MR | Academy

Offerta formativa Legal 2025

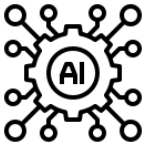
I nostri servizi di aggiornamento normativo
in ambito Data Protection, TMT e Intelligenza Artificiale

La nostra proposta di aggiornamento legal riguarda i seguenti ambiti:

«Data Protection»

«TMT»

«Intelligenza Artificiale»



Il nostro approccio

Caratteristica distintiva dei nostri corsi di aggiornamento è il loro **approccio eminentemente pratico**, basato sull'esperienza dei relatori: i partecipanti hanno modo di apprendere non solo la teoria, ma anche come applicarla efficacemente nel contesto specifico della loro organizzazione.
Inoltre, incoraggiamo un dialogo aperto e costruttivo, dove domande specifiche e sfide organizzative dei partecipanti possono essere esplorate e risolte insieme, rendendo questi corsi non solo un'esperienza formativa, ma anche un'opportunità di crescita e adattamento diretto alle esigenze aziendali.

Modalità di erogazione

Sistema FLEXI & Multimedia

Lezioni **in presenza** o in **videoconferenza**, con invio preliminare dei materiali per aumentare l'efficacia e stimolare l'approfondimento.

La **durata** di ogni corso può essere calibrata **in funzione del grado di approfondimento** che ogni Azienda ritiene funzionale alle proprie esigenze.

È possibile **adeguare i contenuti** in relazione alle necessità dell'Azienda che ha richiesto il corso.

Al termine di ogni corso è previsto un momento di **confronto su casi pratici**, dubbi ed eventuali domande, con il rilascio di un attestato di frequenza o di un attestato al superamento di un test, a seconda delle esigenze aziendali.

Tailor-made approach

Il nostro team di esperti è a disposizione per elaborare una **proposta formativa personalizzata**, sulla base della specifica realtà aziendale.

I corsi possono essere erogati a **tutto il personale aziendale**. Il contenuto di ogni modulo, infatti, può essere adattato in modo da soddisfare le specifiche esigenze aziendali, quali, ad esempio, la necessità di accrescere o aggiornare il livello di conoscenza di tutto il personale su una specifica tematica trasversale (anche in un'ottica di accountability), o consentire a funzioni aziendali specializzate di aggiornare o approfondire le proprie competenze.

Ove necessario, è previsto un **pre-assessment** volto a comprendere meglio le peculiarità dell'organizzazione aziendale e a elaborare una proposta formativa che sia realmente utile e ritagliata sulle esigenze di ogni cliente.

I nostri corsi di formazione sono progettati per fornire ai partecipanti una **conoscenza approfondita delle tematiche** legali connesse alle peculiarità della società richiedente. L'**approccio tailor-made** garantisce che la formazione sia anche un'occasione di consulenza, che fornisce ai partecipanti gli strumenti necessari per applicare le conoscenze acquisite al loro business.

MR | Academy

Data Protection

Introduzione

Considerando l’utilizzo sempre maggiore di dati personali da parte delle società, da ultimo anche per lo sviluppo e l’implementazione di sistemi di intelligenza artificiale, e l’attenzione posta dalle Autorità di controllo al rispetto della normativa applicabile in materia di protezione dei dati personali, risulta fondamentale avere chiari gli obblighi e gli adempimenti che le società devono porre in essere, in qualità di titolari e responsabili del trattamento.

Per soddisfare le esigenze di formazione continuativa nel campo della protezione dei dati personali, presentiamo, pertanto, dei corsi di aggiornamento modulari, ideali per DPO e personale di alcune funzioni aziendali.

Il programma offre un'esperienza coinvolgente, suddivisa in moduli e possibilità di integrazione, che consente ai partecipanti di personalizzare il percorso formativo in base alle proprie esigenze aziendali.

A chi è rivolto

- ❑ Funzione DPO
- ❑ Privacy Manager, Privacy Specialist, Data Scientist, CIO e CDO
- ❑ Funzioni apicali, referenti privacy e altre funzioni che ricoprono un ruolo nella governance e nel sistema di gestione e protezione dei dati aziendale
- ❑ Funzione marketing
- ❑ Funzione HR
- ❑ Funzione Procurement
- ❑ Tutto il personale aziendale, etc.

Obiettivi formativi

- ❑ Comprendere la normativa in materia di protezione dei dati personali
- ❑ Identificare i rischi connessi al trattamento dei dati personali e le misure di sicurezza tecniche e organizzative da adottare, anche in caso di sviluppo e/o implementazione di sistemi di IA
- ❑ Gestire i processi di trattamento dei dati personali in modo conforme alla normativa

Moduli e argomenti

1 – GDPR: principi generali

- ❑ Principi e regole per il trattamento dei dati personali nel nuovo quadro normativo europeo e nazionale;
- ❑ panoramica del GDPR:
  - principali definizioni tecniche fornite dal GDPR;
  - trattamento di dati personali comuni, di categoria particolare e giudiziari;
  - ruoli e i rapporti tra i vari soggetti, interni ed esterni al contesto aziendale, coinvolti nei trattamenti di dati personali e principali obblighi connessi;
  - principi di accountability e di privacy by design e by default;
  - principali obblighi in capo al titolare del trattamento;
  - profili sanzionatori.

