Mosys consulting

cecilia & PARTNERS

COMPLIANCE
GDPR

marzo / 2019

Indice

Approccio Mosys ed esperienza

Il Regolamento GDPR sta dimostrando di avere un impatto molto consistente sulle organizzazioni pubbliche e private a seguito del cambio di paradigma che prevede l'accountability del titolare del trattamento, il quale è responsabile delle misure operative e tecniche che riterrà opportune, efficaci e dunque adeguate per salvaguardare i dati che tratta.
Le conseguenze stanno dimostrando che è necessario avere una visione «olistica» degli impatti del Regolamento sui processi aziendali e sui sistemi informativi ed avere la capacità di valutare i rischi, ingenti, della mancanza della compliance.

Mosys, sulla base di esperienze dirette presso grandi organizzazioni nel settore ICT, ha sviluppato un approccio basato sull'integrazione delle competenze di un team multidisciplinare che garantisce ai propri clienti analisi complete ed accurate dei rischi in atto e delle relative contromisure.

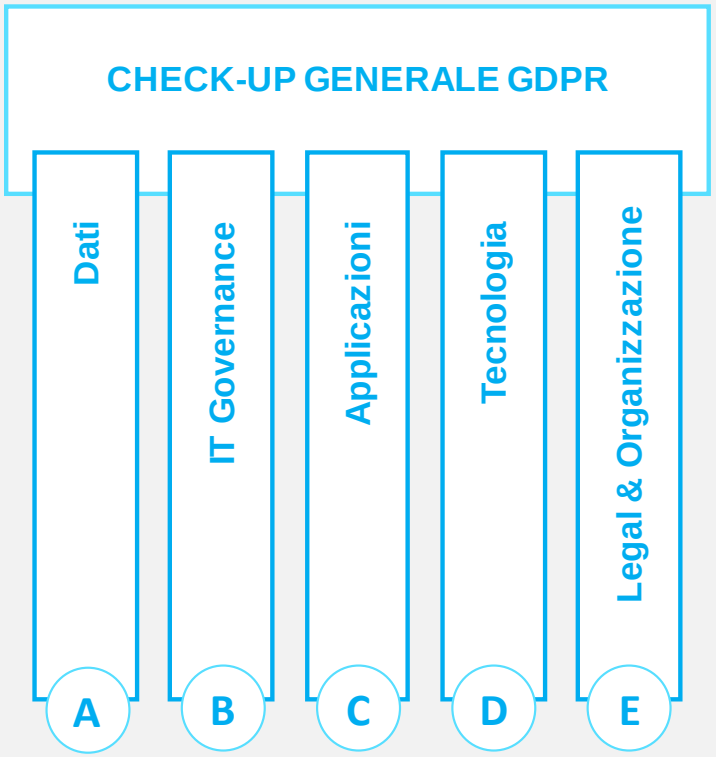
La metodologia Mosys

La metodologia integrata Mosys è strutturata in 6 moduli, applicabili anche separatamente, che consentono di supportare organizzazioni pubbliche e private nelle fasi di assessment della compliance GDPR e nelle attività di gestione delle azioni di remediation, operando su processi ed organizzazione aziendale, asset ICT, processi ICT ed aspetti legali.

L'approccio è caratterizzato da:

- Analisi estesa a tutta l'organizzazione mediante un **check-up iniziale;**
- Esame di tutte le aree di rischio interessate: **aspetti legali ed organizzativi, dati, applicazioni, tecnologia, processi di governo IT;**
- Approccio **flessibile**, **modulare** e **scalabile** in funzione della complessità e del contesto delle organizzazioni;
- Approccio «**risk-based**», che consente la predisposizione di piani di remediation orientati al **rapporto costi/benefici** per il cliente.

