CON IL PATROCINIO DEL

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

ORGANIZZATO DA

UNIONE GIURISTI
PER L'IMPRESA

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

L'esperienza del DPO dopo un anno di attività

GRUPPO MONDADORI

Avv. Ugo Ettore Di Stefano

Presidente UGI - General Counsel e DPO Gruppo Mondadori

IN COLLABORAZIONE CON

大成 DENTONS

GIANNI·ORIGONI
GRIPPO·CAPPELLI
PARTNERS

pwc | PwC TLS
Avvocati e Commercialisti

STUDIO PREVITI
ASSOCIAZIONE PROFESSIONALE

WHITE & CASE

MEDIA PARTNER

GRUPPO 24 ORE

I compiti del Data Protection Officer

assicurare la conformità delle società del Gruppo alle disposizioni del Regolamento Europeo n.679/2016 nonché ai provvedimenti emanati dalle autorità competenti e alle norme applicabili. Il DPO svolge attività di monitoraggio e affianca i business nei processi aziendali per valutare ogni impatto sul trattamento dei dati personali evitando eventuali data breach. Il DPO è chiamato ad implementare quanto necessario al fine di facilitare la corretta gestione delle attività aziendali.

Requisiti del Data Protection Officer

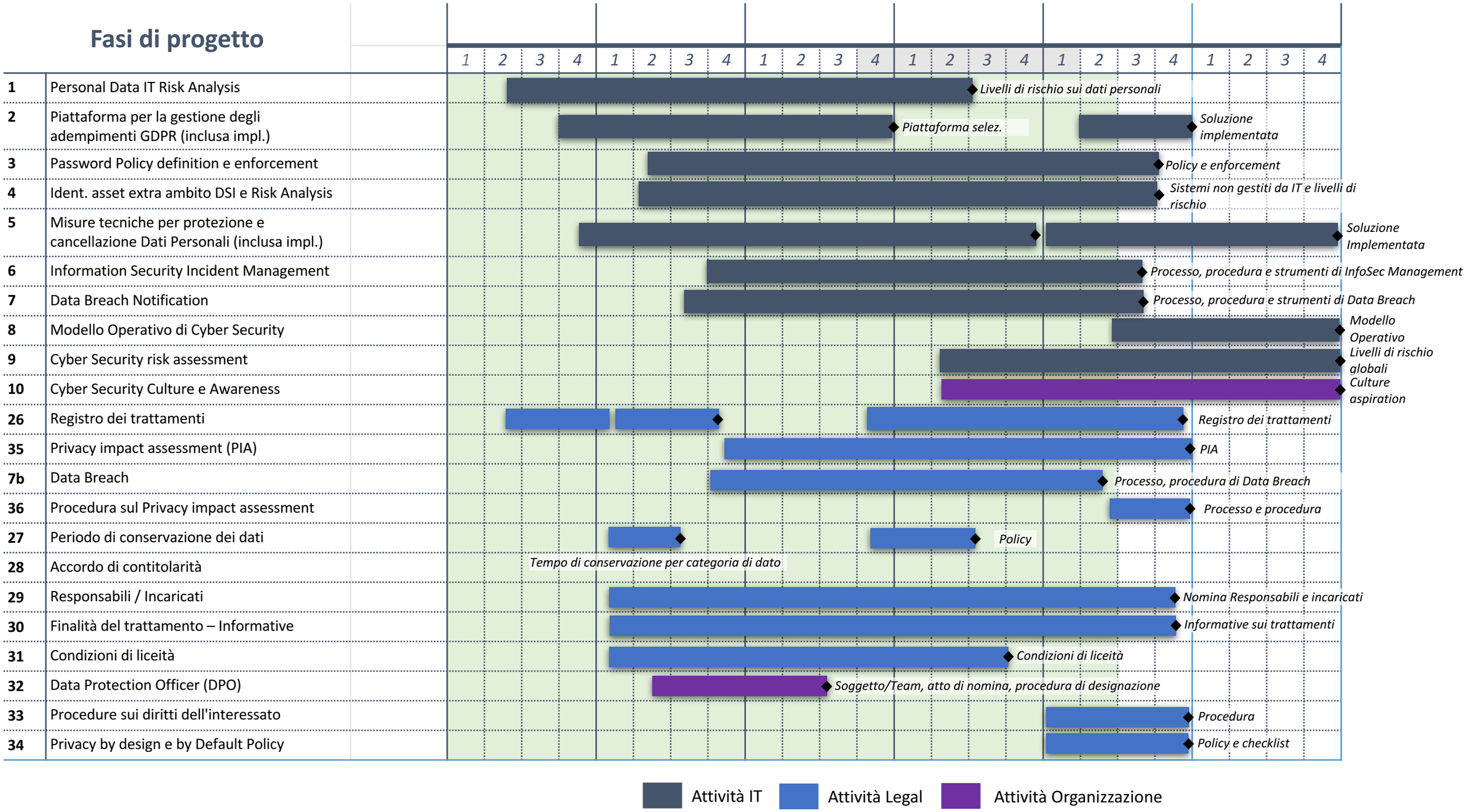
a) approfondita conoscenza del quadro normativo nazionale ed internazionale in materia di privacy e dei provvedimenti emanati dall'Autorità Garante e delle linee guida;
b) esperienza nella gestione degli adempimenti previsti dalla normativa;
c) conoscenza dei processi aziendali e meccanismi di ogni singolo business di riferimento;
d) eccellenti capacità organizzative e gestionali;
e) ottime doti comunicative e relazionali;
f) esperienza nella gestione dei rapporti istituzionali con le Autorità;
g) ottima conoscenza del diritto delle nuove tecnologie e di impresa;
h) ottime conoscenze sui processi informatici e tecnologici;
i) abilità a lavorare sia in team che autonomamente;
j) ottime doti nella gestione di rapporti di rapporti con soggetti stranieri;
k) aver redatto articoli e tenuto corsi in materia di privacy e aver conseguito master in diritto e gestione dell'impresa e diritto delle nuove tecnologie.

