Principali informazioni sull'insegnamento	
Titolo insegnamento	"TRATTAMENTO DEI DATI SENSIBILI"
Corso di studio	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@yahoo.it

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

Modalità di erogazione	
Periodo di erogazione	Semestre I°
Anno di corso	ANNO ACCADEMICO 2018/2019
Modalità di erogazione	LEZIONI FRONTALI, STUDIO CASI PRATICI E ESERCITAZIONI IN AULA *Le attività didattiche verranno erogate in modalità frontale, attraverso lo studio del Regolamento generale sulla protezione dei dati personali UE 2016/679 e degli impatti dal punto di vista giudico e informatico. Il docente, al fine di coinvolgere in maniera proattiva gli studenti nel processo di apprendimento, settimanalmente assegna a gruppi di lavoro l'analisi, l'esposizione e il commento di provvedimenti dell'Autorità Garante per la protezione dei dati personali. Quest'ultima attività si rende necessaria per fornire elementi di natura pratica oltre che teorica.* *Tra le modalità di erogazione della didattica, sono previsti n. 3 lezioni organizzate in seminari formativi (in videoconferenza) tenute da dirigenti e funzionari dell'Autorità Garante per la protezione dei dati personali (a titolo gratuito per il Dipartimento di Informatica dell'Università degli Studi di Bari). Alla fine delle predette iniziative formative, è data possibilità agli studenti di formulare domande sugli argomenti trattati e di consultare materiale didattico messo a disposizione dall'Autorità sul sito istituzionale.*

Organizzazione della didattica	
Ore totali	N. 225
Ore di corso	N. 72
Ore di studio individuale	N. 153

Calendario	
Inizio attività didattiche	Febbraio 2018
Fine attività didattiche	Giugno 2019

Syllabus	
Prerequisiti	*- Conoscenza livello base della nozione di dato personali, dato sensibili o particolare (art. 9 del Regolamento UE 2016/679), trattamento, misure di sicurezza, titolare del trattamento, referente interno del trattamento, incaricato al trattamento e data breach.* *- Conoscenza livello base degli adempimenti previsti dal legislatore europeo in materia di protezione dei dati personali quali il registro delle operazioni di trattamento (art. 30 Regolamento UE 2016/679) e valutazione di impatto privacy (art. 35 Regolamento UE 2016/679)* *- Conoscenza livello base del ruolo dell'Autorità Garante per la protezione dei dati personali e delle Autorità di Controllo europee.*
Risultati di apprendimento previsti (declinare rispetto ai Descrittori di Dublino) (si raccomanda che siano coerenti con i risultati di apprendimento del CdS, compreso i risultati di apprendimento trasversali)	• <u>*Conoscenza e capacità di comprensione*</u> *In primo luogo, l'obiettivo è quello di rendere lo studente informato circa l'importanza della tutela della privacy, sia dal punto di vista giuridico che dal punto di vista informatico. Il corso pone le basi essenziali a coloro i quali vorranno dedicarsi alla tematica privacy nel percorso di formazione individuale, alla luce anche della nuova figura professionale prevista dal Regolamento generale sulla protezione dei dati personali UE 2016/679. La mission, quindi, è quella di istruire sotto il profilo pratico e teorico 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.* *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 l 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. • *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 dall'individuazione del titolare. 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, designare referenti interni al trattamento 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. Allo stesso di quanto previsto per il referente, la nomina a incaricato del trattamento avviene mediante atto scritto. Inoltre, ogni volta che il titolare decide di effettuare all'esterno un trattamento (Azienda di servizi esterna alla struttura sanitaria), dovrà procedere con la nomina a responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679. 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. Recentemente, 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. I 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 (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). Oggi, con l'entrata in vigore del Nuovo Regolamento Europeo sulla protezione dei dati personali (2016/679), le ultime resistenze stanno venendo meno e si assiste ad un cambiamento culturale importante, nel quale la tutela dei dati personali da "ostacolo" diviene valore: la privacy, infatti, viene intesa come "strumento per conoscere i limiti per non avere limiti". Questo che appare un assurdo si risolve nell'osservanza della normativa e nel rispetto della persona: i punti di forza e di debolezza, emergenti dall'analisi effettuata, costituiscono un sicuro punto di partenza per un fluido e corretto funzionamento della "macchina" operativa. A tal riguardo, dunque, è importante considerare che il contesto nel quale viviamo è in continuo divenire ed il cambiamento tecnologico al quale assistiamo è più veloce delle intenzioni del legislatore. Le Aziende, nell'ottica di miglioramento della qualità di vita dell'individuo sono "affascinate" da nuovi strumenti tecnologici appetibili, che garantiscono notevoli vantaggi per il cittadino, ma molto spesso non rappresentano un'adeguata tutela sotto il profilo della riservatezza e della tutela dei dati sensibili che rappresentano quanto di più intimo il cittadino