2 – Il DPO: mansioni e profili rilevanti, in base alla normativa italiana ed europea

- ❑ La figura del DPO:
  - inquadramento normativo e linee guida dell'EDPB applicabili in materia;
  - designazione del DPO (possibili configurazioni e risorse a disposizione);
  - qualifiche, competenze e posizione del DPO;
  - necessità di nomina in caso di utilizzo di sistemi di IA;
  - funzione e compiti del DPO, anche con riferimento allo specifico contesto aziendale;
  - certificazione UNI ISO.
- ❑ I compiti del DPO:
  - funzioni organizzative;
  - supporto nella predisposizione e aggiornamento del registro delle attività di trattamento;
  - funzioni di controllo e funzioni consultive;
  - rapporti con il titolare, le Autorità e gli interessati;
  - valutazione dei rischi posti dalle attività di trattamento svolte dalla società, ivi compresa l’implementazione di sistemi di IA e checklist dell’EDPB per l’audit dei sistemi di IA;
  - coinvolgimento nella gestione dei trattamenti che possono comportare un rischio elevato: la DPIA;
  - coinvolgimento nella gestione dei data breach;
  - compiti di indagine del DPO – pianificazione degli audit;
  - compiti di informazione e sensibilizzazione interna ed esterna;
  - flussi informativi interni alla società tra il DPO e le altre funzioni aziendali.

3 – Il trattamento dei dati personali nell’ambito delle attività di HR

- Inquadramento normativo – Autorizzazione generale del Garante Privacy n. 1/2016 e Statuto dei lavoratori;
- trattamenti dei dati personali nelle differenti fasi del ciclo lavorativo del dipendente (selezione, assunzione e cessazione del rapporto di lavoro);
- raccolta e trattamento dei dati contenuti nei curricula;
- modalità di trattamento dei dati di categoria particolare dei dipendenti;
- profili in tema di protezione dei dati personali in caso di smart working, nonché in caso di utilizzo e/o implementazione di sistemi di AI nel contesto lavorativo;
- qualificazioni soggettive ai fini privacy di specifiche figure (ad es. medico competente, RSPP, agenzie di somministrazione e lavoratori somministrati, società di head hunting, etc.);
- funzioni di supporto e controllo, consultive, formative e informative del DPO.

4 – Il trattamento di dati personali nell’ambito di attività di marketing

- Inquadramento normativo e linee guida del Garante Privacy e dell'EDPB applicabili in materia;
- adempimenti privacy in caso di svolgimento di attività di marketing, anche mediante canali digitali, nonché tramite l’utilizzo di sistemi di IA;
- disamina dei possibili rischi in materia di protezione dei dati personali connessi all’utilizzo e/o all’implementazione di sistemi di IA nelle attività di marketing;
- adempimenti privacy in caso di attività di profilazione volta a migliorare la promozione e la comunicazione pubblicitaria della società;
- comunicazioni di dati personali a livello infragruppo per finalità di marketing e profilazione;
- presentazione di casi pratici che illustrino l’applicazione della normativa privacy nell’utilizzo di specifici strumenti di IA (chatbot, raccomandazioni personalizzate, analisi dei sentiment, ecc.);
- funzioni di supporto e controllo, consultive, formative e informative del DPO.

5 – Data Breach: adempimenti, previsioni normative e procedure da osservare e coinvolgimento del DPO

- ❑ Inquadramento normativo e linee guida dell'EDPB applicabili in materia;
- ❑ definizione di data breach;
- ❑ accertamento, riconoscimento e valutazione di un data breach;
- ❑ ragioni per le quali si verifica un data breach;
- ❑ gestione di un data breach, procedura e notificazione al Garante Privacy e/o agli interessati in caso di data breach;
- ❑ funzioni coinvolte o da coinvolgere nell'ambito della gestione di un data breach;
- ❑ funzioni di supporto e controllo, consultive, formative e informative del DPO;
- ❑ esempi di sanzioni del Garante Privacy in caso di data breach;
- ❑ rischio di violazione dei dati trattati con sistemi di IA e ruolo dell’IA nella prevenzione, rilevamento e risoluzione delle violazioni;
- ❑ politiche di sicurezza informatica, piani di risposta agli incidenti, business continuity e disaster recovery, penetration test e formazione del personale.

6 – Data Protection Impact Assessment (DPIA) e coinvolgimento del DPO

- ❑ Inquadramento normativo e linee guida dell'EDPB applicabili in materia;
- ❑ definizione di DPIA; rapporti con la FRIA nell’ambito dei sistemi di IA ad alto rischio;
- ❑ casi di obbligatorietà;
- ❑ tempistiche, svolgimento e responsabile dello svolgimento della DPIA;
- ❑ consultazione preventiva con l'Autorità di controllo;
- ❑ funzioni di supporto e controllo, consultive, formative e informative del DPO.

