Mosys consulting

C&P Cecilia & Partners

GDPR: una soluzione completa ed integrata a misura per le aziende

febbraio 2018

Sommario

1. Mosys
2. Il nuovo regolamento GDPR
3. Metodologia generale MOSYS
4. Approccio proposto
5. Il Team

Mosys

Mosys Consulting opera nel settore della consulenza ICT di alto livello dal 2010, supportando Clienti pubblici e privati negli ambiti della Governance ICT.

Il Team di Mosys è composto da esperti provenienti dai settori della consulenza, della ricerca e dei servizi ICT, che integrano le loro esperienze specifiche per definire approcci che coniugano il rigore metodologico con la pragmaticità della loro applicazione.

Mosys affianca le organizzazioni orientando la relazione verso rapporti di partnership, fornendo un supporto integrato e un «front-end» unico per la risoluzione di problemi complessi.

Mosys opera nel settore della compliance integrando le esperienze di un network di imprese altamente specializzate su aree specifiche, quali la compliance alla norma GDPR, armonizzando le approfondite esperienze specifiche in un contesto metodologico omogeneo ed efficace.


IL NUOVO REGOLAMENTO
GDPR

Introduzione

Il Regolamento (UE) 679/2016 è entrato in vigore il 24 maggio 2016 e sarà direttamente applicabile in tutti gli Stati Membri dell'Unione Europea a partire dal 25 maggio 2018.

Il percorso per il recepimento delle disposizioni del GDPR presenta molte sfide e sottopone le organizzazioni a numerosi rischi, sia in relazione alle multe potenziali erogabili a fronte della non compliance GDPR (fino al 4% del fatturato annuale globale o fino 20 milioni di Euro ovvero, in certi casi, addiritttura la sospensione del trattamento e del relativo servizio connesso), sia in relazione ai costi di adeguamento, potenzialmente molto elevati.

Per l'ottimizzazione dei costi di adeguamento a fronte dei rischi rilevati è necessario estendere le analisi all'intera organizzazione, evitando di intraprendere piani di remediation solo in riferimento ad alcuni dei «silos» aziendali, e considerare tutti gli aspetti coinvolti dalla normativa GDPR, che comprendono aspetti legali, aspetti di organizzazione e processi di business, nonché la gestione ICT, in termini di asset e processi di governo.

L'approccio di Mosys e dei suoi partner all'adeguamento GDPR considera non solamente l'aspetto della compliance, ma affronta in modo sistemico tutti gli aspetti in ottica di «*Enterprise Risk Management*», consentendo alle organizzazioni di massimizzare i benefici dei piani di adeguamento in relazione alla loro strategia di business.

Descrizione generale GDPR – Oggetto e Finalità – art.1

1. Il regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati allo scopo di protegge i diritti e le libertà fondamentali delle persone fisiche.

Il Regolamento (UE) 679/2016 è entrato in vigore il 24 maggio 2016 e sarà direttamente applicabile in tutti gli Stati Membri dell'Unione Europea a partire dal 25 maggio 2018.

Descrizione generale GDPR – Definizioni – art. 2

1. «**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.

2. «**Trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

3. «**Titolare del trattamento**»: il Titolare del trattamento (*data controller*) è colui che "da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali" e decide quali categorie di dati personali devono essere registrate. Il Titolare decide il motivo e le modalità del trattamento, ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa. Nel settore privato il titolare del trattamento può essere una persona fisica oppure una persona giuridica. Nel settore pubblico in genere il titolare del trattamento è una persona giuridica.

4. «**Responsabile del trattamento**»: Il responsabile del trattamento (*data processor*) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento. Il responsabile è, quindi, colui che deve attenersi alle istruzioni del titolare.

Descrizione generale GDPR – Trattamenti particolari – artt.9,**10**

1. È vietato (a meno di specifiche condizioni normate dall'art.9) trattare dati personali che rivelino **l'origine razziale o etnica**, le **opinioni politiche**, le **convinzioni religiose o filosofiche**, o l'**appartenenza sindacale**, nonché trattare **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.

2. Il trattamento dei dati personali relativi alle **condanne penali** e ai **reati** o a **connesse misure di sicurezza**, deve avvenire soltanto sotto il controllo dell'autorità pubblica o, se il trattamento è autorizzato, dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

GDPR - Sintesi dei principali requisiti

1. **Accountability di titolari e responsabili del trattamento (approccio Risk based):** Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull' adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

2. **Obblighi di Trasparenza e Diritti degli interessati:** Il principio di trasparenza nei confronti degli interessati assume un ruolo di assoluta rilevanza nel GDPR ed è un elemento necessario e imprescindibile per convalidare tutti quei trattamenti che vedono come propria base di legittimità il **consenso informato** e consente all'interessato di avere, in ogni momento, il **controllo dei propri dati**.

3. **Nomina Titolare, Responsabile del trattamento e Responsabile Protezione Dati (RPD - DPO):** Il regolamento definisce caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento ed introduce come obbligatoria (nell'ambito di determinate attività) la figura del **Data Protection Officer** (DPO) o **Responsabile della protezione dei dati** (RPD). Il DPO informa il Titolare sugli obblighi del Regolamento e ne verifica l'attuazione. La figura è obbligatoria per le PA e per le imprese private rientranti in casistiche specifiche (quando le attività core business del Titolare o del Responsabile richiedono il monitoraggio degli interessati).

