
Art. 4 GDPR

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento **a un identificativo** come il nome, **un numero di identificazione**, **dati relativi all'ubicazione**, **un identificativo online** o a uno o più elementi caratteristici della **sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;**

Ampliamento della definizione rispetto alla precedente normativa

Contesto Normativo
Punti Chiave del Regolamento (1/11)

Area	*Elementi chiave*
Disposizioni Generali e Principi	▪ Principio di Liceità, Correttezza e Trasparenza del Trattamento , Limitazione della Finalità, Minimizzazione, Esattezza, Limitazione della Conservazione, Integrità e Riservatezza, Responsabilizzazione(Art. 5) ▪ Il titolare del trattamento è competente per il rispetto di questi principi e in grado di comprovarlo («responsabilizzazione») ▪ Definizione delle condizioni di validità del Consenso ▪ Trattamento dei «dati sensibili» e dei «dati giudiziari» a determinate condizioni (da Art.9)

Verifica delle modalità di acquisizione del **Consenso** degli interessati (La richiesta del consenso deve essere presentata in modo distinto da altre richieste, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro)

Consenso ✓	Consenso ✗
Barrare apposita casella	Consenso assenso
Firma	Lettura di caselle pre-compilate

Definizione dato sensibile: dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Definizione dato giudiziario :dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Contesto Normativo
Punti Chiave del Regolamento (2/11)

Area	*Elementi chiave*
Diritti dell' Interessato	▪ Formalizzazione dei Diritti degli Interessati comprendenti il Diritto di Accesso ai Dati (Art. 15) Rettifica (Art. 16), Cancellazione (Diritto All'oblio Art. 17) e Diritto alla Limitazione del Trattamento (Art. 18) ▪ Introduzione del tema della Portabilità dei Dati dell'interessato (Art. 20) ▪ Definizione Norme relative alla Profilazione e Marketing Diretto sui dati personali trattati (Art. 21- 22)

- Redazione dell'informativa (art. 13) in modo che contenga come previsto già nel D.lgs. 196/2003, specifiche informazioni relative a:
  - l'identità del titolare ed i dati di contatto;
  - le finalità e le modalità di trattamento;
  - la possibilità di trasferimento dei dati a terzi.

In aggiunta il GDPR richiede di informare l'interessato in merito al:
- il periodo di conservazione dei dati trattati;
- i diritti dell'interessato;
- la possibilità di revocare il consenso;
- il diritto di proporre un reclamo all'autorità di controllo;
- le conseguenze della mancata comunicazione del dato.

Le informazioni contenute nell'informativa devono essere precise ed esposte con un linguaggio chiaro.

- Definire ed implementare procedure che consentano di rispondere tempestivamente alle richieste dell' interessato in merito all'esercizio dei propri diritti (il Regolamento richiede una tempistica di 30 giorni).

Contesto Normativo
Punti Chiave del Regolamento (3/11)

Area	*Elementi chiave*
Responsabilità del Titolare del Trattamento	▪ «*Tenuto conto della natura, dell'ambito di applicazione del contesto e delle finalità del trattamento nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, Il Titolare del trattamento mette in atto* ***misure tecniche organizzative adeguate*** *per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*». (Art. 24) ▪ «*Dette misure sono riesaminate e aggiornate se necessario*». (Art. 24) ▪ *Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui sopra includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del Titolare del trattamento (proporzionalità)* (Art. 24)

- Principio di ACCOUNTABILITY
- Dimostrazione della conformità
- Proporzionalità
- Adeguate misure tecniche e organizzative

Misure minime di Sicurezza?

Allegato B al D.Lgs. 196/03.

Misure tecniche?

