

A V V E R A

B U S I N E S S C O M P L I A N C E





L'introduzione di normative sempre più stringenti in materia di Responsabilità Amministrativa degli Enti, Antiriciclaggio, Data Protection e Salute e Sicurezza nei Luoghi di Lavoro ha determinato un'estensione degli obblighi che gravano sulle imprese e un allargamento del perimetro di responsabilità del management.

Le sanzioni di natura penale e patrimoniale, in alcuni casi notevolmente afflittive, impongono l'adozione di nuovi modelli organizzativi e di strategie di riduzione dei rischi capaci di salvaguardare il management e il patrimonio economico e reputazionale dell'impresa.

L'ampiezza dei processi, delle funzioni e dei sistemi coinvolti, richiede un approccio innovativo e maggiormente integrato rispetto a quello della tradizionale consulenza legale.

Il team di Avvera è formato da professionisti affiatati - legali, psicologi, esperti di processi, specialisti IT e HR - in grado di analizzare le specificità della vostra azienda, disegnare una soluzione su misura e dotare la vostra organizzazione di sistemi di gestione del rischio che vi consentano di continuare ad operare con serenità e agilità, in conformità con le norme e le disposizioni di legge.

## **NUOVE SFIDE PER IL BOARD DELL'IMPRESA**





**IL NOSTRO IMPEGNO:**

**PROTEGGERE  
IL MANAGEMENT  
E IL VALORE  
DELLA VOSTRA IMPRESA**

Avvera nasce con la missione di fornire alle aziende un supporto consulenziale e operativo per la gestione dei rischi operativi e legali d'impresa.

L'impegno è quello di affiancare le aziende nello sviluppo di un efficace sistema di riduzione del rischio con un approccio innovativo, in grado di ricondurre ogni azione di conformità all'interno di una strategia più ampia e integrata di Governance, Risk Management e Compliance.

Il nostro contributo non si limita a dotare il management di modelli, strumenti e procedure formali in grado di proteggere l'impresa e le figure che ricoprono un ruolo di responsabilità, ma si estende a tutti i livelli della vostra organizzazione per garantirvi, con un supporto operativo diretto, l'effettività delle misure adottate, il rispetto delle scadenze e la correttezza degli adempimenti.

# I NOSTRI SERVIZI



## COMPLIANCE NORMATIVA

### Consulenza specialistica

Avvera opera su tutto il territorio nazionale con un team di esperti che si occupa specificamente di Compliance e Sistemi di Gestione. Nel team collaborano figure con competenze multidisciplinari avanzate: avvocati, ingegneri gestionali, consulenti organizzativi, consulenti HR, psicologi del lavoro, ingegneri informatici, esperti di security, safety auditor, specialisti in salute e sicurezza sul lavoro.

I servizi sono strutturati come moduli integrati di un processo iterativo di miglioramento continuo - l'Enterprise Compliance Lifecycle Management di Avvera - articolato in 6 fasi:

- **Risk Assessment**
- **Implementazione**
- **Formazione**
- **Controllo preventivo**
- **Analisi di effettività**
- **Audit e Due diligence**

### Supporto operativo

Avvera vi affianca anche nello svolgimento delle incombenze operative, supportando le vostre strutture interne o prendendo direttamente in carico gli adempimenti normativi.

## DPO OUTSOURCING

### La nuova figura del DPO

Tra le numerose novità introdotte dal Nuovo Regolamento (EU) n.2016/679 è prevista l'istituzione del DPO (Data Protection Officer), figura chiave per assicurare il corretto funzionamento del Sistema di Gestione dei Dati Personali.

Per alcune organizzazioni la designazione del Data Protection Officer è obbligatoria, mentre per altre può rappresentare una scelta volontaria opportuna.

### Perché affidarsi a un DPO Avvera

L'incarico di DPO può essere ricoperto anche da un soggetto esterno dotato di congrui requisiti. Avvera vi offre la possibilità di esternalizzare la figura e i compiti del DPO sgravandovi dalle incombenze previste. Affidandovi ad Avvera potrete contare sul contributo di un team di legali e di esperti con competenze specifiche in materia.



## DIGITAL TRANSFORMATION

### Compliance di progetti digitali

La digitalizzazione dei processi di business e l'erogazione di servizi ad alto contenuto tecnologico richiedono un'implementazione nel rispetto delle normative vigenti sia italiane che europee, delle regole tecniche emanate e delle indicazioni formulate dalle autorità competenti, in particolare AGID - Agenzia per l'Italia Digitale - e Garante per la protezione dei dati personali.

Il contributo di Avvera consente di innovare l'approccio al business o le modalità di erogazione di servizi senza perdere di vista le esigenze di conformità.

