

Protezione dei dati personali, Cybersicurezza e Diritto delle nuove tecnologie: Data protection officer, Chief information security officer e Chief artificial intelligence officer

PARTE I - INFORMAZIONI GENERALI

Tipologia di corso

Master di secondo livello

Titolo del corso

Protezione dei dati personali, Cybersicurezza e Diritto delle nuove tecnologie: Data protection officer, Chief information security officer e Chief artificial intelligence officer

PARTE II - REGOLAMENTO DIDATTICO ORGANIZZATIVO

Indirizzo web del corso

<https://masterprotezionedatipersonali.it>

Il Corso di Studio in breve

Il Master universitario di secondo Livello in "Protezione dei dati personali, Cybersicurezza e Diritto delle nuove tecnologie: Data protection officer, Chief information security officer e Chief artificial intelligence officer" prosegue, rinnovandosi, il percorso del Master in "Responsabile della protezione dei dati personali: Data Protection Officer e Privacy Expert", attivato dall'a.a. 2015/2016 presso il Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre, oramai giunto alla decima edizione. Il Master, che si fregia del patrocinio del Garante per la protezione dei dati personali, si propone l'obiettivo di una formazione specialistica post lauream in materia di protezione dei dati personali, cybersecurity e diritto dell'intelligenza artificiale, con riferimento al contesto italiano ed europeo. L'iter formativo prevede l'acquisizione di elevate competenze teoriche e pratiche in materia, con l'esame delle questioni che risultano più attuali rispetto alle nuove e mutate prospettive di protezione dei dati personali e diritto delle nuove tecnologie in ambito pubblico e privato, alla luce dello sviluppo tecnologico e della nuova normativa UE. L'ampio spettro delle materie in costante aggiornamento, accuratamente selezionate per il programma del Master, rappresenta un ambito di conoscenze necessario e non più trascurabile per operare al meglio nel campo della protezione dei dati e, più in generale, della società digitale, come testimonia l'importanza acquisita in breve tempo dalle figure professionali del Chief AI Officer (CAIO) e del Chief Information Security Officer (CISO) e che il Master intende formare insieme a quelle del Data Protection Officer (DPO) e Privacy Expert.

Sbocchi occupazionali e professionali previsti per i laureati

Data Protection Officer (DPO), Chief AI Officer (CAIO) e Chief Information Security Officer (CISO), funzionario/consulente, avvocato specializzato in materia di privacy, cybersecurity, intelligenza artificiale.

Obiettivi formativi specifici del Corso

Il percorso formativo è in grado di assicurare una preparazione adeguata sia dal punto di vista del quadro teorico di riferimento, che delle conoscenze pratico-applicative necessarie a ricoprire la figura professionale di Data Protection Officer (DPO), al pari di altre figure professionali delegate all'attuazione e implementazione della disciplina in materia di protezione dei dati personali, alla cybersecurity e al diritto dell'intelligenza artificiale, formando parimenti i futuri Chief AI Officer (CAIO) e Chief Information Security Officer (CISO). Lo scopo del Master è quello di fornire gli strumenti adeguati ad implementare le conoscenze di Dirigenti e Funzionari sia del settore pubblico sia di quello privato, Avvocati, Commercialisti, Professionisti (in particolare in ambito amministrativo, lavoristico, sanitario, bancario, finanziario e assicurativo, nonché nei settori delle comunicazioni elettroniche) nell'ambito della protezione dei dati personali, della cybersecurity, dell'intelligenza artificiale e in generale delle questioni giuridiche legate alle nuove tecnologie.

Capacità di apprendimento

Attraverso le prove intermedie, previste alla fine di ogni modulo, e mediante la prova finale, consistente nella discussione dell'elaborato di ciascun candidato, sarà verificato il conseguimento degli obiettivi formativi, come sopra specificati. I risultati di apprendimento attesi consistono, pertanto, nella puntuale verifica dell'acquisizione delle competenze e delle conoscenze indicate come idonee al perseguimento degli sbocchi professionali indicati al punto precedente.

Conoscenza e capacità di comprensione

Alla fine del Master, gli iscritti avranno acquisito competenze specialistiche di elevato livello nell'ambito della protezione dei dati personali e delle responsabilità ad essa connesse. Saranno in grado di avere piena consapevolezza della normativa, nazionale e sovranazionale, dell'organizzazione e del funzionamento del Garante per la protezione dei dati personali, dei più rilevanti provvedimenti e degli indirizzi della giurisprudenza, nazionale ed europea, in materia di data protection.

