Icmq S.p.A. (A Socio Unico)
Società Benefit
Via G. De Castillia, 10 – 20124 Milano
Tel. 02 7015081 – Fax 02 70150854
icmq@icmq.org – www.icmq.it
P.I. 13218350158

PERCORSO FORMATIVO
INTELLIGENZA ARTIFICIALE
(AI ACT- GDPR – NIS 2 - PRIVACY- VIDEOSORVEGLIANZA E DRONI NELLA VIGILANZA)

- **9 MARZO 2026** | 9:00 – 13:00 | **L'INTELLIGENZA ARTIFICIALE: OLTRE L'ALGORITMO;** *INTRODUZIONE E ANALISI DELL'AI ACT COME FONDAMENTALE DELLA NUOVA ERA REGOLATORIA* **(MODULO A – 4 ORE)**
- **16 e 20 MARZO 2026** | 9:00 – 13:00 | **AI DI FRONTIERA:** GESTIONE DOCUMENTALE, PRIVACY E CASI D'USO (*VIDEOSORVEGLIANZA, GEOLOCALIZZAZIONE E TECNOLOGIE AVANZATE*) **(MODULO B – 8 ORE)**
- **23 MARZO 2026** | 9:00 – 13:00 | **AI ACT E DRONI NELLA VIGILANZA:** ADEMPIMENTI, TECNOLOGIE E BEST PRACTICE PER GLI ISTITUTI DI VIGILANZA **(MODULO C – 4 ORE)**

MODULO A - L'INTELLIGENZA ARTIFICIALE: OLTRE L'ALGORITMO; *INTRODUZIONE E ANALISI DELL'AI ACT COME FONDAMENTALE DELLA NUOVA ERA REGOLATORIA*

PRESENTAZIONE

Un percorso essenziale per comprendere l'Intelligenza Artificiale tra potenzialità e rischi, con un focus operativo sul nuovo Regolamento UE (AI Act). I partecipanti impareranno a mappare ruoli e responsabilità, distinguere le pratiche vietate e gestire correttamente i sistemi ad alto rischio e gli obblighi di trasparenza. Dalla teoria alla conformità normativa, verranno fornite le basi necessarie per **governare l'innovazione** in modo etico, sicuro e legalmente protetto. Il corso esamina con particolare attenzione **l'intelligenza artificiale applicata a tecnologie avanzate di sorveglianza**, quali la **videosorveglianza, la biometria, la geolocalizzazione** e l'impiego dei droni in generale e, in particolare, **per gli istituti di vigilanza**.

OBIETTIVI

Fornire una comprensione chiara di cosa sia l'IA, del suo potenziale (benefici e pericoli) e della struttura del Regolamento UE (AI Act), focalizzandosi sull'ambito di applicazione, le definizioni e le prime classificazioni dei sistemi, senza trascurare una sezione di cenni agli aspetti sanzionatori.

TAKEWAYS PRINCIPALI: Saper definire l'IA e comprendere lo scopo, l'applicabilità e lo schema normativo del Regolamento. **Pratiche Vietate:** Identificare le pratiche di IA **espressamente proibite**. **Classificazione del Rischio:** Comprendere la logica dei **sistemi ad alto rischio** e l'importanza della **trasparenza** come requisito chiave.

PROGRAMMA E CONTENUTI

- Artificial Intelligence: di cosa stiamo parlando?
- Regolamento sulla Intelligenza Artificiale: cos'è, perché e schema di lettura
- Ambito di applicazione: a chi si applica e a chi non
- I ruoli nel Regolamento: fornitori, deployer, importatori, distributori
- Pratiche vietate (da subito)
- Sistemi ad alto rischio: quali sono (teoria ed esempi)
- E gli altri sistemi?
- Macchine intelligenti, fantascienza e prospettive future
- Trasparenza: regole fondamentali
- Test finale di valutazione dell'apprendimento

MODULO B- AI DI FRONTIERA: GESTIONE DOCUMENTALE, PRIVACY E CASI D'USO - *FOCUS SU VIDEOSORVEGLIANZA, BIOMETRIA, GEOLOCALIZZAZIONE E TECNOLOGIE AVANZATE*

PRESENTAZIONE

Dalla Teoria alla Compliance Operativa: Il percorso formativo è progettato per **fornire gli strumenti necessari** a navigare l'intersezione tra **il nuovo Regolamento UE** sull'Intelligenza Artificiale (**AI Act**) e **il GDPR.** L'obiettivo è trasformare obblighi complessi in flussi di lavoro documentali e tecnici sostenibili, anche con un focus particolare per le tecnologie di sorveglianza.

