Principali informazioni sull'insegnamento	
Titolo insegnamento	TRATTAMENTO DATI SENSIBILI
Corso di studio	Corso di Laurea Magistrale in SICUREZZA INFORMATICA
Crediti formativi	CFU 9
Denominazione inglese	DATA PROTECTION LAW
Obbligo di frequenza	NO
Lingua di erogazione	ITALIANO

Docente responsabile	Nome Cognome	Indirizzo Mail
	Filippo Lorè	Filippo.lore@uniba.it

Dettaglio credi formativi	Ambito disciplinare	SSD	Crediti
	Giuridico	IUS/04	9

Modalità di erogazione	
Periodo di erogazione	I° semestre
Anno di corso	2020/2021
Modalità di erogazione	E-learning

Organizzazione della didattica	
Ore totali	72
Ore di corso	62
Ore di studio individuale	10

Calendario	
Inizio attività didattiche	Ottobre 2020
Fine attività didattiche	Gennaio 2021

Syllabus	*- diritto alla riservatezza, all'identità personale e alla protezione dati personali;* *- dato personale e interessato;* *- Protagonisti della normativa privacy (titolare, responsabile, autorizzato, designato al trattamento, amministratore di sistema, terzo);* *- principi applicabili al trattamento (liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, responsabilizzazione);* *- GDPR, D.Lgs n. 196/2003 e ss.mm.ii, accountability, privacy by design e privacy by default, risk based approach, profilazione, DPIA, registro delle operazioni di trattamento, misure di sicurezza, data breach, ruolo Garante per la protezione dei dati personali, sicurezza informatica e misure di sicurezza.*
Prerequisiti	

Risultati di apprendimento previsti	• *Conoscenza e capacità di comprensione* In primo luogo, l'obiettivo è quello di rendere lo studente edotto circa l'importanza della tutela della privacy, concetto inquadrabile sia sotto il profilo giuridico che sotto quello informatico. Il corso proposto cercherà di fornire le basi essenziali in merito a concetti giuridici per tutti coloro i quali, nel prosieguo del percorso formativo e professionale, dovranno tenere in dovuta considerazione la tematica privacy, alla luce anche del continuo raccordo in un contesto PA e/o Azienda (lì dove prevista) con la nuova figura professionale, il Data Protection Officer, espressamente prevista dal Regolamento generale sulla protezione dei dati personali UE 2016/679. La mission, quindi, è quella di istruire sotto il profilo teorico e pratico lo studente per rispondere al meglio alle evoluzioni normative in materia di privacy e sicurezza del dato e, conseguentemente, alle richieste del mercato del lavoro. Durante il corso, saranno esaminati i concetti fondamentali della disciplina italiana ed europea in materia di protezione dati personali. Le basi giuridiche dalle quali muovere i primi passi sono rispettivamente il Regolamento generale sulla protezione dati personali e il Codice in materia di protezione dati, così come novellato dal D.Lgs n. 101/2018. Pertanto, risulta necessario partire della definizione di dato personali ai sensi dell'art. 4, n. 1 del Regolamento UE 2016/679, inteso come "qualsiasi informazione riguardante una persona fisica identificata o identificabile (Interessato), proseguire nello studio della definizione di trattamento, art. 4, lett. 2 del Regolamento UE 2016/679, inteso come "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. Una volta definiti questi concetti preliminari, è fondamentale definire i principi applicabili al trattamento dei dati personali come la liceità, la correttezza, la trasparenza, la limitazione delle finalità, la minimizzazione dei dati, l'esattezza, l'integrità e la riservatezza (art. 5 del Regolamento UE 2016/679). Nella definizione delle linee generali della normativa privacy, durante il corso si approfondirà il principio di accountability del titolare (art. 24 Regolamento UE 2016/679) secondo cui spetta al titolare definire le misure tecniche e organizzative per garantire una piena adesione al dettato ed essere in grado, contestualmente, di comprovare la compliance alla normativa privacy in sede di ispezione dell'Autorità Garante per la protezione dei dati personali. I risultati di apprendimento previsti per lo studente