4. **Regole per Trasferimenti di dati verso Paesi terzi e organismi internazionali**: Il regolamento stabilisce le modalità, i requisiti, le clausole contrattuali per la garanzia del Trattamenti dei dati personali in caso di Trasferimenti di dati verso Paesi terzi e organismi internazionali.

Accountability di titolari e responsabili del trattamento (approccio Risk based)

1. **Responsabilizzazione:** Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull' adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (**artt. 23-25** e l'intero Capo IV del regolamento).

2. **Misure minime di sicurezza:** Non esiste un elenco tassativo di misure minime da adottare. Il Titolare è chiamato ad implementare misure adeguate a seguito della **valutazione del contesto e delle specifiche circostanze relative al trattamento**.

Il principio di «**responsabilizzazione**» del Titolare si traduce nell'adozione di comportamenti proattivi, specificati anche da alcuni specifici «**criteri**» dal Regolamento, tali da dimostrare la concreta attuazione di misure volte ad assicurare l'applicazione del Regolamento e i diritti dell'interessato.

Accountability – Criteri Specifici

1. **Data protection by default and by design: s**i tratta della necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Ciò deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio (**art. 25**) e richiede, pertanto, un'analisi preventiva e un impegno documentato da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

2. **Valutazione d'impatto sulla protezione dei dati (DPIA) e consultazione preventiva :** ogniqualvolta ci siano cambiamenti significativi del sistema (tecnologici, applicativi o nuove modalità di trattamento) è necessaria una valutazione del **rischio di impatti negativi sulle libertà e i diritti degli interessati** che tali cambiamenti inducono. Tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (**artt. 35 , 36**).

Accountability – Registro dei Trattamenti

1. **Registro dei Trattamenti (RT):** Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti (ma solo se non effettuano trattamenti a rischio) devono tenere un **registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30**. Si tratta di uno strumento fondamentale che ha lo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

2. **Alcuni contenuti del RT:** dati di contatto del **Titolare**, dell'eventuale **Contitolare**, del **Rappresentante** del Titolare, del **DPO**; **finalità del trattamento**; **categorie di interessati**; **categorie di dati personali** trattati; **categorie di destinatari** cui i dati personali saranno comunicati; termini previsti per la **cancellazione** dei dati personali per ogni categoria; descrizione ed evidenze **delle misure di sicurezza tecniche ed organizzative** previste ed attuate;

Accountability – Misure di Sicurezza

1. **Ampiezza e profondità delle misure di sicurezza: l**e misure di sicurezza devono "**garantire un livello di sicurezza adeguato al rischio**" del trattamento individuato dal Titolare (**art. 32**). Non esistono obblighi generalizzati di adozione di misure "minime" di sicurezza ne liste esaustive di misure prescritte. La responsabilità è lasciata in capo al Titolare secondo una propria valutazione del rischio.

2. **Alcuni misure di sicurezza indicate dal Regolamento (Art. 32 paragrafo 1):**
    1. pseudonimizzazione e la cifratura dei dati personali,
    2. capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento ,
    3. capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico,
    4. procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Accountability – Notifica delle violazioni

1. **Modalità e prescrizioni:** i titolari del trattamento devono notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo" ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Se la valutazione del rischio sui diritti degli interessati lo richiede , il Titolare deve informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo". Tutti i titolari di trattamento **dovranno in ogni caso documentare** le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (**art. 33**).

2. **Contenuti della notifica**: i contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento.

Obblighi di Trasparenza e Diritti degli interessati

1. **Trasparenza**: il principio di trasparenza nei confronti degli interessati assume un ruolo di assoluta rilevanza nel GDPR; solo attraverso un'informazione completa e trasparente è possibile creare una reale e piena consapevolezza degli interessati circa il trattamento dei loro dati personali.

2. Il principio di **Trasparenza** si manifesta:
   1. **prima del trattamento,** tramite l'informativa e la raccolta del consenso: Il Titolare del trattamento deve fornire agli interessati un'informativa adeguata, rispettando gli «**obblighi di contenuti**» e «**obblighi di forma**» (**artt. 13, 14**). Il consenso, nella maggior parte dei casi, deve essere "esplicito", anche per trattamenti automatizzati (compresa la profilazione – rif. **artt. 7, 22**). In tutti i casi, deve essere libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).
   2. **durante il trattamento**: Il titolare del trattamento deve fornire all'interessato tutte le azioni e le informazioni da questo richieste nell'esercizio dei propri diritti (**diritto di accesso, oblio, limitazione, portabilità**…).

Diritti degli interessati

1. **Diritto di accesso (art.15)**: l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali (diritto di ricevere **una copia** dei dati personali oggetto di trattamento).

2. **Diritto di cancellazione (art.17)**: Il diritto cosiddetto "**all'oblio**" si configura come un **diritto alla cancellazione dei propri dati personali** in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato, ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati.

3. **Diritto di limitazione del trattamento (art.18)**: si tratta del diritto dell'interessato ad **opporsi al trattamento dei propri dati personali**, quando ad esempio ne contesta l'esattezza o anche in forma transitoria (ad es. se l'interessato chiede la rettifica dei dati, in attesa di tale rettifica da parte del titolare).

