

# NETWORK DIGITAL 360

## E.GUIDE

È già in vigore, anche se entrerà a regime in tutta l'UE il 25 maggio 2018, il nuovo Regolamento Europeo per la protezione dei dati personali (GDPR). Cosa implica l'adeguamento al GDPR per aziende e organizzazioni pubbliche? Cosa cambia nella gestione della privacy degli utenti? Come fare a capire se il proprio impianto di sicurezza è conforme? In questo documento, realizzato dagli esperti legali di NetworkDigital360, indicazioni e consigli su come procedere per fare il corretto assessment

## COME ADEGUARSI AL GDPR: UN MODELLO DI ASSESSMENT

- Inquadramento alle nuove direttive del GDPR (General Data Protection Regulation)
- Come effettuare l'assessment: un piano di adeguamento in 6 fasi
- Auto-assessment, assessment online o partner esterni: qual è l'approccio migliore?
- Come vanno interpretati i risultati dell'assessment

IN COLLABORAZIONE CON

**FASTWEB**

# 1. GENERAL DATA PROTECTION REGULATION: DI CHE SI TRATTA

Il regolamento generale sulla protezione dei dati personali UE 2016/679 (in breve «GDPR»), già in vigore ma pienamente applicabile dal 25 maggio 2018, ha portato a un vero e proprio cambio di filosofia rispetto alla gestione dei dati. Il GDPR, infatti, abbandona un approccio marcatamente formalistico, basato su regole e adempimenti analiticamente definiti (ad esempio, l'elenco delle misure minime di sicurezza da adottare), per passare a un approccio che responsabilizza maggiormente il Titolare del Trattamento, lasciando allo stesso una maggiore libertà decisionale, seppur nel rispetto dei principi in esso definiti.

## IL TITOLARE DEL TRATTAMENTO: COSA CAMBIA

Il Titolare del Trattamento è chiamato a prendere una serie di decisioni in merito al proprio modello di protezione dei dati personali. Decisioni che hanno impatti significativi sull'operatività dell'organizzazione (ad esempio lo sviluppo di un nuovo prodotto o servizio, la selezione di un fornitore, la gestione delle richieste degli interessati e via dicendo), ma utili a dimostrare la conformità al GDPR del modello di data protection nell'ottica del principio della cosiddetta *accountability* (responsabilizzazione).

## L'IMPORTANZA DELL'ASSESSMENT

Non essendo la regolamentazione della protezione dei dati personali una novità assoluta nel



contesto giuridico dell'Unione Europea, diventa fondamentale per il Titolare del Trattamento effettuare un assessment efficace del modello di protezione dei dati personali già adottato, rilevando i disallineamenti rispetto alle numerose

novità introdotte dal GDPR (ad esempio Data Protection Officer, Registro dei trattamenti, Data Protection Impact Assessment) e studiando opportune contromisure da inserire all'interno di un piano di adeguamento completo e sostenibile.

## COSA RILEVARE NELL'ASSESSMENT: UN MODELLO A 6 COMPONENTI

È necessario focalizzare le attività di assessment sul modello di protezione dei dati personali attualmente adottato dal Titolare del Trattamento, ovvero sulle scelte effettuate dall'organizzazione per essere conforme alle normative vigenti in materia di protezione dei dati personali. Per facilitare la comprensione del modello, è opportuno scomporre lo stesso in 6 componenti che ruotano attorno al concetto centrale di **dato personale\***, la cui definizione è rimasta sostanzialmente invariata nel GDPR.



### \*Che cos'è un dato personale?

*S'intende come "dato personale" qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato») attraverso dati quali il nome, il cognome, un codice identificativo on line, dati relativi all'ubicazione nonché tutti i dati indicanti le sue caratteristiche fisiche, fisiologiche, genetiche, psichiche, economiche, culturali o sociali.*

## ASSESSMENT: QUALI SONO LE 6 COMPONENTI IN DETTAGLIO

**Analizziamo ciascun asse del modello di protezione dei dati personali, mettendo in evidenza i principali collegamenti al GDPR**

**1 ORGANIZZAZIONE E RUOLI:** comprende le strutture, i comitati e i ruoli adottati dall'organizzazione per indirizzare e governare, eseguire e controllare il modello di protezione dei dati personali. In particolare, il GDPR introduce il Data Protection Officer (DPO), figura avente compiti eterogenei, alcuni di natura ispettiva interna (sorvegliare), altri consulenziali (dare pareri), alcuni interni all'organizzazione del Titolare, altri esterni (rapporto con gli interessati e con l'autorità di controllo).

