MARSH RISK CONSULTING

RISK. DISPUTES. STRATEGY.

NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY

APPROCCIO METODOLOGICO PER LE ATTIVITÀ DI ADEGUAMENTO AL GDPR

20 Febbraio 2019

MARSH

AGENDA

- **INTRODUZIONE**
- METODOLOGIA DI ADEGUAMENTO
- APPROCCIO PROGETTUALE PROPOSTO
- ORGANIZZAZIONE DEL PROGETTO

OBIETTIVO DEL DOCUMENTO

- Quanto riportato nel presente documento intende soddisfare l'esigenza di disporre un supporto metodologico e operativo per l'adeguamento al General Data Protection Regulation (GDPR) ovvero il Regolamento Europeo 679/2016 in materia di protezione di dati personali che sostituisce la precedente Direttiva 95/46/EC e che dovrà essere implementato a partire da Maggio 2018.

- In particolare, Marsh Risk Consulting ha sviluppato un approccio consulenziale finalizzato a:
  - ✓ Analizzare le modalità di trattamento (raccolta, conservazione e utilizzo) dei dati personali;
  - ✓ Identificare gli scostamenti (Gap) rispetto alle disposizioni del GDPR;
  - ✓ Predisporre il piano di azioni delle misure necessarie da implementare nel percorso di adeguamento al GDPR;
  - ✓ Supportare le Misericordie nell'implementazione delle sopraindicate misure, nonché indirizzare attraverso la definizione di Linee Guida alla valutazione del proprio modello di Data Privacy ai fini della compliance.

In tale contesto, il presente documento si propone di:

- illustrare e descrivere l'approccio metodologico che MRC intende adottare, con il dettaglio circa le fasi, le attività, i documenti che verranno rilasciati;
- condividere pianificazione temporale stimata delle attività previste per l'adeguamento

AGENDA

- INTRODUZIONE
- **METODOLOGIA DI ADEGUAMENTO**
- APPROCCIO PROGETTUALE PROPOSTO
- ORGANIZZAZIONE DEL PROGETTO

SCENARIO REALIZZATIVO

Di seguito è rappresentato lo scenario realizzativo definito per le attività in ambito :

ADEGUAMENTO AL NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY (GDPR)

Strategia Realizzativa	▪ Si prevede un'analisi verticale sugli ambiti della *Data privacy* (ambito organizzativo, procedurale, legale e tecnologico) volta a predisporre le misure idonee per ottemperare alle disposizioni del GDPR.
Metodologia di Analisi	▪ Analisi dell'impianto organizzativo, procedurale e tecnologico dei servizi in essere, combinando raccolta documentale e pre-compilazione *checklist* in modo da minimizzare il numero di interviste/workshop necessari.
Deliverable	▪ Report AS – IS; ▪ *Gap Assessment*; ▪ *Road Map* interventi di adeguamento al GDPR (con l'indicazione e prioritizzazione delle attività afferenti all'ambito operativo, organizzativo e tecnologico); ▪ Supporto per la realizzazione degli interventi definiti negli ambiti di interesse; ▪ Linee Guida per indirizzare la Misericordia nella gestione del Modello di Data Privacy; ▪ Report Finale.

AGENDA

- INTRODUZIONE
- METODOLOGIA DI ADEGUAMENTO
- **APPROCCIO PROGETTUALE PROPOSTO**
- ORGANIZZAZIONE DEL PROGETTO

APPROCCIO PROGETTUALE PROPOSTO

OVERVIEW ATTIVITÀ PROGETTUALI

Fasi progettuali	Principali Obiettivi
1 **Analisi** *Analisi preliminare in ambito Data Privacy*	▪ Raccogliere e analizzare la documentazione e le informazioni in essere in materia di Data Privacy ▪ Predisposizione *Report AS IS*
2 **Gap Assessment e Road Map** *Svolgimento Gap Analysis stato AS-IS vs. GDPR e definizione piano di adeguamento*	▪ Individuazione degli scostamenti (*Gap*) tra lo stato AS IS e gli adempimenti previsti dal GDPR ▪ Predisposizione *Report di Gap Analysis* ▪ Predisposizione del piano di dettagliato (*Road Map*) delle azioni da porre in essere per l'adeguamento al GDPR
3 **Implementazione** *Realizzazione delle azioni di adeguamento al GDPR*	▪ Predisposizione dei seguenti documenti di adeguamento: ✓Registro delle attività di trattamento ✓Informative *Privacy* (ad es. dipendenti, volontari) ✓*Policy Privacy* e *Cookie Policy* per Siti *internet* (ove presenti) ✓Linee Guida per la gestione della *Privacy* ✓Svolgimento DPIA (Data Protection Impact Assessment – Valutazione di impatto) ✓Clausola contrattuale *privacy* per contratti con terze parti ✓Modelli di nomina per la designazione di Responsabili esterni al trattamento ✓Istruzioni per Autorizzati al trattamento di dati personali