Ambiti di intervento:

- **Sistemi di conservazione digitale**
- **Sistemi di firma elettronica avanzata**
- **Sistemi di workflow documentale**
- **Servizi digitali: documentazione e manualistica obbligatoria**

## COMPLIANCE COCKPIT

### Cruscotto informativo

Intactor è una soluzione software studiata da Avvera per aiutare le organizzazioni a gestire e tenere sotto controllo tutte le attività finalizzate a mitigare il rischio operativo e legale d'impresa. Intactor offre a imprese, enti e organizzazioni un set di strumenti avanzati per gestire e monitorare gli adempimenti e le azioni di conformità in materia di:

- **Regolamento (UE) 2016/679 e D.Lgs. 196/2003**
- **Responsabilità Amministrativo/Penale degli Enti (D.Lgs. 231/2001)**
- **ISO 27001**
- **Impatto Patrimoniale**

La soluzione fornisce al management cruscotti grafici analitici e di sintesi che consentono di valutare il grado di rischio e di monitorare lo stato degli adempimenti.

Gli automatismi integrati generano le attività previste e ne gestiscono le scadenze inviando alle funzioni interessate notifiche di sollecito e promemoria.

Il sistema, compatibile con tutti gli ambienti IT, è completamente personalizzabile in funzione delle differenti specificità aziendali.



# I NOSTRI TESTIMONIAL: OLTRE 400 CLIENTI ATTIVI

**BANCHE, ISTITUZIONI, GRUPPI INDUSTRIALI,  
SOCIETÀ DI DISTRIBUZIONE E DI SERVIZI  
NAZIONALI E INTERNAZIONALI**

Lavoriamo per istituzioni, grandi gruppi, medie imprese e organizzazioni di ogni dimensione. Contiamo tra i nostri clienti realtà importanti che operano nei seguenti settori:

- Automotive
- Assicurazioni
- Banche e Finanziarie
- Edilizia e Costruzioni
- Energia e Utility
- Grande Distribuzione e Retail
- Industrie Alimentari
- Industrie Chimiche
- Industrie Farmaceutiche
- Information Technology
- Produzione Meccanica
- Logistica e trasporti
- Luxury & Fashion
- Materie prime
- Media & Editoria
- Ospitalità e Ristorazione
- Sanità
- Servizi on-line
- Telecomunicazioni
- Tessile e abbigliamento
- Università
- Viaggi e turismo

## IL NOSTRO MODELLO

# ENTERPRISE COMPLIANCE LIFECYCLE MANAGEMENT

La compliance è un processo continuo che si sviluppa nel tempo. L'Enterprise Compliance Lifecycle Management di Avvera è un insieme di servizi integrati che consente di minimizzare i rischi operativi mantenendo l'impresa costantemente allineata ai requisiti normativi. L'approccio è modulare: l'impresa può affidare ad Avvera la gestione dell'intero ciclo o di una o più operazioni.

### Risk Assessment

Analisi del rischio con verifica formale del modello organizzativo e gestionale e di tutta la documentazione relativa esistente.

### Implementazione

Preso in carico di tutte le attività operative necessarie per ottemperare alle disposizioni legislative.

### Formazione

Piani di formazione on-site o attraverso piattaforma e-learning per indirizzare i collaboratori verso comportamenti adeguati e consapevoli.

### Controllo preventivo

Affiancamento delle funzioni interne aziendali nell'esercizio delle verifiche di effettività previste, nella gestione delle scadenze e nell'aggiornamento della documentazione e delle procedure.

### Analisi di effettività

Verifica sostanziale e di effettività del modello di organizzazione, di gestione e di controllo adottato.

### Audit & Due diligence

Verifica formale del modello di organizzazione, gestione e controllo adottato e della documentazione prodotta per la sua istituzione e il suo funzionamento.



## COME OPERIAMO

### Individuazione e gestione del rischio

Il nostro processo di risk management ci permette di individuare, materia per materia, quale area, funzione aziendale o singola persona è soggetta al rischio rispetto a determinati reati o infrazioni:

- Esaminiamo le attività e i processi che possono esporvi al rischio
- Valutiamo il rischio in termini di gravità e probabilità
- Analizziamo con quali norme, procedure, misure informatiche o fisiche viene prevenuto il rischio
- Definiamo il nuovo piano di gestione del rischio

### Compliance

Una volta disegnato il piano di gestione del rischio decidiamo insieme a voi le azioni da intraprendere: dal perfezionamento degli strumenti di governo della società (statuto, deleghe CDA, ecc.) fino alla redazione delle istruzioni di lavoro per le mansioni esecutive.

- Affianchiamo le vostre funzioni organizzative nell'implementazione delle procedure e dei controlli e le supportiamo nello svolgimento degli adempimenti normativi
- Formiamo e sensibilizziamo i vostri collaboratori affinché il loro comportamento sia consapevole e conforme
- Verifichiamo che la loro condotta si trasformi effettivamente in prassi operativa

### Monitoring e reporting

Monitoriamo con controlli periodici lo stato e l'evoluzione del sistema, risolvendo le problematiche che possono emergere nel tempo.

