POLITECNICO DI MILANO

MASTER UNIVERSITARIO II LIVELLO "DATA PROTECTION OFFICER" – II EDIZIONE – 2020/21 – BOZZA DI PROGRAMMA

MODULO I - LA PROTEZIONE DEI DATI PERSONALI NELL'ORDINAMENTO ITALIANO ED EUROPEO

I.1 *Fonti nell'ordinamento italiano, europeo ed internazionale;* - Introduzione. Fonti del diritto interno e sovranazionale in materia di tutela della riservatezza e protezione dei dati personali; - Le fonti del diritto dell'Unione europea. Il pacchetto europeo *privacy*: Il Regolamento UE n. 2016/679 (I principi, gli obblighi per i titolari e le definizioni di *privacy by design* e *privacy by default*; il trasferimento di dati personali verso paesi terzi; la cooperazione internazionale); - Le fonti del diritto dell'Unione europea. Il pacchetto europeo *privacy*: La Direttiva del Parlamento europeo e del Consiglio n. 2016/680 concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione dei dati; - Le fonti del diritto interno. La *privacy* nell'ordinamento costituzionale italiano e la giurisprudenza nazionale; - Le fonti del diritto interno. Il Codice in materia di protezione dei dati personali (d.lgs. n. 196/2003)

I.2 *Soggetti e responsabilità*

- Il Garante per la protezione dei dati personali: compiti, funzioni e poteri; le vie di accesso; i provvedimenti e la tutela giurisdizionale; - I soggetti coinvolti nelle operazioni di trattamento: interessato, titolare, responsabile e incaricato; - Introduzione alla figura del *Data Protection Officer* (definizione, compiti e obblighi); - Le responsabilità connesse al trattamento dei dati personali. Parte I (I poteri istruttori, ispettivi e di accertamento; tutela dell'interessato e sanzioni; titolarità e misure di sicurezza); - Le responsabilità connesse al trattamento dei dati personali. Parte II (Responsabilità civile e amministrativa; responsabilità penale)

MODULO II - MODALITÀ ORGANIZZATIVE E INDICAZIONI OPERATIVE PER L'ADEGUAMENTO ALLE PREVISIONI DEL REGOLAMENTO UE N. 2016/679 (GDPR)

II.I *Le attività preliminari all'individuazione del Data Protection Officer*

- Analisi di contesto interno (tipologie di dati trattati, del flusso dati, della loro conservazione, della loro gestione, dell'aggiornamento; database e CED; eventuali trattamenti effettuati su larga scala); - Analisi di contesto esterno (interlocutori economici e dei connessi flussi di dati, distinguendo i flussi di dati in fra ed extra UE; Autorità pubbliche con cui vengono scambiati i dati); - Identificazione delle caratteristiche del DPO, delle modalità di scelta e di designazione alla luce delle principali best practices

II.2 *Modalità di strutturazione ed implementazione dell'ufficio del DPO*

- Organizzazione del DPO (predisposizione del regolamento di organizzazione e funzionamento del DPO; definizione dei compiti di vigilanza del DPO e condizioni per istituire un unico DPO nei gruppi societari); - I flussi informativi che devono essere veicolati al DPO (analisi tipologica delle informazioni, presupposti e modalità per la loro veicolazione); - Rapporti tra DPO e altri organi e Autorità pubbliche (rapporto e il raccordo con altri organi di controllo, quale ad es. *compliance officer*); le relazioni con il Garante della *privacy*

II.3 *Certificazione di conformità al regolamento (analisi e illustrazione costi benefici della certificazione; la procedura di certificazione)*

II.4 *Strumenti per l'analisi, la revisione e la valutazione delle informative, dei consensi e delle policy aziendali relativamente ai flussi e alla sicurezza dei dati*

- Istituzione dei registri dei trattamenti (indicazione delle banche dati, del soggetto che le gestisce, chi può accedervi e le finalità); - Verifica, analisi, revisione e valutazione delle modalità di trattamento (identificazione dei soggetti preposti al trattamento, degli atti di nomina e dello stato dei processi; rendiconto contenente una specifica *gap analysis* al fine di circoscrivere le attività da implementare successivamente; - Gli adempimenti privacy connessi: all'uso dei BIG DATA; all'M2M (Machine-to-Machine); all'IOT (Internet of Things); alla profilazione con AI (Artificial intelligence)