7 – Privacy by design & Privacy by default

- ❑ Inquadramento normativo e linee guida dell'EDPB applicabili in materia;
- ❑ implementazione di un nuovo prodotto/servizio (anche di un sistema di IA) in un'ottica di privacy by design e di privacy by default e policy di pre-audit dei responsabili del trattamento;
- ❑ provvedimenti delle Autorità di controllo competenti e casi pratici di applicazione nel contesto aziendale;
- ❑ qualificazione privacy dei soggetti coinvolti;
- ❑ funzioni di supporto e controllo, consultive, formative e informative del DPO.

8 – Diritti degli interessati ai sensi del GDPR e il coinvolgimento del DPO

- ❑ Inquadramento normativo e linee guida dell'EDPB applicabili in materia;
- ❑ ruolo del DPO nell'ambito della gestione delle richieste degli interessati;
- ❑ funzioni di supporto e controllo, consultive, formative e informative del DPO.
- ❑ disamina dei diritti degli interessati ai sensi degli artt. 15-22 del GDPR:
  - diritto di accesso;
  - diritto di rettifica;
  - diritto di cancellazione;
  - diritto di limitazione del trattamento;
  - diritto alla portabilità dei dati;
  - diritto di opposizione;
  - diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione.
- ❑ esercizio dei diritti degli interessati in caso di utilizzo e/o implementazione di sistemi di IA.

9 – Obblighi e garanzie in tema di trasferimenti di dati in Paesi extra UE e infragruppo

- ❑ Inquadramento normativo e condizioni richieste per il trasferimento dei dati in Paesi extra UE;
- ❑ trasferimenti infragruppo e trasferimenti di dati personali verso altre società del gruppo o non aventi sede in Paesi extra UE;
- ❑ trasferimenti da e verso gli Stati Uniti: il Data Privacy Framework;
- ❑ misure da adottare in caso di trasferimenti;
- ❑ funzioni di supporto e controllo, consultive, formative e informative del DPO.

10 – Regolamento sull'utilizzo degli strumenti IT: adempimenti connessi all'utilizzo della posta elettronica aziendale e coinvolgimento del DPO

- Definizione e criteri di utilizzo degli strumenti informatici;
- gestione delle comunicazioni telematiche (posta elettronica, rete Internet e social media);
- procedura ad hoc per l'utilizzo degli strumenti informatici e dei sistemi di IA generativa;
- funzioni di supporto e controllo, consultive, formative e informative del DPO.
- Focus sulla posta elettronica:
  - regole di utilizzo della posta elettronica;
  - accesso alla casella di posta elettronica del lavoratore assente (assenze prolungate e programmate, assenze non programmate e nomina di un fiduciario);
  - cessazione del rapporto di lavoro e sorti della casella di posta elettronica dell'ex dipendente;
  - disattivazione e cancellazione della casella di posta elettronica dell'ex dipendente;
  - controllo a distanza dei dipendenti: divieti, deroghe e adempimenti giuslavoristici e privacy;
  - conservazione dei metadati delle e-mail aziendali.

11 – Figure di data governance aziendale

- Introduzione alla data governance e ruolo strategico all'interno delle organizzazioni;
- ruoli e delle responsabilità delle figure di data governance con focus sulle figure coinvolte; utilità delle figure di data governance aziendale;
- modelli organizzativi e tecnologici di gestione dei dati; gestione dei rischi e degli incidenti informatici;
- approfondimento dei processi di governance dei dati, dalla raccolta alla gestione e alla distribuzione:
- panoramica su strumenti e tecnologie a supporto delle aziende per facilitare l'implementazione e il mantenimento di una robusta data governance;
- analisi delle possibili misure di tutela da adottare per garantire la qualità dei dati;
- adempimenti da porre in essere per garantire la conformità alla normativa in materia di privacy;
- misure da adottare per migliorare l'efficienza operativa dell'azienda attraverso una gestione più efficace dei dati;
- attività per identificare e mitigare i rischi associati alla gestione inadeguata dei dati.