1. fornire pareri relativamente alla normativa privacy nonché ai provvedimenti ed all'orientamento delle Autorità;
2. partecipare ai processi che implicano il trattamento di dati e fornire la consulenza in merito agli accorgimenti da adottare ed ai profili di rischio da valutare secondo i principi di Privacy by Design e Privacy by Default;
3. coordinare, nel corso delle valutazioni sugli impatti privacy, referenti aziendali delle direzioni aziendali coinvolte (e.g. IT, Risorse Umane, Amministrazione, Controller, Legale, Audit interno);
4. definire e aggiornare costantemente il Registro dei Trattamenti istituito;
5. definire, congiuntamente a tutti dipartimenti aziendali, le politiche di protezione dei dati personali nonché le procedure di trattamento sulla delle attività di trattamento indicate nel Registro dei trattamenti;
6. predisporre ed aggiornare la documentazione privacy obbligatoria quale a titolo esemplificativo e non esaustivo informative privacy, cookie e privacy policy, moduli per la raccolta del consenso, nomine a incaricati del trattamento, redazione contratti di nomina di responsabili esterno del trattamento;
7. effettuare le valutazioni richieste dal GDPR, per la nomina di responsabili esterni del trattamento, in merito ad ogni fornitore a cui il Gruppo intende affidare in toto e/o in parte attività di trattamento di dati personali;
8. gestione e coordinamento di tutte le attività di riscontro alle istanze proposte dai soggetti interessati;
9. gestione degli aspetti legali connessi al funzionamento del CRM nonché dell'impianto di contitolarità istituito
10. gestione dei rapporti istituzionali con le Autorità a livello europeo nonché con le associazioni di categoria;
11. gestione e coordinamento delle attività nel corso di eventuali ispezioni;
12. gestione del contenzioso amministrativo, ricorsi, reclami e segnalazioni trasmesse all'Autorità Garante per la Protezione dei Dati Personali nei confronti di ciascuna società del Gruppo Mondadori;
13. svolgere, in virtù degli obblighi previsti dal GDPR, attività di formazione continuativa ed obbligatoria in tema di protezione dei dati personali a tutti i dipendenti del Gruppo Mondadori;
14. Svolgere specifiche gap analysis al fine di valutare la costante conformità del Gruppo alle prescrizioni
15. verificare, con cadenza periodica, il rispetto da parte dei responsabili esterni del trattamento delle prescrizioni fornite dal Gruppo Mondadori in merito ai trattamenti di dati personali esternalizzati.