	riguarderanno la capacità di esaminare le criticità, lato privacy, emergenti dalla fase di sviluppo di un prodotto informatico e durante tutta la sua vita. Il professionista della sicurezza informatica, chiamato alle attività di analisi e di adozione di misure di sicurezza per quelle che sono grandi quantità di dati, ordinati e non ordinati, dovrà tenere conto della protezione dati, in ottica accountability. • *Conoscenza e capacità di comprensione applicate* Definiti i principi, fondamentale è la definizione dei "protagonisti della privacy". Il protagonista assoluto della normativa privacy è l'interessato, la persona fisica cui si riferiscono i dati. Egli è il soggetto che, ricevuta la debita nota informativa, deve esprimere il proprio consenso affinché quei dati personali possano essere trattati. Il Regolamento UE 2016/679, dagli artt.15 a 22, definisce una serie di diritti a tutela dell'interessato. Il corso si propone di approfondire, tra gli altri, tali diritti degli interessati (ad es. diritto all'oblio). Lo studio della disciplina in materia di protezione dei dati personali non deve prescindere da una corretta individuazione del titolare, attività non scontata nel caso dell'intelligenza artificiale, lì dove si parla di "catena dei titolari del trattamento". Per titolare del trattamento, ai sensi dagli artt. 4, n. 7, è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali. All'interno della disciplina privacy questa figura è obbligatoria. Il responsabile del trattamento, come veniva espressamente previsto dagli artt. 4, lett. g e 29 del Codice, invece, viene meno formalmente potendo il titolare, in applicazione del principio di accountability, nominare all'interno dell'organizzazione, designati al trattamento (art. 2-quaterdecies del Codice in materia di protezione dati personali) cui spetteranno determinati compiti in ordine alle operazioni sui dati personali. Anche la figura dell'incaricato del trattamento, (cosi come veniva previsto ai sensi dagli artt. 4, lett. h e 30 del Codice), verrebbe meno formalmente meno anche se l'Autorità Garante per la protezione dei dati personali interpreta gli art. 4, n.10, l'art. 29 e l'art. 32, paragrafo 4, come una riproposizione della stessa figura, inquadrabile più precisamente quale autorizzato al trattamento. Inoltre, ogni volta che il titolare decide di effettuare all'esterno un trattamento, dovrà procedere con la nomina a responsabile del trattamento, ai sensi dell'art. 28 del Regolamento UE 2016/679, a soli soggetti che, per esperienza, affidabilità e capacità, possano garantire la compliance normativa. Il titolare, in questi casi, ha l'obbligo di verificare, attraverso attività di audit, la corretta applicazione della normativa in materia di protezione dei dati personali. La figura dell'amministratore di sistema richiederà specifico approfondimento. Con un provvedimento dell'Autorità Garante per la protezione dei dati personali

	(27 novembre 2008), è stata "normata" questa figura: esperti che hanno capacità di accedere ai dati risiedenti sulle reti aziendali e che sono chiamati alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. l percorso formativo non può prescindere nella sua parte centrale dall'analisi dell'assunto sostenuto in più occasioni dal Dirigente del Dipartimento Sanità e Ricerca (ex Dirigente del Dipartimento Attività Ispettive e sanzioni) dell'Autorità Garante per la protezione dei dati personali, dott. Francesco Modafferi, secondo il quale "garantire i diritti essenziali del cittadino significa prendersi cura anche dei suoi dati". Questa che appare una tesi pacificamente condivisibile, fino a qualche anno fa, non ha trovato concreta applicazione a causa della mancanza comune di sensibilità alla tematica privacy. La protezione dei dati personali, infatti, in passato è stata concepita dall'opinione pubblica come "ostacolo" al processo di crescita della consapevolezza del paziente attraverso l'utilizzo di tecnologie avanzate; a tal riguardo, nel corso degli ultimi anni, numerosi sono stati gli interventi dell'Autorità finalizzati alla corretta osservanza della disciplina in materia di protezione dei dati personali in attraverso attività di promozione e formazione, il rilascio di autorizzazioni generali, di provvedimenti (ancora Provv. "Amministratori di sistema" del 27/11/2008) generali o su casi specifici, la redazione di linee guida (si pensi a quelle che disciplinano il dossier sanitario elettronico del 4 giugno 2015) e l'instaurazione di procedimenti ispettivi nelle strutture nelle quali si sono verificate violazioni di dati personali (anche in ambito informatico).Di qui la necessità per lo studente di fare fronte alle criticità privacy, oltre che con una lettura in combinato disposto del Regolamento UE 2016/679 e del Codice in materia di protezione (così come modificato dal D.Lgs n. 101/2018, anche tenendo conto degli orientamenti del Garante per la protezione dei dati personali. Con particolare riferimento agli adempimenti demandati dal legislatore europeo in materia di protezione dati personali, si provvederà ad esaminare le caratteristiche del registro delle operazioni di trattamento, espressamente previsto dall'art. 30 del Regolamento UE 2016/679. Tale attività si rende necessario per due ragioni fondamentali: mappare i trattamenti all'interno dell'organizzazione e, contestualmente, essere in grado di esibire il registro in caso di ispezione da parte dell'Autorità di controllo. Ulteriore adempimento previsto riguarda la valutazione di impatto privacy che si renderà necessaria all'interno di una organizzazione qualora un trattamento metta in serio pericolo diritti e libertà fondamentali degli interessati. A tal riguardo, l'attività di studio verterà su una simulazione di DPIA, resa più completa dall'utilizzo del software della CNIL, rivisto dal Garante italiano per la protezione dati. Con riferimento invece ai requisiti di integrità, disponibilità e riservatezza del dato, si provvederà ad