Contesto Normativo
Punti Chiave del Regolamento (4/11)

Area	*Elementi chiave*
Protezione dei dati dalla progettazione ed impostazione predefinita	▪ *Privacy by Design* – Introdotto il tema della *Data Minimization* e adozione delle tecniche di cifratura o pseudonimizzazione (Art. 25) ▪ *Privacy by Default* Introduzione del tema della «impostazione predefinita» all'interno del processo di raccolta dei dati (Art. 25)
Responsabile del trattamento	▪ Definita la responsabilità (solidale) del Titolare e Responsabile per la verifica delle Misure Tecniche ed Organizzative messe in atto (Art. 28)
Sicurezza dei dati personali	▪ Adozione di Misure Tecniche e Organizzative che garantiscano la protezione dei dati trattati (pseudonimizzazione e cifratura), la garanzia di Riservatezza, Integrità e Disponibilità dei dati e la Resilienza dei sistemi (oltre alla capacità di ripristino da incidenti) (Art. 32) ▪ Adozione di procedure di valutazione cicliche dell'efficacia delle misure adottate al fine di garantire la sicurezza del trattamento. (Art. 32)

- Revisione di tutti i contratti con i terzi Responsabili esterni
- Predisposizione d'istruzioni documentate da parte del Titolare
- Identificazione/Revisione delle Misure Tecniche ed Organizzative
- Valutazione del Rischio di incidenti di Sicurezza, attacchi *Cyber*

Contesto Normativo
Punti Chiave del Regolamento (5/11)

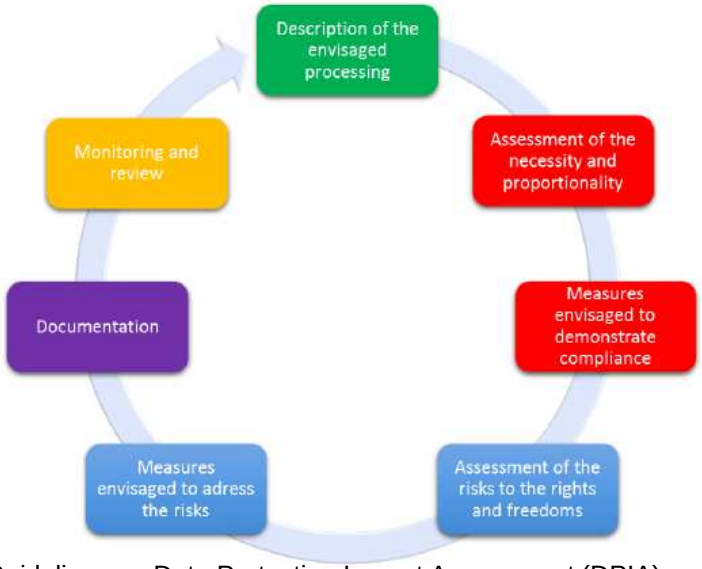
Area	*Elementi chiave*
Registro delle attività	▪ Adozione del Registro delle Attività, non obbligatorietà per dimensioni societari < 250 dipendenti a determinate condizioni (Art. 30)

- Deve essere adottato se il numero dei dipendenti è superiore a 250.
- Deve contenere:
  - Nome del Titolare, Contitolare, Responsabile e DPO;
  - Finalità del trattamento
  - Descrizione delle categorie d'interessati e di dati personali
  - Categorie di dati che saranno comunicati e destinatari (anche in paesi terzi od organizzazioni internazionali)
  - I trasferimenti di dati in paesi terzi
  - I termini previsti per la cancellazione dei dati (se possibile)
  - Descrizione delle misure tecniche di sicurezza e delle misure organizzative;
- Deve essere tenuto in forma scritta, anche in formato elettronico
- Su richiesta, il titolare del trattamento o il responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Contesto Normativo
Punti Chiave del Regolamento (6/11)

Area	*Elementi chiave*
Valutazione d'impatto sulla protezione dei dati	▪ Introduzione del *Privacy Impact Assessment* (PIA) per la valutazione dell'impatto sulla protezione dei dati (rischio di distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali) e la descrizione delle misure di mitigazione dei Rischi (Art. 35)

- Obbligatorietà nel caso in cui il trattamento preveda l'utilizzo di nuove tecnologie e può presentare un rischio elevato per i diritti e le libertà delle persone fisiche- in particolare se:
  - una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata sul trattamento dei dati automatizzati, compresa la profilazione;
  - trattamento di dati particolari su larga scala;
  - sorveglianza sistematica su larga scala di una zona accessibile al pubblico
- Sarà previsto un elenco specifico da parte del Governo



Fonte: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

- Framework di riferimento: Information commissioner's Office (ICO), Autorità **Inglese**; Commission nationale de l'informatique et des libertés (CNIL), Autorità **Francese**; Agencia española de protección de datos (AGPD) Autorità **Spagnola**; Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn , Autorità **Tedesca**.