DETTAGLIO FASI PROGETTUALI: FASE 1

1 ANALISI

Obiettivi

- *Raccogliere e analizzare la documentazione e le informazioni in essere in materia di Data Privacy*
- *Predisposizione Report AS IS*

Attività

- Preparazione e organizzazione *Kick - Off Meeting* con i referenti di progetto
- Valutazione preliminare dei provvedimenti del Garante ancora in vigore e applicabili alla realtà in atto.
- Raccolta informazioni necessarie per lo svolgimento delle attività progettuali, comprendenti:
  - Raccolta e analisi delle informazioni relative alla tipologia di dati raccolti e al loro trattamento;
  - Raccolta di tutti i documenti afferenti la gestione della Privacy (nomine responsabili e incaricati del trattamento, nomine responsabili della videosorveglianza, eventuale DPS, regolamento informatico, accettazione delle nomine etc.)
  - Analisi delle informative e della modalità di acquisizione dei consensi;
  - Analisi delle modalità e dei tempi di conservazione dei dati;
  - Identificazione dei responsabili (interni ed esterni) al trattamento dei dati, etc.

Deliverable (solo a fini illustrativi)

Report AS - IS

  - Identificazione eventuali rischi relativi a Terze Parti o provider di servizi;
  - Analisi delle misure esistenti per la protezione dei dati;
- Predisposizione del report AS – IS

APPROCCIO PROGETTUALE PROPOSTO

DETTAGLIO FASI PROGETTUALI: FASE 2

2 GAP ASSESSMENT E ROAD MAP (1/4)

Obiettivi

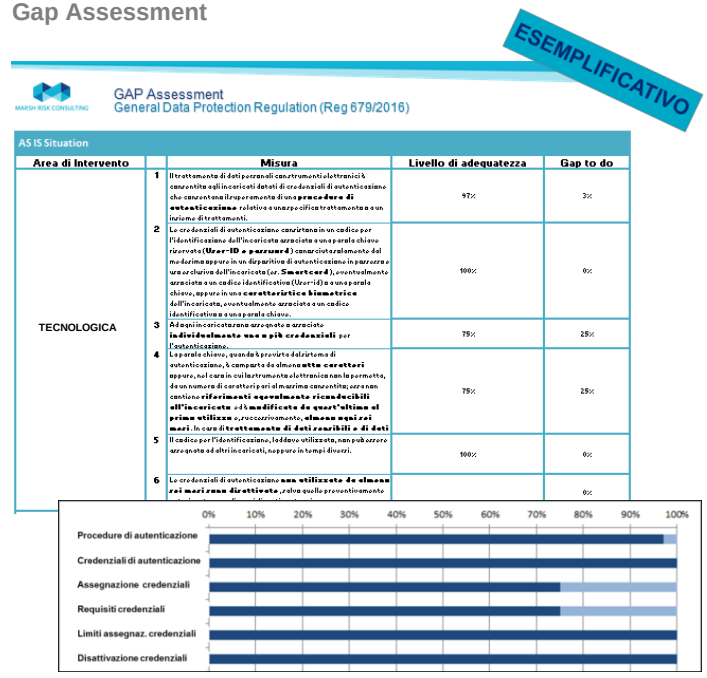
- *Individuazione degli scostamenti (Gap) tra lo stato AS IS e gli adempimenti previsti dal GDPR*
- *Predisposizione Report di Gap Analysis*
- *Predisposizione del piano di dettagliato (Road Map) delle azioni da porre in essere per l'adeguamento al GDPR*

Attività

- Valutazione aree di non conformità rispetto al GDPR e *predisposizione Gap Analysis* rispetto agli ambiti:
  - Operativo
    - identificazione delle non conformità dal punto di vista del *framework* documentale (es. in relazione alla redazione del documento "Registro del Trattamento").
  - Organizzativo
    - identificazione delle non conformità in relazione alla individuazione di risorse cui assegnare ruoli e responsabilità in materia di protezione dei dati personali e sicurezza delle informazioni.
  - Tecnologico
    - identificazione delle non conformità dal punto di vista delle misure tecnologiche adottate (es. monitoraggio di eventuali *Data Breach*);

Deliverable (solo a fini illustrativi)

Gap Assessment



- identificazione del livello di esposizione al rischio delle categorie di dati trattati e indicazioni per la definizione del livello di adeguatezza delle misure tecnologiche adottate.