PROGETTO GDPR IN MONDADORI – PIANO ATTIVITA'

UNIONE GIURISTI PER L'IMPRESA

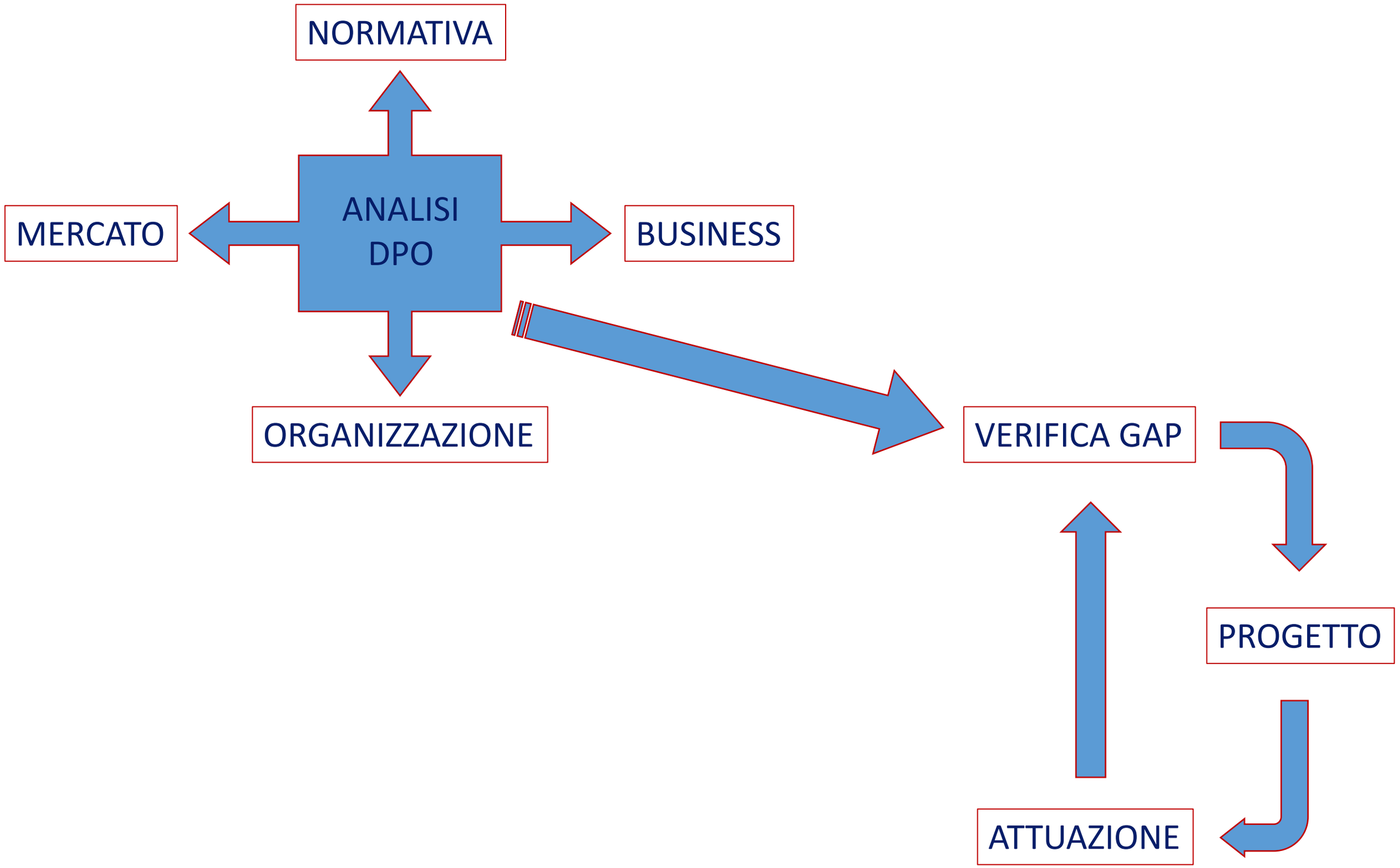
GRUPPO



ATTIVITA' DPO E ALTRE FUNZIONI PROGETTO GDPR

ID	Iniziativa	Proprietà	Tipologia	Recurring
1	Personal Data IT Risk Analysis	Non IT	Processo/Analisi	gg/uomo (AME+EXT)
2	Piattaforma per la gestione degli adempimenti GDPR Implementazione piattaforma	IT	Implementazione	Licenza SAAS
3	Password Policy definition e enforcement	IT	Processo/Analisi/Gestione	
4	Shadow IT identification e IT Risk Analysis	IT	Processo/Analisi	gg/uomo (AME+EXT)
5	Misure tecniche per protezione e canc Dati Personali Implementazione sist. di cifratura/mascheramento	IT IT	Implementazione	Maintenance SW
6	Information Security Incident Management	IT	Processo/Gestione	
7	Data Breach Notification	IT	Processo/Gestione	
8	Modello Operativo di Cyber Security	IT	Processo/Gestione	
9	Cyber Security risk assessment	IT	Processo/Analisi	gg/uomo (AME+EXT)
10	Cyber Security Culture e Awareness	Non IT	Processo/Formazione	gg/uomo (AME+EXT)
11	Privacy by Design e by Default Enforcement	Non IT	Processo/Formazione/Gestione	gg/uomo (EXT)
12	SIEM/LOG Management selection e PoC SIEM/LOG Management solution implementation	IT	Implementazione	Maintenance SW o gg/uomo (AME)
13	Identity and Access Management Identity and Access Management solution implementation	IT	Implementazione	Maintenance SW
14	Data Discovery selection e PoC Data Discovery solution implementation	IT	Implementazione	gg/uomo (AME+EXT) + Licenze