**2 PERSONE, CULTURA E COMPETENZE:** comprende il personale individuato dall'organizzazione (interno ed esterno) per ricoprire i ruoli previsti dal modello, ma anche le azioni messe in campo dalla stessa per sensibilizzare e formare opportunamente il personale. Nello specifico, il GDPR pone particolare attenzione ai requisiti che deve soddisfare la persona che ricoprirà il ruolo di DPO, tra cui assenza di conflitto di interessi e conoscenza specialistica di normativa e prassi in materia di protezione dei dati.

**3 PROCESSI E REGOLE:** comprende le norme di autoregolamentazione e le disposizioni interne di cui si è dotata l'organizzazione per essere conforme alla normativa. In particolare, il GDPR richiede di rivedere radicalmente il sistema di processi e regole dell'organizzazione, introducendo una serie di elementi che hanno impatti significativi sull'operatività della stessa, tra cui Data Protection by Design / Data Protection By Default, Data Protection Impact Assessment e violazioni di dati personali (data breach).

**4 DOCUMENTAZIONE:** comprende policy e procedure che formalizzano le norme di autoregolamentazione e le disposizioni interne di cui si è dotata l'organizzazione ma anche la documentazione utilizzata per l'implementazione delle stesse, quale ad esempio informative e consensi, contratti e lettere di nomina. In particolare, il GDPR introduce il registro dei trattamenti dei dati personali, la cui tenuta è in carico al Titolare del Trattamento e, se nominato, al Responsabile del trattamento, che consente di tenere traccia delle operazioni di trattamento effettuate all'interno dell'organizzazione.

**5 TECNOLOGIA E STRUMENTI:** comprende i sistemi informativi adottati per il trattamento dei dati personali, sia lato applicativi sia lato infrastrutture, e le relative misure di sicurezza predisposte dall'organizzazione. In particolare, il GDPR prevede l'adozione di misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio (es. la pseudonimizzazione e la cifratura dei dati personali), tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

**6 SISTEMA DI CONTROLLO:** comprende le azioni e gli strumenti messi in campo dall'organizzazione per verificare l'esistenza, l'adeguatezza e l'effettiva applicazione del modello di protezione dei dati personali, con riferimento a tutte le componenti sopra indicate. In particolare, il GDPR sottolinea l'importanza di dimostrare le scelte effettuate dall'organizzazione ("accountability"), motivo per il quale diventa fondamentale dimostrare l'effettuazione di controlli periodici, opportunamente documentati, e l'esistenza di piani di remediation a fronte di eventuali non conformità rilevate.

## 2. COME EFFETTUARE L'ASSESSMENT ATTRAVERSO UN PIANO DI ADEGUAMENTO IN SEI FASI

L'esecuzione di un assessment passa attraverso il completamento di 6 passi (step) in grado di portare l'organizzazione ad avere un

quadro chiaro delle azioni da implementare per essere conforme al GDPR, opportunamente inserite all'interno di un piano di adeguamento.

### I PRINCIPALI STEP DELL'ASSESSMENT



#### 1) IDENTIFICAZIONE, COMPrensIONE E CLASSIFICAZIONE DEI REQUISITI

Identificazione, comprensione e classificazione dei requisiti del GDPR in funzione degli assi del modello di protezione dei dati personali, mettendo in evidenza eventuali legami con normative settoriali (es. settore bancario - circolare n.285 del 17 dicembre 2013) e tenendo costantemente monitorata l'emanazione di nuove disposizioni e linee guida delle competenti Autorità nazionali ed europee (es. linee guida del Gruppo di lavoro ex articolo 29).