Contesto Normativo
Punti Chiave del Regolamento (7/11)

Area	*Elementi chiave*
Notifica delle Violazioni	Introduzione della Responsabilità di Notifica verso l'Autorità di Controllo e verso gli Interessati i cui dati sono stati oggetto di violazione entro 72 ore dalla violazione, quando la violazione presenta un rischio per le persone fisiche (Artt. 33 -34)

- Verifiche misure tecnologiche di Monitoraggio, Rilevazione e Risposta ad attacchi Cyber
- Coordinamento delle persone coinvolte
- Realizzazione di simulazioni
- Verifiche coperture Assicurative in caso di *data breaches*

Interrogativi da porsi:

- Dove sono archiviati i dati personali? Dove posso avvenire delle violazioni al trattamento?
- L'organizzazione è in grado di rilevare le violazioni?
- Sono implementate le procedure per rispondere adeguatamente alla violazione? Quanto tempo è necessario per rispondere alla violazione? Più di 72 ore?

Contesto Normativo
Punti Chiave del Regolamento (8/11)

Area	*Elementi chiave*
Data Protection Officer	▪ Introduzione della figura del *Data Protection Officer* (DPO) per supportare il Titolare e il Responsabile del Trattamento nonché vigilare sulla corretta adozione del GDPR e cooperare con le autorità di controllo (Artt. 38-39)

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala;

Il responsabile della protezione dei dati è incaricato **almeno** dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento;

b) sorvegliare l'osservanza del regolamento;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati;

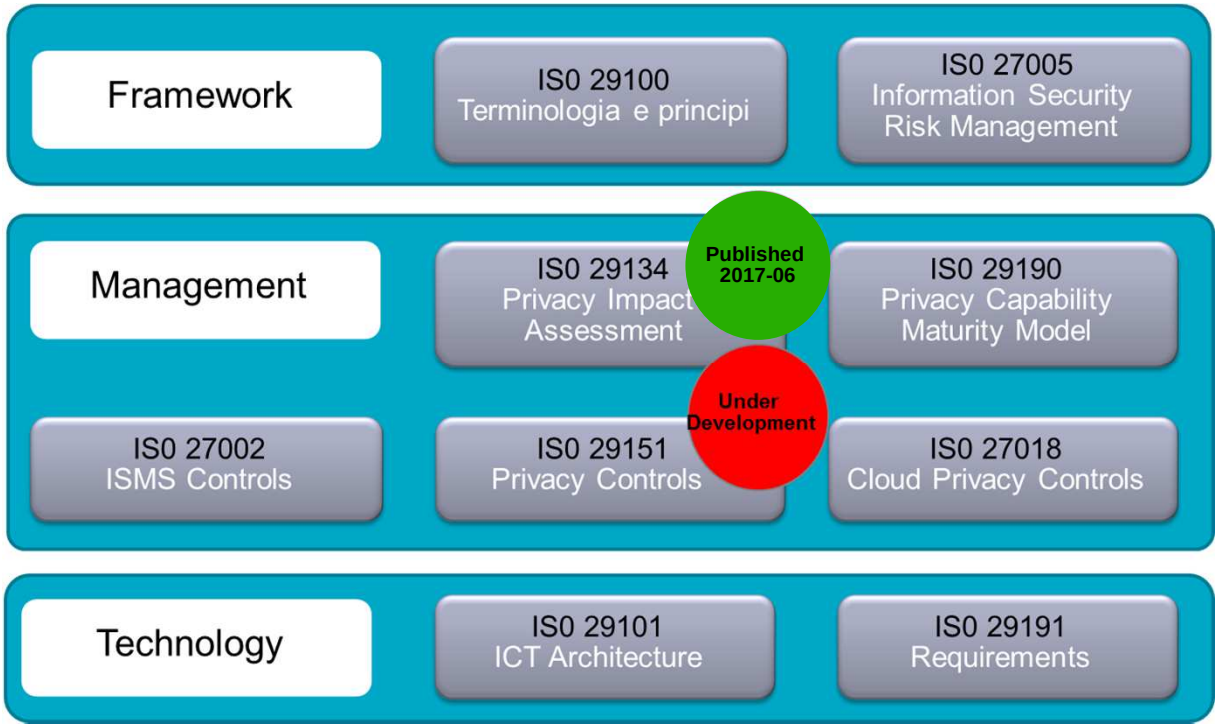
d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

