Principali informazioni sull'insegnamento	A.A. 2017/2018
Titolo insegnamento	**Trattamento Dei Dati Sensibili (A.A.2017/2018)**
Corso di studio	Magistrale In Sicurezza Informatica
Crediti formativi	9 CFU
Denominazione inglese	Data Protection Law
Obbligo di frequenza	NO
Lingua di erogazione	Italiana

Docente responsabile	Nome Cognome	Indirizzo Mail
	Filippo Lorè	

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

Modalità di erogazione	
Periodo di erogazione	I semestre
Anno di corso	I
Modalità di erogazione	Lezioni frontali Studio di casi pratici Esercitazioni in aula

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

Calendario	
Inizio attività didattiche	02/10/2017
Fine attività didattiche	12/01/2018

Syllabus	
Prerequisiti	*Conoscenza livello base della nozione di dato personale, dato sensibile, trattamento, misure di sicurezza, titolare del trattamento, responsabile del trattamento, incaricato al trattamento* e *data breach. Consapevolezza del ruolo svolto dall'Autorità Garante per la protezione dei dati personali*
Risultati di apprendimento previsti (declinare rispetto ai Descrittori di Dublino - si raccomanda che siano coerenti con i risultati di apprendimento esplicitati nel Regolamento del CdS, compresi i risultati di apprendimento trasversali)	• <u>*Conoscenza e capacità di comprensione*</u> In primo luogo viene in rilievo la definizione di dato personale, inteso ai sensi dell'art. 4, lett.b, del Codice in materia di protezione dei dati personali come "qualsiasi informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale" e la nozione di dato sensibile (art.4, lett.d), secondo la quale sono "i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonchè i dati personali idonei a rivelare lo stato di salute". Fondamentale per

	comprendere le modalità di trattamento dei dati personali risulta essere lo studio dei principi fondamentali: l'art. 11 Codice che contribuisce a codificare il "principio di necessità" (di cui all'art. 3 del Codice), imponendo che il trattamento dei dati personali (di qualsiasi natura) avvenga in modo "non eccedente rispetto alle finalità per le quali sono stati raccolti o successivamente trattati". Ne deriva che il dato personale deve essere trattato preferibilmente in maniera anonima o aggregata per scopi di carattere organizzativo, di controllo di gestione, per verifica finanziaria; mentre, solo in caso di stretta necessità, è possibile trattare il dato personale. L'art. 3, comma 1, infatti, nel tipizzare il principio di necessità stabilisce che "i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi…". • *Conoscenza e capacità di comprensione applicate* Definiti i principi, definiamo i "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. Per titolare del trattamento, ai sensi dagli artt. 4, lett f e 28 del Codice, si intende la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. All'interno della disciplina privacy questa figura è obbligatoria. Il responsabile del trattamento, ai sensi dagli artt.4, lett. g e 29 del Codice, invece, è designato dal titolare tra i soggetti che per capacità ed esperienza garantiscono un elevato livello di tutela sotto il profilo della sicurezza e della protezione dei dati personali. La nomina a responsabile del trattamento da parte del titolare avviene tramite atto scritto, datato e firmato da entrambe le parti, nel quale vengono delegati i poteri di organizzazione, gestione e controllo nelle operazioni di trattamento. L'incaricato del trattamento, ai sensi dagli artt. 4, lett. h e 30 del Codice, è colui che effettua operazioni di trattamento sotto la direzione del titolare o del responsabile. Allo stesso di quanto previsto per il responsabile, 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 esterno al trattamento dei dati personali del soggetto prescelto. Il titolare, in questi casi, ha l'obbligo di verificare, attraverso attività di audit, la corretta applicazione della normativa i materia di protezione dei dati personali. Recentemente, con un provvedimento dell'Autorità Garante per la protezione dei dati personali (25 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 Libertà Pubbliche e Sanità (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 25/11/2008) 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 la prossima 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	l 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 -Codice in materia di protezione dei dati personali -"Allegato B" al Codice in materia di protezione dei dati personali -Regolamento Europeo sulla protezione dei dati personali (2016/679)

Note ai testi di riferimento	Le lezioni sono integrate dagli appunti di lezione del docente e dallo studio dei provvedimenti sul sito istituzionale del Garante per la protezione dei dati personali
Metodi didattici	Il materiale didattico è arricchito dalle slides in formato PPT, esercitazioni degli studenti che riferiranno in aula sullo studio individuale dei provvedimenti del Garante.
Metodi di valutazione (indicare almeno la tipologia scritto, orale, altro)	Scritto e orale.
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	