Forniamo al management feedback periodici che consentono una gestione prudente e consapevole.

## PERCHÉ SCEGLIERCI

### Studiamo soluzioni su misura

Ogni azienda è un sistema con moltissime variabili interne ed esterne. Noi siamo in grado di analizzare e comprendere la differenza di ciascuno dei nostri clienti e sappiamo calare un sistema di regole generale e astratto all'interno della loro specifica realtà con il minimo impatto sull'esistente.

### Forniamo un supporto completo

Non ci limitiamo a indicarvi la soluzione, ma vi affianchiamo anche sul piano operativo, integrando i vostri controlli interni e prendendo in carico le incombenze burocratiche e amministrative.

### Conosciamo tutte le dimensioni della materia e i suoi impatti sull'organizzazione

Il nostro team è costituito da professionisti con competenze multidisciplinari e anni di esperienza sul campo.

### Privilegiamo la concretezza

Adottiamo un approccio pragmatico, che punta dritto ai risultati. I nostri clienti ci stimano e ci apprezzano per la competenza, la disponibilità e il rispetto della parola data.



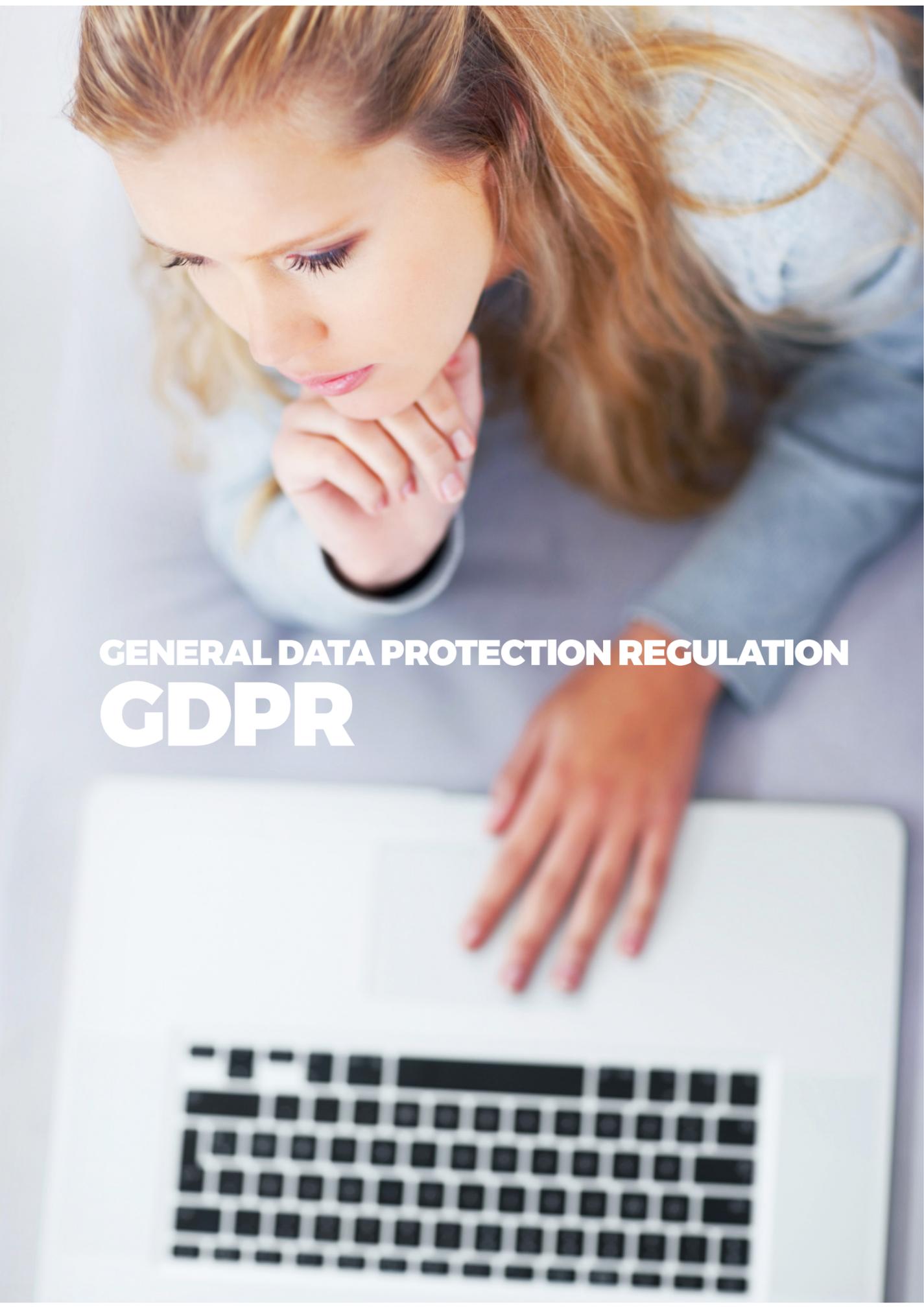
# COMPLIANCE NORMATIVA

Imprese, enti privati e pubblici hanno assunto un ruolo primario nell'economia e nella società e il legislatore ne disciplina in modo sempre più incisivo e penetrante gli aspetti organizzativi e le attività.