II.5 *La procedimentalizzazione delle attività per l'adeguamento al GDPR*

- Predisposizione di un piano di attività ai fini dell'adeguamento delle policy aziendali al GDPR e alle altre norme rilevanti in tema di tutela dei dati; - Predisposizione di una Check GDPR; - Strutturazione del Master Plan GDPR

MODULO III - STRUMENTI TECNICI PER L'ADEGUAMENTO ALLE PREVISIONI DEL REGOLAMENTO UE N. 2016/679

III.1 *Privacy Impact Assessment set-up*

- Strumenti per l'individuazione e documentazione del processo di *Privacy Impact Assessment* (PIA). In particolare: normativa tecnica (ISO/IEC 29134, ISO 29100 - 29101, ISO 29151 e ISO 27001/2) (ISO 270018); descrizione dei trattamenti e della finalità; identificazione delle aree a rischio; identificazione dei processi a rischio; valutazione dei rischi residui; valutazione di necessità e proporzionalità dei trattamenti comparativa dei rischi e istituzione di un registro dei rischi; protocolli finalizzati alla riduzione del rischio; procedure atte a declinare i protocolli; sistema di vigilanza; - Linee guida per il PIA. In particolare: identificazione del ciclo di vita del trattamento; modalità della valutazione periodica di rischi

III.2 *Processi di privacy by design e privacy by default*

- tecniche di progettazione dei trattamenti finalizzata alla riduzione dei rischi *privacy;* - tecniche di *privacy project management;* - tecniche di verifica dell'applicabilità PET di soluzioni tecnologiche necessarie per la *privacy by design* (es. standard Enisa e OASIS); - *segregation of duties*

III.3 *Software, protocolli e requisiti di compliance alla GDPR*

- *accounting*; strutture di dati; importazione / esportazione; - diritto all'oblio e architettura dei dati; pseudonimizzazione dei dati; crittografia end to end; *key management*

III.4 *Data Breach Notification* e *Data Breach Management*

- definizione e strutturazione di processi e sistemi che consentano di evitare o minimizzare rivelazioni di dati per errori o sinistri, attacchi dall'esterno, fughe di dati ed accessi indebiti; - prassi formali e procedure di *incident management;* - *tools* o soluzioni informatiche di segnalazione e gestione degli incidenti; - meccanismi assicurativi a copertura dei costi di *data breach notification;* - simulazione di *data breach*

III.5 *Revisione dei contratti e del sistema di allocazione di funzioni e responsabilità*

- Adeguamento dei database alle nuove regole; la definizione dei tempi di scadenza dei database; - La c.d. rivitalizzazione del "patto di utilizzo"; le misure e forme di segregazione; le tecniche di pseudonimizzazione; - Tecniche di integrazione funzionale tra gli organi e le attività in materia di privacy e gli altri organi di controllo (ad es. *compliance officer* 231, RSPP in materia di sicurezza del lavoro ecc), in modo da ottimizzare i processi e le procedure e evitare duplicazioni (necessità di tracciamento delle attività a rischio proprio del modello 231 sia sul versante 231 sia sul fronte *privacy*; necessità di integrazione funzionale del PIA con le valutazioni dei rischi - aziendali e interferenziali - in materia di sicurezza sui luoghi di lavoro)

MODULO IV PRIVACY, COMUNICAZIONI ELETTRONICHE E INTERNET

IV.1 *Privacy e comunicazioni elettroniche*

- Inquadramento generale e disposizioni del Codice privacy in materia; - Gli obblighi di legge per i fornitori di servizi di comunicazione elettronica e in materia di data retention; - Trattamento dei dati personali nell'ambito del marketing e della profilazione: la disciplina del Codice privacy e i provvedimenti del Garante per la protezione dei dati personali; - Privacy e comunicazioni indesiderate: telemarketing e telefonate mute. La disciplina del Codice privacy e i provvedimenti del Garante per la protezione dei dati personali; - Obblighi di informativa e prestazione del consenso per attività promozionali degli utenti effettuate tramite sistemi automatizzati e non automatizzati (Linee guida spam); - Le misure del Garante in materia di mobile payment

