# *RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI: DATA PROTECTION OFFICER E PRIVACY EXPERT*

## PARTE I - INFORMAZIONI GENERALI

### Tipologia di corso

*Master di secondo livello*

### Titolo del corso

*RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI: DATA PROTECTION OFFICER E PRIVACY EXPERT*

## 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 "Responsabile della protezione dei dati personali: Data Protection Officer e Privacy Expert" è attivato dall'a.a. 2015/2016 presso il Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre. 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 nel 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 in ambito pubblico e privato, alla luce dello sviluppo tecnologico e della nuova normativa UE. In particolare, rinnovata linfa allo studio della materia deriva dal Regolamento UE n. 2016/679, dal novellato Codice per la protezione dei dati personali, ai sensi del d.lgs. n. 101/2018 e dalla proposta di Regolamento E-Privacy.*

### Sbocchi occupazionali e professionali previsti per i laureati

*Data Protection Officer, Privacy Expert, funzionario/consulente con specifiche responsabilità nel campo della protezione dei dati personali, avvocato specializzato in materia di privacy.*

### 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 e di Privacy Expert, al pari di altre figure professionali delegate all'attuazione e implementazione della disciplina in materia di protezione dei dati personali, nonché di tutti coloro che in ambito forense si trovano a lavorare nell'ambito della protezione dei dati personali. Lo scopo del Master e# quello di fornire gli strumenti adeguati per implementare le conoscenze in materia di protezione dei dati personali 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, della cybersecurity e dell'intelligenza artificiale.*

### 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

*Scadenza delle domande di ammissione: Domande di ammissione entro il 21 gennaio 2024 Iscrizione entro il 31 gennaio 2024. 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 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 e di Privacy Expert, al pari di altre figure professionali delegate all'attuazione e implementazione della disciplina in materia di protezione dei dati personali, nonché di tutti coloro che in ambito forense si trovano a lavorare nell'ambito della protezione dei dati personali. Lo scopo del Master e# quello di fornire gli strumenti adeguati per implementare le conoscenze in materia di protezione dei dati personali 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, della cybersecurity e dell'intelligenza artificiale.*

## Informazioni utili agli studenti

*-*

## Descrizione modalità di svolgimento

*Informazioni utili agli studenti Nell'ambito del piano didattico del Master e# 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 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.*

## Requisiti di ammissione

*Scadenza delle domande di ammissione: Domande di ammissione entro il 21 gennaio 2024 Iscrizione entro il 31 gennaio 2024. 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 4.000*
*Euro 3.200 (per i soggetti iscritti ad Ordini professionali o altri soggetti con i quali sia stata sottoscritta apposita Convenzione)*
*Euro 3.000 (per i soggetti che beneficiano della Convenzione PA 110 e lode)*
*I rata:*
*Euro 2.000*
*Euro 2.000 (per i soggetti iscritti ad Ordini professionali o altri soggetti con i quali sia stata sottoscritta apposita Convenzione)*
*Euro 2.000 (per i soggetti che beneficiano della Convenzione PA 110 e lode)*
*II rata:*
*Euro 2.000*
*Euro 1.200 (per i soggetti iscritti ad Ordini professionali o altri soggetti con i quali sia stata sottoscritta apposita Convenzione)*
*Euro 1.000 (per i soggetti che beneficiano della Convenzione PA 110 e lode)*
*Scad. I rata 31 gennaio 2024*
*Scad. II rata 31 maggio 2024*
*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*
*Coloro i quali si trovino in condizioni di disabilità, con riconoscimento di handicap ai sensi dell'artIcolo 3, commi*

*Per usufruire dell'esonero è 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 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. 2023/2024).*
*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 2.000*

*b) Percorsi 2, 3, 4, 5, 6 e 7: euro 2.500 ciascuno*

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

*a) Modulo 1: euro 2.000*

*b) Modulo 6: euro 1.000*

*c) Moduli 2, 3, 4, 5 e 7: euro 800 ciascuno*
*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 3.000 per l'intero Master (riduzione del 25%).*

## 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 | **20110434 - Data protection e nuove tecnologie** | IUS/04 | 9 | 45 | AP | ITA |
| 1 | **20110718 - E-privacy e Telco** | IUS/01 | 5 | 25 | AP | ITA |
| 1 | **20110430 - Il trattamento dei dati personali in ambito pubblico** | | 7 | 35 | AP | ITA |
| 1 | **20110431 - La protezione dei dati personali in ambito sanitario e per scopi scientifici** | | 7 | 35 | AP | ITA |
| 1 | **20110429 - La protezione dei dati personali nell'ordinamento italiano ed europeo: norme, prassi e apparato sanzionatorio.** | | 23 | 115 | AP | ITA |
| 1 | **20110435 - Trattamento dei dati personali in ambito bancario, finanziario e assicurativo** | IUS/04 | 5 | 25 | AP | ITA |
| 1 | **20110432 - Trattamento dei dati personali in ambito lavorativo** | IUS/07 | 7 | 35 | AP | ITA |