I regolamenti in materia di protezione dei dati personali, salute e sicurezza sul lavoro, antiriciclaggio e la disciplina sulla responsabilità degli enti mostrano come le normative siano divenute stringenti e abbraccino uno spettro sempre più ampio di funzioni e responsabilità.

L'operato delle società è costantemente sottoposto al vaglio degli azionisti, della comunità e degli organismi di controllo.

Non sorprende, quindi, che la compliance normativa sia balzata all'attenzione del management occupando un ruolo determinante nel contenimento del rischio operativo e legale e assumendo una valenza strategica per la tutela del valore dell'impresa.



# GENERAL DATA PROTECTION REGULATION GDPR



## COMPLIANCE NORMATIVA



### GDPR

Il nuovo regolamento europeo ha l'obiettivo di armonizzare le diverse normative nazionali per favorire la circolazione dei dati dei cittadini europei in maniera sicura e protetta. Con l'avvento del GDPR le imprese si devono confrontare con un impianto normativo che richiede un approccio diverso da quello del passato. La nuova disciplina pone l'accento sugli obiettivi sostanziali e sul principio di accountability, attribuendo all'azienda più ampi margini di autonomia ma caricandola di responsabilità più gravose.

Nella primavera 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea, il nuovo Regolamento (UE) n. 2016/679 General Data Protection Regulation (GDPR), che abroga e sostituisce la Direttiva 95/46/CE in materia di protezione dei dati personali e della libera circolazione degli stessi.

L'intento del legislatore europeo è quello di unificare e rafforzare, all'interno degli Stati Membri, i processi, le procedure e gli standard per la raccolta, la gestione e la protezione dei dati personali all'interno e al di fuori dei confini dell'UE. Il Regolamento è entrato in vigore 20 giorni dopo la pubblicazione in GUUE, per diventare definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018, senza necessità di atti normativi di recepimento da parte dei singoli ordinamenti; il legislatore nazionale è comunque intervenuto con un decreto legislativo, il 101/2018, con lo scopo di armonizzare il previgente Codice Privacy con il nuovo Regolamento UE. Il Regolamento crea diritti e doveri per gli individui e può pertanto essere fatto valere dinanzi ai giudici nazionali.

#### Obiettivi dell'azione di compliance:

- **Valutare l'entità dei rischi e degli effetti conseguenti alla violazione dei dati personali**
- **Attivare processi, misure e controlli continui finalizzati alla mitigazione effettiva del rischio e al rispetto degli obblighi normativi**
- **Individuare le figure interne/esterne a cui assegnare la responsabilità e i compiti di vigilanza**
- **Garantire i diritti degli interessati, compresi il diritto all'oblio e alla portabilità dei dati**
- **Abbatere il rischio di sanzioni pecuniarie o azioni legali**
- **Gestire in modo razionale, sostenibile ed efficace gli obblighi normativi**



## Principali ambiti di adeguamento

### Revisione modello organizzativo

Riformulazione di deleghe, compiti e funzioni interne: non è più prevista la figura del responsabile interno del trattamento, ma non viene meno la necessità organizzativa di assegnare compiti e funzioni ai diversi livelli gerarchici già presenti in azienda.

Introduzione del Data Protection Officer (DPO): ha il compito di sorvegliare la corretta applicazione della normativa, effettuare ispezioni e consultazioni e fungere da contact point con i vertici e con il Garante.

### Informativa e consensi

Diritto dell'interessato a ricevere le informazioni in modo trasparente e la richiesta di consenso in modo distinguibile e non condizionato. Obbligo del titolare di dimostrare l'ottenimento del consenso.

### Accountability

Si riducono notevolmente i casi in cui è necessario chiedere autorizzazioni o interpellare all'autorità Garante. Maggiori poteri del Titolare del trattamento di decidere in autonomia, con la consapevolezza che tali poteri sono bilanciati da sanzioni amministrative estremamente rilevanti.

### Data Protection

Obbligo di mettere in atto misure di protezione dei dati personali (es. pseudonimizzazione e cifratura) per garantire un livello di sicurezza adeguato ai rischi tra cui quelli di distruzione, perdita, modifica indebita, accesso non autorizzato.

### Privacy by design / by default

Obbligo di mettere in atto misure adeguate in fase di progettazione (by design) o per impostazione predefinita (by default) sulla base della criticità dei dati trattati.