4. **Diritto alla portabilità (art.20)**: Si tratta di uno dei nuovi diritti previsti dal regolamento, simile per analogia al diritto alla portabilità del numero telefonico di un individuo. Permette all'interessato di ottenere i propri dati personali in un formato compatibile con le applicazioni standard, per permetterne il trasferimento su altre piattaforme di propria scelta.

Nomina Titolare, Responsabile del trattamento e Responsabile Protezione Dati (RPD - DPO)

1. **Titolare e Responsabile**: il regolamento definisce le **caratteristiche soggettive e le responsabilità di titolare** e **responsabile del trattamento** negli stessi termini di cui alla direttiva 95/46/CE e, quindi, al Codice italiano attualmente in vigore d.lgs. 196/2003. Il regolamento disciplina anche la «**contitolarità**» del trattamento, permettendo di definire (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati.

2. **Responsabile della protezione dei dati (DPO):** Il regolamento ha introdotto come obbligatoria (nell'ambito di determinate attività, rif. **art. 37**) la figura del **Data Protection Officer** (**DPO**) o **Responsabile della protezione dei dati (RDP)** e ne tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali, rif. **art. 38 e 39**) . Il DPO è obbligatorio nei casi (**art.37**):
    1. autorità o organismi pubblici,
    2. monitoraggio regolare e sistematico di interessati su larga scala,
    3. trattamento su larga scala di dati sensibili e giudiziari.

Regole per Trasferimenti di dati verso Paesi terzi e organismi internazionali

1. **Regole per il Trasferimento**: Il regolamento stabilisce le modalità, i requisiti, le **clausole contrattuali** per la garanzia dei Trattamenti dei dati personali in caso di Trasferimenti di dati verso Paesi terzi e organismi internazionali, annullando il requisito dell'autorizzazione nazionale precedentemente previsto con il d.lgs. 196/2003. Tuttavia, l'autorizzazione del Garante è ancora necessaria se un titolare desidera utilizzare **clausole contrattuali ad-hoc** oppure **accordi amministrativi** stipulati tra autorità pubbliche.

2. Il regolamento consente di ricorrere anche a **codici di condotta ovvero a schemi di certificazione** per dimostrare il possesso da parte dei Terzi delle «garanzie adeguate» previste dall'**art. 46**.

3. Il regolamento (si veda Capo V) ha confermato l'approccio attualmente vigente in base alla direttiva 95/46 e al Codice italiano (d.lgs. 196/2003) per quanto riguarda i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo, **prevedendo che tali flussi sono vietati**, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca.

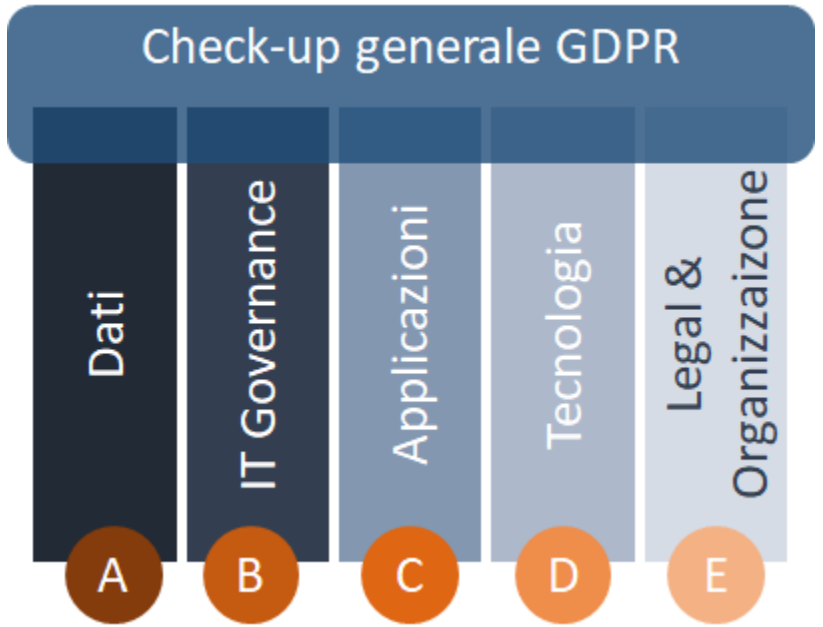

METODOLOGIA GENERALE
MOSYS

Metodologia generale 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.

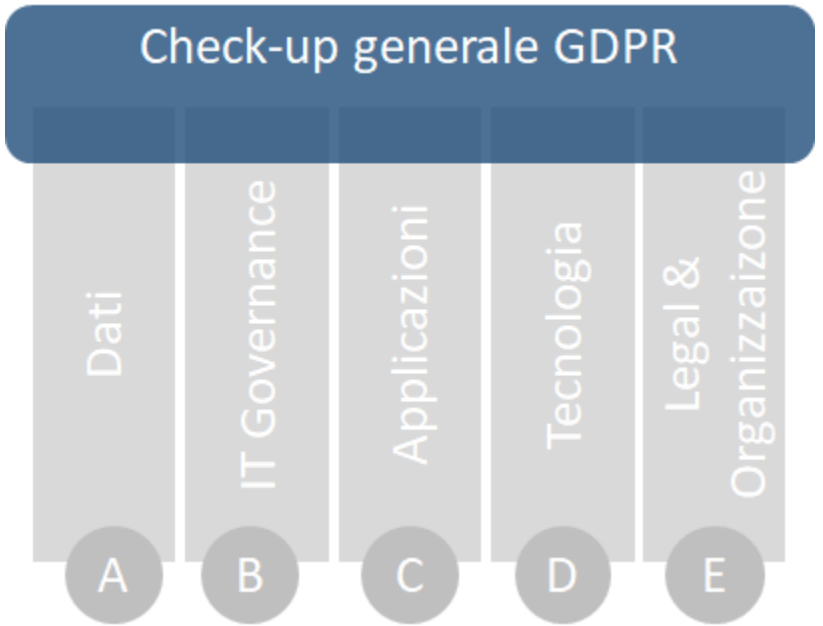
L'approccio è caratterizzato da:

- 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

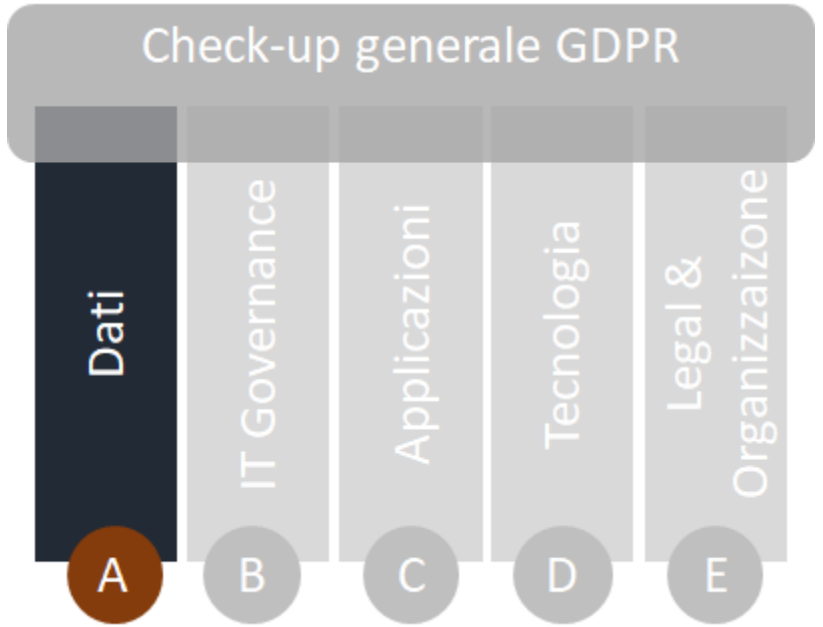
- Il check-up consiste in un assessment rapido ed esteso a tutta l'organizzazione per individuare le principali aree di rischio GDPR, articolate sulle 5 aree specifiche: Rischio Dati, Rischio IT Governance, Rischio Applicazioni, Rischio Tecnologia, Rischio Organizzazione.
- L'assessment è condotto in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

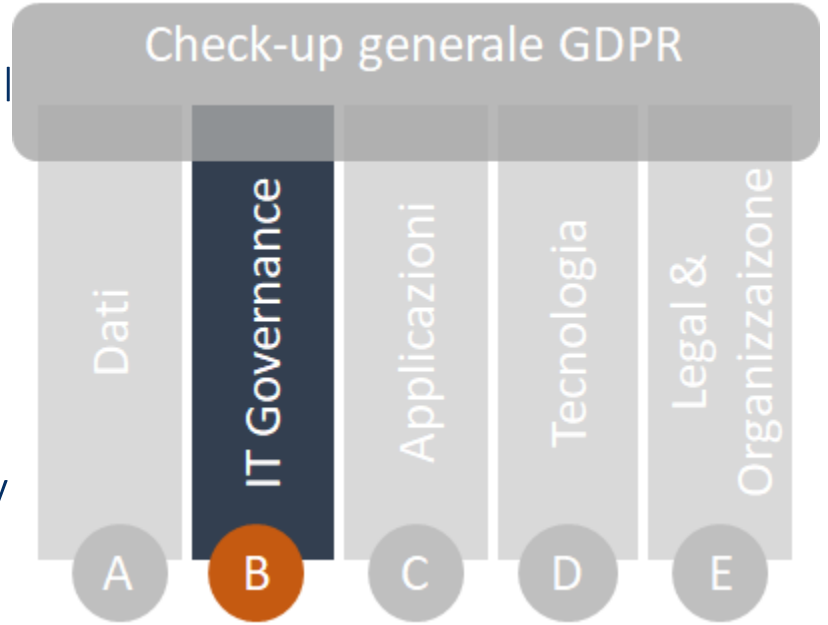
Area IT Governance

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 default e by design*» 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.



