MR | Academy

Offerta formativa Legal 2024

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

Corsi legal per aziende - 2024

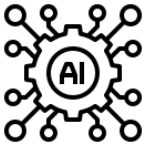
MR

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 / Q&A 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

Corso «Data Protection» 1/7

Introduzione

Considerando l'utilizzo sempre maggiore di dati personali da parte delle società 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 e Privacy Specialist
- ❑ 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
- ❑ Gestire i processi di trattamento dei dati personali in modo conforme alla normativa

MR

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;
  - 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;
  - 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.

Corso «Data Protection» 3/7

MR

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;
- ❑ 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 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;
- ❑ 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;
- ❑ funzioni di supporto e controllo, consultive, formative e informative del DPO.

Corso «Data Protection» 4/7

MR

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 di un *data breach*;
- ❑ ragioni per le quali si verifica un *data breach*;
- ❑ riconoscimento e valutazione di un *data breach*;
- ❑ gestione di un *data breach*;
- ❑ notificazione al Garante Privacy e/o agli interessati in caso di *data breach;*
- ❑ procedura da seguire 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*.

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

- ❑ inquadramento normativo e linee guida dell'EDPB applicabili in materia;
- ❑ definizione di DPIA e sua importanza;
- ❑ 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° Modulo – Privacy by design & Privacy by default

- ❑ inquadramento normativo e linee guida dell'EDPB applicabili in materia;
- ❑ implementazione di un nuovo prodotto/servizio 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.

Corso «Data Protection» 5/7

MR

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.

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 nuovo *Data Privacy Framework*;
- ❑ misure da adottare in caso di trasferimenti;
- ❑ funzioni di supporto e controllo, consultive, formative e informative del DPO.

Corso «Data Protection» 6/7

MR

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;
- 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.

11 – Figure di *data governance* aziendale

- Introduzione alla data governance e ruolo strategico all'interno delle organizzazioni;
- analisi dei 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;
- 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 protezione dei dati personali;
- 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.

Corso «Data Protection» 7/7

MR

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;
- ❑ 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

Corso «TMT» 1/3

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 di attività che desiderano ampliare e migliorare il proprio business attraverso la creazione e gestione di piattaforme digitali
- ❑ Responsabili e-commerce e manager aziendali che si occupano di e-commerce
- ❑ Responsabili marketing
- ❑ Manager aziendali

Obiettivi formativi

- ❑ Comprendere i requisiti legali 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/o delle attività di marketing alla normativa applicabile

Corso «TMT» 2/3

MR

Moduli e argomenti

1 - Creazione di piattaforme digitali e profili legali

- ❑ Inquadramento normativo e linee guida;
- ❑ panoramica sui nuovi regolamenti europei applicabili (Digital Services Act e Digital Markets Act);
- ❑ principi generali e principali obblighi normativi;
- ❑ 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;
- ❑ 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;
- ❑ 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;
- ❑ 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).

Corso «TMT» 3/3

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, 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;
- sfide e criticità con identificazione e gestione dei rischi legali connessi alle attività di marketing.

MR | Academy

Intelligenza Artificiale (IA) e profili legali

Corso «Intelligenza Artificiale» 1/5

Introduzione

Considerando l'impiego sempre crescente dei sistemi di intelligenza artificiale («IA») da parte delle aziende, 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 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 sistemi di IA
- ❑ Responsabili legali e *compliance* di società che utilizzano sistemi di IA

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

MR

Moduli e argomenti

1 – Il Regolamento UE sull'IA

- ❑ Introduzione alla proposta europea di Regolamento Generale sull'IA (c.d. «AI Act»);
- ❑ oggetto e finalità dell'AI Act;
- ❑ ambito di applicazione oggettivo e soggettivo della normativa;
- ❑ definizioni chiave contenute nella normativa;
- ❑ tipologie di sistemi dell'IA;
- ❑ pratiche di IA vietate;
- ❑ classificazione dei sistemi di IA ad alto rischio;
- ❑ requisiti per i sistemi di IA ad altro 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 dei fornitori e degli utenti dei sistemi di IA ad altro rischio e di altre parti;
- ❑ obblighi di trasparenza per determinati sistemi di IA;
- ❑ obblighi riguardano 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;
- ❑ profili sanzionatori.

Corso «Intelligenza Artificiale» 3/5

MR

2 – 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 (inadeguatezza dell'attuale disciplina);
- 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;
- introduzione alla proposta di direttiva europea relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'IA (c.d. «*AI Liability Directive*»);
- applicabilità, definizioni, 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 previsti dall'AI Liability Directive.

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

- tutela fornita dall'attuale sistema normativo europeo;
- sfide e criticità che i sistemi di IA pongono alle attuali norme in materia di responsabilità per danno da prodotto difettoso;
- possibile imputazione della responsabilità per danno da prodotto difettoso ai soggetti coinvolti nella filiera produttiva e che utilizzano sistemi di IA (ruoli, funzioni e conseguenze);
- necessità di adattamento della normativa all'attuale scenario tecnologico e digitale;
- introduzione alla proposta di direttiva europea sulla responsabilità per danno da prodotto difettoso;
- nuova definizione di «*prodotto*»;
- applicabilità, definizioni, 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 previsti dalla proposta di direttiva.