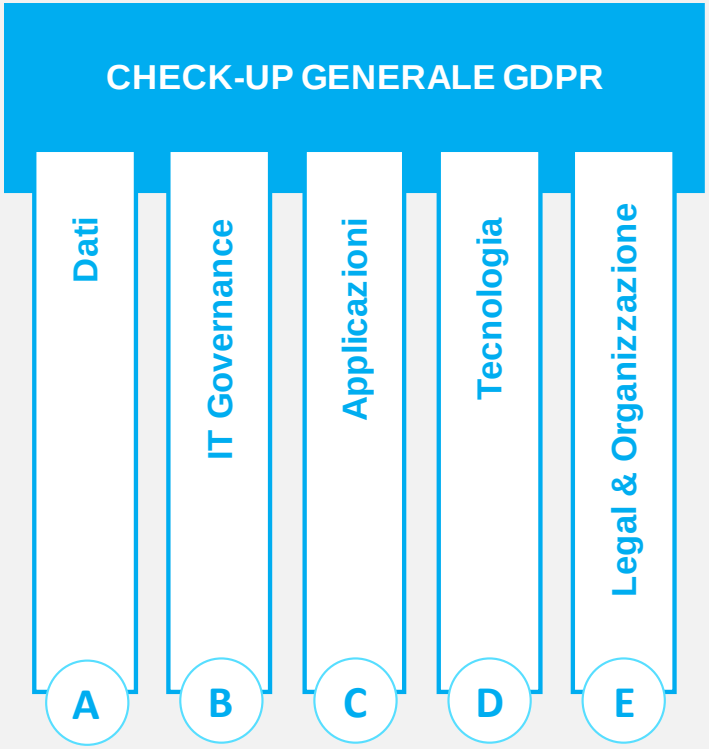
Ogni modulo comprende fasi di risk assessment, fasi di definizione di piani di remediation e fasi di esecuzione di interventi specialistici.



Check-up generale GDPR

Il check-up consiste in un assessment rapido ed esteso a tutta l'organizzazione per individuare le principali aree di rischio GDPR, articolate sulle 5 aree specifiche: Rischio Dati, Rischio IT Governance, Rischio Applicazioni, Rischio Tecnologia, Rischio Organizzazione.

L'assessment è condotto in modo strutturato da un team multidisciplinare con l'ausilio di un repository di riferimento della conoscenza in ambito GDPR.
I risultati del check-up indirizzeranno la «**Road-map**» degli interventi, i quali saranno rivolti non solo alla compliance GDPR, ma anche a massimizzare il rapporto tra i benefici conseguiti ed i costi delle azioni di remediation, considerando le strategie di business dell'organizzazione.
La Road-map potrà prevedere fasi di approfondimento dell'analisi di eventuali aree particolarmente rischiose o la messa in opera di azioni migliorative specifiche attivando altri specifici moduli della metodologia.