### Attenzione!

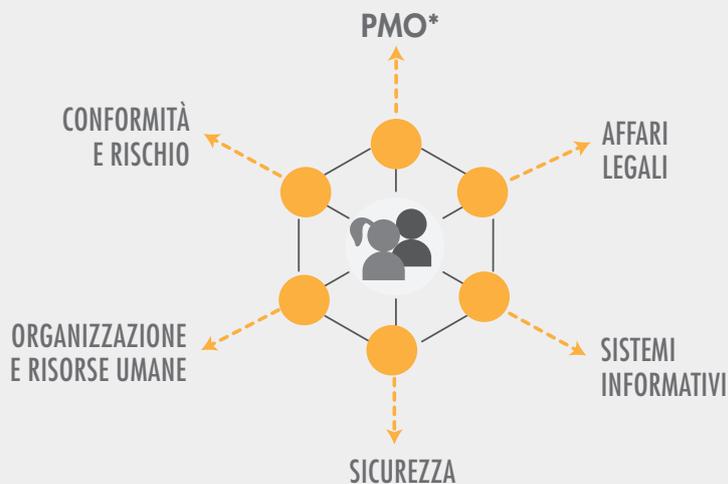
*Consigliamo di leggere attentamente gli articoli (e i considerando del GDPR) e, per ciascun articolo, mappare i requisiti in funzione degli assi del modello di protezione dei dati personali (ad esempio gli artt. 37,38,39 del GDPR relativi al DPO hanno impatti sugli assi "Organizzazione e ruoli" e "Persone, cultura e competenze; l'art. 30 del GDPR ha impatti sugli assi "Processi e regole" e "Documentazione")*

## 2) INDIVIDUAZIONE E INGAGGIO ATTORI AVENTI UN RUOLO “ATTIVO”

Individuazione e ingaggio di tutti gli attori, sia interni sia esterni, chiamati a ricoprire un ruolo «attivo» in fase di pianificazione, esecuzione e monitoraggio del percorso di adeguamento, ma anche nella gestione del modello di protezione dei dati personali a regime.

### Attenzione!

*Coinvolgere, fin da subito, uno o più referenti delle seguenti funzioni aventi il ruolo di indirizzo e governo del modello: Affari Legali, Sistemi Informativi, Sicurezza (Safety e Security), Organizzazione e Risorse Umane, Conformità e Rischio*



**\*Per garantire il governo delle attività e facilitare il commitment di tutti gli attori, è necessario individuare una figura, interna o esterna, che ricopra il ruolo di PMO (Project Management Officer)**

## 3) CREAZIONE E IMPLEMENTAZIONE DI UN MODELLO DI ANALISI

Creazione e implementazione di un modello di analisi per l'individuazione del livello di maturità dell'organizzazione in relazione al Regolamento. Le analisi svolte per classificare i requisiti del GDPR e il contributo dei referenti ingaggiati nell'assessment possono essere messi a sistema

al fine di generare un modello di rilevazione strutturato e completo (Data Protection Maturity Model), a garanzia della copertura delle aree funzionali maggiormente impattate dal Regolamento (ad esempio IT, Sicurezza) e dell'indirizzamento di tutti i requisiti (ad esempio aggiornamento informative e contratti, creazione procedure Privacy by Design, Data Breach).

### Attenzione!

*Consigliamo di creare uno o più strumenti (es. questionario) che comprendano domande legate ai requisiti del GDPR, organizzate in funzione delle 6 componenti del modello: Organizzazione e ruoli, Persone, competenze e cultura, Processi e regole, Documentazione, Tecnologie e strumenti, Sistema di controllo.*

*Per esempio: per l'asse Documentazione: è stato elaborato un registro dei trattamenti conforme ai requisiti del GDPR? Sono state predisposte o aggiornate informative e consensi in funzione dei requisiti del GDPR? Sono state predisposte o aggiornate le lettere di nomina a Responsabili esterni del trattamento in funzione dei requisiti del GDPR?*

