PARADIGMA
Ricerca e cultura d'impresa

Percorso formativo

Privacy

Basi di legittimità del trattamento
Milano, 11 ottobre 2018

DPIA e Registro dei trattamenti
Milano, 25 ottobre 2018

Conservazione dei dati, portabilità, tutela del know how aziendale
Milano, 8 novembre 2018

Sicurezza e data breach
Milano, 22 novembre 2018

Baglioni Hotel Carlton

Evento disponibile in videoconferenza
La qualità e l'interattività degli eventi PARADIGMA direttamente su personal computer o tablet

PARADIGMA SpA

Tel. 011.538686
Fax 011.5621123

C.so Vittorio Emanuele II, 68 - 10121 Torino
P.IVA 06222110014
www.paradigma.it
info@paradigma.it

UNI EN ISO 9001:2008

Elenco dei relatori

Avv. Gianluca De Cristofaro
Partner
Intellectual Property, Information Technology and Data Protection
LCA Studio Legale

Prof. Avv. Alessandro Del Ninno
Professore a Contratto di Informatica Giuridica
LUISS Guido Carli di Roma
Of Counsel
Responsabile Dipartimento ICT & Internet Law
Studio Legale Tonucci & Partners

Avv. Adriano D'Ottavio
Associate
Chiomenti
KnowledgeNet Chapter Chair - Roma
International Association of Privacy Professionals (IAPP)

Avv. Nadia Martini
Head of Data Protection (Italy)
Certified Privacy Officer
Associate Partner
Rödl & Partner

Avv. Rocco Panetta
Managing Partner
Panetta & Associati
IAPP Country Leader Italia

Prof. Avv. Pierluigi Perri
Professore di Informatica Giuridica
Coordinatore del Corso di Perfezionamento in Informatica Forense e Protezione Dati
Università Statale di Milano
Avvocato in Milano

Avv. Sonia Piani*
Esperta di Privacy Compliance

Dott. Tommaso Stranieri
DCL Data CompLetence Lab
Data Protection Officer del Network Deloitte

** Il relatore è attualmente Legal Counsel and Data Protection Officer presso General Motors. In questa sede il suo intervento è tuttavia svolto a titolo esclusivamente personale*

Agevolazioni e formazione finanziata

EARLY BOOKING -20%
Alle preiscrizioni formalizzate entro il **10 ottobre** sarà riservata una **riduzione del 20%.**

PROGETTO GIOVANI ECCELLENZE -50%
Iscrivi una seconda risorsa che non abbia compiuto il 35° anno di età con una **riduzione del 50%.**

FORMAZIONE FINANZIATA
Finanzia la tua formazione utilizzando i **Fondi Paritetici Interprofessionali**. Paradigma offre la **completa e gratuita gestione** dei necessari adempimenti.

EVENTO ACQUISTABILE SUL MEPA
Paradigma opera sul MePA e sui principali mercati elettronici di soggetti aggregatori e centrali di committenza

Programma dei lavori

Milano, giovedì 11 ottobre 2018

I MODULO
BASI DI LEGITTIMITÀ DEL TRATTAMENTO

LE LINEE GUIDA WP29 SULLA TRASPARENZA

La nozione di trasparenza nel GDPR
Analisi puntuale di alcune definizioni presenti all'art. 12, c. 1 GDPR
La nozione di "trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile"
La nozione di "linguaggio semplice e chiaro"
Il requisito del linguaggio semplice e chiaro in relazione a bambini e altre persone vulnerabili
Significato di "per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici"
La corretta interpretazione del periodo "Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato"
Il concetto di "free of charge" (art. 12, c. 5 GDPR)

Le informazioni da fornire all'interessato (artt.13 e 14 GDPR)
L'onere, in capo al titolare del trattamento, di adottare "misure appropriate" per fornire all'interessato le informazioni richieste a fini di trasparenza
La tempistica di resa delle informazioni
L'obbligo della trasparenza come obbligo costante di tutto il ciclo del trattamento e l'obbligo di informazione all'interessato circa modifiche sostanziali o materiali del trattamento; i tempi entro cui notificare all'interessato le modifiche
Le modalità di resa delle informazioni: il format (informativa)
L'approccio a più livelli in un ambiente digitale e l'individuazione dei livelli di "Privacy Statements"/avvisi
L'approccio a più livelli in un ambiente non digitale
Avvisi "push" e "pull"
Le misure appropriate diverse dall'informativa "tradizionale"
Informazioni su profilazione e processo decisionale automatizzato
Rischi, regole, salvaguardie ulteriori:
- opportunità di pubblicazione del DPIA (o di una sua parte) quale modalità per promuovere la fiducia nelle operazioni di elaborazione e dimostrare la trasparenza e l'accountability;
- adesione a un Codice di Condotta che meglio dettagli, ad es.: trattamento equo e trasparente; informazioni fornite al pubblico e agli interessati; informazioni fornite ai, e protezione dei, bambini;
- misure che rispondano ai requisiti della protezione dei dati by design e by default, comprese le misure di trasparenza per quanto riguarda le funzioni e il trattamento dei dati personali (Considerando 78 GDPR);
- messa a disposizione degli interessati dei contenuti essenziali di un accordo di contitolarità, in modo da rendere chiaro il titolare a cui rivolgersi per l'esercizio dei propri diritti ex GDPR