15	Vulnerability Management e Patch Management	IT	Processo/Gestione	
16	Data Loss Prevention selection e PoC Data Loss Prevention solution implementation	IT	Implementazione	Maintenance SW o gg/uomo (AME +EXT)
17	Crisis Management e Business Continuity	Non IT	Processo/Gestione	
18	VA Applicativo e Infrastrutturale applicazioni GDPR	IT	Processo/Gestione	gg/uomo (AME+EXT)
19	Secure Software Development	IT	Processo/Formazione	
20	Supporto specialistico Cyber Security e Privacy	N/A	Processo/Gestione	gg/uomo (AME+EXT)
21	VA Applicativo e Infrastrutturale applicazioni critiche	IT	Processo/Gestione	gg/uomo (AME+EXT)
22	Secure Configuration management	IT	Processo/Gestione	
23	Third Party Security Management	Non IT	Processo/Gestione	
24	Cyber Security Framework	IT	Processo/Analisi	
25	Security Operation Center Selection & POC Security Operation Center implementation	N/A N/A	Processo/Gestione	gg/uomo (AME+EXT)

METODOLOGIA DPO ATTIVITA' GDPR



PROGETTO GDPR IN MONDADORI – GRUPPI LAVORO

UNIONE GIURISTI PER L'IMPRESA

GRUPPO

Cantieri

- IT
- Legal
- HR & O
- Compliance

PMO

- PMO interno
- PMO esterno — PWC
- DPO — Di Stefano

Ruoli e responsabilità

- Avanzamento lavori sui diversi cantieri e su attività dei fornitori (**inclusa attività in Francia**)

Steering

- Steering Committee — Di Stefano
- PMO
- IT
- Legal — *D'Agostino*
- HR & O
- DCI

Rapporto CLUSIT 2019-8° Ed.

