



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**



Un anno di Regolamento UE 2016/679

La privacy nel settore privato: spunti e riflessioni con esponenti
del Garante per la Protezione dei Dati Personali

Avv. Andrea d'Agostino LL.M.

Vice Presidente dell'Unione Giuristi per l'Impresa

Senior Legal Counsel e Responsabile Privacy

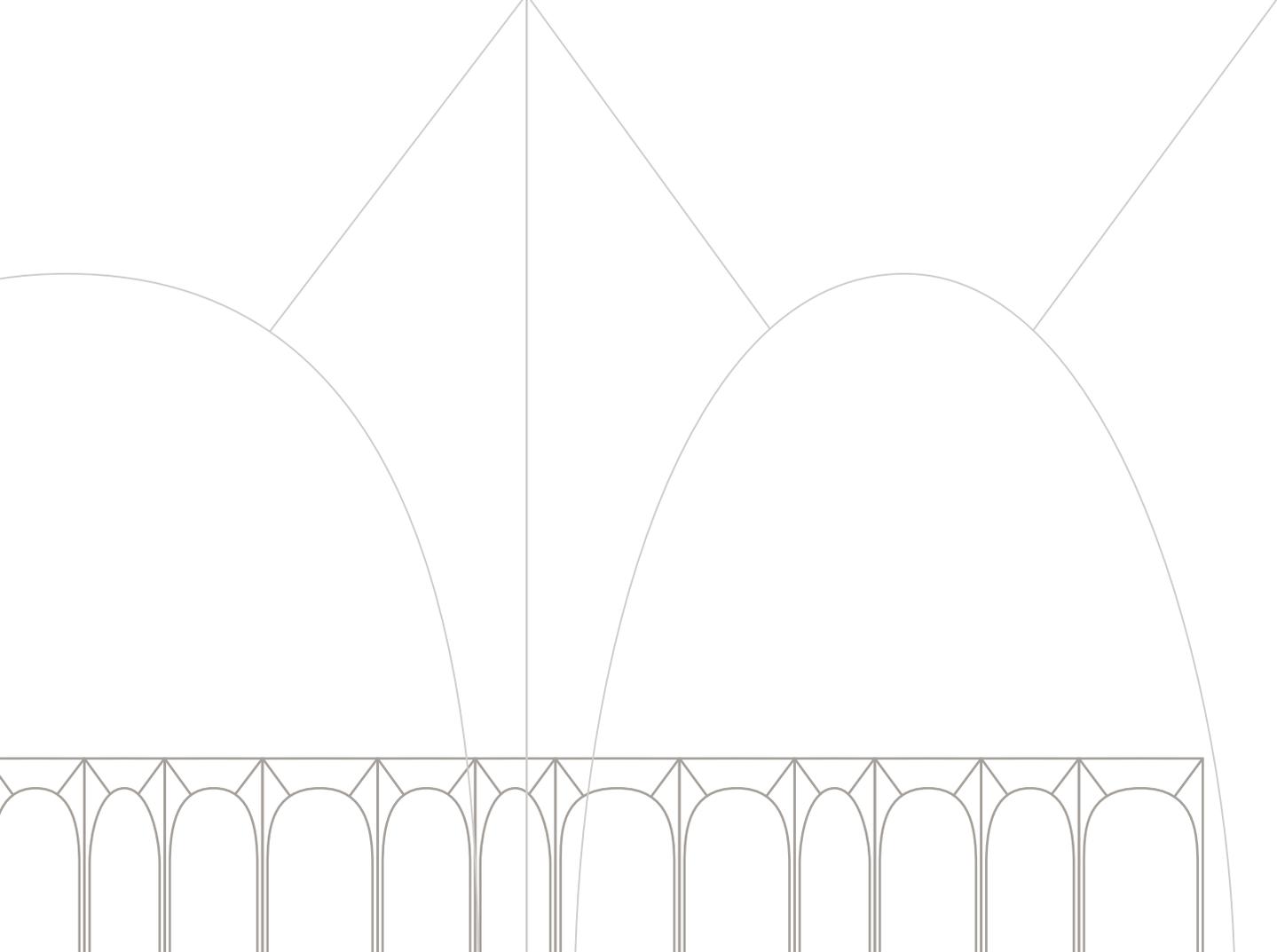
GRUPPO  MONDADORI

Milano, 9 aprile 2019

IN COLLABORAZIONE CON

MEDIA PARTNER





**Il processo di adeguamento al
Regolamento UE 2016/679**

Il processo di adeguamento al Regolamento UE 2016/679

Notifica della violazione entro 72 ore (Data Breach)

La violazione deve essere segnalata entro 72 ore dal momento in cui se ne viene a conoscenza



Il Responsabile per la Protezione dei Dati (DPO)

La sua nomina, in alcuni casi, è obbligatoria e ha il compito di monitorare l'osservanza del GDPR in azienda e fungere da punto di contatto con gli interessati e l'autorità di controllo

Il nuovo sistema sanzionatorio

Le violazioni del GDPR possono essere sanzionate fino al 2% o 4% del fatturato globale annuo o fino a 10 milioni o 20 milioni di Euro