OBIETTIVI

Trasmettere le competenze pratiche necessarie per la conformità sostanziale e documentale ai sensi dell'AI Act e del GDPR.

Prima parte

Trasmettere le informazioni di base per la gestione del rischio nell'uso della AI. Trasmettere le competenze pratiche necessarie per la conformità sostanziale e documentale ai sensi dell'AI Act e del GDPR. Analizzare i requisiti di trasparenza derivanti dalla norma, compresi quelli relativi al lavoro. Case study ed esercitazioni.

Seconda parte

Le tecnologie di sorveglianza proibite dall'AI Act. Effetti pratici delle tecnologie di sorveglianza nei sistemi ad alto rischio. Geolocalizzazione, profilazione e intelligenza artificiale: casistiche pratiche. Analizzare l'applicazione dei requisiti per i sistemi intelligenti a casi operativi specifici (videoanalisi, biometria, allarmi e infrarosso, centrali intelligenti) e le implicazioni per la privacy. Case study ed esercitazioni.

TAKEWAYS PRINCIPALI:

Compliance Documentale: Essere in grado di individuare gli **obblighi documentali specifici** dell'AI Act (es. registri, informative) e come integrarli con gli adempimenti **GDPR/Privacy**.

Requisiti di Rischio: Padroneggiare i requisiti per i sistemi ad alto rischio o che presentano un rischio e la loro applicazione concreta in contesti di tecnologia di sicurezza avanzate.

Applicazioni Operative: Comprendere le **implicazioni legali e tecniche** nell'uso congiunto di IA, sorveglianza a distanza, videosorveglianza, sistemi di **profilazione**, **geolocalizzazione** e **sensoristica avanzata.**

PROGRAMMA E CONTENUTI

Prima parte

- Sistemi ad alto rischio: adempimenti analizzati per ruolo (fornitore, deployer, distributore)
- Modelli con finalità generali: di che si tratta?
- Trasparenza: obblighi per fornitori e deployer
- Sistema sanzionatorio
- Le rimanenti tempistiche di applicazione dell'AI Act
- IA e sorveglianza a distanza, le basi normative
- Checklist di autovalutazione: suggerimenti operativi per la progettazione e dimostrazione della conformità
- Test finale di valutazione dell'apprendimento

Seconda parte

- La normativa ISO sull'AI. Riferimenti e concetti
- Biometria: introduzione alla tecnologia e nell'AI Act
- I sistemi intelligenti nella videosorveglianza: panorama delle tecnologie
- Termocamere, lettura targhe e sistemi di profilazione
- Geolocalizzazione e gestione delle flotte
- Trattamenti automatizzati, AI e protezione dei dati
- Provenienza, impiego e conservazione dei datiQuando e come effettuare la FRIA (Fundamental Rights Impact Assessment)
- Test finale di valutazione dell'apprendimento

MODULO C - AI ACT E DRONI NELLA VIGILANZA: ADEMPIMENTI, TECNOLOGIE E BEST PRACTICE PER GLI ISTITUTI DI VIGILANZA

PRESENTAZIONE

Un modulo pratico dedicato agli istituti di vigilanza per affrontare gli adempimenti imminenti dell'AI Act, **integrando** la conformità al **GDPR** e alla **Direttiva NIS2** sulla cybersicurezza nel settore degli **istituti di vigilanza** e dei suoi clienti. I partecipanti impareranno a gestire droni (UAV/UGV), biometria, geolocalizzazione, videoanalisi e centrali operative evolute, acquisendo il know-how per il censimento dei sistemi e la valutazione integrata dei rischi (FRIA e DPIA), con l'obiettivo di trasformare l'innovazione tecnologica e la sensoristica d'avanguardia in servizi di sorveglianza sicuri, legali e protetti da minacce informatiche o utilizzi illeciti.

OBIETTIVI

Preparare gli istituti di vigilanza e i soggetti che godono di servizi del genere agli **adempimenti operativi** imminenti (censimento, classificazione del rischio, revisione procedure) in relazione all'AI Act. Analizzare le **sfide e le opportunità** delle tecnologie emergenti (**videoanalisi, sensoristica d'avanguardia, droni UAV/UGV**). Le tecnologie intelligenti nei **centri di Monitoraggio e Ricezione di Allarme** (MARC). Effetti nei servizi acquistati presso terzi e/o forniti ai clienti finali. Valutazione dei rischi congiunte per il GDPR e l'AI Act. L'impatto critico della **Cybersicurezza (NIS2)**.