#### 4) MAPPATURA PRELIMINARE DEI TRATTAMENTI E CREAZIONE DEL REGISTRO

Mappatura preliminare dei trattamenti e creazione del registro dei trattamenti, che costituisce una delle novità di maggior rilievo introdotte dal GDPR. All'interno del percorso di adeguamento, la costruzione del registro dei trattamenti ha un ruolo di centrale importanza in quanto, oltre

a essere un obbligo legale, rappresenta un elemento imprescindibile per la realizzazione di un numero significativo di azioni inserite nel piano di adeguamento, quali ad esempio la revisione documentale (informative e consensi, contratti e lettere di nomina) e l'implementazione di misure di sicurezza adeguate in funzione del rischio associato al trattamento.

### Attenzione!

*Consigliamo di adottare un modello di registro dei trattamenti che integri le informazioni minime richieste dal Regolamento con elementi aggiuntivi in grado di trasformare il registro in un vero e proprio asset aziendale, mantenendo un collegamento diretto con i principali «oggetti aziendali». Nello specifico, consigliamo di inserire i seguenti elementi:*

- **PROCESSI/MACRO-ATTIVITÀ**, per poter inquadrare i trattamenti all'interno delle attività svolte da ciascuna Unità Organizzativa e facilitarne la comprensione e l'aggiornamento da parte dei responsabili
- **BASE GIURIDICA E MODALITÀ DI RACCOLTA DEL CONSENSO**, per facilitare la predisposizione dell'informativa da fornire all'interessato. Al riguardo, ricordiamo che l'art. 13 co. 1 l. c) del GDPR ricomprende la base giuridica del trattamento tra gli elementi che devono essere contenuti all'interno dell'informativa
- **REFERENTE INTERNO E CATEGORIE DI SOGGETTI AUTORIZZATI AL TRATTAMENTO**, per fornire indicazioni utili in merito a persone che, limitatamente ai trattamenti di propria competenza, avranno dei compiti esecutivi all'interno del modello di protezione dei dati personali
- **MODALITÀ DI TRATTAMENTO DEI DATI**, per poter mappare con precisione, attraverso l'elencazione dei soli applicativi utilizzati per il trattamento dei dati personali, le misure di sicurezza implementate/da implementare, nonché per poter condurre efficacemente la valutazione dei rischi
- **EFFETTUARE UNA MAPPATURA PRELIMINARE DEI TRATTAMENTI DI CIASCUNA UNITÀ ORGANIZZATIVA**, prima di coinvolgere i relativi referenti per una opportuna validazione/integrazione, partendo dalle informazioni contenute nella documentazione aziendale disponibile (es. organigramma, funzionigramma, mappa dei processi, mappa applicativi) evidenziando, in particolare, se i trattamenti sono eseguiti con supporto di partner esterni e se il servizio/sistema/applicativo utilizzato per il trattamento è in outsourcing.

## 5) IDENTIFICAZIONE E CLASSIFICAZIONE DEI GAP DA COLMARE

Identificazione e classificazione dei gap da colmare per conformarsi al GDPR, a livello sia di modello di protezione dei dati personali complessivo (es. introduzione della figura del DPO) sia di singoli trattamenti censiti (es. modifica di informative e consensi per attività di profilazione), per i quali è necessario valutare attentamente i rischi di non conformità.

### Attenzione!

*Consigliamo di predisporre un elenco delle non conformità con specifica, per ciascuna voce, di: riferimenti normativi (articoli e considerando del GDPR, ma anche linee guida WP29), asse/i del modello impattato/i, rischi di non conformità connessi (sanzioni, perdite finanziarie rilevanti o danni reputazionali), impatti per gli interessati.*

## 6) DEFINIZIONE DEL PIANO DI ADEGUAMENTO COMPLESSIVO

Definizione del piano di adeguamento complessivo, comprensivo di un elenco di azioni, opportunamente priorizzate, finalizzate a colmare i

gap evidenziati. Per ciascuna azione inserita nel piano è necessario fornire indicazioni in merito alle attività da completare, agli attori e alle loro relative responsabilità, alle tempistiche e milestone nonché alle modalità di rilascio attese.