12 – Whistleblowing e tutela dei dati personali

- Introduzione al whistleblowing e nuovi obblighi in materia a seguito del D.lgs. 24/2023;
- diritti e tutele dei soggetti segnalanti e segnalati in base alla disciplina sulla protezione dei dati personali;
- GDPR e principio di accountability;
- adempimento degli obblighi informativi ex artt. 13 e 14 del GDPR nei confronti di soggetti segnalanti e altri soggetti coinvolti;
- definizione di un canale di segnalazione nel rispetto dei principi previsti dal GDPR, tra cui il principio di privacy by design e by default;
- gruppi di imprese e condivisione del canale di segnalazione:
- misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato e volte a tutelare la riservatezza del segnalante, l’integrità e la confidenzialità dei dati personali oggetto di segnalazione;
- svolgimento di una valutazione di impatto sulla protezione dei dati ex art. 35 del GDPR per adeguare le misure tecniche e organizzative agli specifici rischi derivanti dai trattamenti;
- ruoli e responsabilità dei soggetti coinvolti nel trattamento dei dati personali nell’ambito del whistleblowing;
- nomina di eventuali fornitori esterni ex art. 28 del GDPR e dei soggetti interni, competenti e specificamente formati per la gestione del canale interno di segnalazione, ex artt. 29 e 32 del GDPR e art. 2-quaterdecies del Codice Privacy;
- divieto di utilizzo delle segnalazioni, se non per darvi seguito, per rivelare l’identità del segnalante a soggetti diversi da quelli specificatamente nominati, salvo consenso espresso del segnalante;
- periodo di conservazione della documentazione inerente la segnalazione per il tempo necessario al trattamento della segnalazione;
- funzioni di supporto e controllo, consultive, formative e informative del DPO.

MR | Academy

TMT

Introduzione

La tecnologia è in continua evoluzione e le società, considerando il sempre più crescente spostamento verso il mondo digitale, devono essere in grado di stare al passo con i tempi per rimanere competitive. Un corso modulare sui profili legali connessi allo sviluppo o all’utilizzo di tecnologia nell’ambito del proprio business può fornire alle aziende le conoscenze e le competenze necessarie per comprendere le ultime tendenze tecnologiche e i rispettivi profili regolatori, in modo tale da implementarle in modo efficace.

Per soddisfare le esigenze aziendali nei diversi campi tecnologici, presentiamo, pertanto, un corso modulare e integrabile, ideale per tutti coloro che vogliono ampliare o aggiornare il proprio livello di conoscenza.

A chi è rivolto

- ❑ Imprese di qualsiasi dimensione e settore che desiderano ampliare e migliorare il proprio business attraverso la creazione e gestione di piattaforme digitali
- ❑ Digital Product Manager, Data Scientist, Manager ICT, CIO e CDO
- ❑ Responsabili e-commerce e manager aziendali che si occupano di e-commerce
- ❑ Responsabili marketing
- ❑ Manager aziendali

Obiettivi formativi

- ❑ Comprendere i requisiti legali e regolatori applicabili alla creazione e gestione di piattaforme digitali e/o alle attività di marketing
- ❑ Identificare i rischi legali connessi alla creazione e gestione di piattaforme digitali e/o alle attività di marketing
- ❑ Migliorare la conformità delle piattaforme digitali e/ delle attività di marketing alla normativa applicabile

Moduli e argomenti

1 – Creazione di piattaforme digitali e profili legali

- ❑ Inquadramento normativo e linee guida;
- ❑ panoramica sulla normativa nazionale ed europea applicabile (D. lgs. 70/2003, Digital Services Act e Digital Markets Act);
- ❑ principi generali e principali obblighi normativi, nonché obblighi specifici in base al tipo di servizi forniti;
- ❑ regole e condizioni che i titolari di piattaforme digitali devono rispettare;
- ❑ contrattualistica digitale con analisi dei contratti fondamentali per la creazione e gestione di piattaforme digitali;
- ❑ profili di proprietà intellettuale con analisi della protezione e gestione dei diritti di proprietà intellettuale nel contesto digitale, compresi marchi, brevetti e diritto d'autore (compresi i profili relativi ad attività quali il web scraping e il text and data mining da parte di sistemi di IA);
- ❑ profili di privacy e sicurezza dei dati con analisi della normativa in materia di protezione dei dati personali e delle best practice.

2 – E-Commerce: Profili legali e fiscali

- ❑ Inquadramento normativo e linee guida;
- ❑ panoramica sui regolamenti europei (Digital Services Act, Product Liability Directive e Regolamento Geoblocking);
- ❑ analisi delle opzioni di struttura per un sito e-commerce (B2B, B2C, C2C), con relativo approfondimento delle regolamentazioni applicabili allo specifico contesto aziendale;
- ❑ contrattualistica e termini e condizioni di utilizzo con analisi dei contratti e delle condizioni d'uso rilevanti;
- ❑ profili di proprietà intellettuale con focus sulla tutela di marchi e diritti d'autore associati al sito e-commerce;
- ❑ profili di protezione dei dati personali e sicurezza dei dati con analisi degli adempimenti da porre in essere;
- ❑ profili di fiscalità dell'e-commerce con analisi delle implicazioni fiscali specifiche per le attività di e-commerce;
- ❑ profili di tutela del consumatore e obblighi informativi dovuti sulla base del D.lgs. 70/2003 (c.d. Decreto e-commerce) e obblighi previsti dal D.lgs. 206/2005 (c.d. Codice del consumo).