Capacità di applicare conoscenza e comprensione

Le competenze teoriche e pratiche acquisite durante il Master permetteranno allo studente di padroneggiare la complessa materia della protezione dei dati personali e di svolgere attività professionali in tale campo, tanto nel settore pubblico quanto in quello privato.

Requisiti di ammissione

- Scadenza delle domande di ammissione: Domande di ammissione entro il 12 gennaio 2025; Iscrizione entro il 31 gennaio 2025. - Classi di laurea dei titoli di accesso e ogni altro requisito specifico: Laurea magistrale, specialistica o titolo di studio equipollente in Giurisprudenza, Scienze politiche, Economia, Ingegneria, Medicina. In presenza di posti disponibili, si valuteranno, ai fini della ammissione, lauree conseguite presso Dipartimenti diversi da quelli sopra indicati, sulla base del percorso formativo dell'interessato. - Criteri di selezione nel caso in cui le domande di ammissione superino il numero massimo di ammessi: Curriculum vitae ed eventuale colloquio. - Procedure e criteri per il riconoscimento di crediti maturati dagli studenti nel corso degli studi universitari precedenti ai fini di una eventuale riduzione del percorso formativo e delle tasse d'iscrizione: Nessuno.

Prova finale

Le prove intermedie, collocate al termine dei singoli moduli didattici, consistono in esercitazioni su casi pratici e/o simulazioni e test di verifica. La prova finale consiste nella redazione di un elaborato scritto sui risultati della field research, assegnata nell'ambito degli insegnamenti e dei moduli.

Obiettivi formativi specifici

Il percorso formativo è in grado di assicurare una preparazione adeguata sia dal punto di vista del quadro teorico di riferimento, che delle conoscenze pratico-applicative necessarie a ricoprire la figura professionale di Data Protection Officer (DPO), al pari di altre figure professionali delegate all'attuazione e implementazione della disciplina in materia di protezione dei dati personali, alla cybersecurity e al diritto dell'intelligenza artificiale, formando parimenti i futuri Chief AI Officer (CAIO) e Chief Information Security Officer (CISO). Lo scopo del Master è quello di fornire gli strumenti adeguati ad implementare le conoscenze di Dirigenti e Funzionari sia del settore pubblico sia di quello privato, Avvocati, Commercialisti, Professionisti (in particolare in ambito amministrativo, lavoristico, sanitario, bancario, finanziario e assicurativo, nonché nei settori delle comunicazioni elettroniche) nell'ambito della protezione dei dati personali, della cybersecurity, dell'intelligenza artificiale e in generale delle questioni giuridiche legate alle nuove tecnologie.

Informazioni utili agli studenti

-

Descrizione modalità di svolgimento

Informazioni utili agli studenti Nell'ambito del piano didattico del Master è possibile: 1) l'iscrizione all'intero Corso di Master; 2) l'iscrizione a singoli Percorsi ed, eventualmente, 3) a singoli Moduli (si v. infra). Possono essere ammessi al Master, in qualità di uditori, soggetti non in possesso del diploma di laurea magistrale o specialistica, per venire incontro alle esigenze di numerose figure professionali che si misurano Area

Studenti quotidianamente con problemi relativi alla protezione dei dati personali, ma che non hanno conseguito il titolo necessario all'iscrizione al Master. Tali uditori – selezionati anch'essi in base al curriculum vitae – potranno partecipare alle lezioni e alle attività didattiche organizzate nell'ambito del Master, senza sostenere le prove di verifica e la prova finale. Al termine verrà consegnato loro un attestato di partecipazione, senza riconoscimento di crediti formativi. Agli uditori si riconosce la riduzione del 25% della quota di iscrizione all'intero Master. Sede del corso Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre, Via Ostiense, 159, Roma Segreteria amministrativa del corso Dott.ssa Silvia Passarelli Tel. 06 5733.2445 Email: silvia.passarelli@uniroma3.it Segreteria didattica del corso www.masterprotezionedatipersonali.it masterprivacy@uniroma3.it