### Attenzione!

*Consigliamo di scomporre il piano di adeguamento in “cantieri di lavoro” che richiami gli attori a cui sarà attribuita l'ownership delle azioni in essi contenute (Affari Legali; Sistemi Informativi; Compliance; ...). Per ciascun cantiere, inoltre, dovranno essere individuate azioni facilmente riconducibili ad articoli e considerando del GDPR, anche in termini di nomenclatura, opportunamente integrate con azioni trasversali a supporto della buona riuscita del percorso (per esempio: piano degli investimenti; piattaforma GRC; attività di coordinamento). Ad esempio, al Cantiere di lavoro “Affari Legali” potranno essere attribuite le seguenti azioni: informative e consensi; registro dei trattamenti; termini di conservazione; gestione diritti degli interessati; fornitori e contratti; trasferimento dati extra UE.*

*Tra le azioni da non trascurare per mettere a terra e far funzionare correttamente il modello di protezione dei dati personali, vi è sicuramente la definizione e implementazione di un piano di formazione delle persone, le cui azioni verticali dovranno essere opportunamente differenziate in funzione della tipologia di ruolo ricoperto all'interno dell'organizzazione (ad esempio referenti interni del trattamento, soggetti autorizzati al trattamento, popolazione aziendale). Le persone dovranno essere messe nelle condizioni da un lato di comprendere i requisiti del GDPR, ivi comprese l'entità delle sanzioni collegate a eventuali non conformità, e dall'altro di comprendere le disposizioni e le norme di*

*autoregolamentazione di cui si è dotata l'organizzazione, con particolare riferimento al comportamento da tenere verso l'esterno (ad esempio la gestione diritti degli interessati).*

*La definizione e l'implementazione di un processo di analisi del rischio, per giustificare le contromisure, valutare che siano efficaci, di costo ragionevole, effettivamente applicabili al contesto, in grado di rispondere in tempo alle minacce e assegnare una priorità di trattamento dei rischi, consente di determinare l'investimento necessario all'azienda per proteggersi. Il processo, per essere efficace, deve utilizzare una metodologia che permetta la riproducibilità dei risultati e deve prevedere come prima attività la definizione di un "risk appetite" anche qualitativo, vale a dire una soglia oltre la quale si ritiene l'impatto e/o la probabilità del realizzarsi di un rischio non accettabile. Questo permetterà di comprendere, a valle dell'analisi effettuata, quali applicazioni tutelino a sufficienza i dati e su quali, invece, sia necessario intervenire, al fine di implementare ulteriori opportune misure tese a mitigare il rischio, fino a renderlo accettabile. Gli interventi tecnico-organizzativo individuati diventeranno evidentemente parte del piano di adeguamento.*



## 3. COME EFFETTUARE L'ASSESSMENT NEI CASI DI OUTSOURCING

L'assessment deve tenere conto dei rischi connessi all'esternalizzazione di prodotti o sistemi che devono essere gestiti attraverso controlli adeguati, che comprendono una combinazione di controlli legali, fisici, logici, procedura-

li e manageriali. L'assessment, oltre a essere un metodo per dimostrare la propria accountability, nel caso degli outsourcer è anche un'attività che rientra nel principio di "data protection by design and by default" ai sensi dell'art. 25 del GDPR.

### Attenzione!

*Consigliamo di predisporre una checklist che non consideri solo la sicurezza dei dati, ma anche gli obblighi di conformità a normative o a standard industriali a cui l'azienda cliente è sottoposta in virtù del Paese di appartenenza, del settore di attività o di entrambi. In particolare, per rispondere alle esigenze specifiche in materia di:*

#### SICUREZZA DEL CLOUD

*Richiedere l'esibizione dell'ottenimento di certificazioni specifiche e relative al contesto di outsourcing in esame, comprese anche le attività di audit di conformità eseguite in caso di adesione a codici di condotta specifici. In caso di mancanza di certificazione e/o adesione a codici di condotta, le checklist dovrebbero contenere i controlli descritti dalla ISO 27017 o quelli per l'ottenimento della certificazione CSA STAR.*