Una maggiore portata territoriale

Il GDPR prevede specifici meccanismi per individuare a quali soggetti e trattamenti si applica indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione Europea



La nuova informativa privacy

Gli interessati devono essere adeguatamente informati circa ogni attività di trattamento che riguardano i loro dati. Il GDPR prevede nuovi elementi obbligatori da inserire nell'informativa

Il Data Protection Impact Assessment (DPIA)

Per tutte le attività di trattamento che rappresentano particolari rischi per i diritti e le libertà degli interessati risulta opportuno effettuare una valutazione d'impatto ai sensi del GDPR



I nuovi diritti degli interessati

Il GDPR amplia le possibilità per gli interessati di far valere i propri diritti introducendo nuovi concetti come la portabilità dei dati e normando altri come il diritto all'oblio



Privacy by design e Privacy by default

Il lancio di un nuovo prodotto o servizio richiede una valutazione preliminare in merito al rispetto della privacy adottando un approccio by design o by default

Dal prodotto...



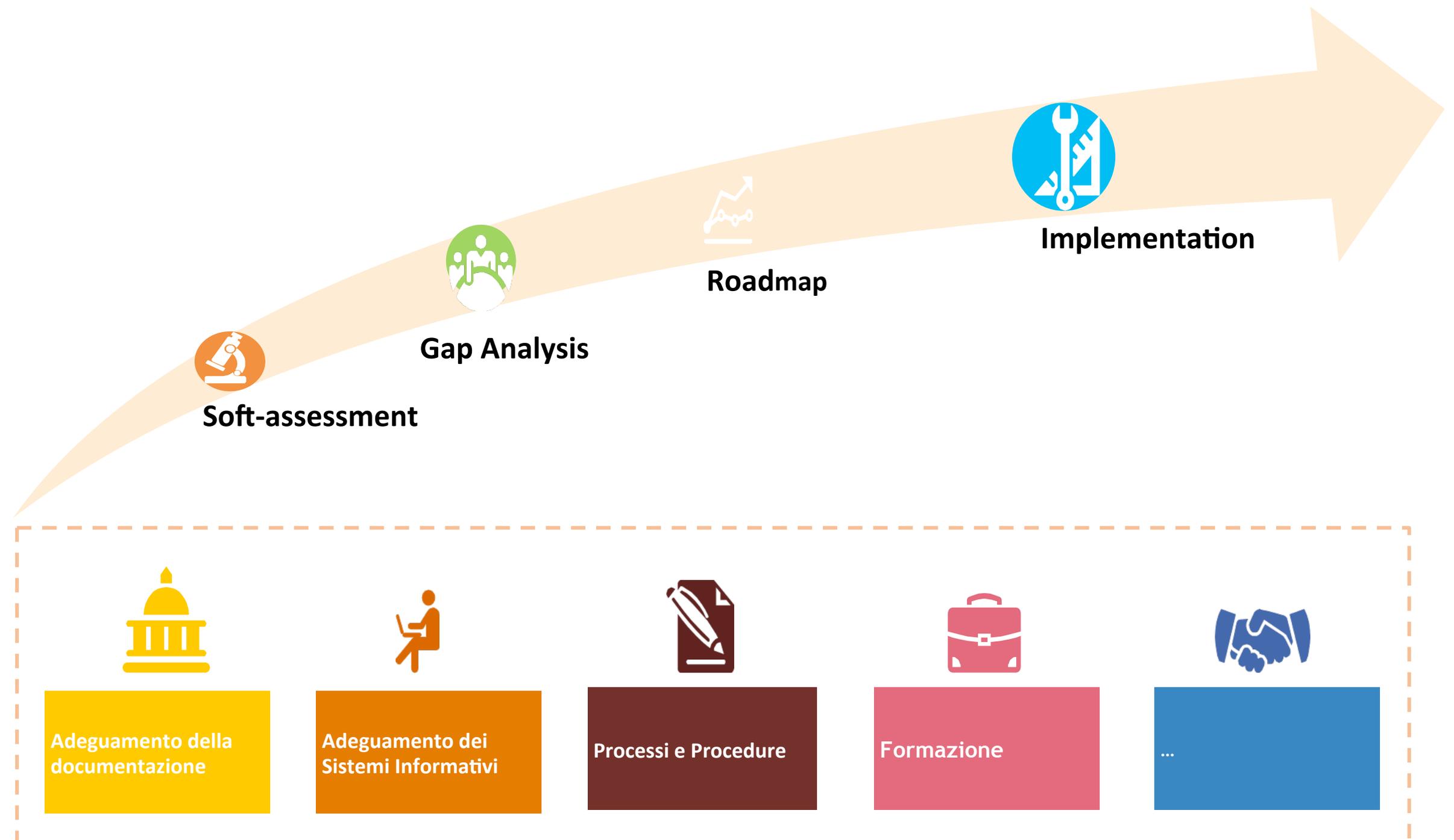
...ai nostri lettori



Il processo di adeguamento al Regolamento UE 2016/679



Il processo di adeguamento al Regolamento UE 2016/679

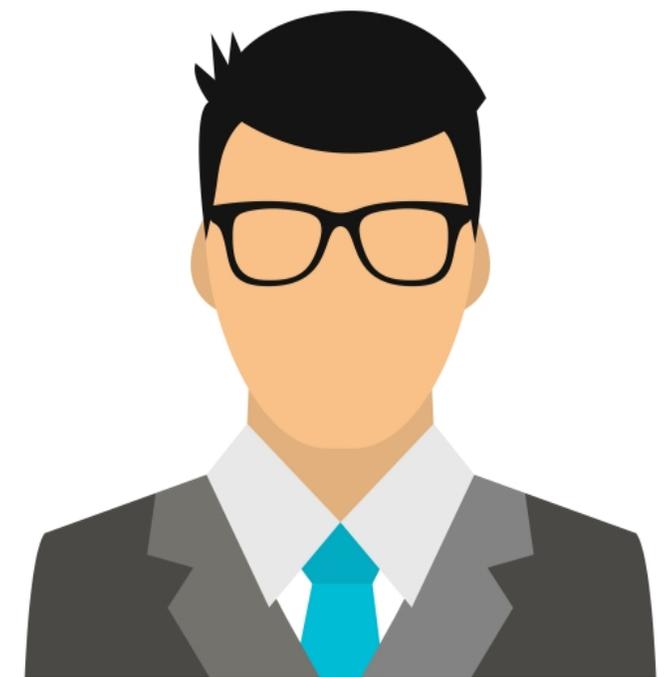


a) Adeguamento della documentazione



Adeguamento della
documentazione

1. Mappatura di tutte le attività di trattamento effettuate dal Gruppo Mondadori
2. Revisione di tutte le informative privacy e cookie policy
3. Revisione di tutte le clausole contrattuali in uso per il trattamento dei dati personali
4. Predisposizione dei verbali interni per le valutazioni legali sulle attività di trattamento
5. Predisposizione degli standard contrattuali da utilizzare per la nomina dei responsabili del trattamento



Legal Department

b) Adeguamento dei sistemi informativi



Adeguamento dei
sistemi informativi

1. Definizione delle nuove misure di sicurezza sulla base dei principi di privacy by design e by default
2. Implementazione dei nuovi sistemi informativi
3. Verifica dei fornitori dei servizi IT e revisione delle nomine ad amministratori di sistema
4. Adozione di un sistema di Information Security Incident Management
5. Adozione di un sistema di verifiche periodiche delle infrastrutture IT



IT Department

c) Processi e procedure



Processi e Procedure

1. Data Retention Policy