Requisiti di ammissione

Scadenza delle domande di ammissione: Domande di ammissione entro il 12 gennaio 2025; Iscrizione entro il 31 gennaio 2025. - Classi di laurea dei titoli di accesso e ogni altro requisito specifico: Laurea magistrale, specialistica o titolo di studio equipollente in Giurisprudenza, Scienze politiche, Economia, Ingegneria, Medicina. In presenza di posti disponibili, si valuteranno, ai fini della ammissione, lauree conseguite presso Dipartimenti diversi da quelli sopra indicati, sulla base del percorso formativo dell'interessato. - Criteri di selezione nel caso in cui le domande di ammissione superino il numero massimo di ammessi: Curriculum vitae ed eventuale colloquio. - Procedure e criteri per il riconoscimento di crediti maturati dagli studenti nel corso degli studi universitari precedenti ai fini di una eventuale riduzione del percorso formativo e delle tasse d'iscrizione: Nessuno.

Numero di posti

50

Durata prevista

1 Anno

Crediti previsti

60

Lingua di insegnamento

ITA

Modalità didattica

Convenzionale

Tasse di iscrizione ed eventuali esoneri

Importo totale Euro 6.000 - I rata 3.000 euro II rata 3.000 euro Scad. I rata 31 gennaio 2025 Scad. II rata 31 maggio 2025

Importo totale Euro 4.500 (per i soggetti iscritti ad Ordini professionali o altri soggetti con i quali sia stata sottoscritta apposita Convenzione) I rata 3.000 euro II rata 1.500 euro Scad. I rata 31 gennaio 2025 Scad. II rata 31 maggio 2025

Importo totale Euro 4.000 (per i soggetti che beneficiano della Convenzione PA 110 e lode) I rata 3.000 euro II rata 1.000 euro Scad. I rata 31 gennaio 2025 Scad. II rata 31 maggio 2025

All'importo della prima rata sono aggiunti l'imposta fissa di bollo e il contributo per il rilascio del diploma o dell'attestato.

Le quote di iscrizione non sono rimborsate in caso di volontaria rinuncia, ovvero in caso di non perfezionamento della documentazione prevista per l'iscrizione al Corso.

Esonero dalle tasse di iscrizione

Area Studenti

1. È previsto l'esonero dal pagamento della II rata di iscrizione per gli studenti con disabilità documentata pari o superiore al 66%. Per usufruire dell'esonero è necessario allegare alla domanda di ammissione un certificato di invalidità rilasciato dalla struttura sanitaria competente indicante la percentuale riconosciuta.

2. Non sono previste borse di studio al di fuori di quelle erogate eventualmente dall'INPS, al fine di

garantire l'alta formazione e l'aggiornamento professionale qualificato del personale dipendente delle Pubbliche Amministrazioni, a seguito dell'accREDITamento e del convenzionamento (a.a. 2024/2025), nonché di quelle eventualmente erogate dal Centro di Ricerca Interdipartimentale Europeo di Studi Avanzati sull'Innovazione Digitale (Innovation Digital European Advanced Studies # IDEAS).

Tassa di iscrizione a percorsi e moduli di Master

La tassa di iscrizione ai singoli percorsi è stabilita come di seguito specificato:

- a) Percorso 1: euro 2.500*
- b) Percorsi 2, 3, 4, 5, 6: euro 3.000 ciascuno*
- c) Percorsi 7, 8: euro 4.000 ciascuno*

La tassa di iscrizione ai singoli moduli è stabilita come di seguito specificato:

- a) Modulo 1: euro 2.500*
- b) Modulo 7 e 8: euro 1.750 ciascuno*
- c) Moduli 2, 3, 4, 5, 6: euro 750 ciascuno*

A tali importi è aggiunta l'imposta fissa di bollo. Le quote di iscrizione non sono rimborsate in caso di volontaria rinuncia, ovvero in caso di non perfezionamento della documentazione prevista per l'iscrizione al Corso

Tassa di iscrizione in qualità di uditori

La tassa di iscrizione ai Corsi in qualità di uditori è fissata in euro 4.000 per l'intero Master.