DETTAGLIO FASI PROGETTUALI: FASE 2

2 GAP ASSESSMENT E ROAD MAP (2/4)

Obiettivi

- *Individuazione degli scostamenti (Gap) tra lo stato AS IS e gli adempimenti previsti dal GDPR*
- *Predisposizione Report di Gap Analysis*
- *Predisposizione del piano di dettagliato (Road Map) delle azioni da porre in essere per l'adeguamento al GDPR*

Attività

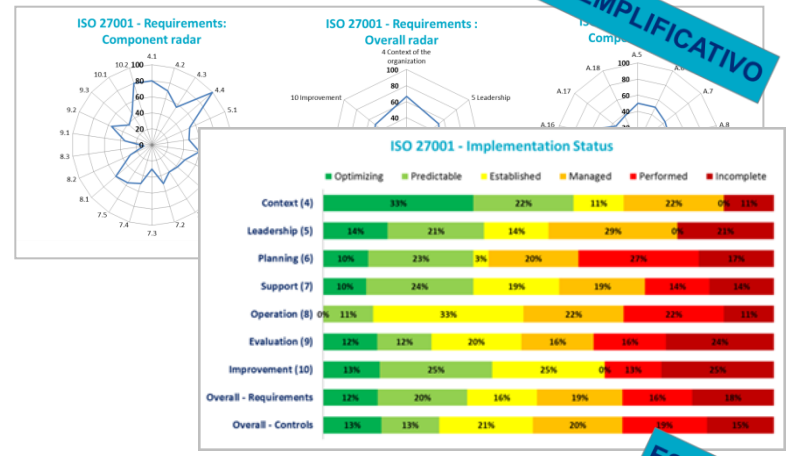
- La valutazione verrà effettuata utilizzando dei *tool* (checklist ad hoc) sviluppati da MRC basati sui *requirements* del GDPR.
- In funzione dei risultati del *gap assessment*, pianificazione degli interventi in ordine di priorità per l'adeguamento a quanto predisposto dal GDPR, con riferimento ai seguenti ambiti (a titolo esemplificativo e non esaustivo):

  Organizzativo, per il quale si prevede:

  - l'identificazione delle attività preparatorie ed esecutive per l'istituzione di nuove figure aziendali (ad es. *Data Protection Officer* – DPO) coinvolte nel processo di trattamento dei dati personali;
  - l'indicazione delle attività rivolte alla definizione puntuale dei ruoli e dell'*accountability* del Titolare e delle altre figure coinvolte nella *governance*.

Tool (solo a fini illustrativi)

ESEMPLIFICATIVO



ESEMPLIFICATIVO

Rilievo	Azione rientro	Scadenza di rientro
Misura 1	Richiesta dichiarazione che attesti il rispetto della normativa vigente	CONCLUSA
Misura 1, 2, 3, 4 ,5 , 6 , 7, 8, 9, 10, 11	-Richiesta autocertificazione e screenshot delle policy autenticazione (password, …); -l'elenco delle utenze; -copia della lettera di incarico al TdP; -screenshot della policy autenticazione (password, …)	CONCLUSA
Misura 5	Policy in corso di aggiornamento.	TBD
Misura 13,14	Copia della procedura.	TBD
Misura 15,16,17,18	Estratto del contratto con il fornitore che gestisce le macchine.	20/3/2018
Misure 20,21,22,23,24,26,27,28,2	-Copia delle procedure afferenti i punti aperti; -Estratto del contratto con il fornitore che gestisce le macchine	1/5/2018

DETTAGLIO FASI PROGETTUALI: FASE 2

2 GAP ASSESSMENT E ROAD MAP (3/4)

Obiettivi

- *Individuazione degli scostamenti (Gap) tra lo stato AS IS e gli adempimenti previsti dal GDPR*
- *Predisposizione Report di Gap Analysis*
- *Predisposizione del piano di dettagliato (Road Map) delle azioni da porre in essere per l'adeguamento al GDPR*