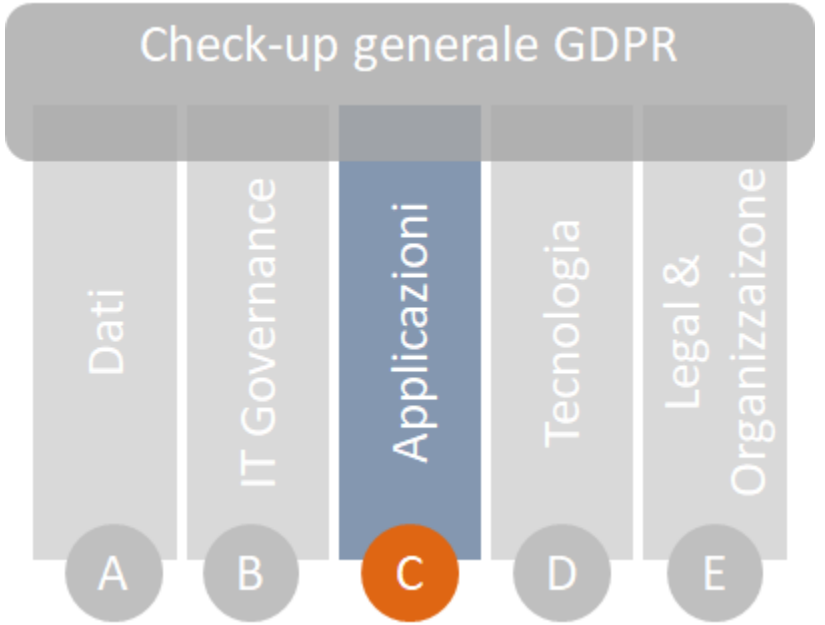
Area Applicazioni

In 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 default e by design*», 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.



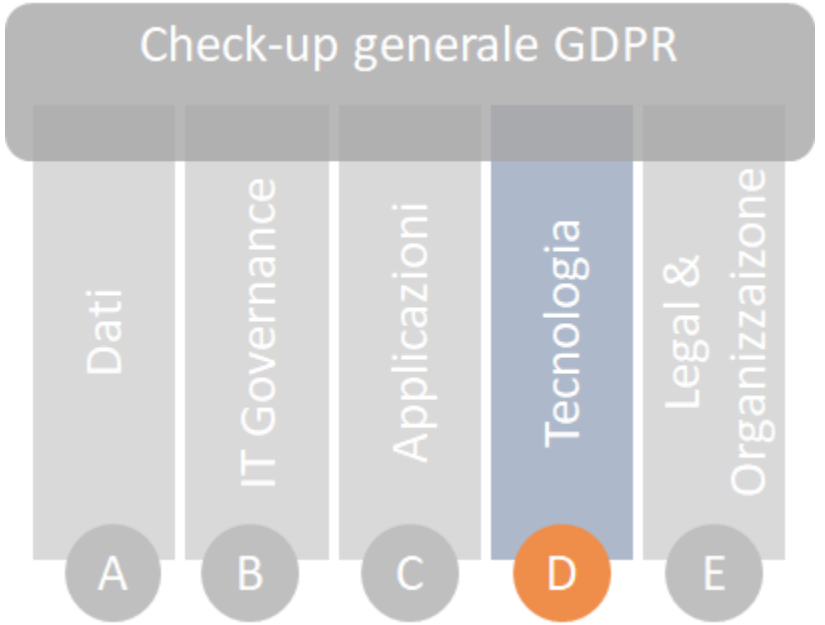
Area Tecnologia

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 default e by design*», 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.

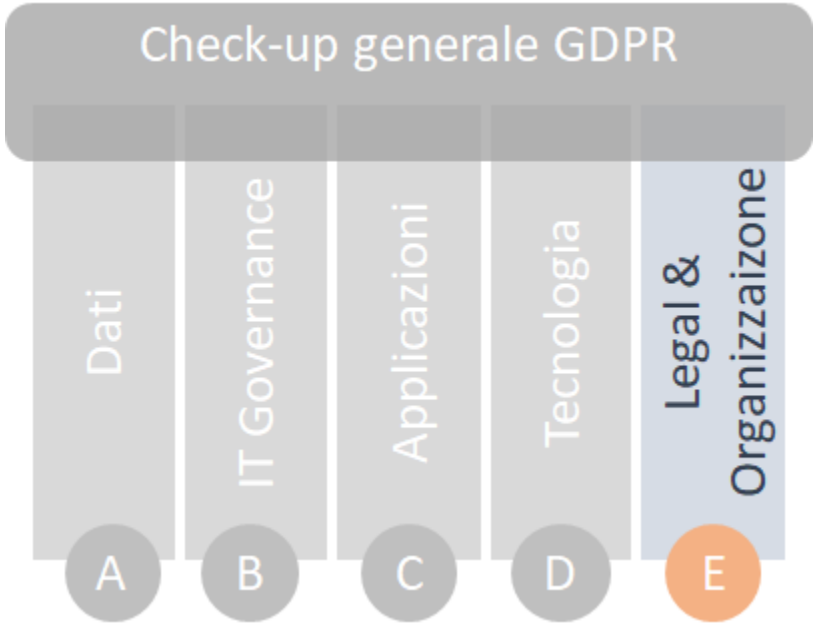


Area Legal & Organizzazione

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:

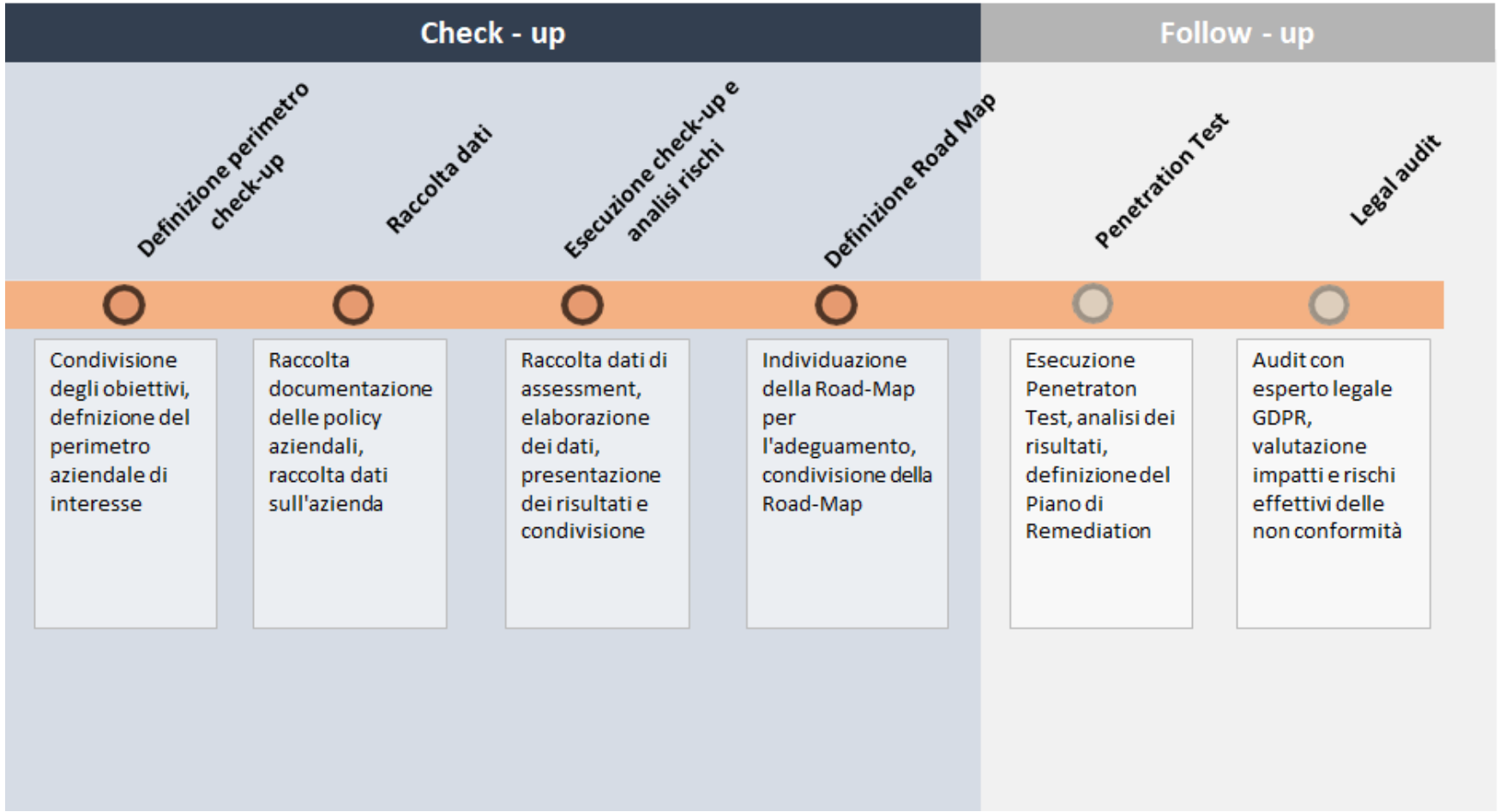
- verifica della compliance rispetto alla accountability di titolari e responsabili del trattamento, agli obblighi di Trasparenza e Diritti degli interessati, alla nomina RPD, DPO, alla adozione degli strumenti indicati dalla norma (Registro Trattamento Dati…);
- verifica delle policy aziendali e delle 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…).




APPROCCIO PROPOSTO

Approccio proposto

Per l'esecuzione delle attività verrà condotto un processo strutturato caratterizzato dalla fase di check-up e, se ritenuto necessario, da un follow-up di approfondimento sugli aspetti legati ai rischi applicativi e tecnologici e sugli impatti legali ad essi legati.



Definizione del perimetro del Check-up

I consulenti, di concerto con i responsabili aziendali, provvederanno a individuare ex ante il perimetro di analisi di interesse definendo:

- le finalità dell'intervento a seguito delle aspettative dell'Organizzazione;
- i processi principali da verificare e le aree aziendali coinvolte;
- le aree percepite come maggiormente critiche;
- le sedi da includere nel perimetro.

La fase verrà preceduta da un incontro formativo-informativo durante il quale saranno illustrati ai principali stakeholder aziendali i contenuti della norma GDPR, gli obiettivi dell'intervento e le modalità di effettuazione.

La collaborazione con tutto il personale coinvolto nelle attività e la corretta individuazione del perimetro di analisi favoriscono il raggiungimento degli obiettivi di massimizzazione del rapporto costi/benefici dell'intervento e delle successive azioni di remediation.