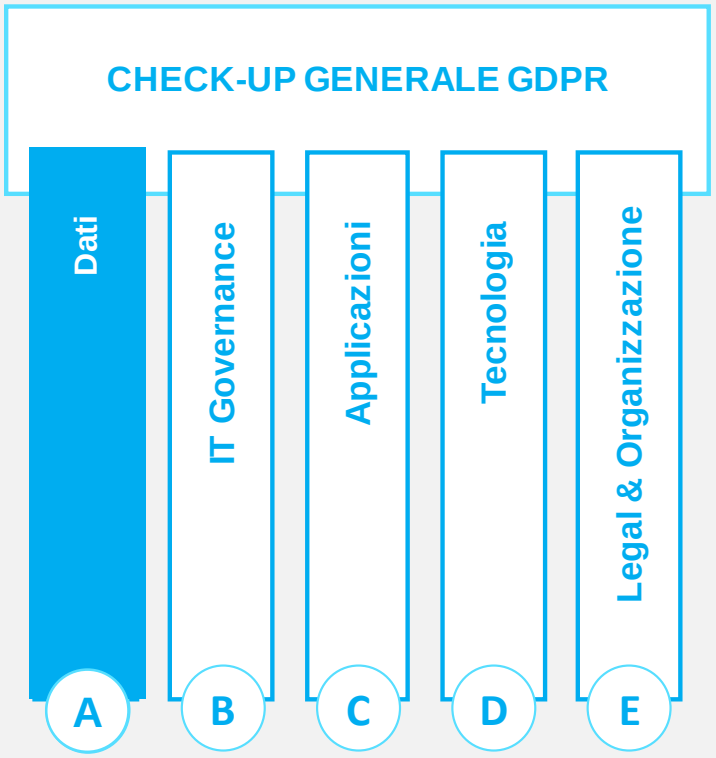


Area Dati

Le organizzazioni devono dimostrare di gestire i dati acquisiti da clienti, personale altre aziende, in modo appropriato, avendo il controllo completo dei flussi procedurali che, dalla loro acquisizione, li portano all'interno dell'organizzazione e dei processi aziendali, nei repository del sistema informativo, a terze parti autorizzate. In questo modulo viene effettuata una analisi approfondita delle modalità di gestione dei dati, mediante un assessment dettagliato delle modalità di gestione dei dati in tutte le aree aziendali rilevanti e la stima del relativo rischio in relazione alle prescrizioni GDPR quali «Diritto all'oblio», «Diritto di accesso» e «Portabilità dei Dati».

Il Piano di Remediation potrà prevedere:

- l'identificazione dei dati ed il loro tracciamento in un «**Inventario Dati**», anche mediante attività di «**Data Discovery**» dettagliate;
- il miglioramento o la predisposizione del **Registro Trattamento Dati**;
- la ridefinizione dell'**architettura di gestione dei dati** per favorire la loro gestione in ottica GDPR (dati pseudo-anonimi, funzioni di cancellazione dati…).



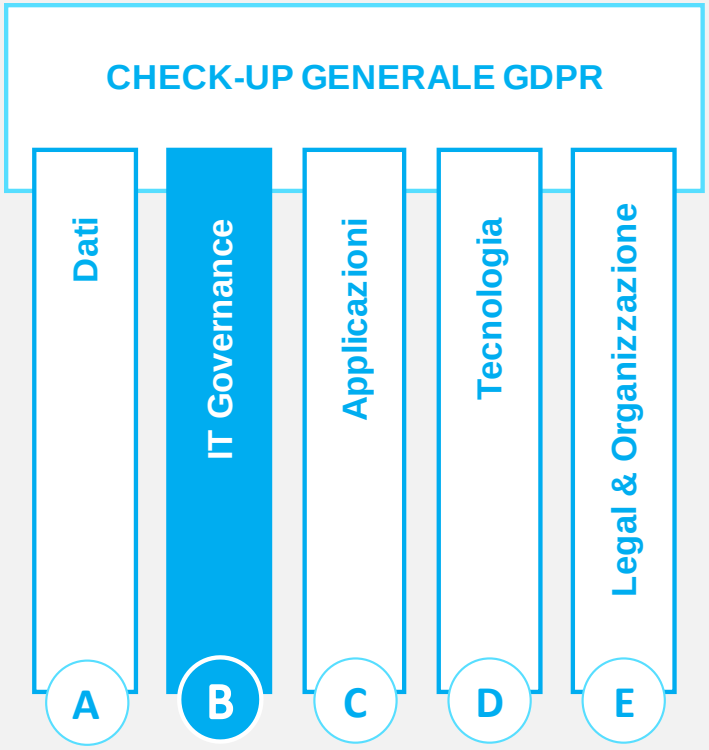
Area IT Governance

In questo modulo vengono analizzati i processi di governo delle fasi di sviluppo e gestione dei sistemi informativi da parte dell'Organizzazione, i quali sono essenziali per garantire requisiti GDPR quali la «data protection by design e by default» e, in generale, l'adeguatezza degli asset ICT.

Le attività prevedono un risk assessment per valutare i rischi dovuti ad inadeguatezze dei processi ICT che comprendono:

- la verifica dell'applicazione dei **processi di enforcement delle policy** relative al GDPR e dei processi operativi di attuazione (rispetto di procedure interne e linee guida per acquisto/sviluppo applicazioni e tecnologia, gestione in esercizio…);
- la verifica delle **misure di controllo per gli outsourcer** e i fornitori critici (adeguatezza contratti, analisi delle attività svolte…).

Il Piano di Remediation tipicamente prevede azioni volte a migliorare processi e procedure di gestione IT, orientandoli all'applicazione delle policy GDPR.