TAKEWAYS PRINCIPALI:

Piano di Implementazione AI Act: Acquisire il *know-how* per **censire i sistemi**, effettuare la **valutazione dei rischi** e implementare o aggiornare le **procedure di *compliance*** (incluse le FRIA, le DPIA e quelle integrate). **Gestione Droni e Video:** Comprendere i problemi operativi e normativi legati all'uso congiunto di **AI e Droni (UAV/UGV)**, nonché le criticità nella gestione dei sistemi video. Focus sul rischio di hackeraggio o utilizzo illecito delle immagini. **Cybersicurezza e Best Practice:** Applicazione della **Direttiva NIS2** ai servizi offerti ai clienti. **I centri di Monitoraggio e Ricezione di Allarme** secondo le logiche delle **Centrali Operative Evolute (PSIM). Esame dei case studies europei** e **best practice** per un'adozione sicura e legale e altre nuove tecnologie.

PROGRAMMA E CONTENUTI

- L'obbligo di informazione degli interessati
- L'intelligenza negli APR, UAV, UAS, UGV **e** ROV. Quando un drone è domestico
- L'impiego professionale nella sorveglianza: limiti e utilizzi
- Il portale D-flight e l'utilizzo di telecamere, nonché di altre funzionalità sui droni
- L'AI nelle ronde, la televigilanza e la telesorveglianza supportata dai droni
- La videoanalisi nella vigilanza giurata
- Allarmi, sensori e telecamere termiche intelligenti
- Le centrali operative e la gestione degli allarmi con l'AI, incluso il telesoccorso
- L'effettuazione della DPIA e della FRIA nelle tecnologie di sorveglianza
- Le PSIM, la sicurezza informatica e la NIS2
- Test finale di valutazione dell'apprendimento

DESTINATARI

I corsi sono rivolti ad un'ampia platea di professionisti, siano essi lavoratori autonomi o dipendenti, che operano quasi in ogni settore lavorativo. Sono particolarmente indicati per tutti i membri dei team dei sistemi informativi aziendali, di Security e Safety, RSPP e ASPP, HR, Operation, Responsabili di istituti di vigilanza e di Centrale operativa, Manager e dirigenti.

RELATORI

Chiara Delaini consulente specializzata in protezione dei dati, sicurezza delle informazioni, gestione e archiviazione digitale e relative valutazioni di conformità, disegno organizzativo ed ingegneria di processo. Certificata Data Protection Officer secondo la *UNI CEI EN 17740*, si occupa di consulenza e formazione, scrive articoli per riviste specializzate in ambito giuridico, tecnologico o organizzativo e ricopre il ruolo di esaminatrice per certificazioni delle persone in materia di protezione dei dati personali.

Aldo Agostini ex funzionario di Polizia, poi passato al privato. Auditor, consulente e formatore, è specializzato in Security, Data protection, Sicurezza delle informazioni, nonché sistemi e tecnologie avanzate come la videosorveglianza, la biometria e l'Intelligenza Artificiale. E' laureato in giurisprudenza, con all'attivo diversi corsi di perfezionamento post-universitario, inclusi quelli sull'AI. E' certificato ISO 27001, UNI 10459 e UNI CEI EN 17740. In materia di Privacy, è Data Protection Officer in ambito pubblico e privato.

REQUISITI

Non sono richiesti requisiti specifici per partecipare al corso.

ATTESTATI E CREDITI FORMATIVI

Verrà rilasciato un attestato di frequenza e saranno riconosciuti **4 crediti formativi per ogni corso (4 ore),** validi per il mantenimento della certificazione **Professionisti della Security UNI 10459,** al superamento del test di valutazione.

STRUTTURA DEL CORSO

Durata complessiva percorso: 16 ore

Durata moduli A e C: 4 ore Durata modulo B:8 ore

I corsi si svolgeranno in modalità FAD dalle 9:00 alle 13:00 nei giorni e orari indicati in prima pagina.

METODOLOGIA

Il corso sarà erogato tramite piattaforma e-learning che permetterà lo scambio interattivo tra i partecipanti e i docenti coinvolti, favorendo lo scambio di idee, opinioni ed esperienze.