### Data Breach Notification

Obbligo di comunicare senza ingiustificato ritardo ed entro 72 ore all'Autorità competente eventuali violazioni dei dati personali (e, in presenza di determinate condizioni, obbligo di rendere nota la violazione anche agli interessati).

### Registro dei trattamenti

Obbligo di tenuta di un registro delle attività di trattamento dei dati personali contenente, tra le altre informazioni, le finalità, le categorie di interessati e di trattamenti, la descrizione delle misure di sicurezza.

### Data Privacy Impact Assessment (DPIA)

Obbligo di effettuare una valutazione preventiva dell'impatto derivante da un trattamento sulla protezione dei dati personali che include una valutazione dei rischi e delle misure di sicurezza.

### Trasferimento dei dati

Obbligo di verifica di sussistenza delle condizioni previste dal Regolamento prima del trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale.

# GDPR

## Il percorso di adeguamento proposto da Avvera

### Il nuovo ruolo del DPO

Il regolamento prevede l'introduzione di una nuova figura di alto profilo caratterizzata da ampia autonomia e indipendenza, con il compito di sorvegliare la corretta applicazione della normativa. Il ruolo può essere ricoperto da una risorsa interna o esterna a condizione che sia provvista delle necessarie competenze e priva di ruoli e responsabilità che possano configurare conflitti di interesse. Avvera offre alle aziende la possibilità di affidarsi a una figura esterna qualificata che porta in dote tutto il know-how di un team di esperti specializzati.



### Consapevolezza

- Identificazione dei principali gap.
- Esecuzione del programma di adeguamento al GDPR in base alle evidenze di Risk Assessment.

### Avvio

- Definizione del perimetro delle attività del programma di adeguamento al GDPR.
- Approvazione delle stime e del budget.

### Risoluzione

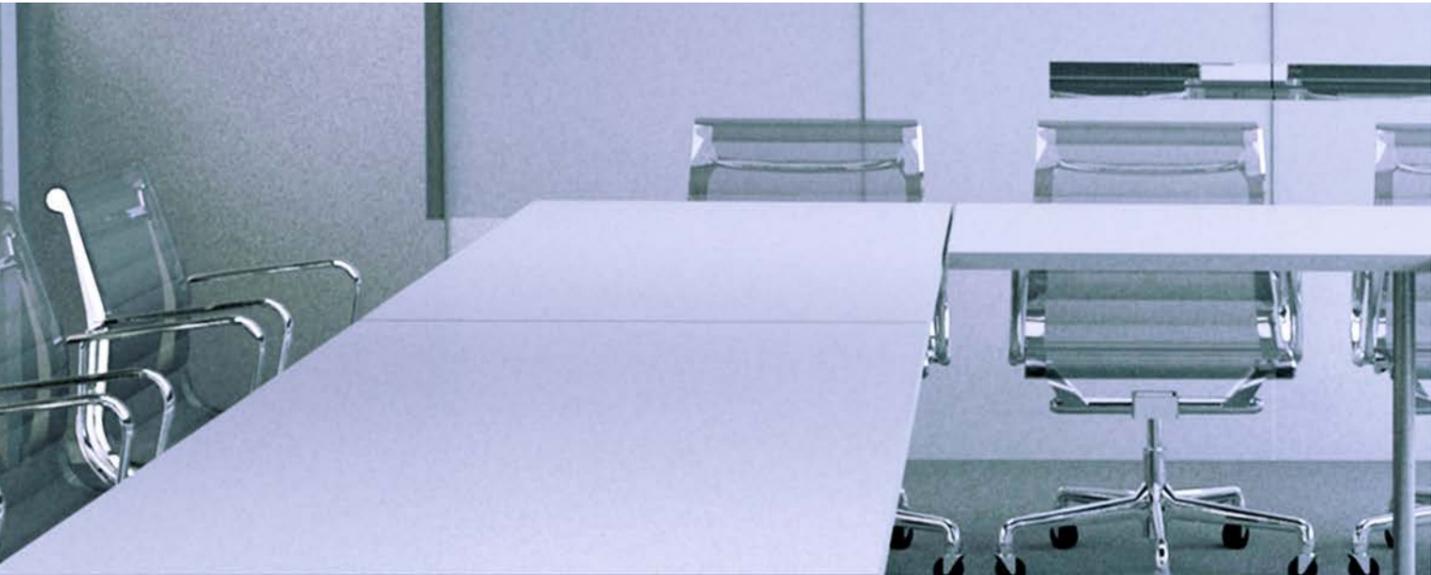
- Definizione di un programma integrato di adeguamento con identificazione/prioritizzazione degli interventi.

