DATA SCIENCE PER LE SCIENZE UMANE E SOCIALI (LM81)

(Università degli Studi)

Insegnamento Privacy, sicurezza e dati sensibili per la Data Science

GenCod A007255

Docente titolare Marco MANCARELLA

Insegnamento Privacy, sicurezza e dati sensibili per la Data Science

Insegnamento in inglese Privacy, Security and Special categories of

Settore disciplinare IUS/20

Corso di studi di riferimento DATA SCIENCE PER LE SCIENZE UMANE E

Tipo corso di studi Laurea Magistrale

Crediti 6.0

Ripartizione oraria Ore Attività frontale: 36.0

Per immatricolati nel 2023/2024

Erogato nel 2024/2025

Anno di corso 2

Lingua ITALIANO

Percorso Percorso comune

Sede

Periodo

Tipo esame Orale

Valutazione Voto Finale

Orario dell'insegnamento https://easyroom.unisalento.it/Orario

BREVE DESCRIZIONE DEL CORSO

Il corso si propone di fornire agli studenti gli elementi per orientarsi nella complessa relazione tra diritto e nuove tecnologie. Spazio rilevante sarà dedicato all'evoluzione normativa privacy e dell'Amministrazione digitale.

PREREQUISITI

È sufficiente aver sostenuto il colloquio di accesso al Corso di studio.

OBIETTIVI FORMATIVI

- *Conoscenze e comprensione :* Gli studenti dovranno imparare ad orientarsi al meglio all'interno dell'universo giuridico della privacy, soprattutto in ambito digitale. Dovranno saper distinguere le diverse normative di settore, nel contesto dell'ordinamento giuridico di riferimento (internazionale, europeo e nazionale).
- *Capacità di applicare conoscenze e comprensione :* Le conoscenze acquisite dovranno essere applicate alle nuove tecnologie nel settore pubblico e privato. Gli studenti dovranno essere in grado di analizzare le problematiche giuridico-informatiche della quotidianeità lavorativa, mettendole in relazione alle norme studiate.
- *Autonomia di giudizio :* Gli studenti saranno messi in condizione di analizzare le norme privacy puntando a sviluppare il proprio senso critico. Diverrà abitudine degli studenti discutere con il docente di fatti d'attualità riportati dai media per aumentare le capacità di analisi e l'autonomia di giudizio individuale.
- *Abilità comunicative :* Saranno incentivate le abilità comunicative attraverso l'organizzazione di "exposés" nei quali gruppi di volontari esporranno un tema a loro scelta e si relazioneranno con l'uditorio.
- *Capacità di apprendimento :* Le capacità di apprendimento considerate obiettivo formativo sono riconducibili a quanto affermato al punto "Conoscenze e comprensione".

METODI DIDATTICI	Dopo un primo blocco di lezioni del docente in modalità frontale (avvalendosi, quando ritenuto necessario, della presentazione di materiali, on line e non), saranno organizzati gruppi di studio tra studenti con l'obiettivo di sviluppare l'analisi intorno ad una problematica giuridico-informatica di rilievo, con successiva discussione in aula (cd. Exposé). Tale attività comporta un forte sviluppo della capacità di elaborazione e comunicazione dei discenti.
MODALITA' D'ESAME	L'esame si svolge tramite verifica orale, incentrata sugli argomenti di programma e, se realizzato, sul contenuto del lavoro volontario di exposé, svolto durante il corso.Di tale eventuale exposé il docente tiene conto per formulare la valutazione finale. L'esame, complessivamente, verificherà: - la conoscenza delle discipline normative di cui agli argomenti di programma; - la capacità di sintesi espositiva; - la capacità di applicare le conoscenze apprese a casi concreti e nuovi rispetto a quelli trattati nelle lezioni; - l'acquisizione di una corretta terminologia tecnica relativa alla disciplina.
APPELLI D'ESAME	Consultare la bacheca online.
ALTRE INFORMAZIONI UTILI	La frequenza al corso è fortemente consigliata dal docente, non solo per l'acquisizione di maggiori strumenti rispetto alo studio individuale, ma anche per poter partecipare ai lavori di gruppo tra studenti. Ricevimento: al fine di assicurare un immediato ricevimento e supporto agli studenti, è possibile contattare il docente all'indirizzo marco.mancarella@unisalento.it e fissare una call su Teams. In base alle esigenze, sarà anche possibile fissare un ricevimento presso Studium 2000 - Ed. 5 - primo piano - Uff. 3. Ogni informazione attinente al corso sarà comunicata tramite bacheca del profilo UniSalento o room su Teams, se utilizzata.

PROGRAMMA ESTESO

Saranno trattati i seguenti argomenti:

- 1. - Inquadramento e ambito di applicazione materiale e territoriale della disciplina; individuazione dei ruoli privacy e costruzione dell'organigramma privacy; i soggetti della fattispecie di trattamento e gli atti/accordi per la loro designazione (titolare, contitolare, responsabile del trattamento, responsabile della protezione dei dati o Data Protection Officer, amministratore di sistema, soggetti designati/incaricati, interessato, soggetti terzi; l'autorità Garante per la protezione dei dati personali e le autorità di controllo degli altri Paesi); i principi in materia di protezione dei dati personali e l'accountability; i luoghi del trattamento e gli strumenti del trattamento; le condizioni di liceità del trattamento; l'informativa e gli altri diritti dell'interessato; individuazione e mappatura dei trattamenti; il registro delle attività di trattamento per il titolare e per il responsabile; la privacy by design e by default; l'analisi per processi e la gestione del rischio; norme ISO e processi di trattamento; i privacy audit; le misure di sicurezza; la valutazione d'impatto (PIA/DPIA); la consultazione preventiva; il data breach e la gestione delle violazioni; il flusso transfrontaliero e internazionale di dati personali; trattamenti illeciti, risarcimento del danno, sanzioni; il ruolo dell'Autorità garante; il trattamento dei dati personali in ambito sanitario, bancario, nei rapporti di lavoro, nelle comunicazioni elettroniche e nel marketing; il trattamento dei dati personali da parte degli enti pubblici, etc.); i singoli adempimenti; operatività del Data Protection Officer, linee guida, casistica ed esercitazioni su temi settoriali; connessioni tra privacy e Codice dell'Amministrazione Digitale (D.Lgs. 82/2005) e sue LG Agid.

2. - Principio di accountability e gestione degli incidenti informatici; la documentazione del data breach e la gestione dell'incident responce; specificità del cloud; il ruolo e competenze investigative del Data Protection Officer in caso di data breach; collaborazione fra Garante, forze dell'ordine e DPO in caso di data breach); le misure di sicurezza informatiche nelle pubbliche amministrazioni e nelle aziende; sistema integrato di gestione e norme ISO; il sistema di gestione della sicurezza delle informazioni e il sistema di gestione della privacy; gli audit.

3. - Introduzione alla security aziendale e al risk management; metodologia della sicurezza; strumenti e tecniche per la conduzione del Data Protection Impact Assessment (DPIA); Privacy e controllo a distanza dei lavoratori. Analisi della disciplina e case study; Privacy e dati biometrici (analisi della disciplina e case study); Privacy, comunicazioni elettroniche e marketing (analisi della disciplina e case study); Privacy e sanità elettronica (analisi della disciplina e case study).

4. - Cyber Crime e il mercato del crimine on line; perché il Cyber Crime è interessato alle aziende e ai nostri computer; le persone sono la prima vulnerabilità di un sistema informatico; tipologie di eventi/incidenti Cyber.

TESTI DI RIFERIMENTO

I testi di riferimento saranno comunicati entro la data di inizio del Corso.