# OBIETTIVI FORMATIVI

## 20110434 - Data protection e nuove tecnologie

### Italiano

Il modulo, i cui contenuti sono specificati nell'ambito dei submoduli in cui è articolato (6.1, 6.2 e 6.3), mira ad esaminare il rapporto tra la protezione dei dati personali e le innovazioni tecnologiche più rilevanti. La prima parte del modulo affronta il tema dell'Intelligenza Artificiale esaminando le 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. Infine, sono analizzate le questioni etiche ed economiche che caratterizzano lo sviluppo di simile tecnologia, affinché dalla sua applicazione non vengano a verificarsi ingiustificate compressioni dei diritti e delle libertà della persona. 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 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 module, whose contents are specified within the submodules in which it is articulated (6.1, 6.2 and 6.3), aims to examine the relationship between the protection of personal data and the most relevant technological innovations. The first part of the module deals with the topic of Artificial Intelligence by examining the main techniques - such as machine learning, neural networks and deep learning - for the implementation of artificial systems and deepening the most relevant regulatory provisions on Artificial Intelligence together with Code of ethics drawn up on the same issue by the European Union. Furthermore, the complex link that is established between Artificial Intelligence and the regulation on the protection of personal data is also examined, also through the analysis of the provisions contained in EU Regulation 2016/679 which can be applied 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 can derive from a distorted use of Artificial Intelligence are examined. Finally, the ethical and economic issues that characterize the development of this technology are analyzed, so that from its application there are no unjustified compressions of the rights and freedoms of the person. The second part of the module is aimed at analyzing the Blockchain technology in its main forms (public-permissionless, public-permissioned, private), as well as the related mechanisms through which the validation of consent takes place. The link between the protection of personal data and the Blockchain is investigated, also with regard to the possible use of the latter to ensure innovative protection tools for those concerned. 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.

## 20110718 - E-privacy e Telco

### Italiano

Il modulo mira a fornire competenze sulla protezione dei dati personali in rapporto con le comunicazioni elettroniche. Sono analizzati, da un lato, i più importanti provvedimenti del Garante per la protezione dei dati personali e, dall'altro lato, la normativa in materia, con specifico riferimento alle disposizioni del Codice della privacy (come modificato dal d.lgs. n. 101/2018) ed alla bozza di Regolamento E-privacy. Si approfondisce il trattamento dei dati personali effettuati nei seguenti ambiti: telemarketing e telefonate mute; profilazione commerciale e marketing; raccolta dati on line tramite siti internet; spam; mobile payment; cookies; web advertising. Si pone attenzione, inoltre, alle modalità con cui gestire la contrattualistica e i rapporti con i fornitori, con particolare riguardo alla negoziazione delle clausole relative alla protezione dei dati personali e al cloud.

### Inglese

The module aims to provide skills on the protection of personal data in relation to electronic communications. On the one hand, the most important provisions of the Guarantor for the protection of personal data are analysed, and, on the other hand, the relevant legislation, with specific reference to the provisions of the Privacy Code (as amended by

Legislative Decree no. 101/2018) and the draft of the E-privacy Regulation. The processing of personal data carried out in the following areas is studied in detail: telemarketing and silent calls; commercial profiling and marketing; online data collection via websites; spam; mobile payments; Cookies; web advertising. Attention is also paid to the ways in which to manage contracts and relations with suppliers, with particular regard to the negotiation of clauses relating to the protection of personal data and the cloud.

**20110430 - Il trattamento dei dati personali in ambito pubblico**

## 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. 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, ai profili più innovativi della P.A. legati al suo processo di digitalizzazione, all'open government, alla cittadinanza digitale e alla data localization.

## Inglese

The purpose of the module is to provide students with a complete and updated picture of the legislation on transparency and anti-corruption which, in recent years, has undergone an impetuous development, with particular attention to the need to take into account the necessary balance with protection of personal data. Therefore, the path of transparency in Italy is deepened, from l. n. 241/1990 to the legislative decree n. 97/2016, as well as the rights of the citizen (documentary access, civic access and generalized access) and the obligations imposed on the P.A. In order to deepen the complex relationship between the principle of transparency and the right to privacy, the most important jurisprudential provisions and the Guarantor for the protection of personal data are examined. Lastly, particular attention is paid to the most innovative profiles of the P.A. related to its digitization process, open government, digital citizenship and data localization.