3 – Profili legali connessi ad iniziative di marketing

- Inquadramento normativo e linee guida applicabili in materia;
- analisi della contrattualistica connessa alle attività di marketing con approfondimento dei contratti di influencer marketing, sponsorizzazione e co-branding;
- panoramica della regolamentazione di settore (ad es. D. Lgs. 206/2005, Regolamento «Digital Chart»), linee guida delle autorità applicabili e gli adempimenti da porre in essere in caso di specifiche iniziative (ad es. normativa applicabile agli influencer, concorsi a premio e programmi fedeltà);
- profili in materia di protezione dei dati personali con approfondimento dell'inquadramento normativo e linee guida del Garante Privacy e dell'EDPB applicabili in materia;
- adempimenti privacy in caso di svolgimento di attività di marketing, anche mediante canali digitali (in particolare, informativa e consenso, gestione dei consensi e rinnovi);
- adempimenti privacy in caso di attività di profilazione volta a migliorare la promozione e la comunicazione pubblicitaria della società;
- profili regolatori in caso di svolgimento di attività di marketing con l’utilizzo e/o l’implementazione di sistemi di IA;
- sfide e criticità con identificazione e gestione dei rischi legali (ivi compresi quelli legati all’utilizzo di sistemi di IA e tutela dei consumatori) connessi alle attività di marketing.

4 – Cybersicurezza

- Ambito di applicazione del D. Lgs. 138/2024 che ha recepito la Direttiva (UE) 2555/2022 (c.d. «NIS2»);
- criteri per l’individuazione dei soggetti cui si applicano precisi obblighi di sicurezza informatica;
- obbligo di registrazione e aggiornamento di specifici soggetti;
- obblighi in materia di gestione del rischio per la sicurezza informatica e, in particolare, misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi alla sicurezza di sistemi informativi e di rete;
- procedura di notifica di incidenti;
- profili sanzionatori;
- attività di formazione e sensibilizzazione del personale.

5 – Sicurezza digitale nel settore finanziario

- Inquadramento normativo e ambito di applicazione con focus sul Regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario (c.d. «DORA»);
- adempimenti e obblighi previsti dalla normativa;
- quadro di governance e organizzazione interna che garantisca una gestione efficace e prudente di tutti i rischi ICT;
- utilizzo e aggiornamento di sistemi, protocolli e strumenti di TIC (tecnologie dell’informazione e della comunicazione) idonei, affidabili, dotati di capacità sufficiente per elaborare i dati e resilienti;
- piano per la gestione dei rischi informatici;
- strategia di resilienza digitale in materia di business continuity e disaster recovery;
- classificazione degli incidenti connessi ai fornitori ICT e delle minacce informatiche;
- profili sanzionatori;
- attività di formazione del personale.

MR | Academy

AI

Intelligenza Artificiale e profili legali

Introduzione

Considerando l'impiego sempre più diffuso dei sistemi di intelligenza artificiale («IA») da parte delle aziende e di tutti i soggetti, presentiamo un programma di formazione all'avanguardia e mirato.

Il corso è stato appositamente sviluppato per assistere le aziende nella comprensione dei profili legali connessi all'implementazione, allo sviluppo e all'utilizzo di queste nuove tecnologie.

Il programma offre un'esperienza coinvolgente, suddivisa in moduli e possibilità di integrazione, che consente ai partecipanti di personalizzare il percorso formativo in base alle proprie esigenze aziendali.

A chi è rivolto

- ❑ Società e manager aziendali che implementano o intendono implementare sistemi di IA
- ❑ Società che utilizzano e/o implementano sistemi di IA
- ❑ Società che sviluppano, forniscono e/o importano sistemi di IA
- ❑ Responsabili legali e compliance di società che utilizzano sistemi di IA
- ❑ Digital Product Manager, Data Scientist, Manager ICT, CIO e CDO

Obiettivi formativi

- ❑ Analizzare e comprendere l’attuale quadro normativo in materia di IA
- ❑ Comprendere gli obblighi legali in caso di sistemi di IA (responsabilità civile, da prodotto difettoso, IP, data protection, marketing e HR)
- ❑ Identificare i rischi legali connessi all'uso di sistemi di IA
- ❑ Migliorare la conformità dell'azienda alla normativa applicabile