Corso «Intelligenza Artificiale» 4/5

MR

4° Modulo – 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 del GDPR e del Codice della Privacy;
- ❑ panoramica dei principali provvedimenti e linee guida emanati dalle Autorità di controllo nazionali (Garante Privacy) ed europee (EDPB);
- ❑ principali definizioni tecniche fornite dal GDPR;
- ❑ 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;
- ❑ misure di sicurezza tecniche e organizzative da adottare in caso di utilizzo di sistemi di IA;
- ❑ panoramica dei provvedimenti emessi dal Garante Privacy italiano rispetto a sistemi di IA; profili sanzionatori.

5° Modulo – IA e profili connessi alle 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 (ad es. informativa privacy, raccolta/gestione e rinnovo del consenso);
- ❑ adempimenti privacy in caso di attività di profilazione volta a migliorare la promozione e la comunicazione pubblicitaria della società;
- ❑ panoramica sui possibili utilizzi dei sistemi di IA nelle attività di marketing;
- ❑ definizione di neuromarketing;
- ❑ definizione di dati personali e di dati di categoria particolare;
- ❑ sfide e criticità connesse all'uso di sistemi di IA nelle attività di marketing con focus sui profili privacy e tutela dei consumatori;
- ❑ panoramica dei pareri e dei provvedimenti delle autorità giurisdizionali e di controllo sul tema.

Corso «Intelligenza Artificiale» 5/5

MR

6° Modulo – 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;
- ❑ eccezione alla violazione del diritto d'autore (ad es. con il «*text and data mining*»);
- ❑ panoramica su recenti pronunce giurisprudenziali (anche di Paesi extra-UE) relative ai diritti di proprietà intellettuale in caso di uso di sistemi di IA.

7° Modulo – IA e profili legali connessi al suo utilizzo nel contesto lavorativo

- ❑ Quadro normativo di riferimento e, in particolare, 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 sui profili privacy (ad es. selezione del personale attraverso algoritmi di *machine learning*; monitoraggio dei dipendenti; controlli aziendali; misurazione delle prestazioni dei dipendenti);
- ❑ trattamenti dei dati personali con sistemi di IA nelle differenti fasi del ciclo lavorativo del dipendente (selezione, assunzione e cessazione del rapporto di lavoro);
- ❑ raccolta e trattamento dei dati contenuti nei curricula con sistemi di IA.

Coordinatore dei corsi

Avv. Carlo Impalà

Partner e Responsabile Dip. TMT & Data Protection

Carlo.Impala@MorriRossetti.it

Laureato a pieni voti in Giurisprudenza presso l'Università di Palermo, ha frequentato l'Università Georg August di Göttingen e conseguito un LL.M. in *Advanced European Legal Studies* presso il *College of Europe* di Bruges in Belgio.

Ha frequentato un Master executive in materia di Business digitale presso la Business School de Il Sole24Ore, in collaborazione con Netcomm, e conseguito la certificazione di *Data Protection Officer*, nonché gli attestati di competenza nelle aree «*Data Protection Officer: Area Data Security*» e «*Sistema privacy in azienda: le attività di audit*» rilasciati da TÜV Italia. È socio ordinario di diverse associazioni (Federprivacy, IAPP, Assofintech e *Italian Academy of Internet Code*).

È responsabile dell'Osservatorio TMT e Data Protection di Morri Rossetti (www.osservatorio-dataprotection.it), nonché Co-Head del Gruppo *data protection* di FLI (*First Law International*), network internazionale di studi legali.

L'Avv. Impalà ha maturato, inoltre, diverse esperienze professionali in primari studi internazionali, sia in Italia che all'estero.

Si occupa prevalentemente di assistenza stragiudiziale in ambito tmt e data protection e predisposizione ed implementazione di modelli di *corporate governance* e *compliance* aziendale (soprattutto in materia di privacy e *data protection*), nonché di normativa applicabile in materia di internet, editoria *online*, privacy e protezione dei dati personali, pubblicità, TLC, diritto d'autore, *e-commerce*, *information technology*, media e *outsourcing*.

E' autore di numerosi contributi editoriali e articoli in materia di *data protection* e TMT (per le testate Sole 24Ore, IICJ.NET, Agenda Digitale, Riskmanagement360.it, etc.) e ha partecipato in qualità di relatore a numerosi convegni e corsi di formazione e aggiornamento.

Il nostro *sharing knowledge system*

MR

Il Centro Studi

Abbiamo una straordinaria passione per l'approfondimento e la ricerca nell'ambito delle questioni legali e fiscali.
Diversi professionisti lavorano esclusivamente per il Centro Studi, mentre gli altri contribuiscono con regolarità.

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

24.000+ 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

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*.

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 Milano (IT) | T +39 02 76 07 971
info@MorriRossetti.it | MorriRossetti.it