**20110431 - 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 su informativa e consenso, refertazione elettronica, dossier sanitario e fascicolo sanitario elettronico, utilizzo dei Big data in ambito sanitario, nonché sul tema della Telemedicina e delle App mediche, anche con riguardo a contesti emergenziali. Si approfondiscono, inoltre, le peculiarità connesse al trattamento dei dati genetici e, nell'ambito dell'attività di ricerca scientifica, allo svolgimento delle sperimentazioni cliniche.

## Inglese

The module is entirely dedicated to the protection of privacy in the health sector, with specific in-depth information on information and consent, electronic reporting, health dossier and electronic health file, use of Big data in the health sector, as well as on the subject of Telemedicine and medical apps, also with regard to emergency contexts. Furthermore, the peculiarities related to the processing of genetic data and, in the context of scientific research, to the conduct of clinical trials are investigated.

**20110429 - 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, 1.2 e 1.3), 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 gli istituti dell'accountability e i profili di cybersecurity legati al trattamento dei dati. In questo senso, sono esaminati i contenuti dei principi di privacy by design e di privacy by default, e sono analizzati l'istituto della DPIA e le ipotesi di data breach. È analizzata la normativa di riferimento in materia di cybersecurity, venendo approfondite, inoltre, le tematiche dell'hacking e del computer crimes. Da ultimo, si pone attenzione all'utilizzo delle certificazioni (ISO ed ex art. 42 GDPR) e dei codici di condotta in ambito data protection. L'ultima parte del modulo illustra gli strumenti di tutela degli interessati e i tipi di responsabilità - civile, penale, amministrativa - che possono sorgere in caso di violazione della normativa privacy. Uno specifico approfondimento è dedicato all'ambito di applicazione del GDPR e al trasferimento dei dati extra UE, anche con riguardo alla circolazione

dei dati mortis causa. Sono esaminati, infine, i poteri ispettivi e sanzionatori delle Autorità di controllo oltre che gli strumenti previsti per il loro coordinamento, sia attraverso il meccanismo di coerenza sia tramite il Comitato europeo per la protezione dei dati personali (EDPB).

## Inglese

The module, whose contents are specified within the submodules in which it is articulated (1.1, 1.2 and 1.3), aims to provide a general introduction on the protection of personal data at national and supranational level. The first part of the module examines the historical evolutionary path and the main regulatory sources regarding privacy and protection of personal data, also in a comparative perspective, including: the ECHR, the EU Charter of Fundamental Rights, the EU Regulation n. 2016/679 (so-called GDPR) and the Privacy Code recently amended with Legislative Decree no. 101/2018. Particular attention is paid to the principles, legal bases and the 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 data processing register, carrying out the DPIA), as well as the role of the Guarantor for the protection of personal data. The second part of the module examines the accountability institutions and cybersecurity profiles related to data processing. In this sense, the contents of the principles of privacy by design and privacy by default are examined, and the DPIA institution and data breach hypotheses are analyzed. The reference legislation on cybersecurity is analyzed, furthermore, the issues of hacking and computer crimes are analyzed. Lastly, attention is paid to the use of certifications (ISO and pursuant to art. 42 GDPR) and codes of conduct in the field of data protection. The last part of the form illustrates the tools for the protection of data subjects and the types of liability - civil, criminal, administrative - that may arise in the event of violation of the privacy legislation. A specific study is dedicated to the scope of application of the GDPR and to the transfer of data outside the EU, also with regard to the circulation of mortis causa data. Finally, the inspection and sanctioning powers of the supervisory authorities are examined as well as the tools provided for their coordination, both through the consistency mechanism and through the European Committee for the protection of personal data (EDPB).

### 20110435 - Trattamento dei dati personali in ambito bancario, finanziario e assicurativo

## Italiano

Nel corso del modulo sarà approfondito il tema del trattamento dei dati personali (anche attraverso l'utilizzo di Big data) in ambito bancario, finanziario e assicurativo, con particolare attenzione ai dati relativi al comportamento debitorio, alle informazioni commerciali, ai rapporti tra banca e cliente, internet banking compliance e furto di identità, tracciabilità delle operazioni bancarie e sicurezza dei dati, attività di recupero crediti e trattamento dei dati personali, dati sui sinistri e perizie assicurative.

## Inglese

During the module, the subject of the processing of personal data (also through the use of Big data) in the banking, financial and insurance fields will be explored, with particular attention to data relating to debtor behavior, commercial information, relations between the bank and customer, internet banking compliance and identity theft, traceability of banking operations and data security, credit recovery and personal data processing, data on claims and insurance appraisals.

### 20110432 - Trattamento dei dati personali in ambito lavorativo

## Italiano

Il modulo è 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 in-depth study of the provisions of positive, national and European law, and the provisions of the Guarantor for the protection of personal data, the issues of video surveillance, geolocation, the methods of use of work tools and remote controls are addressed ( e-mail, use of social networks, internet browsing).