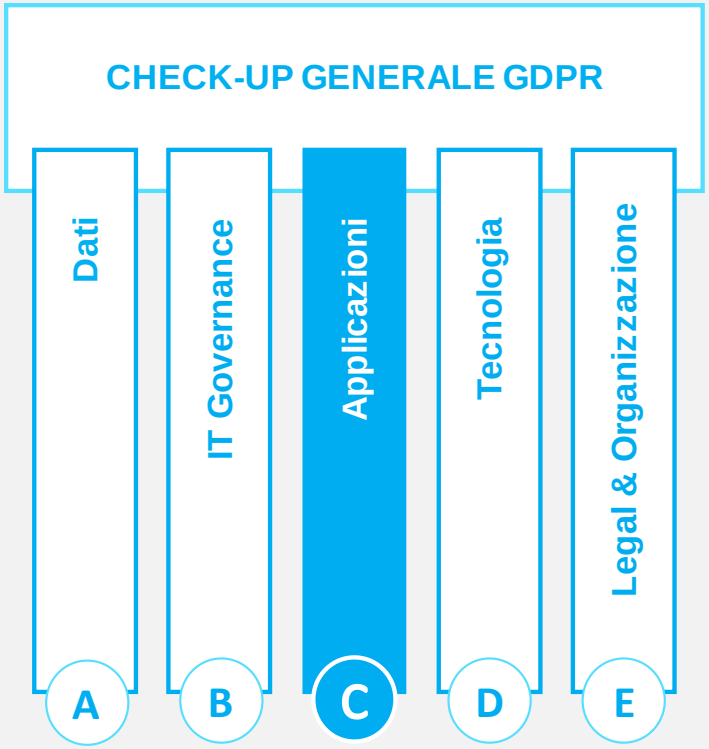
Area Applicazioni

Questo modulo vengono analizzate le applicazioni coinvolte nel processo di trattamento dei dati sensibili per verificare la loro adeguatezza in relazione a requisiti GDPR quali la «data protection by design e by default», e la loro robustezza in relazione alla «protezione dei dati trattati» in termini di riservatezza, integrità, disponibilità.

Le attività prevedono un risk assessment per valutare i rischi dovuti ad inadeguatezze delle applicazioni che comprendono:

- **analisi del patrimonio applicativo** e mappatura in relazione al rischio GDPR;
- analisi sulla **robustezza delle applicazioni** mediante **Penetration Test** e **Vulnerability assessment**;
- **analisi del codice**.

Il Piano di Remediation prevede l'individuazione degli interventi di adeguamento (Portfolio degli interventi di adeguamento applicativo) facendo riferimento ad un approccio di ottimizzazione del rapporto costi/benefici complessivo.