Moduli e argomenti

1 – Il Regolamento UE sull’IA

- ❑ Introduzione al Regolamento (UE) 1689/2024, noto come «AI Act»;
- ❑ oggetto e finalità dell'AI Act;
- ❑ ambito di applicazione oggettivo e soggettivo della normativa;
- ❑ definizioni chiave contenute nella normativa;
- ❑ individuazione dei soggetti definiti dall’AI Act;
- ❑ tipologie di sistemi dell’IA;
- ❑ pratiche di IA vietate e relative eccezioni;
- ❑ classificazione dei sistemi di IA ad alto rischio;
- ❑ requisiti per i sistemi di IA ad alto rischio quale presupposto per la sua immissione sul mercato e messa in servizio (ad es. valutazioni d'impatto sui diritti umani obbligatorie, misure di mitigazione del rischio, set di dati di alta qualità, standard di robustezza, accuratezza e sicurezza informatica);
- ❑ obblighi di trasparenza per determinati sistemi di IA;
- ❑ obblighi riguardanti i modelli di IA per finalità generali;
- ❑ ruolo delle autorità nazionali competenti e loro poteri in qualità di autorità di vigilanza;
- ❑ obbligo di monitoraggio successivo all'immissione sul mercato effettuato dai fornitori;
- ❑ piano di monitoraggio successivo all'immissione sul mercato per i sistemi di IA ad alto rischio;
- ❑ obbligo di segnalazione di incidenti gravi o malfunzionamenti dei sistemi di IA;
- ❑ linee guida e altri provvedimenti applicabili in materia (compreso l’AI Pact);
- ❑ attività di formazione del personale idonea a garantire un livello sufficiente di alfabetizzazione in materia di IA, ai sensi dell’AI Act;
- ❑ valutazione di sistemi di governance e controllo interno con coinvolgimento di varie funzioni aziendali;
- ❑ profili sanzionatori.

Moduli e argomenti

2 – Focus: Adempimenti e obblighi per sistemi di IA ad alto rischio

- ❑ Requisiti per i sistemi di IA ad alto rischio:
  - ❑ sistema di gestione dei rischi, obblighi e misure di gestione degli stessi;
  - ❑ dati e governance dei dati, nonché criteri di qualità dei set di dati;
  - ❑ condizioni da rispettare in caso di trattamento di categorie particolari di dati;
  - ❑ tempistiche, modalità di redazione e contenuto minimo della documentazione tecnica;
  - ❑ conservazione delle registrazioni;
  - ❑ trasparenza, informazioni e istruzioni per l’uso ai deployer;
  - ❑ sorveglianza umana durante il periodo in cui i sistemi di IA sono in uso;
  - ❑ livello di accuratezza, robustezza e cybersicurezza, nonché connessi obblighi e adempimenti.
- ❑ obblighi per i fornitori di sistemi di IA ad alto rischio:
  - ❑ sistema di gestione della qualità e sua documentazione;
  - ❑ conservazione dei documenti;
  - ❑ log generati automaticamente e loro conservazione;
  - ❑ misure correttive e dovere di informazione;
  - ❑ cooperazione con le autorità competenti;
  - ❑ rappresentanti autorizzati dei fornitori dei sistemi di IA ad alto rischio.
- ❑ obblighi per gli importatori di sistemi di IA ad alto rischio;
- ❑ obblighi per i distributori di sistemi di IA ad alto rischio;
- ❑ obblighi dei deployer dei sistemi di IA ad alto rischio e di altre parti;
- ❑ responsabilità lungo la catena del valore dell’IA;
- ❑ valutazione d’impatto sui diritti fondamentali per i sistemi di IA ad alto rischio («FRIA»);
- ❑ dichiarazione di conformità UE, marcatura CE e registrazione dei sistemi di IA ad alto rischio.

Moduli e argomenti

3 – Fundamental Rights Impact Assessment (FRIA) per I sistemi di IA ad alto rischio

- ❑ Definizione di FRIA e sua importanza, nonché rapporti con la DPIA nell’ambito della normativa in materia di protezione dei dati personali;
- ❑ casi di obbligatorietà ed eccezioni;
- ❑ tempistiche e modalità di svolgimento della FRIA;
- ❑ contenuto della FRIA;
- ❑ notifica all’autorità di vigilanza del mercato dei risultati della FRIA e casi di esenzione.

4 – Determinati sistemi di IA e modelli di IA per finalità generali

- ❑ Obblighi di trasparenza per i fornitori di determinati sistemi di IA, compresi i sistemi di IA generativa;
- ❑ obblighi di trasparenza per i deployer di determinati sistemi di IA, compresi i sistemi di IA generativa;
- ❑ modelli di IA per finalità generali con rischio sistemico;
- ❑ procedura di notifica alla Commissione;
- ❑ obblighi dei fornitori di modelli di IA per finalità generali con rischio sistemico;
- ❑ obblighi dei fornitori di modelli di IA per finalità generali;
- ❑ rappresentanti autorizzati dei fornitori di modelli di IA per finalità generali;
- ❑ gestione delle richieste da parte delle autorità;
- ❑ casi pratici, best practice e overview di framework da considerare per effettuare valutazioni di rischi e misure (e.g. General-Purpose AI Code of Practice);
- ❑ procedura aziendale ad hoc per l'utilizzo dei sistemi di IA generativa.

Moduli e argomenti

5 – IA e cybersecurity

- ❑ Introduzione ai campi di utilizzo dei sistemi di IA nell’ambito della cybersecurity;
- ❑ linee guida a cui ha aderito l’Agenzia italiana per la cybersicurezza nazionale atte a garantire resilienza, privacy, correttezza ed affidabilità dei sistemi di IA;
- ❑ minacce legate ai sistemi di IA;
- ❑ utilizzo dei sistemi di IA per scopi malevoli (creazione di deep fake, attacchi informatici, data breach, etc.);
- ❑ misure di sicurezza per i sistemi di IA;
- ❑ casi pratici e best practices;
- ❑ altre normative applicabili in materia (e.g. NIS2).