Attività

Operativo, per il quale si prevede:

- l'individuazione dei documenti la cui realizzazione è prevista dal GDPR (ad es. Registro del trattamento) e delle attività rivolte alla loro realizzazione;
- l'indicazione dei documenti (Linee Guida/Policy, Procedure e istruzioni Operative in materia di Data Privacy) da revisionare / aggiornare e l'indicazione delle attività di revisione / aggiornamento da eseguire.
- l'indicazione attività rivolte all'aggiornamento / adeguamento delle informative privacy per gli interessati e delle modalità di richiesta e rilevazione del consensi;
- l'indicazione delle attività per la definizione delle misure di protezione dei dati personali da includere all'interno dei contratti con le terze parti;
- l'indicazione dei trattamenti per i quali si ritiene necessario svolgere un *Data Protection Impact Assessment* (DPIA).

Deliverable (solo a fini illustrativi)

DETTAGLIO FASI PROGETTUALI: FASE 2

2 GAP ASSESSMENT E ROAD MAP (4/4)

Obiettivi

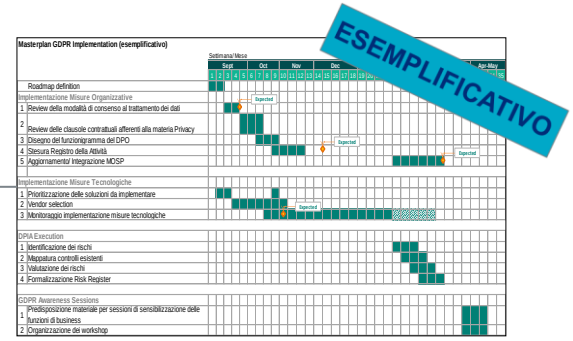
- *Individuazione degli scostamenti (Gap) tra lo stato AS IS e gli adempimenti previsti dal GDPR*
- *Predisposizione Report di Gap Analysis*
- *Predisposizione del piano di dettagliato (Road Map) delle azioni da porre in essere per l'adeguamento al GDPR*

Attività

Tecnologico, per il quale si prevede:

- l'indicazione dei principi per l'implementazione delle soluzioni rivolte a garantire che il trattamento sia svolto in maniera coerente con quanto richiesto dal GDPR, (ad es. per l' applicazione dei principi di "*Privacy By Design*" e "*Privacy By Default*");
- l'indicazione dei principi per l'implementazione delle soluzioni rivolte garantire i diritti previsti per l'interessato (ad es. "diritto alla portabilità dei dati, alla rettifica, alla limitazione del trattamento") e gli obblighi per il Titolare del trattamento (ad es. comunicazione di una violazione dei dati personali dell'interessato).

Deliverable (solo a fini illustrativi)



Piano di dettaglio condiviso con le strutture competenti per la realizzazione degli interventi individuati per l'adeguamento al GDPR

Documentazione esplicativa del piano di dettaglio, illustrativa delle modalità per la conduzione delle attività, degli obiettivi da raggiungere e degli adempimenti normativi raggiunti con l'esecuzione delle attività

DETTAGLIO FASI PROGETTUALI: FASE 3

3 IMPLEMENTAZIONE (1/2)

Obiettivi

- *Predisposizione della documentazione e dei report per l'adempimento degli obblighi previsti dal GDPR*

Attività

- In funzione della Road Map definita nella fase precedente, supporto nell'esecuzione degli interventi, in ordine di priorità, per l'adeguamento a quanto predisposto dal GDPR. Gli interventi saranno implementati con riferimento ai seguenti ambiti di lavoro, come a titolo esemplificativo e non esaustivo:

  Organizzativo, per il quale si prevede:

  - il supporto per la realizzazione delle attività esecutive rivolte all'istituzione delle nuove figure aziendali coinvolte nel processo di trattamento dei dati personali (ad es. definizione dei documenti descrittivi di ruoli e responsabilità del *Data Protection Officer* – DPO);
  - la pianificazione dell'iter di firma e/o pubblicazione dei documenti.