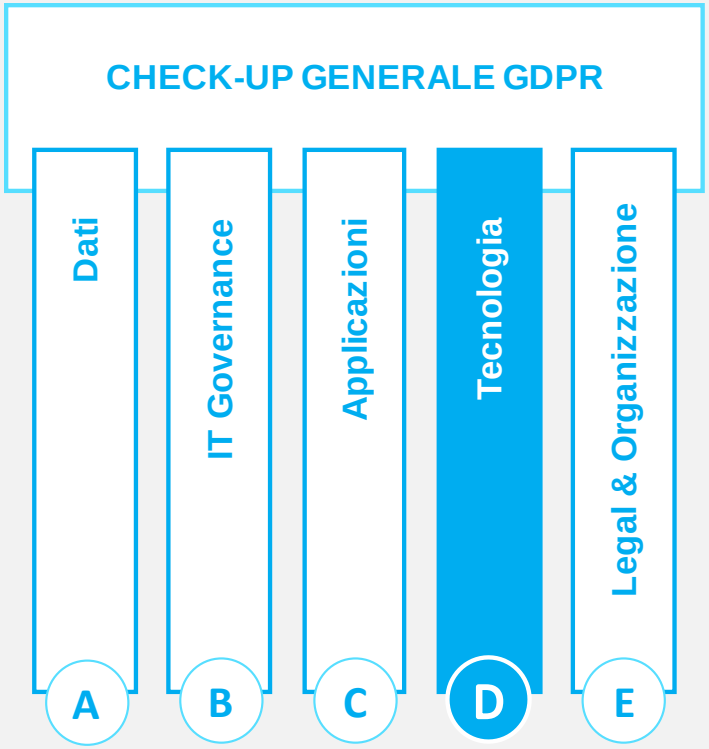
Area Tecnologia

In questo modulo vengono analizzati gli aspetti legati alla tecnologia per verificare la loro adeguatezza in relazione a requisiti GDPR quali la «data protection by design e by default», e la «protezione dei dati trattati» in termini di riservatezza, integrità, disponibilità e resilienza.

Le attività prevedono un risk assessment per valutare i rischi dovuti ad inadeguatezze della tecnologia che comprendono:

- la verifica della **protezione logica** delle risorse informatiche (policy di profilazione degli utenti, prodotti antimalware, sistemi di criptatura, network management,…);
- la verifica delle modalità di **continuità operativa** e di gestione degli incidenti;
- la verifica della **protezione fisica** dei locali critici e delle infrastrutture critiche.

Il Piano di Remediation prevede l'individuazione degli interventi di adeguamento (Portfolio degli interventi di adeguamento tecnologico) facendo riferimento ad un approccio di ottimizzazione del rapporto costi/benefici complessivo.

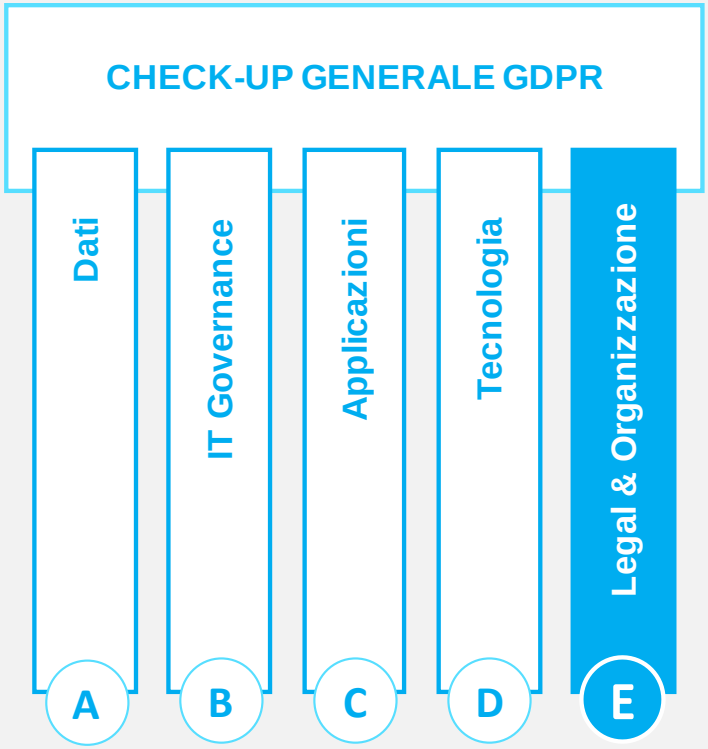


Area Legal & Organizzazione

In questo modulo vengono analizzati gli aspetti legati alla compliance in relazione a requisiti GDPR e vengono valutati i potenziali impatti, anche in termini economici, in caso di non conformità: gli impatti saranno stimati con il supporto di esperti legali in grado di valutare gli impatti effettivi, anche in relazione allo stato della giurisprudenza in materia.