- Il DPO deve possedere competenze legali e IT;
- Può essere esterno e supportato da un Data Protection Office.
- Caratteristiche di indipendenza

Contesto Normativo
Punti Chiave del Regolamento (9/11)

Area	*Elementi chiave*
Codice di Condotta e Certificazione	▪ Adozione del Codice di Condotta e della Certificazione come elementi di garanzia per la conformità ai requisiti (Art. 25) ▪ Introduzione dei requisiti di dettaglio su formalizzazione e contenuti dei Codici di Condotta e Monitoraggio degli aggiornamenti (Artt. 40-41-42) ▪ Introdotte norme per enti certificatori e modalità di certificazione (Art. 43)



- Codici di condotta «per determinati settori» già presenti nel vecchio Codice (Art. 12 e allegato A). Teoricamente non avranno più efficacia dal 25 Maggio 2018, tuttavia il Garante si sta adoperando affinché possano rimanere in vigore.
- Valutazione percorso di certificazione
- Realizzazione del Programma di certificazione

Contesto Normativo
Punti Chiave del Regolamento (10/11)

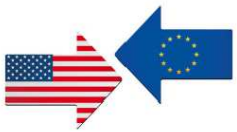
Area	*Elementi chiave*
Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali	▪ Introduzione delle Norme per il trasferimento dei Dati (per esempio dovuti ad adozione di servizi in *Cloud* extra EU o utilizzo di servizi di Outsourcing extra EU o relazioni extra EU) che comportano trasferimento dei Dati Personali (Artt.- 44-50))

Divieto del trasferimento nel Codice (articolo 25, comma 1, della Direttiva 95/46/CE), a meno che il Paese in questione avesse garantito un livello di protezione «adeguato».

La Commissione Europea ha il potere di stabilire tale adeguatezza attraverso una specifica decisione. Le decisioni sono state stabilite per i seguenti Stati: Andorra, Argentina, Australia, Canada, Faer Oer, Guernsey; Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay e **USA - Privacy Shield di ottobre 2016 che ha invalidato il precedente «del Safe Harbour».**

Le imprese americane
- Autocertificheranno su base annuale il rispetto degli obblighi
- Dovranno pubblicare una *privacy policy* (informativa privacy) sul loro sito
- Dovranno rispondere tempestivamente ai reclami
- Dovranno collaborare con le Autorità europee per la protezione dei dati e dare seguito alle loro richieste (se trattano dati relativi al personale/alle risorse umane)

Gli interessati in Europa
- Godranno di più trasparenza rispetto ai trasferimenti di dati personali negli USA e di una tutela rafforzata per questi dati
- Avranno a disposizione strumenti di tutela giuridica più facili da utilizzare e meno costosi in caso di reclami, che potranno gestire da soli oppure con l'aiuto dell'Autorità nazionale di protezione dei dati



Inoltre per il trasferimento transfrontaliero di dati tra società facenti parte dello stesso gruppo di imprese è prevista la stipula di **Binding Corporate Rules**. Tali clausole erano già presenti nel vecchio codice e sono state riprese dal GDPR che ha snellito il meccanismo di predisposizione del testo delle clausole (es. laddove previsto le singole autorità nazionali non devono più approvare il testo).