### Conformità

- Istituzione del DPO e dei processi di riferimento, con adeguamento degli assetti organizzativi e relativi flussi informativi e procedure.
- Implementazione della Privacy by design/default, definizione di un processo di escalation in caso di data breach, mediante l'adozione di procedure operative.
- Formazione delle persone che trattano dati personali.

### Ottimizzazione

- Ottimizzazione dei processi sulla base dei data breach.
- Rafforzamento delle misure di sicurezza sui dati personali.



## **CORPORATE GOVERNANCE E RESPONSABILITÀ DEGLI ENTI 231/2001**



## **COMPLIANCE NORMATIVA**

Il D.Lgs. 8 giugno 2001, n. 231 ha introdotto in Italia la responsabilità degli enti per i reati commessi dal personale, sia esso apicale o sottoposto, nell'interesse o a vantaggio dell'ente. Il rischio sanzionatorio è elevato e può consistere in sanzioni sia pecuniarie che interdittive.

### **231/2001**

Con l'introduzione del D.Lgs.231/2001 società, enti e associazioni forniti di personalità giuridica sono tenute a rispondere amministrativamente dei reati commessi nel loro interesse o a loro vantaggio da soggetti che ricoprono un ruolo apicale o da persone che operano sotto la direzione di questi ultimi. L'impatto delle sanzioni pecuniarie e interdittive e il danno reputazionale conseguente possono compromettere la fiducia degli stakeholder e incidere negativamente sul valore dell'azienda.

Le imprese sono chiamate ad adottare modelli organizzativi e gestionali efficaci ed effettivi, in grado di prevenire la commissione dei reati. Ogni impresa deve effettuare un'adeguata valutazione del rischio di commissione dei singoli reati richiamati e dotarsi di specifici regolamenti, procedure, codici di condotta e programmi di formazione per il personale e per coloro che agiscono nel suo interesse.

Il decreto prevede inoltre l'istituzione obbligatoria di un organismo interno di vigilanza dotato di autonomi poteri di iniziativa e controllo.

#### **Obiettivi dell'azione di compliance:**

- **Impedire lo sviluppo di pratiche scorrette e comportamenti illegali all'interno dell'organizzazione aziendale**
- **Garantire la tutela dei dipendenti che segnalano illeciti (whistleblowing)**
- **Abbatere il rischio di sanzioni pecuniarie o interdittive**
- **Prevenire danni patrimoniali e d'immagine all'azienda**
- **Proteggere il capitale reputazionale e la fiducia degli stakeholder**
- **Mantenere il valore per gli azionisti**
- **Gestire in modo razionale, sostenibile ed efficace gli obblighi normativi**



**PREVENZIONE E CONTRASTO  
DEL RICICLAGGIO  
231/2007**



**COMPLIANCE NORMATIVA**

## 231/2007

Il D. Lgs. 21 novembre 2007, n. 231 costituisce l'atto di recepimento della disciplina europea in materia di contrasto al riciclaggio del denaro e del finanziamento al terrorismo.

Il decreto, profondamente modificato dal D. Lgs. 90/2017, disciplina l'azione di prevenzione e contrasto del riciclaggio, cui sono chiamati i soggetti obbligati e si esplica attraverso l'introduzione di presidi volti a garantire la conoscenza del rischio, la piena conoscenza del cliente e l'individuazione delle operazioni sospette.

Il D.lgs. 90/2017, pubblicato nel mese di luglio 2017, ha profondamente modificato il D.Lgs. 231/2007.

L'azione di prevenzione e contrasto del riciclaggio, cui sono chiamati i soggetti obbligati, si esplica attraverso l'introduzione di presidi volti a garantire la conoscenza del rischio, la piena conoscenza del cliente e l'individuazione delle operazioni sospette. In particolare, la normativa poggia su un sistema di obblighi, ispirati ai seguenti istituti fondamentali:

- adeguata verifica della clientela con la quale si instaurano rapporti o si effettuano operazioni (customer due diligence);
- identificazione del titolare effettivo;
- conservazione e protezione dei documenti, dati e informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo;
- segnalazione delle operazioni sospette.

Tra i destinatari di tutti o parte degli obblighi, oltre a banche ed intermediari finanziari, imprese ed intermediari assicurativi che operano nei rami di cui all'articolo 2, comma 1, CAP, dottori commercialisti, revisori contabili, avvocati, notai, cambio valuta, case d'asta, gallerie d'arte, operatori in oro, custodia e trasporto valori, operatori del gioco on line ed altri.

**Obiettivi dell'azione di compliance:**

- Impedire il coinvolgimento dell'azienda o del professionista nella commissione di reati di riciclaggio e finanziamento del terrorismo
- Abbattere il rischio di sanzioni penali e amministrative
- Salvaguardare il patrimonio e la reputazione dell'azienda
- Conservare la fiducia degli stakeholder
- Gestire in modo razionale, sostenibile ed efficace gli obblighi normativi



## COMPLIANCE NORMATIVA

# SALUTE E SICUREZZA SUI LUOGHI DI LAVORO 81/2008

## 81/2008

Il decreto prescrive le azioni e i controlli preventivi a carico delle aziende atti a proteggere i lavoratori da possibili danni fisici e psicologici conseguenti a modalità operative e ambienti di lavoro inadeguati.