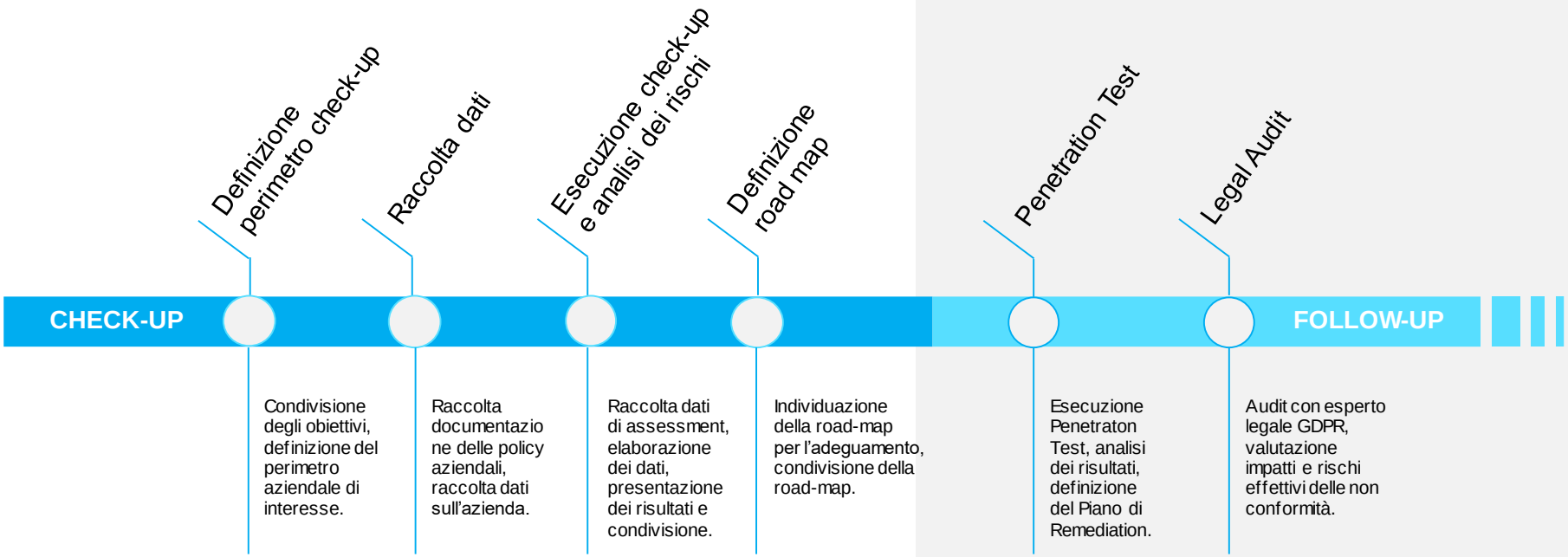
Le attività prevedono un risk assessment per valutare i rischi dovuti a non conformità che comprendono:

- verifica della compliance rispetto alla accountability di titolari e responsabili del trattamento, agli obblighi di Trasparenza e Diritti degli interessati, alla nomina RPD, DPO, alla adozione degli strumenti indicati dalla norma (Registro Trattamento Dati…);
- verifica delle policy aziendali e delle procedure attuative in relazione a GDPR, sicurezza, privacy;
- verifica delle procedure di gestione del personale (criteri di assunzione per i ruoli critici, Formazione e training, vincoli di sicurezza e riservatezza imposti dall'azienda a dipendenti e collaboratori…).



Una possibile Road-map

Per l'esecuzione delle attività di verifica della compliance GDPR verrà condotto un processo strutturato caratterizzato dalla fase di check-up sul perimetro di interesse e, se necessario, da un follow-up di approfondimento sugli aspetti legati ai rischi e relativi impatti sulle aree critiche messe in evidenza.