Scheda di Iscrizione

Codici Corso **AI ACT_032026** oppure **AI FRONT_032026** oppure **AI DRONI_032026**

Cognome e Nome*			
Società		***Attività Società***	
Posizione Aziendale			
Indirizzo (via , città , prov, cap)*			
Telefono *		***Cell****	
e-mail*		***P.IVA / C.F.****	
Tipologia Cliente	Business Unit CERSA ☐	ICMQ ☐	ALTRO ☐
Professionista Certificato	☐ Security Uni 10459 ☐ Perito Liquidatore Uni 11628 ☐ Altro _____		

** dati anagrafici della persona che si iscrive al corso*

Dati per intestazione fattura

Il partecipante al corso inoltra la presente richiesta come:

☐ **PRIVATO** per la fatturazione saranno utilizzati i dati sopra indicati ☐ **AZIENDA** compilare i campi sottostanti

Ragione sociale							
C.F		P.IVA					
Via		Città		Prov		Cap	
Cell.		Cell. Az.					
Ref. amministrativo							
e- mail - recapito fatture		Mail PEC					
CODICE UNIVOCO		Eventuale n° d'ordine di Acquisto					
☐ Ente Pubblico		☐ Operazione soggetta alla scissione dei pagamenti-Art.17 Ter DPR 633/72 – Split Payment					
Indicare numero c.i.g.:							
Allegare ordine di Acquisto:							

TARIFFE: per tutti i professionisti che si iscriveranno a due o più corsi, verrà applicata la tariffa PROMO PIU' CORSI:

	LISTINO	**PROMO PIU' CORSI**	**LISTINO CLIENTI ICMQ - BU CERSA**	**PROMO PIU' CORSI CLIENTI ICMQ - BU CERSA**
Modulo A o C	€ 300,00 + IVA ☐	-	€ 250,00 + IVA ☐	-
Modulo B	€ 450,00 + IVA ☐	-	€ 350,00 + IVA ☐	-
Moduli A + C	€ 600,00 + IVA ☐	**€ 550,00 + IVA** ☐	€ 500,00 + IVA ☐	**€ 450,00 + IVA**
Moduli (A o C) + B	€ 750,00 + IVA ☐	**€ 700,00 + IVA** ☐	€ 650,00 + IVA ☐	**€ 600,00 + IVA** ☐
Percorso A+B+C	€ 900,00 + IVA ☐	**€ 850,00 + IVA** ☐	€ 800,00 + IVA ☐	**€ 750,00 + IVA** ☐
AI ACT_032026 MOD. A ☐		**AI FRONT_032026 MOD.B** ☐		**AI DRONI_032026 MOD.C** ☐

Modalità di pagamento:

Bonifico Bancario anticipato all'atto dell'iscrizione:

ICMQ S.p.A. IT 69 C 02008 09448 000103847651- UNICREDIT (**nella causale indicare il nominativo del discente e codice del corso**)

Inviare scheda di iscrizione tramite e-mail: **formazionecersa@icmq.org**

Iscrivendosi al corso ed apponendo timbro e firma sulla presente scheda di iscrizione si prende atto e si accettano le condizioni presenti nel Regolamento e Condizioni di fornitura dei servizi di formazione riportate nella pagina successiva

Data di iscrizione	***Timbro e Firma***
_____/___/_____	

Modalità FAD (Formazione a Distanza)

Informativa UE 2016/679 riguardante l'utilizzo dei dati personali è disponibile su https://www.icmq.it/privacy/privacy-policy.php

Servizi di formazione - Condizioni generali di contratto e Regolamento

Oggetto delle presenti condizioni generali è la fornitura da parte di ICMQ S.p.A. di corsi di formazione come descritti nei documenti di presentazione degli stessi a favore di Terzi (Clienti)

Iscrizione ai Corsi
L'iscrizione ai corsi si intende perfezionata alla ricezione del pagamento del corso e conferma da parte di ICMQ S.p.A, che verrà inviata al raggiungimento del numero minimo di partecipanti.

Sede e date dei corsi
I corsi si terranno nelle date e nelle località riportate nei documenti di presentazione dei corsi. ICMQ S.p.A. potrà in ogni momento comunicare eventuali variazioni relative alla sede o alle date dei corsi.