Deliverable (solo a fini illustrativi)

DETTAGLIO FASI PROGETTUALI: FASE 3

3 IMPLEMENTAZIONE (2/2)

Obiettivi

- *Predisposizione della documentazione e dei report per l'adempimento degli obblighi previsti dal GDPR*

Attività

Operativo, per il quale si prevede:

- la predisposizione dei documenti previsti dal GDPR (ad es. Registro del trattamento - ex art 30 GDPR, 1, Policy *Data Privacy* e *Information Security*, metodologia e strumento per esecuzione di Privacy Risk Assessment e DPIA, clausole contrattuali privacy per contratti, Istruzioni per autorizzati al trattamento);
- l'aggiornamento / adeguamento delle informative privacy da erogare agli interessati e la definizione delle modalità di richiesta e rilevazione del consensi (l'attività comprende la predisposizione di Privacy Policy e Cookie Policy del Sito Internet della Misericordia se presente)
- stesura del modello di Nomina a Responsabile esterno del trattamento da inserire nei contratti con le Terze Parti per vincolarle al rispetto degli obblighi imposti dal GDPR.
- Svolgimento report DPIA

Tecnologico, per il quale si prevede:

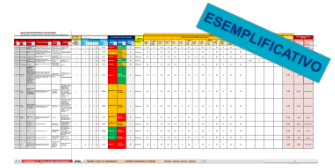
- la predisposizione dei documenti previsti dal GDPR (ad es. l'integrazione del documento di Policy / Linee guida conm le indicazioni per indirizzare la Misericordia nel definire i requisiti per l'implementazione delle soluzioni tecnologiche in funzione a quanto richiesto dal GDPR, in particolare per l' applicazione dei principi di "*Privacy By Design*" e "*Privacy By Default*").

Deliverable (solo a fini illustrativi)

Registro delle attività di trattamento (ex art. 30 GDPR, c1)

Linee Guida e per la gestione della Privacy in funzione delle novità previste dal GDPR (con indicazione delle modalità di gestione dei Data Breach, della gestione delle richieste degli interessati per l'esercizio dei diritti privacy, dell'applicazione dei principi di Privacy By Design e By Default)

- Clausola contrattuale Privacy per contratti con terze parti
- Istruzioni per gli autorizzati al trattamento
- Informative privacy aggiornate secondo quanto previsto dal GDPR e descrizione delle modalità richiesta / rilevazione consensi
- Modelli di nomina a Responsabile esterno dei trattamenti da inserire sui contratti con i fornitori



Report DPIA (Data Protection Impact Assessment – Valutazione d'impatto)

AGENDA

- INTRODUZIONE
- METODOLOGIA DI PROGETTO
- APPROCCIO PROGETTUALE PROPOSTO
- **ORGANIZZAZIONE DEL PROGETTO**

COMPOSIZIONE TEAM DI PROGETTO

In funzione del raggiungimento degli obiettivi di progetto, MRC prevede di impiegare un Gruppo di Lavoro studiato coerentemente con le necessità progettuali e composto dalle seguenti figure professionali:

Figura professionale	Profilo
Project Manager(*)	Professionista che ha la responsabilità di supervisione di tutte le attività contemplate dal progetto a garanzia del rispetto delle tempistiche, del regolare svolgimento delle attività e della qualità della documentazione rilasciata.
Senior Consultant(*)	Professionista, con esperienza consolidata in ambito *Data Privacy Compliance* e *Information Security* con la responsabilità operativa delle attività progettuali con un forte orientamento al risultato, capacità di lavoro di gruppo, autonomia e affidabilità della conduzione di interviste e nella predisposizione di *deliverable* progettuali
Subject Matter Experts (2)	Team di professionisti che supporta, laddove necessario, il *core team* di progetto in funzione delle specifiche competenze maturate nel corso del proprio percorso professionale in materia di *Legal & Compliance*, *Data Protection* e IT/*Cyber Security e IT Risk Management*

TEMPISTICHE DI PROGETTO

Di seguito si riporta una ipotesi di macro pianificazione temporale preliminare per le attività progettuali:

Moduli / Fasi		Mese 1				Mese 2				Mese 3			
		1	2	3	4	1	2	3	4	1	2	3	4
MODULO 1	FASE 1 – Analisi	*Kick-off Meeting*			*Report AS-IS*								
	FASE 2 - Gap Assessment e Road Map							*Gap Assessment Report e Road Map interventi*					
	FASE 3 – Implementazione									*Erogazione incrementale dei deliverable per l'adeguamento al GDPR*			

Fasi Progettuali

Meeting / SAL previsti

MARSH RISK CONSULTING