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://giurisprudenza.uniroma3.it/didattica/post-lauream/master-DPO-CISO-CAIO/

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 undicesima 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. In particolare, da quest'anno i corsisti interessati avranno la possibilità di frequentare anche un "Corso di perfezionamento per la qualifica professionale di Data Protection Officer (DPO)" – un percorso ufficiale conforme alle norme nazionali ed europee UNI EN 17740:2024, UNI 11697:2017 e UNI PdR 66:2019 svolto in collaborazione con la società ITHUM – all'esito del quale i corsisti che avranno superato l'esame finale otterranno la qualifica ufficiale di DPO (Data Protection Officer), anche valida come prerequisito formativo per l'accesso ai registri di Accredia come "professionista" certificato secondo la legge n. 4 del 2013. Per l'articolazione del Corso, le modalità di iscrizione ed i relativi costi si rinvia al Regolamento didattico del Corso disponibile sul sito web del Master (www.masterprotezionedatipersonali.it).

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 e# 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 cybersecurty e al diritto

dell'intelligenza artificiale, formando parimenti i futuri Chief AI Officer (CAIO) e Chief Information Security Officer (CISO). Lo scopo del Master e# 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

AAttraverso 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

Requisiti per l'ammissione, criteri di selezione e riconoscimento delle competenze pregresse Scadenza: domande di ammissione entro il 14 gennaio 2026; iscrizione entro il 25 gennaio 2026. 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 prove scritte con domande a risposta aperta. 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 e# 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 cybersecurty e al diritto dell'intelligenza artificiale, formando parimenti i futuri Chief AI Officer (CAIO) e Chief Information Security Officer (CISO). Lo scopo del Master e# 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

Le attività didattiche si svolgono presso la sede del Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre, con docenza in presenza. Tuttavia, le lezioni sono fruibili anche in modalità a distanza tramite piattaforma Teams. Informazioni utili agli studenti Nell'ambito del piano didattico del Master e# possibile: 1) l'iscrizione all'intero Corso di Master; 2) l'iscrizione ai 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 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.

Requisiti di ammissione

Scadenza delle domande di ammissione: Domande di ammissione entro il 14 gennaio 2026; Iscrizione entro il 31 gennaio 2026. 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 -
prima rata 3.000 euro - scadenza prima rata - 25 gennaio 2026
seconda rata 3.000 euro - scadenza seconda rata 31 maggio 2026

Euro 4.500 (per i laureati presso l'Università Roma Tre e per gli iscritti ad Ordini professionali o altri istituti/società con i quali sia stata sottoscritta apposita

Convenzione)
prima rata 3.000 euro - scadenza prima rata - 25 gennaio 2026
seconda rata 1.500 euro - scadenza seconda rata 31 maggio 2026

Euro 4.000 per i soggetti che beneficiano della Convenzione PA 110 e lode)
prima rata 3.000 euro - scadenza prima rata - 25 gennaio 2026
seconda rata 1.000 euro - scadenza seconda rata 31 maggio 2026

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
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 e# necessario allegare alla domanda di ammissione un certificato di invalidità rilasciato dalla struttura sanitaria competente indicante la percentuale riconosciuta.

Non sono previste borse di studio al di fuori di quelle erogate eventualmente e direttamente ai corsisti dall’INPS, 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 ai singoli moduli del Master

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

Modulo 1: euro 2.500

Modulo 7 e 8: euro 1.750 ciascuno

Moduli 2, 3, 4, 5, 6: euro 750 ciascuno

A tali importi e# 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 4.500 per l’intero Master.

Rilascio titolo congiunto

Titolo normale

Direttore del Corso

Colapietro Carlo

ROMA TRE
UNIVERSITÀ DEGLI STUDI

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/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/04 IUS/09 IUS/10 IUS/14 IUS/15 IUS/17 IUS/21	14	70	AP	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 knowledge that is necessary and no longer negligible to operate at best in the field of data protection and, more generally, of the digital society. With this module, students are offered the acquisition and/or refinement of the knowledge essential to take on the role of Chief Information Security Officer (CISO). The first part of the module outlines the regulatory framework of Cybersecurity (NIS Directive, NIS2 Directive and national cybersecurity perimeter) at national, European and international level. Next, the relationship of cyber security with the protection of personal data and with emerging technologies is analyzed, analyzing the techniques of risk minimization and reaction to attack cases, hacking practices, the most virtuous business organizational models, profiles of corporate law, tax, 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 e# 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 the protection of personal data in relation to electronic communications, with particular attention to the case of social networks and the phenomena of paywall and monetization, profiling and personalized advertising. Related is the issue of the right to be forgotten and the portability of online data. It also examines in depth the processing of personal data carried out for telemarketing purposes, the phenomenon of silent phone calls and the protection tool 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. Specifico è il focus relativo al nuovo Regolamento DORA, così come ai profili privacy connessi al Digital Euro e al Fintech