Obbligo di frequenza e condizione di rilascio dell'attestato
I corsisti devono attenersi agli orari prestabiliti e frequentare le sessioni previste dal programma, altresì sono tenuti a firmare quotidianamente un registro di presenza predisposto da ICMQ S.p.A. nel quale sono indicate le eventuali ore di assenza, che devono essere preventivamente autorizzate dal docente. Nel caso di corsi erogati in modalità online, si farà riferimento ai tracciati generati dalla piattaforma di videoconferenza.
Corso Completo 40 ore - Auditor di terza parte
Le assenze non dovranno avere una durata superiore a 4 ore consecutive nell'arco della stessa giornata e comunque fino ad un massimo di 8 ore nell'ambito della durata complessiva del corso. Le assenze non sono consentite per le prove d'esame.
Corso 24 ore - Auditor interno/ Corso 24 ore - Upgrade
Le assenze non dovranno avere una durata superiore a 2 ore consecutive nell'arco della stessa giornata e comunque fino ad un massimo di 4 ore nell'ambito della durata complessiva del corso. Le assenze non sono consentite per le prove d'esame.
Corso 8 ore
Le assenze non dovranno avere una durata superiore a 1 ora nell'ambito della durata complessiva del corso. Le assenze non sono consentite per i test.
Corso 4 ore
Non sono consentite assenze.
Per i corsi accreditati presso la Scuola Nazionale dell'Amministrazione le assenze non potranno superare il 20% della durata complessiva del corso.
Nel caso in cui vengano superati tali limiti non sarà possibile sostenere l'esame finale e pertanto verrà rilasciato solo un attestato di frequenza; in ogni caso il partecipante non avrà diritto al rimborso della quota versata per l'intero corso.
Il rilascio dell'attestato di qualifica è subordinato al superamento dei relativi esami.
I corsi non prevedono tirocini, stage e affiancamenti, salvo esplicita dichiarazione nella scheda del corso.

Reclami
Il partecipante al corso che non è soddisfatto del servizio offerto può presentare reclamo a ICMQ S.p.A.
Per Reclamo si intende: la segnalazione di una insoddisfazione relativa alla qualità dell'iniziativa formativa e/o modalità con cui essa si è svolta.
ICMQ S.p.A. conferma il ricevimento del reclamo entro 5 giorni lavorativi dalla sua ricezione.
Il reclamo è esaminato dalla direzione di ICMQ S.p.A. che decide in merito alla sua fondatezza disponendo, se necessario, ulteriori accertamenti. Le decisioni della direzione in merito al reclamo sono comunicate al partecipante.
I tempi per l'accertamento delle cause che hanno determinato il reclamo e quindi la risposta al reclamante dipenderanno dalla tipologia e complessità dello stesso. Le conclusioni sono comunicate al reclamante al termine del processo di istruttoria.
Le spese relative al reclamo sono a carico del partecipante richiedente, fatto salvo il caso di accoglimento del reclamo stesso.

Ricorsi
Il partecipante che ritiene ingiusto un provvedimento di ICMQ S.p.A. può presentare entro 10 gg. dal ricevimento del provvedimento medesimo, un motivato ricorso finalizzato alla sua revoca. Il ricorso è esaminato dalla direzione di ICMQ S.p.A. che decide in merito alla sua fondatezza disponendo, se necessario, ulteriori accertamenti. Le decisioni della direzione in merito al reclamo sono comunicate al partecipante mediante comunicazione con avviso di ricevimento.

Diritto di Recesso
Ogni partecipante può fruire del diritto di recesso inviando la disdetta, tramite e-mail, a ICMQ S.p.A. almeno 5 giorni lavorativi prima della data di inizio del corso. In tal caso, la quota versata sarà interamente rimborsata. Resta inteso che nessun recesso potrà essere esercitato oltre i termini suddetti e che pertanto qualsiasi successiva rinuncia alla partecipazione non darà diritto ad alcun rimborso della quota di iscrizione versata. È però ammessa, in qualsiasi momento, la sostituzione del partecipante (a condizione che, laddove previsti, siano garantiti i prerequisiti di ammissione al corso). Ai fini della fatturazione fa fede la data di iscrizione.

Rinvio e cancellazione dei corsi
ICMQ S.p.A. si riserva il diritto di annullare o rinviare i corsi, dandone comunicazione scritta al Cliente tramite fax o e-mail. I corrispettivi eventualmente già percepiti da ICMQ S.p.A. saranno restituiti al cliente o d'accordo con lo stesso, saranno imputati come pagamento anticipato per eventuale iscrizione a corsi in date successive.

Foro competente
Per qualsiasi controversia il foro competente è quello di Milano.

Per partecipare ai corsi FAD non occorrono particolari strumenti: è sufficiente una buona connessione ad internet ed un PC dotato di videocamera; la piattaforma interattiva per la gestione delle lezioni, GoToMeeting, Zoom, Meet e sarà comunicata successivamente e messa a disposizione da ICMQ. Una volta iscritti, riceverete una mail/calendar con il link per la connessione e l'orario. A questo punto, basterà cliccare sul link indicato, scaricare l'applicazione per accedere alla piattaforma e quindi al vostro corso. Materiale didattico fornito in formato elettronico.