Raccolta dati

- **Analisi del contesto di business**. In questa fase sono raccolte informazioni sulla struttura dell'Azienda, sul suo organico, sulle principali aree di business, sugli obiettivi strategici a medio e breve termine e sulle principali criticità percepite.
- **Analisi delle policy aziendali.** In questa fase i consulenti verificheranno la presenza e l'adeguatezza di documenti e prassi aziendali di alto livello (Policy), e di livello operativo (procedure attuative, linee guida..) volte a definire gli obiettivi di sicurezza delle informazioni e di privacy perseguiti dall'Organizzazione e le principali risorse (*economiche, umane, tecnologiche*) messe a disposizione. Saranno oggetto di analisi:
  - la politica generale dell'Organizzazione;
  - le disposizioni aziendali inerenti la privacy e la sicurezza delle informazioni in genere;
  - le procedure e gli strumenti per l'Analisi del rischio.
- **Analisi del Sistema Informativo.** In questa fase saranno raccolte informazioni sul Sistema Informativo aziendale in termini di parco applicativo, infrastruttura tecnologica, processi e modalità per l'evoluzione e la gestione del Sistema (servizi e contratti acquisiti dall'esterno, servizi interni, contratti e fornitori...).

Esecuzione check-up e analisi dei rischi

In questa fase saranno effettuate le analisi di conformità e di rischio, articolate nelle 5 aree previste dalla metodologia GDPR Mosys, che comprendono:

- la 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 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*…);
- la verifica delle modalità di gestione dei dati sensibili secondo il modello GDPR (*modalità di trattamento, tracciamento, dislocazione dei dati nel sistema informativo*…);
- la verifica dell'applicazione dei processi di implementazione delle policy aziendali e di quelle relative al GDPR, con enfasi sui processi di IT governance (*verifica delle misure di controllo per gli outsourcer e i fornitori critici, adeguatezza contratti*, …);
- La ricognizione dello stato del patrimonio applicativo e della tecnologia in relazione ai rischi GDPR (…). *verifica della protezione fisica e logica delle risorse informatiche e dei locali, analisi delle modalità di assicurazione dei livelli di sicurezza e di robustezza delle applicazioni, gestione degli incidenti, modalità di recovery e di gestione della continuità operativa*

Nell'esecuzione delle attività saranno impiegati framework standard di riferimento integrati nel contesto GDPR, quali le linee guida sulla sicurezza fissate da standard internazionali come la **ISO 27002**, norme sulla compliance aziendali quali quelle relative al **D.Lgs. 231/2001**.

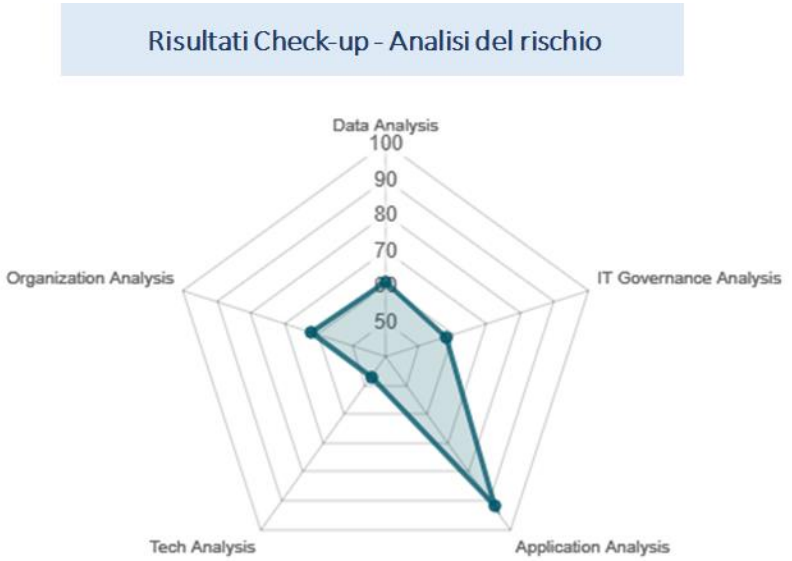
Analisi del rischio e definizione della Road-Map

L'analisi del rischio viene effettuata valutando, secondo metriche predefinite, il livello di criticità articolato nelle aree di indagine della metodologia.

Il livello di rischio delle specifiche aree sarà illustrato e motivato sulla base degli elementi raccolti e valutati, ed indirizzerà la definizione della Road-Map per l'adeguamento GDPR.

La **Road-Map**, tipicamente, considererà le principali milestone del percorso per la compliance GDPR, articolato in interventi quali:

- eventuali approfondimenti del check-up **iniziale mediante attività di penetration test, vulnerability** assessment e di **legal audit**;
- la predisposizione di un **inventario dati** e del **Registro dei Trattamenti;**
- l'analisi approfondita dello stato degli **asset informatici** e il loro adeguamento;
- l'analisi approfondita dei **processi di governo IT** ed il loro adeguamento.



Vulnerability Assessment & Penetration Test

In questa fase, attivata solamente se necessario (alti livello di rischio sugli asset tecnologici rilevato nella prima fase di Check-up), saranno individuate eventuali vulnerabilità sul perimetro degli asset tecnologici per migliorare la valutazione complessiva e definire una Road Map maggiormente adeguata.

Le attività di **Vulnerability Assessment (VA)** e di **Penetration Test (PT)** rientrano in quanto previsto dal GDPR in termini di *Accountability – Misure di Sicurezza*, ovvero nella dimostrazione della capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

Di seguito alcune caratteristiche delle attività:

- **Obiettivi**: individuazione sia delle vulnerabilità note, sia delle vulnerabilità pubbliche, verifica del livello di penetrabilità dei sistemi.
- **Target:** network, applicazioni WEB, applicazioni MOBILE.
- **Modalità:** manual activity, vulnerability scan, fuzzing.