	analizzare l'"istituto" del data breach e della relativa procedura per la gestione e il monitoraggio degli incidenti che mettono in serio pericolo i dati personali degli interessati. • *Autonomia di giudizio* Gli studenti devono considerare le criticità desumibili dalle operazioni di trattamento dati personali e, conseguentemente, operare una valutazione in ordine al rischio per i diritti e le libertà fondamentali delle persone fisiche. • *Abilità comunicative* Le prove di valutazione avranno un taglio pratico, lo studente non deve limitarsi allo studio teorico della materia ma deve confrontarsi, con i propri colleghi, nella risoluzione di casi pratici. Durante la sessione di esame finale, lo studente dovrà essere in grado di rappresentare il lavoro di studio, elaborando una propria tesi in ordine ad un caso di studio e rendersi disponibile ad un confronto con i colleghi. • *Capacità di apprendere* Gli studenti, all'esito della frequenza del corso, possono annoverare un bagaglio tecnico-normativo tale da affrontare le criticità che possono innescarsi nelle dinamiche di sicurezza informatica, con particolare riferimento ai profili della tutela dei dati personali. Le competenze acquisite consentiranno agli studenti di dedicarsi all'ambito privacy come un utile sbocco professionale. A conclusione del percorso, è previsto un colloquio finale finalizzato alla verifica dei concetti fondamentali.
Contenuti di insegnamento	-La protezione dei dati personali nel contesto normativo italiano ed europeo; - Il nuovo regolamento europeo sulla protezione dei dati personali e gli obblighi imposti dal legislatore europeo; - La protezione dei dati personali in ambito pubblico e privato - La responsabilizzazione del titolare dei trattamento; - Le misure di sicurezza a tutela dei dati personali; - Responsabilita', accertamenti ispettivi e sanzioni; - La protezione dei dati personali in ambito lavorativo; - Il Data Breach; - La Valutazione di impatto privacy - La normativa in materia di sicurezza informatica. - L'Autorità di controllo

Programma	
Testi di riferimento	- "*Manuale sul diritto europeo in materia di protezione dati personali*" Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, 2018 - Provvedimenti del Garante per la protezione dei dati personali - Il Regolamento (UE) 2019/881 - Dispense fornite dal docente agli studenti.
Note ai testi di riferimento	----------
Metodi didattici	- Lezioni didattiche in modalità blended e approfondimenti "in presenza"

Metodi di valutazione (indicare almeno la tipologia scritto, orale, altro)	- Valutazione mediante esame orale - Valutazione mediante esame scritto (in seconda ipotesi)
Criteri di valutazione	I criteri di valutazione del docente terranno conto del livello di conoscenza tecnica-normativa acquisita dal corista e la relativa abilità nell'individuare profili di criticità prima, soluzioni operative poi, che permettano la piena aderenza alle disposizioni della normativa europea e italiana in materia di protezione dati personali.