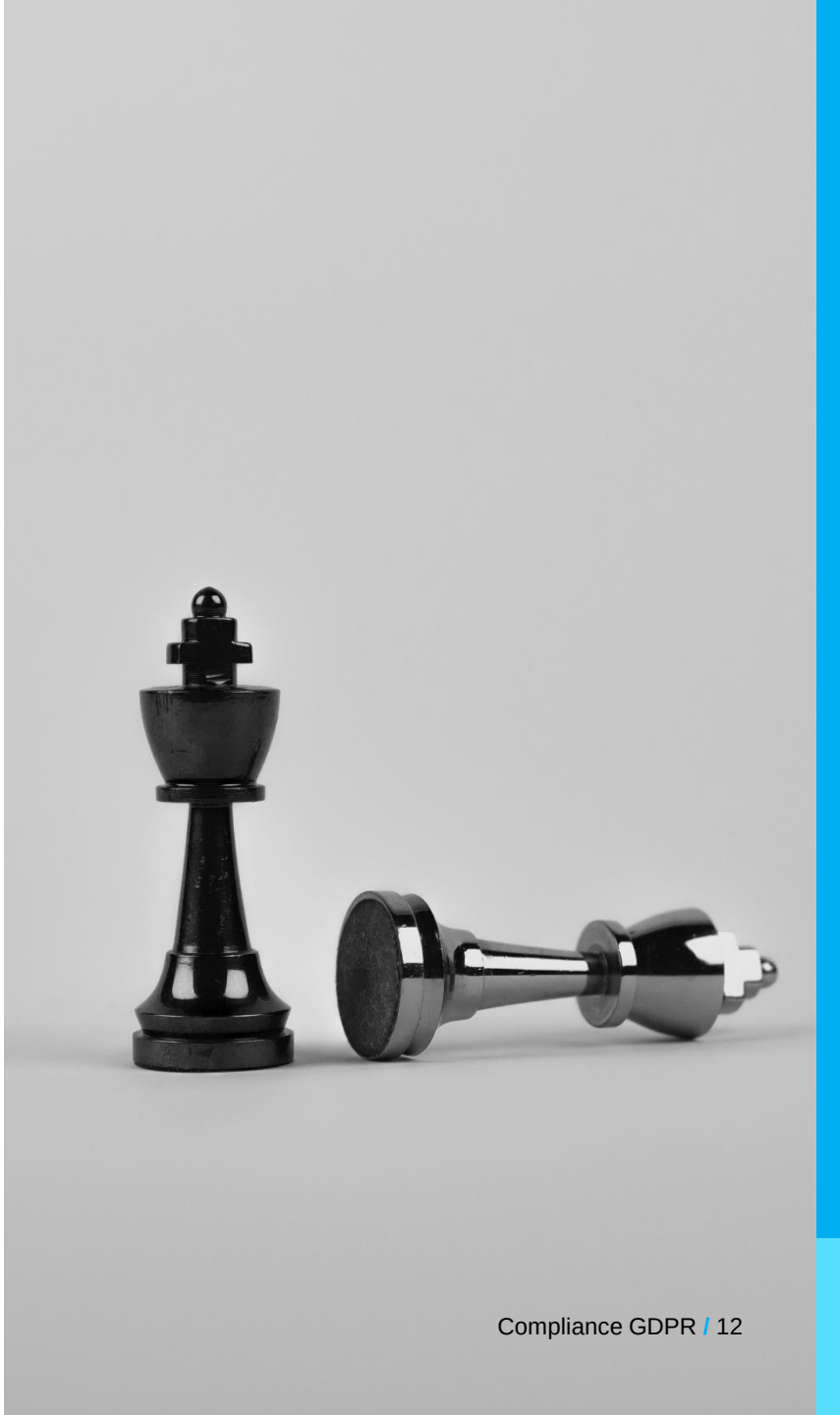


Il Team

Per il conseguimento degli obiettivi indicati nell'approccio proposto, Mosys metterà a disposizione un Team multidisciplinare costituito da:

- esperti della norma GDPR e delle normative collegate, quali ISO 27000, 231, ecc.
- esperti applicativi
- esperti di infrastrutture
- esperti di IT governance
- esperti legali

I componenti del Team sono in possesso di una lunga e consolidata esperienza in attività di auditing di sicurezza delle informazioni, privacy, compliance 231, sistemi informativi ed organizzazione aziendale, maturata in attività di supporto per organizzazioni pubbliche e private di grande rilievo.



Mosys Consulting srl
Società di consulenza indipendente

Piazza Albania, 10
00153 Roma, Italia

+39 06 5655 7949
info@mosysconsulting.it

Cecilia & Partners
Società di consulenza indipendente

Via Barnaba Tortolini 29
00197 Roma, Italia

+39 06 86210647
+39 347 7055074
info@ceciliaepartners.it