	possegga. Tali dispositivi informatici, pur degni di particolare attenzione circa l'indiscutibile utilità, non possono prescindere da una valutazione di impatto privacy così come previsto dai Considerando 6 e 7 al Nuovo Regolamento Europeo sulla protezione dei dati personali (2016/679), i quali specificano che "l'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali". • *Autonomia di giudizio* Il quadro disegnato deve essere arricchito dall'analisi di situazioni reali. E' importante per lo studente verificare le competenze in precedenza acquisite sul piano teorico, successivamente sul campo pratico. Lo studio di casistiche aiuta a comprendere la rilevanza del tema. Si pensi, ad esempio, alla notizia pubblicata dalla stampa mondiale secondo la quale un attacco informatico avrebbe intaccato il sistema sanitario inglese con conseguente accesso abusivo a dati idonei a rivelare lo stato di salute (dati sensibili per eccellenza) dei pazienti. La notizia, di rilevo mondiale, denota quanto i temi della sicurezza informatica e della privacy siano di primaria importanza. Tale attacco ha comportato perdite per svariate milioni di sterline e hanno compromesso la riservatezza e l'intimità dei pazienti inglesi. Tutto questo senza considerare, altresì, un "mercato nero" parallelo: si stima che un singolo dato sanitario sia valutato fino a cinque euro. • *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. • *Capacità di apprendere* Gli studenti hanno 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, in piena aderenza al disposto normativo europeo che prevede l'istituzione della figura del Data Protection Officer. A conclusione del percorso, è previsto un colloquio finale finalizzato alla verifica dei concetti fondamentali.
Contenuti di insegnamento	Il corso si pone, tra gli altri, l'obiettivo di approfondire concetti costituzionalmente garantiti, quale il diritto alla riservatezza, alla protezione dei dati personali e all'identità personale. Il percorso formativo non può prescindere dall'analisi del ruolo del Garante per

	la protezione dei dati personali, dello studio del Codice in materia di protezione dei dati e delle recenti novità introdotte dal legislatore europeo con il Regolamento europeo sulla protezione dei dati personali che introduce l'istituzione di una nuova figura professionale come il Data Protection Officer, chiamato ad essere "figura di supporto" per l'Azienda nell'implementazione delle best practices sotto il profilo della disciplina privacy.

Programma	
Testi di riferimento	-"Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale" scritto da Francesco Modafferi, Dirigente di ruolo dell'Autorità Garante per la protezione dei dati personali -"Privacy e diritto europeo alla protezione dei dati personali" scritto dal Prof. Pizzetti - "Big data e privacy by design" a cura di G. d'Acquisto; -Regolamento Europeo sulla protezione dei dati personali (2016/679);
Note ai testi di riferimento	Oltre ai testi di riferimento, lo studente può approfondire gli argomenti trattati durante le lezioni frontali. *Note: I testi indicati sono suscettibili di integrazione in attesa del decreto legislativo del Governo di prossima entrata in vigore che armonizzerà il passaggio dal Codice in materia di protezione dei dati personali al Regolamento UE 2016/679.*
Metodi didattici	Libri di testo, brochure, classe virtuale, video, slides descrittive.
Metodi di valutazione (indicare almeno la tipologia scritto, orale, altro)	- ESAME ORALE CON COLLOQUIO FINALIZZATO ALLA VERIFICA DEI CONCETTI FONDAMENTALI; - TEST SCRITTO CON SOTTOPOSIZIONE DI DOMANDE A RISPOSTA APERTA E A SCELTA MULTIPLA
Criteri di valutazione (per ogni risultato di apprendimento atteso su indicato, descrivere cosa ci si aspetta lo studente conosca o sia in grado di fare e a quale livello al fine di dimostrare che un risultato di apprendimento è stato raggiunto e a quale livello)	Gli studenti dovranno, attraverso un'analisi che tenga in dovuta considerazione aspetti giuridici e informatici, ponderare il rischio legato a presunte violazioni di dati personali generato dall'utilizzo dei sistemi informatici. Tale consapevolezza deve rendere lo studente capace di discernere se un'attività informatica possa andare a collidere con la legge e, nel caso, rimediare alla violazione privacy accertata.
Altro	