Il datore di lavoro è tenuto a effettuare una valutazione scrupolosa dei fattori critici presenti in azienda per poter intraprendere tutte le iniziative obbligatorie finalizzate all'eliminazione e al contenimento del rischio, quali l'adeguamento delle strutture, degli impianti e delle attrezzature, il controllo sanitario, la formazione dei lavoratori, la revisione dei processi e delle procedure.

La carenza o la mancanza di tali provvedimenti espongono l'azienda a responsabilità di natura civile e penale notevolmente rischiose.

Il D.Lgs. 9 aprile 2008, n. 81 persegue la finalità di garantire l'uniformità della tutela delle lavoratrici e dei lavoratori sul territorio nazionale attraverso il rispetto dei livelli essenziali di sicurezza e si applica a "tutti i settori di attività, privati e pubblici, e a tutte le tipologie di rischio". Il Decreto indirizza ogni impresa verso un miglioramento continuo tramite l'adozione di un Sistema di Gestione della Sicurezza.

La normativa ha un impatto sull'organizzazione, sui processi e i sistemi produttivi aziendali e conferma un regime di responsabilità civile e penale notevolmente rischioso. L'azione di adeguamento alla disciplina e la successiva gestione delle incombenze devono partire da una corretta individuazione del datore di lavoro e adottare, ove possibile, una efficace delega delle responsabilità, avvalendosi di tutti gli strumenti previsti dal decreto.

### Obiettivi dell'azione di compliance:

- **Prevenire le malattie professionali e gli incidenti sul lavoro**
- **Migliorare la sicurezza e il benessere dei lavoratori**
- **Ridurre il rischio legale e operativo**
- **Abbatere il rischio di sanzioni amministrative**
- **Gestire in modo razionale, sostenibile ed efficace gli obblighi normativi**



# SISTEMI DI GESTIONE

I sistemi di gestione sono strumenti utili per migliorare i processi interni, regolare i comportamenti organizzativi e garantire a clienti, partner e istituzioni un servizio qualitativo basato su metodologie certificate. Essi si basano su procedure di controllo attive in grado di regolare i processi e di innescare azioni correttive e misure preventive. I requisiti che un'azienda deve soddisfare per attuare un Sistema di Gestione della Qualità e mantenerlo nel tempo coinvolgono l'organizzazione a vari livelli con un impatto diretto su molti dipartimenti e su un'ampia popolazione aziendale.



# SISTEMA DI GESTIONE DELLA QUALITÀ ISO/9001



## SISTEMI DI GESTIONE

### ISO 9001

ISO 9001 è il sistema di gestione della qualità che aiuta le imprese a identificare i possibili miglioramenti apportabili a ogni singolo processo e al funzionamento complessivo della “macchina aziendale”.

Il sistema agevola il monitoraggio continuo della qualità e la rapida attivazione delle azioni correttive per centrare gli obiettivi qualitativi definiti in sede di pianificazione strategica.

L'azienda può così raggiungere nuovi traguardi di efficienza e ottenere risparmi significativi, offrendo alla clientela un servizio più accurato e in continuo miglioramento.

Il sistema di gestione della qualità è lo strumento organizzativo e di garanzia al processo aziendale di “Gestione della Qualità”, progettato in modo specialistico con l'obiettivo di stimolare il comportamento di tutti ad assumere un “ruolo attivo” rispetto agli obiettivi definiti dalla Direzione Generale.

La norma UNI EN ISO 9001 si basa sul principio della determinazione del “contesto” aziendale attraverso la definizione delle parti interessate e la conseguente valutazione dei “rischi ed opportunità di miglioramento” mantenendo il costante monitoraggio sulla gestione dei processi.

#### Obiettivi

- **Miglioramento organizzativo**
- **Standardizzazione dei processi**
- **Accesso a nuovi clienti e opportunità**

#### Vantaggi

- **Maggiore efficienza e produttività**
- **Processi razionali codificati**
- **Migliore controllo**
- **Migliore servizio al cliente**
- **Aumento della credibilità e della fiducia**



**OCCUPATIONAL HEALTH & SAFETY  
ASSESSMENT SERIES**

# **BS/OHSAS 18001 ISO 45001**



**SISTEMI DI GESTIONE**

## **ISO 45001**

ISO 45001 definisce gli standard minimi per la tutela della salute e del benessere dei lavoratori.

La struttura normativa ripropone, ampliandoli, i contenuti delle norme BS/OHSAS 18001 e 81/2008.