Rilascio titolo congiunto

Titolo normale

Direttore del Corso

Colapietro Carlo

PIANO DELLE ATTIVITA' FORMATIVE
(Insegnamenti, Seminari di studio e di ricerca, Stage, Prova finale)

Anno	Denominazione	SSD	CFU	Ore	Tipo Att.	Lingua
1	20110847 - Cybersecurity	ING-INF/05 IUS/09 IUS/14 IUS/16 IUS/17	11	55	I	ITA
1	20110845 - E-privacy e Telco	IUS/01	4	20	I	ITA
1	20110844 - Il trattamento dei dati personali in ambito finanziario, bancario e assicurativo	IUS/04 IUS/05	4	20	I	ITA
1	20110840 - Il trattamento dei dati personali nell'ambito delle pubbliche amministrazioni	IUS/09 IUS/10	4	20	I	ITA
1	20110846 - Intelligenza artificiale e nuove tecnologie	ING-INF/05 IUS/01 IUS/08 IUS/09 IUS/14 IUS/20	11	55	I	ITA
1	20110842 - La protezione dei dati personali in ambito sanitario e per scopi scientifici	IUS/09 IUS/10	4	20	I	ITA
1	20110841 - La protezione dei dati personali nell'ordinamento italiano ed europeo: norme, prassi e apparato sanzionatorio.	IUS/01 IUS/02 IUS/08 IUS/09 IUS/10 IUS/14 IUS/15 IUS/17 IUS/21	14	70	I	ITA
1	20110848 - Prova finale Maser Privacy		4	20	I	ITA
1	20110843 - Trattamento dei dati personali in ambito lavorativo	IUS/01 IUS/07	4	20	I	ITA

OBIETTIVI FORMATIVI

20110847 - Cybersecurity

Italiano

La Cybersecurity rappresenta un ambito di conoscenze necessarie e non più trascurabili per operare al meglio nel campo della protezione dei dati e, più in generale, della società digitale. Con questo modulo si propone ai corsisti l'acquisizione e/o l'affinamento delle conoscenze indispensabili per rivestire il ruolo di Chief Information Security Officer (CISO). Nella prima parte del modulo viene delineato il quadro normativo di riferimento della Cybersecurity (Direttiva NIS, Direttiva NIS2 e perimetro di sicurezza nazionale cibernetica) a livello nazionale, europeo e internazionale. A seguire, viene analizzato il rapporto della sicurezza cibernetica con la protezione dei dati personali e con le tecnologie emergenti, analizzando le tecniche di minimizzazione dei rischi e reazione a casi di attacco, le pratiche di hacking, i modelli organizzativi aziendali più virtuosi, profili di diritto societario, fiscale, giuslavoristico, assicurativo in relazione alla notifica al Garante

Inglese

Cybersecurity represents an area of necessary and no longer negligible knowledge for operate as best as possible in the field of data protection and, more generally, of digital society. With this module proposes to the students the acquisition and/or the refinement of the knowledge essential for fulfill the role of Chief Information Security Officer (CISO). In the first part of the module it is outlined the Cybersecurity regulatory framework (NIS Directive, NIS2 Directive and security perimeter national cybernetics) at national, European and international. Next, the report is analyzed of cyber security with data protection personal and with emerging technologies, analyzing risk minimization and reaction techniques attack cases, hacking practices, models more virtuous corporate organisations, legal profiles corporate, fiscal, labor law, insurance in relation to the notification to the Guarantor

20110845 - E-privacy e Telco

Italiano

Il modulo mira a fornire le competenze sulla protezione dei dati personali in rapporto alle comunicazioni elettroniche, con particolare attenzione al caso dei social network e ai fenomeni del paywall e della monetizzazione, della profilazione e della pubblicità personalizzata. Connesso è il tema del diritto all'oblio e della portabilità dei dati online. Si approfondisce, inoltre, il trattamento dei dati personali effettuato a fini di telemarketing, il fenomeno delle telefonate mute e lo strumento di tutela del Registro delle opposizioni

Inglese

The module aims to provide skills on protection of personal data in relation to electronic communications, with particular pay attention to the case of social networks and the phenomena of the paywall and monetization, of profiling and personalized advertising. Connected is the issue of the right to be forgotten and online data portability. Furthermore, data processing is explored in greater detail personal data carried out for telemarketing purposes, the phenomenon of silent phone calls and the tool of protection of the Register of Oppositions

20110844 - Il trattamento dei dati personali in ambito finanziario, bancario e assicurativo

Italiano

Nel corso del modulo sarà approfondito il tema del trattamento dei dati personali (anche attraverso l'uso dei Big Data) in ambito bancario, finanziario e assicurativo, con particolare attenzione all'ambito dei rapporti tra banca e cliente, alla tracciabilità delle operazioni e alla attività di recupero crediti. Area Studenti Specifico è il focus relativo al nuovo Regolamento DORA, così come ai profili privacy connessi al Digital Euro e al Fintech