Contesto Normativo
Punti Chiave del Regolamento (11/11)

Area	*Elementi chiave*
Sanzioni	Introduzione di sanzioni più elevate rispetto al precedente Codice: **Sanzione massima**: € 20 M o il 4% del fatturato totale globale dell'anno precedente, se superiore, per il mancato rispetto degli articoli: - 5,6,7,9 (principi di base del trattamento, comprese le condizioni relative al consenso), - da 12 a 22 (diritti degli interessati), - da 44 a 49 (trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli) o per l' inosservanza di un ordine impartito dall'Autorità. **Altre sanzioni:** € 10 M oppure il 2% del fatturato totale globale dell'anno precedente, se superiore, per la rilevazione di non compliance con il Regolamento, in particolare per il mancato rispetto degli articoli: - 8, 11, da 25 a 39, (gli obblighi del titolare del trattamento e del responsabile del trattamento) - 42, 43 (gli obblighi dell'organismo di certificazione) - 41 paragrafo 4 (gli obblighi dell'organismo di controllo)

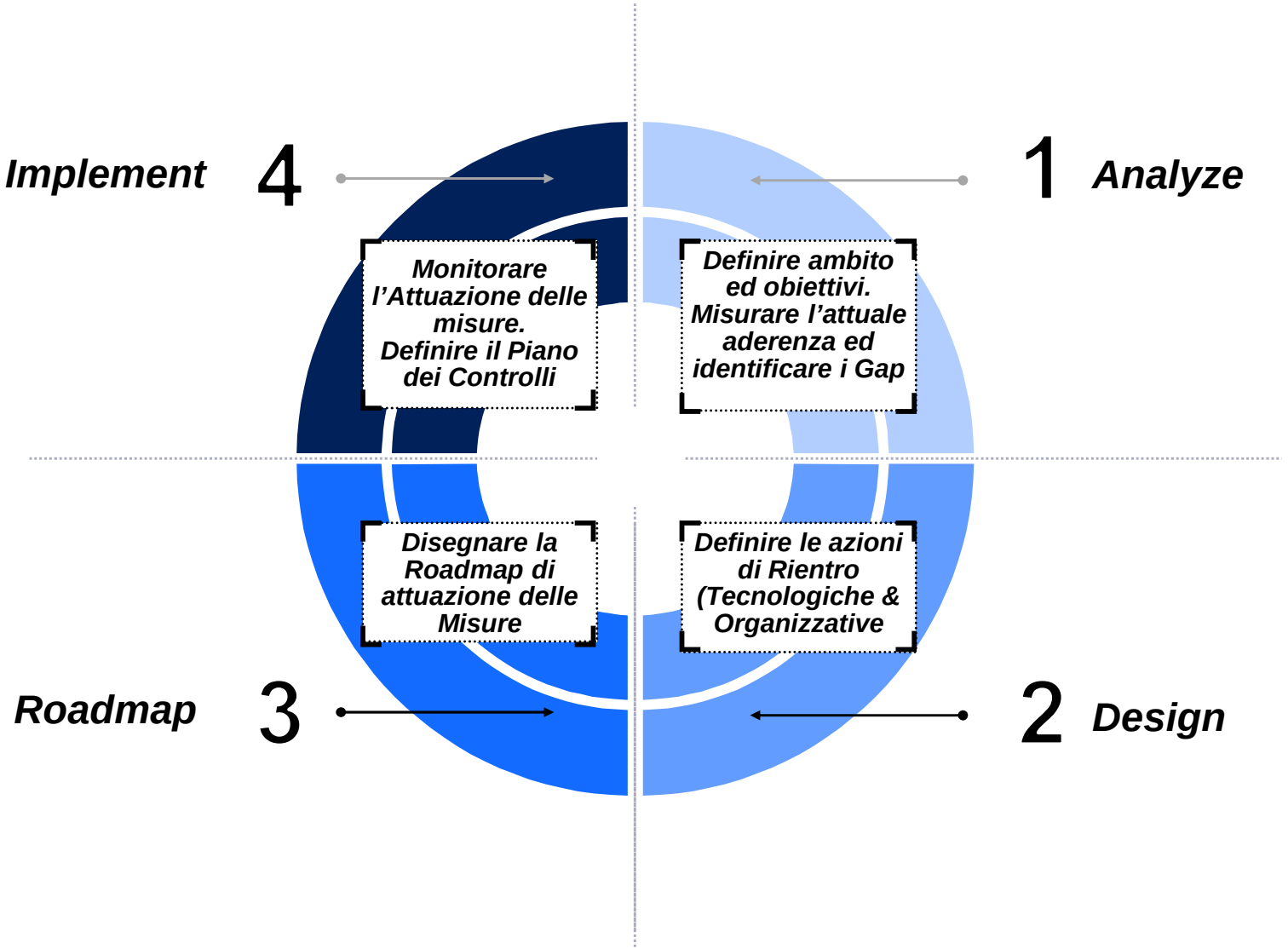
Contesto Normativo
Principali impatti

Le nuove Disposizioni introducono una serie di **impatti** in termini **organizzativi, operativi e tecnologici**, oltre che ad introdurre un **approccio** alla **Data Privacy** indirizzata secondo il **principio del Rischio** associato alla valutazione delle misure applicate ai Dati trattati.

Ambito	*Esempi di Impatti*	*Aree di Intervento*
Organizzazione/ Risk Management	▪ Revisione Ruoli e Responsabilità per Titolare e Responsabili del trattamento, Verifica nomina del DPO (Data Protection Officer); ▪ Valutazione delle misure dei trattamenti sulla base dei Rischi associati ai Dati trattati (esecuzione di un DPIA – Data Privacy Impact Assessment); ▪ Valutazione esposizione rischi relativi a Terze Parti o dipendenti; ▪ Revisione dell'attuale impianto delle Policy e Procedure di Sicurezza e Privacy;	▪ Modello Organizzativo (introduzione DPO) e Modello di gestione Compliance; ▪ Predisposizione DPIA; ▪ Verifiche termini contrattuali verso Clienti, Dipendenti e Terze Parti;