#### GOVERNANCE

*Predisporre dei controlli atti a evitare la perdita di governo sul proprio patrimonio informativo e su processi di gestione chiave.*

#### GESTIONE DELLE IDENTITÀ E DEI RUOLI

*Considerare tutti quei controlli atti a impedire accessi non autorizzati ai dati sia da parte dell'outsourcer che dei suoi eventuali subappaltatori.*

#### GESTIONE DEL CONTRATTO

*I controlli dovrebbero verificare:*

- *La presenza di clausole di riservatezza, salvaguardia e rivendicazione dei diritti di proprietà intellettuale.*

- *Come vengono recepite le normative italiane ed europee in tema di protezione dei dati per quanto attiene alle misure nel dominio tecnologico e organizzativo del fornitore, con particolare riferimento all'adesione a codici di condotta, norme sulla cancellazione sicura dei dati, obblighi relativi agli amministratori di sistema, disponibilità di copie di sicurezza e ripristino di dati e di sistemi, modalità di gestione dei diritti degli interessati, e via dicendo.*
- *L'esistenza di procedure di gestione e notifica degli incidenti di sicurezza verso l'azienda, prestando la dovuta attenzione al modo in cui si deve (o non si deve) comunicare congiuntamente verso i clienti del cloud, consumer o utenti dell'azienda cliente.*
- *La presenza di clausole che specifichino come i contratti devono essere gestiti in relazione all'evoluzione delle esigenze operative e dell'organizzazione aziendale, per tenere conto di eventuali variazioni nel quadro normativo cogente e, infine, per monitorare costantemente il raggiungimento degli obiettivi che avevano giustificato il contratto stesso, tramite parametri di misura del loro raggiungimento (KPI, Key Performance Indicator).*
- *La presenza di coperture assicurative, soprattutto per i fornitori meno strutturati, che permettano di far fronte a eventuali danni cagionati durante l'esecuzione del contratto, ai quali l'outsourcer in autonomia non saprebbe far fronte.*
- *Le misure di sicurezza in essere che permettono di garantire elevati livelli di sicurezza cyber e infrastrutturale (Data center certificato TIER IV e così via), la loro efficacia in risposta alle minacce potenziali o agli incidenti verificatesi e le misure previste a fronte della valutazione del rischio effettuata relativa all'ambito del servizio di outsourcing.*

### STIPULA DI NUOVI CONTRATTI

In caso di stipula di nuovi contratti di outsourcing è consigliabile effettuare dei controlli preliminari che riguardino la reputazione e la storia della società, la qualità dei servizi forniti ad altri clienti, la stabilità finanziaria della società, gli standard di gestione della qualità e della sicurezza attualmente seguiti dalla società (ad esempio conformità certificata con ISO 9000 e ISO/IEC 27001). Questo tipo di attività di assessment po-

trebbe rilevare dei rischi commerciali come la possibilità che l'attività dell'outsourcer fallisca, che non sia in grado di raggiungere livelli di servizio desiderati o che stia fornendo servizi a concorrenti della società. Il risultato dell'assessment, come si può vedere, diventa elemento fondamentale per la scelta dell'outsourcer.



## 4. TRE APPROCCI: AUTO-ASSESSMENT, ASSESSMENT ONLINE OPPURE IN OUTSOURCING

L'assessment deve tenere conto dei rischi connessi all'esternalizzazione di prodotti o sistemi che devono essere gestiti attraverso controlli adeguati, che comprendono una combinazione di controlli legali, fisici, logici, procedurali e manageriali.

L'assessment, oltre a essere un metodo per dimostrare la propria accountability, nel caso degli outsourcer è anche un'attività che rientra nel principio di "data protection by design and by default" ai sensi dell'art. 25 del GDPR.

L'assessment può essere realizzato all'interno dell'organizzazione, con l'eventuale utilizzo di asset disponibili sul mercato o richiedere il coinvolgimento di soggetti terzi. Analizziamo più in dettaglio le principali casistiche evidenziando i limiti dei diversi approcci.