Clusit Associazione Italiana per la Sicurezza Informatica

- *Curioso: 2° sem 2018 no incremento attacchi privacy in Europa; invece nel Mondo (+37%)*
- *2018 anno peggiore di sempre per attacchi cyber*

Osservatorio Information Security & Privacy promosso da:

POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT

- 59% aziende ha in corso un progetto di adeguamento GDPR; nel 23% i progetti sono completati
- Solo 8% ancora in fase analisi requisiti richiesti e piani di attuazione possibili (nel 2017 era 34%)
- 58% dei casi esisteva un budget dedicato, nell'ultimo anno la percentuale è 88%
- azioni implementate: registro trattamenti (85%), individuazione ruoli e responsabilità (81%), raccolta e mappatura dati (78%), modifica modulistica (76%), procedura data breach (68%), definizione politiche sicurezza e valutazione rischi (66%), valutazione impatto protezione dei dati (56%), implementazione processi esercizio diritti interessato (54%) revisione contratti con fornitori servizi tecnologici (48%)
- 52% ha indicato raccolta/mappatura dati come fattore che ha reso difficile l'adeguamento GDPR. Altre criticità riscontrate: mancanza sensibilizzazione dipendenti aziendali (38%), scarsa sponsorizzazione Top Management (37%), difficoltà comprensione normativa (27%), mancanza figure professionali competenti (23%), inadeguatezza budget (20%), inefficacia soluzioni tecnologiche protezione e scarse iniziative organizzative (20%)
- DPO presente nel 65% delle organizzazioni, mentre nel 6% è una presenza di tipo "informale"
- 26% ha registrato criticità organizzative: es. individuazione ruoli e responsabilità, mentre l'8% ha rilevato "incidenti di percorso" come temporanei rallentamenti dei processi e delle attività.
- settori più sensibili: aziende B2C rispetto B2B; settori innovativi più di mercati tradizionali

SUGGERIMENTI PER I DPO

- ✓ periodici **incontri** con vertice aziendale/titolare trattamento, per capire: dove si è, dove sono gli altri, dove si potrebbe essere e dove si sarà
- ✓ evitare tecnicismi non necessari, usare **linguaggio** del business
- ✓ non alimentare la paura delle **sanzioni** (ma spiegarne la rilevanza)
- ✓ concentrarsi sul **buon uso dei dati** come strumento di buona pubblicità al cliente e soddisfazione dello stesso che con fiducia sarà predisposto a fornire dati per finalità utili ad entrambi
- ✓ Non identificare data breach come inadeguatezza; è impossibile non sbagliare, importante però è **capire** ed evitare errori gravi e dannosi per interessati e poi subito **rimediare**
- ✓ aziende chiedono sempre di alzare l'asticella del **rischio**: chiarire che le conseguenze sono gravi per il business e che occorre lavoro di team e gli **investimenti organizzativi** e **tecnologici** sono funzionali ad efficienza dei processi e non un mero costo
- ✓ non trascurare risorse, tempo e budget per **formazione**, a tutti i livelli (non è un software o una password che tutelano l'azienda)

CONCLUSIONI

- tanto è stato fatto, ma ancora molti DPO si preoccupano di approcciare il tema come fosse il mero adempimento tecnicistico di una check list
- puntare sulla **formazione**:

1) *degli operatori del business*
2) *dei vertici aziendali e di chi gestisce l'organizzazione in azienda*
3) *dei clienti/interessati*
4) *e prima…dei DPO (con competenze di business, tecnologiche, comunicative e ovviamente legali)*

bene convegni/master/scuole, ma soprattutto tavoli di lavoro operativi

- tempo e risorse per **progettazione e organizzazione** (chi giudicherà l'operato delle aziende avrà in grande considerazione, più che il singolo errore, dove l'azienda sta andando, quale è la strada tracciata, quale la cultura)
- Il **ruolo del DPO** oggi? Non solo un verificatore e più: a lui viene affidata la costruzione, le linee guida, della strategia culturale della privacy in azienda...il Titolare spesso non ha ancora i "mezzi e preparazione" per farlo

GRAZIE PER L'ATTENZIONE

GRUPPO MONDADORI

Avv. Ugo Ettore Di Stefano

Presidente UGI - General Counsel e DPO Gruppo Mondadori