Inglese

During the module the topic of the processing of personal data (including through use of Big Data) in the banking, financial and insurance, with particular attention to the area of relationships between bank and customer, to the traceability of operations and debt collection activities. Student Area The focus on the new Regulation is specific DORA, as well as the privacy profiles connected to Digital Euro and Fintech

20110840 - Il trattamento dei dati personali nell'ambito delle pubbliche amministrazioni

Italiano

Lo scopo del modulo è quello di fornire agli studenti un quadro completo e aggiornato della normativa in materia di trasparenza e di anticorruzione che, negli ultimi anni, ha subito un impetuoso sviluppo, con particolare attenzione alla necessità di tenere conto del doveroso bilanciamento con la protezione dei dati personali. Si approfondisce, dunque, il cammino della trasparenza in Italia, dalla l. n. 241/1990 al d.lgs. n. 97/2016, nonché i diritti del cittadino (accesso documentale, accesso civico e accesso generalizzato) e gli obblighi gravanti sulla P.A., ivi compresa l'amministrazione della giustizia. Al fine di approfondire il complesso rapporto tra il principio di trasparenza ed il diritto alla privacy, vengono

esaminati i più importanti provvedimenti giurisprudenziali e del Garante per la protezione dei dati personali. Particolare attenzione viene posta, da ultimo, alle tematiche dell'open government e partecipazione democratica elettronica.

Inglese

The purpose of the module is to provide students with a complete and updated picture of the legislation on transparency and anti-corruption that, in recent years, has underwent an impetuous development, with particular attention the need to take into account the necessary balance with the protection of personal data. It goes deeper, therefore, the path of transparency in Italy, from l. No. 241/1990 to Legislative Decree No. 97/2016, as well as citizens' rights (documentary access, civic access and access generalized) and the obligations incumbent on the Public Administration, including therein the administration of justice. In order to delve deeper into the complex relationship between the principle of transparency and the law to privacy, the most important ones are examined jurisprudential provisions and the Guarantor for the protection of personal data. Special attention comes addressed, lastly, to the issues of open government and electronic democratic participation.

20110846 - Intelligenza artificiale e nuove tecnologie

Italiano

Nel corso del modulo sarà approfondito il tema dell'Intelligenza artificiale e delle nuove tecnologie, aggiornato alle questioni giuridiche che emergono dall'impiego sempre più frequente di algoritmi e soluzioni basate su Intelligenza artificiale, anche generativa, nel contesto pubblico e privato, nonché dalle nuove opportunità lavorative che potranno sorgere, come dimostra la nuova figura professionale del Chief AI Officer (CAIO). In una prima parte del modulo viene inquadrata la regolazione dell'IA congiuntamente all'esame delle principali tecniche – quali il machine learning, le reti neurali e il deep learning – per l'implementazione di sistemi artificiali ed approfondendo le più rilevanti disposizioni normative sull'Intelligenza Artificiale assieme al Codice etico elaborato sullo stesso tema da parte dell'Unione europea. È esaminato, inoltre, il complesso legame che si instaura tra l'Intelligenza Artificiale e la disciplina sulla protezione dei dati personali, anche attraverso l'analisi delle previsioni contenute nel Regolamento UE 2016/679 che possono trovare applicazione con riguardo ai trattamenti svolti avvalendosi di algoritmi. Allo stesso tempo, sono approfonditi i profili costituzionali che risultano interessati dallo sviluppo dell'Intelligenza Artificiale e sono esaminati i rischi di trattamenti discriminatori che possono derivare da un utilizzo distorto dell'Intelligenza Artificiale. Attenzione particolare è# dedicata alla governance dell'IA e ai rischi per i sistemi democratici, nonché al processo di digitalizzazione della pubblica amministrazione, tra valorizzazione del patrimonio informativo pubblico e decisioni amministrative algoritmiche. La seconda parte del modulo è volta ad analizzare la tecnologia della Blockchain nelle sue principali forme (pubblica-permissionless, pubblica-permissioned, Area Studenti privata), nonché i relativi meccanismi attraverso cui avviene la validazione del consenso. È approfondito il legame tra la protezione dei dati personali e la Blockchain, anche in merito al possibile utilizzo di quest'ultima per garantire strumenti innovativi di tutela per i gli interessati. Da ultimo, sono esaminati alcuni casi pratici per osservare talune possibili applicazioni della tecnologia Blockchain. La terza parte del modulo esamina il fenomeno dell'Internet of Things e dell'impatto che la diffusione degli oggetti connessi ad internet può avere in materia di protezione dei dati personali. In tal senso, sono analizzati i principali settori applicativi dell'Internet of Things quali: Smart Home, Smart mobility, Smart Cities ed e-Health. L'ultima parte del modulo è# dedicata al trattamento dei dati con riguardo alla realizzazione della Realtà Virtuale e della Realtà Aumentata.