Modello Operativo	▪ Recepimento delle disposizioni relative ai diritti degli Interessati (Richiesta di Modifica, Diritto all'Oblio, etc.) all'interno dell'attuale modello di Privacy; ▪ Verifica modalità di profilazione degli interessati e misure di protezione; ▪ Adozione principio di Privacy by Default e Privacy by Design all'interno del processo di IT Change Management;	▪ Gestione della Raccolta, Modifica e Cancellazione dei dati trattati (Clienti, Dipendenti, Terze Parti); ▪ Adozione dei principi della Privacy all'interno del Processo di sviluppo di prodotti/servizi;
Misure Tecnologiche	▪ Adozione di misure tecnologiche in ambito Data Protection (adozione di pseudonimia, cifratura dati, etc.); ▪ Abilitazione misure di monitoraggio per rilevazione di Data Breach; ▪ Adeguamento misure protezione di accesso ai Dati Sensibili (presenza di Dati Biometrici, etc.)	▪ Data Governance (Mappatura Dati, Owner e tipologie di accessi); ▪ Cyber Threat Intelligence (monitoraggio attacchi Cyber); ▪ Implementazioni Tecnologiche;

Framework di riferimento

L’approccio suggerito distingue 4 Fasi nel processo di gestione e governo della Data Protection e Privacy Compliance ed è basato sui principali standard e best practice di riferimento.



Standards & Best Practices

- **IS0 29100** Terminology and principles
- **IS0 29134** Privacy Impact Assessment
- **IS0 29190** Privacy Capability Maturity Model
- **IS0 27002** ISMS Controls
- **IS0 29151** Privacy Controls
- **IS0 27018** Cloud Privacy Controls
- **IS0 29101** ICT Architecture
- **IS0 29191** Requirements

MARSH RISK CONSULTING

Marsh Risk Consulting Services S.r.l. - Sede Legale: Viale Bodio, 33 - 20158 Milano - Tel. 02 48538 1 - www.marsh.it

Cap. Soc. Euro 10.400,00 i.v. - Reg. Imp. MI - N. Iscriz. e C.F.: 10027410157 - Partita IVA: 10027410157 - R.E.A. MI - N. 1338125

Società con socio unico soggetta al potere di direzione e coordinamento di Marsh S.p.A., ai sensi art. 2497 c.c.