2. Data Breach & Data Incident Management Policy
3. Data Protection Impact Assessment Policy & Procedure
4. Data subject's rights Policy
5. Privacy by Design & by Default Policy
6. Data Processor Identification & Management Policy



**HR – IT – Legal
Departments**

d) Formazione



Formazione

1. Training al management
2. Formazione al personale
3. Sensibilizzazione degli interessati
4. Creazione di GDPR Angels in azienda
5. Training & Assessment ai fornitori
6. Attività di testing



HR Department

Il processo di adeguamento al Regolamento UE 2016/679



Identificazione e mappatura di tutte le attività di trattamento effettuate da ogni singola divisione aziendale e, quindi, predisposizione e compilazione del **registro dei trattamenti** ai sensi dell'art. 30 Reg. UE 2016/679



Predisposizione, sulla base delle attività di trattamento mappate, delle nuove **informative privacy**, ai sensi degli artt. 13 e 14 del Reg. UE 2016/679



Analisi delle attività di trattamento in termini di durata e conservazione per la predisposizione di una procedura volta a identificare il **periodo di conservazione dei dati e successiva cancellazione**



Definizione dei criteri di **Privacy by Design e Privacy by Default** da seguire nella ideazione e progettazione di nuovi prodotti e servizi in conformità al Reg. UE 2016/679

Il processo di adeguamento al Regolamento UE 2016/679



Identificazione e nomina del **Data Protection Officer** e del team a supporto definendone poteri e responsabilità



Esecuzione di un Risk Assessment su tutte le attività di trattamento e sottoporre a un **Data Protection Impact Assessment** quei trattamenti che presentano rischi specifici per i diritti e le libertà degli interessati



Identificazione dei criteri da utilizzare per l'individuazione dei casi di **Data Breach e Data Incident** e definizione di una procedura che disciplini le modalità di gestione e notificazione dei casi di violazione



Predisposizione e formalizzazione di una procedura che disciplini tutti gli adempimenti che gli incaricati dovranno porre in essere per gestire le richieste d'esercizio dei **diritti degli interessati**

GRUPPO  MONDADORI

Grazie per l'attenzione



Avv. Andrea d'Agostino

Senior Legal Counsel & Responsabile Privacy

Direzione Affari Legali e Societari Gruppo Mondadori

5°Piano – Torre Nord

Via Mondadori, 1

20090 Segrate (MI)

Tel. +39.02.75423305

Mob. +39.366.6984568

andrea.dagostino@consulenti.mondadori.it