6 – IA e profili in materia di responsabilità civile

- ❑ Tutela fornita dall'attuale sistema normativo europeo e nazionale in materia di responsabilità civile;
- ❑ sfide e criticità che i sistemi di IA pongono alle attuali norme in materia di responsabilità civile;
- ❑ disposizioni applicabili contenute all’interno dell’AI Act, in caso di incidenti gravi;
- ❑ possibile imputazione della responsabilità civile risarcitoria ai soggetti coinvolti nell'uso dei sistemi di IA (ruoli, funzioni e conseguenze);
- ❑ necessità di adattamento degli attuali principi di responsabilità civile ai sistemi di IA;
- ❑ disamina della proposta di direttiva europea relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'IA (c.d. «AI Liability Directive»).

7 – IA e profili in materia di responsabilità per danno da prodotto difettoso

- ❑ Tutela fornita dall'attuale sistema normativo europeo (e, in particolare, la Direttiva (UE) 2024/2853, nota come Product Liability Directive o «PLD»);
- ❑ oggetto e finalità della PLD;
- ❑ ambito di applicazione della normativa;
- ❑ definizioni chiave contenute nella normativa e ruolo dell’IA nella PLD;
- ❑ novità introdotte dalla PLD;
- ❑ aspetti procedurali per le richieste del risarcimento del danno in caso di danni causati da qualsiasi tipo di sistema di IA e onere della prova;
- ❑ punti di contatto con l’AI Act.

8 – IA e profili in materia di privacy e data protection;

- ❑ Quadro normativo di riferimento e, in particolare, GDPR e Codice Privacy;
- ❑ principi generali e principali obblighi normativi in materia di privacy;
- ❑ panoramica dei principali provvedimenti e linee guida emanati dalle Autorità di controllo nazionali (Garante Privacy) ed europee (EDPB), anche in relazione ai sistemi di IA e audit;
- ❑ principali definizioni tecniche fornite dal GDPR, nonché principi di accountability e privacy by design applicati ai sistemi di IA;
- ❑ principali obblighi in capo al titolare del trattamento;
- ❑ sfide e criticità legate al trattamento dei dati nell'utilizzo di sistemi di IA (ivi compresa individuazione di idonea base giuridica in caso elaborazione di dati personali);
- ❑ misure di sicurezza tecniche e organizzative da adottare in caso di utilizzo di sistemi di IA;
- ❑ profili sanzionatori.

9 – IA e profili connessi alle attività di marketing

- ❑ Inquadramento normativo e linee guida applicabili in materia;
- ❑ adempimenti privacy in caso di svolgimento di attività di marketing, anche mediante canali digitali (ad es. informativa privacy, raccolta/gestione e rinnovo del consenso) o in caso di attività di profilazione;
- ❑ panoramica sui possibili utilizzi dei sistemi di IA nelle attività di marketing;
- ❑ obblighi di trasparenza in caso di output generati o manipolati da sistemi di IA generativa previsti dall’AI Act;
- ❑ obblighi, adempimenti e rischi in caso di utilizzo di sistemi di IA nelle attività di marketing;
- ❑ sfide e criticità connesse all'uso di sistemi di IA nelle attività di marketing e tutela dei consumatori;
- ❑ panoramica dei pareri e dei provvedimenti delle autorità giurisdizionali e di controllo sul tema.

10 – IA e profili in materia di diritto d'autore

- ❑ Quadro normativo di riferimento e, in particolare, legge sul diritto d'autore;
- ❑ panoramica della tutela prevista per le opere dell'ingegno creativo e le opere derivate;
- ❑ diritti riconosciuti in capo all'autore (diritti morali e patrimoniali);
- ❑ impatto dell'AI Act sui profili di proprietà intellettuale collegati all'utilizzo di sistemi di IA, anche generativa;
- ❑ sfide e criticità legate all'utilizzo dell'IA (anche generativa) in contesti creativi;
- ❑ eccezioni alla violazione del diritto d'autore (ad es. con il «text and data mining») e modalità per evitare che ciò avvenga;
- ❑ panoramica su recenti pronunce giurisprudenziali (anche di Paesi extra-UE) relative ai diritti di proprietà intellettuale in caso di uso di sistemi di IA;
- ❑ disamina di casi pratici.

11 – IA e profili legali connessi al suo utilizzo nel contesto lavorativo

- Quadro normativo di riferimento e, in particolare, AI Act, GDPR, Statuto dei Lavoratori e provvedimenti del Garante Privacy (cfr. Autorizzazione generale del Garante Privacy n. 1/2016) e dell'EDPB sul trattamento dei dati personali dei dipendenti da parte dei lavoratori; panoramica sui possibili utilizzi dell'IA nel contesto lavorativo;
- sfide e criticità connesse all'uso di sistemi di IA nel contesto lavorativo con focus sugli obblighi e adempimenti ai sensi dell’AI Act (ad es. selezione del personale attraverso algoritmi di machine learning o sistemi di Affective Computing; monitoraggio dei dipendenti; controlli aziendali; misurazione delle prestazioni dei dipendenti), nonché sui profili privacy;
- trattamenti dei dati personali con sistemi di IA nelle differenti fasi del ciclo lavorativo del dipendente (selezione, assunzione e cessazione del rapporto di lavoro) e classificazione dei sistemi secondo l’AI Act.