Inglese

The module will explore the topic of personal data processing (also through the use of Big Data) in the banking, financial and insurance sectors, with particular attention to the area of bank-customer relationships, the traceability of operations and debt collection activities. The focus is specific on the new DORA Regulation, as well as on privacy profiles connected to the 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 aim of the module is to provide students with a complete and updated overview of the legislation on transparency and anti-corruption which, in recent years, has undergone a rapid development, with particular attention to the need to take into account the necessary balance with the protection of personal data. The path of transparency in Italy is therefore explored in depth, from Law no. 241/1990 to Legislative Decree no. 97/2016, as well as the rights of the citizen (documentary access, civic access and generalized access) and the obligations of the Public Administration, including the administration of justice. In order to delve deeper into the complex relationship between the principle of transparency and the right to privacy, the most important provisions of the jurisprudence and of the Guarantor for the protection of personal data are examined. Particular attention is paid, finally, 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 e# 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, privata), nonché i relativi meccanismi attraverso cui avviene la validazione del consenso. È approfondito il legame tra la protezione dei dati personali e laBlockchain, 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 e# dedicata al trattamento dei dati con riguardo alla realizzazione della Realtà Virtuale e della Realtà Aumentata.

Inglese

The module will explore the topic of Artificial Intelligence and new technologies, updated to the legal issues that emerge from the increasingly frequent use of algorithms and solutions based on Artificial Intelligence, including generative, in the public and private context, as well as from the new job opportunities that may arise, as demonstrated by the new professional figure of the Chief AI Officer (CAIO). In the first part of the module, the regulation of AI is framed together with the examination of the main techniques - such as machine learning, neural networks and deep learning - for the implementation of artificial systems and by examining the most relevant regulatory provisions on Artificial Intelligence together with the Code of Ethics developed on the same topic by the European Union. Furthermore, the complex link that is established between Artificial Intelligence and the regulation on the protection of personal data is examined, also through the analysis of the provisions contained in EU Regulation 2016/679 that may find application with regard to the treatments carried out using algorithms. At the same time, the constitutional profiles that are affected by the development of Artificial Intelligence are examined and the risks of discriminatory treatments that may arise from a distorted use of Artificial Intelligence are examined. Particular attention is paid to AI governance and risks for democratic systems, as well as to the process of digitalization of public administration, between valorization of public information assets and algorithmic administrative decisions. The second part of the module is aimed at analyzing Blockchain technology in its main forms (public-permissionless, public-permissioned, private), as well as the related mechanisms through which the validation of consent occurs. The link between the protection of personal data and Blockchain is explored in depth, also with regard to the possible use of the latter to guarantee innovative protection tools for data subjects. Finally, some practical cases are examined 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 that the spread of objects connected to the Internet can have on the protection of personal data. In this sense, the main application sectors of the Internet of Things are analyzed such as: Smart Home, Smart mobility, Smart Cities and e-Health. The last part of the module is dedicated to the processing of data with regard to the creation of Virtual Reality 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 as more generally on the design of information systems and the use of new technologies in privacy-proof healthcare. The peculiarities connected to healthcare statistics, the scientific research and clinical trials sector, telemedicine and the frontiers of proactive medicine are also explored.

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 nazionaleesovranazionale. 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 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

The module, whose contents are specified in the submodules into which it is divided (1.1 and 1.2), aims to provide a general introduction to the protection of personal data at a national and supranational level. The first part of the module examines the historical evolutionary path and the main regulatory sources on privacy and personal data protection, also in a comparative perspective, including: the ECHR, the Charter of Fundamental Rights of the EU, EU Regulation no. 2016/679 (so-called GDPR) and the Privacy Code lastly amended by Legislative Decree no. 101/2018. Particular attention is paid to the principles, legal bases and role of the subjects involved in data processing activities. Furthermore, the main activities in which the Data Protection Officer is involved are analyzed (e.g. keeping the register of processing, carrying out the DPIA), as well as the role of the Guarantor for the protection of personal data. The second part of the module explores the issues of accountability and security of personal data processing. In this sense, the contents of the principles of privacy by design and privacy by default are examined, as well as the tools of the privacy information and the processing register, the DPIA tool and the role of the Guarantor for the protection of personal data. Finally, attention is paid to the relationship with other regulations on the protection of personal data, as well as the use of codes of conduct, certifications and the functioning of the cooperation and coherence mechanism. The last part of the module illustrates the connection profiles between privacy protection and free expression of thought. There is a broad focus on the tools for the protection of data subjects, with particular attention to minors online, and the various profiles of related liability, with particular focus on criminal, civil and administrative legislation

20110848 - Prova finale Maser Privacy

Italiano

Prova finale

Inglese

Final test

20110848 - Prova finale Maser Privacy

Italiano

Prova finale

Inglese

Final test

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 context of the employment relationship, with particular attention to safeguarding the dignity of the worker. Through the study of the provisions of positive law, national and European, and the provisions of the Guarantor for the protection of personal data, the topics of video surveillance, geolocalization, the way of using work tools and remote controls (email, use of social networks, internet browsing) are addressed.