IV.2 *Trattamento dei dati personali e attività di marketing, profilazione e loyalty*

- Raccolta dati on line tramite siti internet e data protection; - Elementi essenziali per l'adeguamento dei sistemi di mailing list a scopo commerciale e delle informative al Regolamento UE n. 2016/679. Introduzione; - Tecniche per la corretta gestione del sistema delle email marketing; - Tecniche di valutazione dei trattamenti di dati connessi alla luce del Regolamento Europeo Privacy; - La distinzione delle attività di analisi generica su database (segmentazione e clusterizzazione) dalla profilazione in senso tecnico e connessa differenziazione delle misure; - Strutturazione delle misure di consenso ad hoc per la profilazione

IV.3 *Gli attacchi ai sistemi informatici e il crescente fabbisogno di misure minime di sicurezza delle pubbliche amministrazioni*

- Il DPO e la valutazione di impatto nelle p.a.: una nuova opportunità per riprogettare la diffusione dei dati digitali; - Integrità e sicurezza delle reti digitali; - Le nuove infrastrutture critiche

MODULO V - TRATTAMENTO DEI DATI PERSONALI IN AMBITO PUBBLICO E CONOSCIBILITÀ DELLE INFORMAZIONI

V.1 *Principi e regole generali sul trattamento dei dati personali da parte dei soggetti pubblici*

- Il cammino della trasparenza in Italia: dalla l. 241/1990 al d.lgs. 97/2016; - Gli obblighi di pubblicazione e la protezione dei dati personali; - L'accesso documentale e la protezione dei dati personali; - L'accesso civico generalizzato e la protezione dei dati personali

- Public data - la capitalizzazione del patrimonio informativo - Valorizzazione del patrimonio informativo pubblico; Direttiva UE PSI; Interoperabilità; Data science

- Social PA – Public brand reputation; best practice

- L'organizzazione e i processi tra efficienza, trasparenza e anticorruzione - L'esperienza del Comune di Milano

- Profili di responsabilità in ambito pubblico in relazione alla trasparenza e al trattamento dei dati

- Attuazione della Direttiva 680 del 27 aprile 2016 (D. Lgs n. 51 del 18/5/2018) per la protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle Autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali

V.2 *Soggetti pubblici, privacy e nuovo contesto digitale*

- La digitalizzazione della P.A.: banche dati e flussi di informazioni; - Il Codice dell'Amministrazione Digitale; - Il digital first del procedimento amministrativo; - La partecipazione con modalità telematiche ai processi decisionali pubblici; - Digitalizzazione dei contratti pubblici; - La declinazione del Regolamento e i DAS. L'eliminazione delle barriere esistenti all'impiego dei mezzi di identificazione elettronica degli stati membri; - La normativa sulle comunicazioni elettroniche e sulla banda larga e ultra-larga. Il ruolo del DPO; - P.A. ed economia smart (rinvio)

V.3 *Trattamento dei dati personali in ambito lavorativo*

- La disciplina della protezione dei dati personali in ambito lavorativo alla luce del quadro normativo sovranazionale e nazionale; - Privacy e rapporti di lavoro nel GDPR

- Il trattamento dati dei lavoratori per finalità di gestione del rapporto di lavoro; - I controlli a distanza sull'attività del lavoratore: la videosorveglianza e la geo localizzazione; - I controlli a distanza sull'attività del lavoratore: posta elettronica, navigazione in internet e social network; - Trattamento dei dati biometrici in ambito lavorativo; - Nuove tecnologie e modalità di rilevazione delle presenze dei lavoratori

V.4 *La protezione dei dati personali in ambito sanitario e per scopi scientifici*

- Privacy e sanità: tra tutela della dignità della persona e tutela della salute

- L'informativa e il consenso in ambito sanitario; - La disciplina del Codice e i provvedimenti del Garante; - Dossier sanitario e Fascicolo sanitario elettronico

- Privacy e sanità elettronica. Introduzione e case study su refertazione on line; - Sistemi informativi sanitari e privacy: progettazione e realizzazione; - La protezione dei dati personali nel sistema sanitario: complessità e specificità organizzative; - Il trattamento e la tutela dei dati genetici; - La tutela dei diritti nel quadro delle sperimentazioni cliniche