Coordinatore dei corsi

Avv. Carlo Impalà

Partner e Responsabile Dip. TMT & Data Protection

Carlo.Impala@MorriRossetti.it

Prima di collaborare con lo Studio, l'Avv. Carlo Impalà ha maturato diverse esperienze in primari studi internazionali, sia in Italia che all'estero, nonché presso l'Ufficio Cooperazione Giudiziaria della Rappresentanza Permanente d'Italia all'UE a Bruxelles (BE).

Esperto di **AI, Data e Technology**, è **Responsabile del Dipartimento di TMT e Data Protection**, all'interno del quale si occupa prevalentemente di diritto commerciale e predisposizione ed implementazione di modelli di **corporate governance e compliance aziendale** (soprattutto in materia di data protection e IA), nonché di normativa applicabile in materia di internet, IT e technology, AI, media ed editoria online, privacy e protezione dei dati personali, telecomunicazioni, diritto d'autore.

È membro del **'Comitato Digitalizzazione' dello Studio**, occupandosi di tutte le tematiche che riguardano lo sviluppo tecnologico e digitale, inclusa l'integrazione di sistemi di IA nell'attività dei Professionisti.

Possiede diverse certificazioni, tra cui quella di Data Protection Officer e di CIPP/E (Certified Information Privacy Professional Europe) rilasciata da IAPP, nonché diversi attestati di competenza nelle aree "Data Protection Officer: Area Data Security" e "Sistema privacy in azienda: le attività di audit" rilasciati da TÜV Italia.

Ricopre il ruolo di **DPO esterno in diverse aziende**.

È socio ordinario di Federprivacy, di IAPP, AssoDPO e di Assofintech, nonché membro del Gruppo di lavoro "GDPR" dell'American Chamber of Commerce in Italia.

È, inoltre, socio ordinario dell'Italian Academy of Internet Code (IAIC).

È **autore di numerosi contributi editoriali** e articoli in materia di **AI, data protection e TMT** (per le testate del Sole 24 Ore, Agenda Digitale, Riskmanagement360.it, etc.), nonché di numerose **guide legali comparative a livello internazionale** per conto di Chambers & Partners e ICLG.

Il nostro sharing knowledge system

MORRI ROSSETTI

The Knowledge Firm

Abbiamo una straordinaria passione per l'approfondimento e la ricerca nell'ambito delle questioni legali e fiscali.
Tutti i team si dedicano con sistematicità allo studio e alla produzione di contenuti perché la «conoscenza» è alla base dell'eccellenza professionale.

6 Editori con cui collaboriamo

15+ Riviste sulle quali scriviamo

500+ Pubblicazioni

Progetto 'Osservatori'

Portali verticali con finalità di conoscenza e di sharing knowledge multi-specializzata.

Uno strumento editoriale che stimola e valorizza l'integrazione di competenze su uno specifico tema per fornire un servizio specialistico "verticale".

9 Portali verticali*

1.000+ Articoli

30.000+ Follower su LinkedIn

*Compliance 231, Restructuring, TMT & Data Protection, Wealth Management, Fiscalità Internazionale, Giustizia Tributaria, Corporate M&A e Labour (questo disponibile anche in inglese) e Riforma Fiscale.

Il nostro Osservatorio TMT & DP

MORRI ROSSETTI

OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti

L'Osservatorio TMT & Data Protection si propone come un supporto e uno strumento utile per chi si trova ad affrontare tematiche connesse al trattamento e alla protezione dei dati personali, nonché in materia di Tecnologia, Media e Telecomunicazioni.

Oltre ad una particolare attenzione rivolta agli ambiti della sanità, del web, delle telecomunicazioni, dei media e delle nuove tecnologie, il progetto si propone l'obiettivo di estendere il perimetro di riferimento a ulteriori industry particolarmente sensibili alle tematiche connesse alla protezione dei dati personali. Al fine di arricchire l'Osservatorio di contributi sempre attuali e pratici Morri Rossetti collabora con professionisti esterni esperti in materia in cybersecurity e digital forensics.

Non smettiamo mai di studiare per fornire un servizio eccellente.

https://www.osservatorio-dataprotection.it/

MORRI ROSSETTI

«Considerate la vostra semenza: fatti non foste a viver come bruti ma per seguire virtute e canoscenza»

(Dante)

Morri Rossetti

Piazza Eleonora Duse, 2 | 20122 Milan (IT) | T +39 02 76 07 971
info@MorriRossetti.it | MorriRossetti.it