Inglese

The topic will be explored in depth during the module of artificial intelligence and new technologies, updated on emerging legal issues by the increasingly frequent use of algorithms and solutions based on Artificial Intelligence, too generative, in the public and private context, as well from the new job opportunities that may arise arise, as demonstrated by the new professional figure of the Chief AI Officer (CAIO). In a first part of the module the regulation of AI together with the examination of main techniques – such as machine learning, networks neural and deep learning – for the implementation of artificial systems and delving into the most relevant ones regulatory provisions on Artificial Intelligence together with the Code of Ethics developed on the same topic by the European Union. Furthermore, the complex bond that is established between Intelligence Artificial and data protection regulations personal, also through the analysis of forecasts contained in EU Regulation 2016/679 which can find application with regard to treatments carried out using algorithms. At the same time, the constitutional profiles are explored in depth are interested in the development of Intelligence Artificial and the risks of treatments are examined discriminators that may arise from use distorted by Artificial Intelligence. Attention particular is dedicated to the governance of AI and AI risks to democratic systems, as well as to the process of digitalization of public administration, among enhancement of public information assets e algorithmic administrative decisions. The second part of the module is aimed at analyzing the Blockchain technology in its main forms (public-permissionless, public-permissioned, Student Area private), as well as the related mechanisms through which validation of consent takes place. It is in depth the link between the protection of personal data and Blockchain, also regarding the possible use of the latter to guarantee innovative tools protection for the interested parties. Finally, they are examined some practical cases to observe some possible applications of Blockchain technology. The third part of the module examines the phenomenon of the Internet of Things and the impact of its diffusion of objects connected to the internet can have in matter of personal data protection. In this sense, the main application sectors are analysed of the Internet of Things such as: Smart Home, Smart mobility, Smart Cities and e-Health. The last part of the module is dedicated to treatment of data with regard to the realization of Reality Virtual and Augmented Reality.

20110842 - La protezione dei dati personali in ambito sanitario e per scopi scientifici

Italiano

Il modulo è interamente dedicato alla tutela della privacy in ambito sanitario, con specifici approfondimenti sull'informativa e sul consenso, refertazione elettronica, Dossier sanitario elettronico (DSE) e Fascicolo sanitario elettronico (FSE), nonché più in generale sulla progettazione dei sistemi informativi e l'utilizzo delle nuove tecnologie in sanità a prova di privacy. Si approfondiscono inoltre, le peculiarità connesse alla statistica sanitaria, al settore della ricerca scientifica e delle sperimentazioni cliniche, alla telemedicina e alle frontiere della medicina di iniziativa

Inglese

The module is entirely dedicated to the protection of privacy in the healthcare sector, with specific insights into information and consent, electronic reporting, electronic health record (DSE) and Electronic Health Record (FSE), as well more generally on system design information and the use of new technologies in healthcare privacy-proof. The related peculiarities are also explored in depth to health statistics, to the research sector scientific and clinical trials, to telemedicine and at the frontiers of medicine initiative

20110841 - La protezione dei dati personali nell'ordinamento italiano ed europeo: norme, prassi e apparato sanzionatorio.