V.5 Focus sulla digitalizzazione della PA

- L'azione amministrativa digitalizzata. Discrezionalità e Responsabilità- Informazioni base di diritto amministrativo funzionali alla miglior comprensione del mutamento di tali istituti in contesto di transizione digitale P.A. - Giurisprudenza e digitalizzazione P.A. - Commento a pronunce 2019 di TAR Lazio e CdS

- Il Codice dell'Amministrazione Digitale - Ratio legis e struttura CAD; Il documento informatico; Comunicazioni B2G; Digitalizzazione procedimenti amministrativi

- Gli Stakeholders della P.A. digitale (Ministro Innovazione, Dipartimento per la Trasformazione Digitale, AGID e Piano Triennale 2019-2021, Consip S.p.A. e Sogei S.p.A., Poli Strategici Nazionali (PSN)

- Responsabile Transizione Digitale - Attività e Compiti RTD (Circolare Funzione Pubblica n. 3 del 1 ottobre 2018); Responsabile Transizione Digitale; Strumenti di lavoro - Individuazione di standard, processi, rapporti RTD vs terzi, governance.

-Glossario tecnico di sicurezza informatica

MODULO VI - PRIVACY E SMART CITIES

VI.1 *La Privacy Impact Assessment (PIA) e sistema delle città intelligenti*

- Il contesto tecnologico; lo sviluppo delle città; lo sviluppo sensoriale nelle città

- *Smart grid* e *smart metering*; la centralità della progettazione; - Il Data Centric government; - Contratti d'area, accordi di programma e urbanistica negoziata per progetti di smat city; - Il dibattito pubblico; - L'applicazione della *business intelligence*; l'utilizzo dei BIG data nella pianificazione e programmazione urbanistica (inclusa la pianificazione dei parchi tecnologici e degli hub per l'innovazione) ed il ruolo del DPO - L'evoluzione del Sistema Pubblico di Connettività (SPC); il fabbisogno cittadino di tecnologia e strumenti digitali; i nuovi diritti digitali.

VI.2 *Il delicato ruolo del DPO nelle smart city*

- L'intelligent transport system e la mobilità urbana sostenibile; - La nuova normative sull'innovazione nelle concessioni di costruzione e gestione di reti di trasporto; - La regolazione digitale del traffico; - L'affidamento della concessione di parcheggi intelligenti; - Il quadro regolatorio in materia di *connected car*, *self-driving car* e *driverless car;* - La riduzione dei premi assicurativi per scatole nere e altri sistemi digitali: i nuovi mercati; - Il caso Uber nella giurisprudenza nazionale e internazionale

VI.3 *L'Open government per le imprese. Il recente sistema open del SINFI*

- Il digitale nella gestione delle reti di trasporto e distribuzione del gas e dell'energia elettrica; il risparmio energetico; le reti elettriche *smart;* - Convergenza tra *information technology*, automazione e sicurezza; privacy nella regolazione dei droni; - La finanza di progetto per opere di smart city, il dialogo competitivo ed il partenariato per l'innovazione; premialità per la digitalizzazione delle procedure e per l'innovazione dei progetti; - Il rating d'impresa fondato sull'innovazione; - Le nuove prospettive regolatorie del M2M (machine-to-machine); - Il turismo digitale; l'uso a fini produttivi della digitalizzazione del patrimonio culturale pubblico; la valorizzazione digitale dei beni artistici

VI.4 *Nuove opportunità tecnologiche, contrattuali e finanziarie per la PA*

- *Blockchain e Regolamento UE Eidas; Decreto Semplificazioni; Esempi di applicazione Blockchain in ambito P.A.; Artificial intelligence e algoritmi; Data scientist; Verso un mutamento delle competenzeTecnologie 5G e M2M al servizio della PA*

- Regole contrattuali per servizi di digital innovation. Cloud ComputingFramework contrattuale servizi cloud: Entry + exit strategy; Grace period; GDPR compliance; Localizzazione Server; Penali; Responsabilità; La strategicità della governance

- Programmi UE per l'innovazione. Come beneficiare dei fondi europei; Overview accesso fondi diretti UE e fondi strutturali; Focus sul programma Horizon 2020; Logical Framework Approach. Modello di processo analitico nelle scelte della transizione digitale; verso il nuovo settennato. Europa 2021-2027