### AUTO-ASSESSMENT

Nell'auto-assessment l'organizzazione individua un *team di lavoro* interno, composto da referenti cross funzionali, incaricati di effettuare il percorso di valutazione

Questo tipo di approccio presenta diversi limiti. Tra i principali si segnala la criticità legata al livello di preparazione, che deve essere adeguato rispetto al Regolamento e agli ambiti da indirizzare, che si caratterizzano per eterogeneità e

verticalità. Un altro punto critico è la necessità di disporre di risorse ma anche del tempo necessari allo svolgimento dell'attività di assessment (ad esempio le interviste con i referenti delle Unità Organizzative), da bilanciare con l'impegno dedicato a gestire, in parallelo, il lavoro ordinario. Il terzo punto critico è la necessità di dover disporre di asset a supporto della rilevazione delle informazioni (ad esempio il Data Protection Maturity Model) nonché la formalizzazione delle azioni, ovvero un elenco standard di azioni, da personalizzare in funzione della specifica realtà.

Gli esperti segnalano anche la necessità di coinvolgere tutti i referenti che concorrono al corretto svolgimento dell'assessment considerando anche la necessità di creare tutti gli strumenti di supporto relativi.

### ASSESSMENT ONLINE

Nel caso si scelga di procedere con l'assessment online, l'organizzazione deve individuare una o più soluzioni disponibili sul mercato da adottare a supporto della realizzazione dell'assessment quali, ad esempio, tool e questionari sviluppati da società di consulenza e studi legali che restituiscono risultati di alto livello in merito al livello di maturità dell'organizzazione in

ottica GDPR. Questo tipo di approccio presenta dei vantaggi, tra cui un risparmio significativo sull'effort richiesto per la costruzione degli asset e l'individuazione dei requisiti del GDPR. Tuttavia sussistono alcuni limiti. Tra quelli principali va annoverata la personalizzazione dei risultati, in funzione delle peculiarità dell'organizzazione (ad esempio il settore di attività e/o l'area di business) così come la capacità, non scontata, di interpretare e approfondire opportunamente le indicazioni emerse dall'assessment, anche nell'ottica della costruzione dell'action plan. Un altro fattore da considerare è il costo per l'acquisizione e l'implementazione degli asset necessari alla realizzazione dell'assessment, soprattutto per entità rilevanti come, ad esempio, nel caso di gruppi societari.

Come sottolineano gli esperti, è evidente che, soprattutto nei casi di organizzazioni medio-grandi (ad esempio nel caso di gruppi societari) o aventi una complessità importante (ad esempio nel caso di trattamenti su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati), un approccio che restituisca dei risultati esaustivi ma molto di alto livello può essere utile a identificare esclusivamente le macro-aree di intervento, ma non può che costituire un pre-assessment. Per completare l'assessment, infatti, l'organizzazione deve necessariamente effettuare un'analisi approfondita della documentazione in uso (es. informative, consensi, clausole contrattuali) e realizzare una serie di approfondimenti con i referenti di funzione, sia di staff sia di business, prestando particolare attenzione alle funzioni

più impattate dal punto di vista del trattamento dei dati personali (es. Marketing B2C).

### RICORSO A PARTNER ESTERNI

Ricorso a partner esterni: al netto dei costi richiesti per l'approvvigionamento, rappresenta l'approccio più "sicuro" da adottare, tuttavia è fondamentale essere affiancati da partner adeguati. Il partner ideale deve essere in grado di offrire un supporto a 360° all'organizzazione, coprendo l'intero perimetro del modello grazie alla coesistenza al proprio interno di figure fortemente eterogenee, con competenze legali, organizzative/gestionali e tecnologiche. Il coinvolgimento attivo di alcune figure interne all'organizzazione e l'adeguata sponsorship del vertice, tuttavia, rappresentano fattori chiave per la buona riuscita dell'assessment e per il cambiamento culturale a cui mira il GDPR con il concetto di *accountability*.