Italiano

Il modulo, i cui contenuti sono specificati nell'ambito dei submoduli in cui è articolato (1.1 e 1.2), mira a fornire un'introduzione di carattere generale sulla protezione dei dati personali in ambito nazionale e sovranazionale. La prima parte del modulo esamina il percorso storico evolutivo e le principali fonti normative in materia di privacy e di protezione dei dati personali, anche in prospettiva comparata, tra le quali: la CEDU, la Carta dei diritti fondamentali dell'UE, il Regolamento UE n. 2016/679 (c.d. GDPR) e il Codice della privacy novellato da ultimo con il d.lgs. n. 101/2018. Particolare attenzione è dedicata ai principi, alle basi giuridiche e al ruolo dei soggetti coinvolti nelle attività di trattamento dei dati. Sono analizzati, inoltre, le principali attività in cui è coinvolta la figura del Data Protection Officer (es. la tenuta del registro dei trattamenti, lo svolgimento della DPIA), nonché il ruolo del Garante per la protezione dei dati personali. La seconda parte del modulo approfondisce i temi dell'accountability e della sicurezza del trattamento dei dati personali. In questo senso, sono esaminati i contenuti dei principi di privacy by design e di privacy by default, nonché gli strumenti della informativa privacy e del registro dei trattamenti, lo strumento della DPIA e il ruolo del Garante per la protezione dei dati personali. Da ultimo, si pone l'attenzione sul rapporto con le altre normative in tema di protezione dei dati personali, nonché sull'utilizzo dei codici di condotta, delle certificazioni e sul funzionamento del meccanismo di cooperazione e coerenza. L'ultima parte del modulo illustra i profili di connessione tutela della privacy e libera Area Studenti manifestazione del pensiero. Ampio è il focus sugli strumenti a tutela degli interessati, con particolare attenzione ai minori online, e i diversi profili di responsabilità connessi, con particolare focus alla normativa in campo penale, civile e amministrativo

Inglese

Il modulo, i cui contenuti sono specificati nell'ambito dei sottomoduli in cui è articolato (1.1 e 1.2), mira a fornire un'introduzione di carattere generale sulla protezione dei dati personali in ambito nazionale e sovranazionale. La prima parte del modulo esamina il percorso storico evolutivo e le principali fonti normative in materia di privacy e di protezione dei dati personali, anche in prospettiva comparata, tra le quali: la CEDU, la Carta dei diritti fondamentali dell'UE, il Regolamento UE n. 2016/679 (c.d. GDPR) e il Codice della privacy novellato dall'ultimo con il d.lgs. N. 101/2018. Particolare attenzione è dedicata ai principi, alle basi giuridiche e al ruolo dei soggetti coinvolti nelle attività di trattamento dei dati. Sono analizzati, inoltre, le principali attività in cui è coinvolta la figura del Data Responsabile della protezione (es. la tenuta del registro dei trattamenti, lo svolgimento della DPIA), nonché il ruolo del Garante per la protezione dei dati personali. La seconda parte del modulo approfondisce i temi dell'accountability e della sicurezza del trattamento dei dati personali. In questo senso, sono esaminati i contenuti dei principi di privacy by design e di privacy per impostazione predefinita, nonché gli strumenti dell'informativa privacy e del registro dei trattamenti, lo strumento della DPIA e il ruolo del Garante per la protezione dei dati personali. Da ultimo, si pone l'attenzione sul rapporto con le altre normative in tema di protezione dei dati personali, nonché sull'utilizzo dei codici di condotta, delle certificazioni e sul funzionamento del meccanismo di cooperazione e coerenza. L'ultima parte del modulo illustra i profili di connessione tutela della privacy e libera Area Studenti manifestazione del pensiero. Ampio è il focus sugli strumenti a tutela degli interessati, con particolare attenzione ai minori online, e i diversi profili di responsabilità connesse, con particolare focus alla normativa in campo penale, civile e amministrativo

20110848 - Prova finale Maser Privacy

Italiano

Prova finale corso master Privacy

Inglese

Final exam of the Privacy master course

20110848 - Prova finale Maser Privacy

Italiano

Prova finale corso master Privacy

Inglese

Final exam of the Privacy master course

20110843 - Trattamento dei dati personali in ambito lavorativo

Italiano

Il modulo e# incentrato sulla tutela della privacy nell'ambito del rapporto di lavoro, con particolare attenzione alla salvaguardia della dignità del lavoratore. Attraverso l'approfondimento delle norme di diritto positivo, nazionale ed europeo, e dei provvedimenti del Garante per la protezione dei dati personali, vengono affrontati i temi della videosorveglianza, della geolocalizzazione, della modalità di utilizzo degli strumenti di lavoro e dei controlli a distanza (posta elettronica, impiego dei social network, navigazione su internet).

Inglese

The module focuses on the protection of privacy in the field of the employment relationship, with particular attention to safeguarding the dignity of the worker. Through the deepening of the norms of positive, national law and European, and the provisions of the Guarantor for the protection of personal data, the issues of video surveillance, geolocation, the mode of use of work tools and remote controls (email, use of social networks, navigation on the Internet).