In fase di Vulnerability Assessment (VA) saranno individuate le problematiche presenti, senza procedere allo sfruttamento pratico delle stesse, ma focalizzando le proprie attività esclusivamente su un primo livello di frontiera.

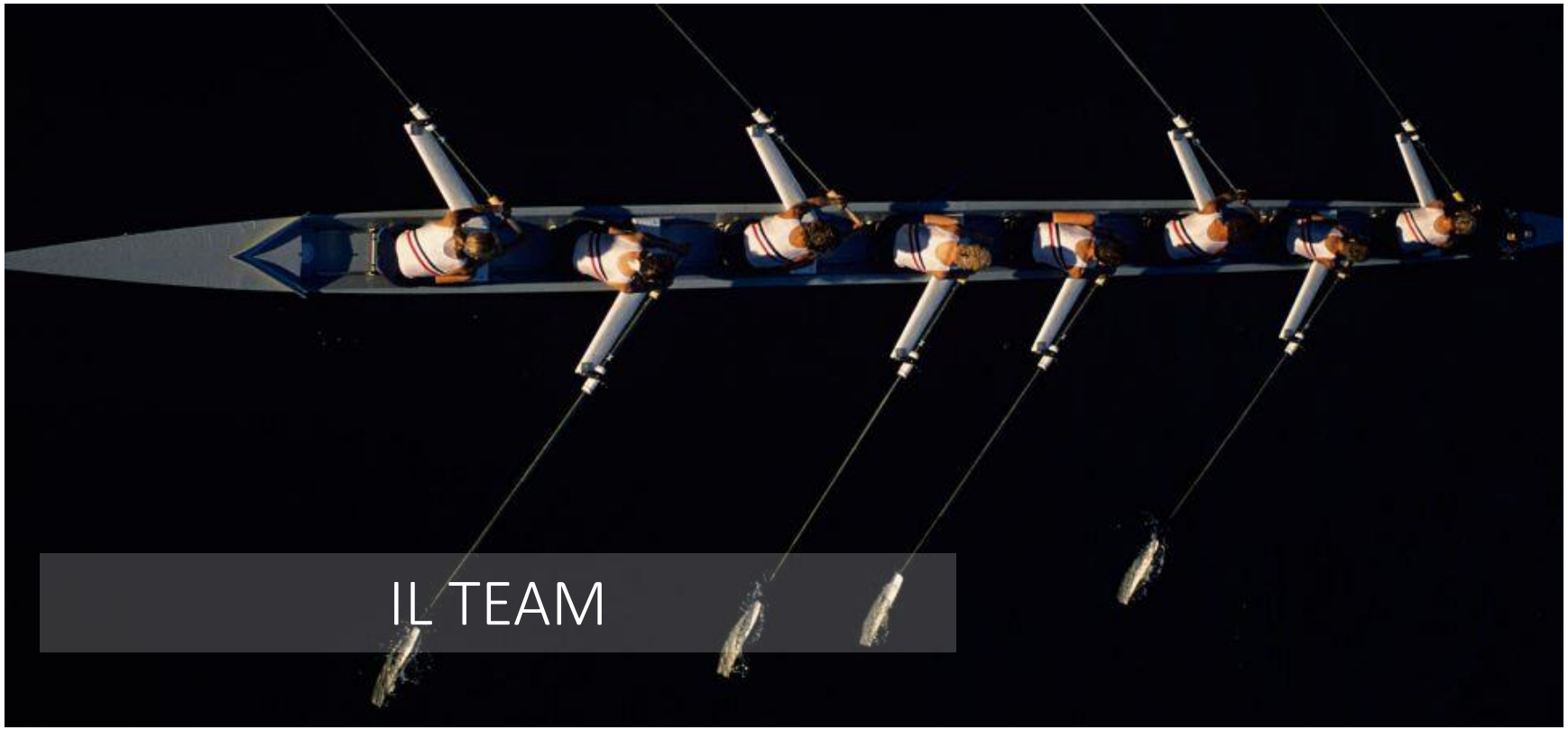
Le operazioni di Penetration Test (PT) rappresentano la parte più mirata e profonda della verifica delle vulnerabilità, e sono realizzate a valle della VA.

Le attività saranno svolte da un team di professionisti certificati **OSCP (Offensive Security Certified Professional)** e al termine delle stesse verrà rilasciata una certificazione per l'avvenuta esecuzione del VA e del PT per le risultanze rilevate.

Legal Audit

In questa fase, attivata solamente se necessario e di interesse per il Cliente, saranno valutate le non conformità rilevate in fase di check-up e, eventualmente, in fase di PT & VA, in termini di **impatti legali**.

La valutazione verrà effettuata mediante la consulenza di esperti legali nel contesto specifico GDPR i quali, sulla base dello stato attuale della normativa e delle linee guida attuative nazionali (*attualmente ancora in fase di predisposizione*) stimeranno gli effettivi rischi ed impatti, valutando concretamente la probabilità di applicazione di multe e sanzioni, anche in base alla giurisprudenza specifica.


IL TEAM

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

Contatti

Mosys Consulting S.r.l.
Via Iris Versari n.72
00128 Rome, Italy
tel.: +39 348 7304611
info@mosysconsulting.it
www.mosysconsulting.it