ISO 45001 è uno standard certificabile riconosciuto a livello internazionale ed è destinata a sostituire la BS/OHSAS 18001 che dal 12 marzo 2021 non sarà più valida.

ISO 45001 fornisce un quadro di riferimento per ridurre i rischi e migliorare la sicurezza attraverso un processo iterativo di miglioramento continuo che coinvolge attivamente tutta l'organizzazione, dai vertici aziendali al singolo lavoratore.

BS/OHSAS 18001

Standard emesso dal British Standard Institute che specifica i requisiti per un sistema di gestione della Sicurezza e Salute sul luogo di Lavoro (SSL).

ISO 45001

Di recente emanazione, è la prima norma internazionale applicabile a qualunque organizzazione che voglia realizzare un sistema di gestione della sicurezza e salute per eliminare o ridurre i rischi per i lavoratori e per tutte le figure che possano risultare esposte ai pericoli sul lavoro associati all'attività.

### **Obiettivi**

- **Prevenzione degli incidenti sul lavoro**
- **Miglioramento delle condizioni di lavoro**
- **Rispetto dei requisiti normativi**

### **Vantaggi**

- **Riduzione del rischio legale e operativo**
- **Maggior benessere dei lavoratori**
- **Minori assenze**
- **Riduzione dei costi assicurativi**
- **Aumento della credibilità e della fiducia**



# SISTEMA DI GESTIONE AMBIENTALE **ISO 14001 - EMAS**



## SISTEMI DI GESTIONE

### ISO 14001

La norma UNI EN ISO 14001 è uno strumento internazionale di carattere volontario, applicabile a tutte le tipologie di imprese, che specifica i requisiti di un sistema di gestione ambientale. Viene rilasciata da un organismo indipendente accreditato che verifica l'impegno concreto nel minimizzare l'impatto ambientale dei processi, prodotti e servizi.

## ISO 14001

Il sistema di gestione ambientale ISO 14001 guida le imprese nella messa a punto di processi, procedure e controlli in grado di ridurre gli impatti negativi delle attività aziendali sull'ambiente e di minimizzare i rischi di inquinamento. La norma, oltre a instaurare un approccio maggiormente consapevole al corretto consumo delle risorse e alla tutela ambientale, consente all'impresa di manifestare una condotta etica e responsabile, con riflessi positivi nella relazione con la comunità e le istituzioni.

### EMAS

EMAS (Environmental Management and Audit Scheme) è un sistema comunitario di ecogestione e audit ambientale che riconosce a livello europeo il raggiungimento di risultati di eccellenza nel miglioramento ambientale. EMAS prevede che il Sistema di Gestione Ambientale di un'organizzazione sia attuato in conformità con i requisiti della norma ISO 14001, sezione 4.

### Obiettivi

- Riduzione dell'impatto ambientale
- Prevenzione dell'inquinamento
- Rispetto dei requisiti normativi

### Vantaggi

- Migliore utilizzo delle risorse di risorse naturali
- Riduzione del rischio legale e operativo
- Aumento della credibilità e della fiducia
- Miglioramento delle relazioni con comunità e istituzioni



# SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI ISO 27001



## SISTEMI DI GESTIONE

### ISO 27001

ISO 27001 definisce un approccio sistematico per l'attuazione di un sistema di gestione della sicurezza capace di assicurare l'integrità, la riservatezza e la disponibilità delle informazioni. Lo standard fornisce un framework di riferimento per l'implementazione di idonee contromisure organizzative atte a impedire la perdita, l'esposizione o il furto di informazioni sensibili e di business a seguito di intrusioni informatiche, errori e accessi interni non autorizzati.

Lo standard ISO/IEC 27001 è una norma internazionale che definisce i requisiti di un Sistema di Gestione della Sicurezza delle Informazioni, in particolare per gli aspetti della sicurezza fisica, logica ed organizzativa (Information Security Management System – ISMS).

L'obiettivo dello standard è quello di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità. Inoltre lo standard ISO 27001 fornisce i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (SGSI) finalizzato ad una corretta utilizzazione dei dati sensibili dell'azienda.

#### Obiettivi

- Protezione del patrimonio informativo
- Rispetto dei requisiti contrattuali e normativi

#### Vantaggi

- Riduzione del rischio legale e operativo associato alla violazione dei dati
- Miglioramento organizzativo
- Aumento della credibilità e della fiducia



AVVERA Srl

MILANO  
ROMA  
UDINE  
PESARO

Largo Umberto Boccioni 1  
21040 Origgio VA  
tel. 02 96515401  
fax 02 96515499

[www.avvera.it](http://www.avvera.it)  
[info@avvera.it](mailto:info@avvera.it)



**ISO 9001**  
Cert.N. 9175.PITC



**ISO/IEC 27001**  
Cert.N° 9194.PIT2



**ISO 45001**  
Cert.N. 9192.AVRA