#### Le competenze necessarie



*Le competenze ideali del partner esterno devono triangolare diversi aspetti: legali, tecnologici e organizzativi*

## 5. COME VANNO INTERPRETATI I RISULTATI DELL'ASSESSMENT

L'assessment restituisce indicazioni importanti in merito al livello di maturità dell'organizzazione in ottica GDPR. Non solo fornisce una fotografia del modello di protezione dei dati personali *così come sono*, ma individua anche tutti i gap da colmare per essere conformi al GDPR. Nella creazione del piano di adeguamento occorre adottare una visione allargata. Gli esperti sottolineano, in particolare, una serie di aspetti da considerare. Il primo, nell'ordine, è l'impatto delle azioni sull'operatività e sul business dell'organizzazione. Può essere il caso dell'erogazione di un servizio *core* basato su attività di profilazione che richiedono la raccolta del consenso degli interessati oppure la partenza di un progetto strategico che comporta un livello di rischio elevato nell'ottica dei diritti e le libertà delle persone fisiche.

Il secondo è relativo ai rischi connessi al mancato adeguamento del modello di protezione

dei dati personali, che possono portare a sanzioni amministrative e perdite finanziarie rilevanti o danni reputazionali. Un terzo punto di attenzione è legato alla gestione dell'outsourcer. Gli esperti suggeriscono di porre attenzione alla prioritizzazione delle attività considerando quanto stipulato a contratto col fornitore, al fine di calcolare correttamente eventuali costi aggiuntivi e/o necessità di revisione del contratto stesso. Un altro elemento importante è la corretta sensibilizzazione del personale (vertice in primis) in merito agli elementi sopra riportati e il corretto stanziamento di risorse per il completamento del percorso diventano la chiave per evitare ripercussioni sull'organizzazione. Il piano di adeguamento rappresenta lo strumento operativo che le organizzazioni non devono mai perdere di vista, in cui sono contenute tutte le azioni da trarre entro i tempi ritenuti sostenibili dall'organizzazione.

### Conclusioni

Alla luce delle importanti novità introdotte dal GDPR, l'esecuzione di un assessment, deve essere:

- Comprensivo di tutti gli assi del modello della protezione dei dati personale (non si tratta solo di aggiornare la documentazione "legale").
- Implementato seguendo degli step ben definiti, con l'obiettivo di generare tutte le informazioni necessarie alla creazione di un piano di adeguamento completo e sostenibile.
- Supportato da partner esterni adeguati, aventi competenze eterogenee a copertura di tutti gli ambiti del GDPR (legali, organizzative/gestionali, tecnologiche).
- Correttamente interpretato, valutando attentamente gli impatti sull'operatività e i rischi di non conformità per l'organizzazione (e il suo benessere).

# DIGITAL 360 | Group

LEADING DIGITAL TRANSFORMATION

Digital360 si pone l'obiettivo di accompagnare imprese e pubbliche amministrazioni nella comprensione e nell'attuazione della Trasformazione Digitale e dell'Innovazione Imprenditoriale, favorendo l'incontro con i migliori fornitori tecnologici, attraverso una piattaforma multicanale unica in Italia composta da Contenuti Editoriali, Comunicazione, Lead Generation, Eventi, Advisory e Advocacy.

Digital360 integra un mix multidisciplinare e multiculturale di professionalità e competenze: professori universitari, giornalisti, consulenti, ricercatori, professionisti degli eventi ed esperti di comunicazione, tutti accumulati da una grande passione e missione: il digitale e l'innovazione, visti come i motori della crescita e dell'ammodernamento di questo Paese.

VIA COPERNICO, 38  
20125 - MILANO

TEL. 02 92852785  
MAIL: [MARKETING@DIGITAL4.BIZ](mailto:MARKETING@DIGITAL4.BIZ)

# NETWORK **DIGITAL** 360 E.GUIDE



©ICT & STRATEGY ■■■ [INFO@DIGITAL4.BIZ](mailto:INFO@DIGITAL4.BIZ)

[WWW.NETWORKDIGITAL360.IT](http://WWW.NETWORKDIGITAL360.IT)