Le informazioni relative a trattamenti ulteriori (artt.13 c. 3 e 14 c. 4 GDPR)
La necessità, per il titolare, di partire dall'analisi di compatibilità di cui all'articolo 6 IV c. GDPR, qualora sia invocata una base giuridica diversa dal consenso o dalla legislazione nazionale/UE per il nuovo scopo di trasformazione

Il principio di trasparenza attuato attraverso strumenti diversi dalla comunicazione linguistica
L'utilizzo di tools e, in particolare, di icone (in combinazione con informazioni, come da Considerando 60 e art. 12 c. 7 GDPR), meccanismi di certificazione della protezione e sigilli e marchi di protezione

Le eccezioni all'obbligo di rendere informazioni
L'operatività (e le conseguenze pratiche) del principio di accountability nel caso in cui l'interessato disponga già delle informazioni (art. 13 c. 3 GDPR)
Gli esempi delle Linee Guida
Le eccezioni ulteriori (rispetto a quella "in comune" con l'art. 13) previste nell'art. 14 c. 5 GDPR

Trasparenza e limitazioni ai diritti degli interessati
Le implicazioni pratiche dell'art. 23 c.1 e c.2 lettera h del GDPR:
- la dimostrabilità, da parte del titolare, di rientrare nell'ambito di operatività della previsione limitativa dei diritti;
- l'informazione della limitazione agli interessati, se non confliggente con le finalità della stessa

Prof. Avv. Alessandro Del Ninno
LUISS Guido Carli di Roma
Studio Legale Tonucci & Partners

LE LINEE GUIDA WP29 SUL CONSENSO

La nozione di consenso nel GDPR
La *sedes materie* del consenso nel GDPR: l'art. 4 c. 11 (e i Considerando 42 e 43)
Le caratteristiche di un valido consenso nell'analisi delle LG:
l'essere libero/liberamente ottenuto
- in assenza di "evidente squilibrio" tra interessato e titolare
- in assenza di condizionalità
- in modo granulare
- in condizioni in cui sia possibile negarlo o revocarlo senza pregiudizio

l'essere specifico
l'essere informato
il costituire espressione inequivoca delle volontà dell'interessato

L'ottenimento del consenso in modo esplicito
Le condizioni aggiuntive di un valido consenso
L'obbligo del titolare di (essere in grado di) dimostrare il consenso dell'interessato
L'essere revocabile

L'interazione tra il consenso e le altre condizioni di liceità di cui all'art. 6 comma 2 GDPR

Particolari aree di operatività del consenso
I minori
La ricerca scientifica
L'esercizio dei diritti dell'interessato in presenza di trattamenti basati su consenso

***Quid iuris* dei consensi ottenuti sotto la vigenza della Direttiva 95/46/CE?**

Avv. Nadia Martini
Rödl & Partner

LE LINEE GUIDA WP29 SULLE DECISIONI AUTOMATIZZATE

La profilazione e la decisione automatizzata nel GDPR
La definizione di "profilazione" all'art. 4, comma 1, n. 4 del GDPR
Il processo decisionale automatizzato nell'art. 22 comma 1 e nel Considerando 71

I principi di data protection e le basi di liceità del trattamento rilevanti per profilazione e decisioni automatizzate
L'art. 5 comma 1 (liceità, correttezza e trasparenza; limitazione delle finalità e trattamenti ulteriori; minimizzazione dei dati; l'esattezza; limitazione della conservazione)
L'art. 6 del GDPR (consenso; trattamento necessario per l'esecuzione di un contratto; trattamento necessario per il rispetto di un obbligo legale; consenso necessario per la salvaguardia di interessi vitali, consenso necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; trattamento necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi)
Il trattamento di categorie particolari di dati con sistemi automatizzati: le condizioni e le azioni da intraprendere in presenza di preferenze e caratteristiche aventi natura "sensibile" che scaturiscono dal trattamento automatizzato
I diritti dell'interessato in relazione ai trattamenti automatizzati

Le specifiche previsioni valevoli per i processi decisionali totalmente automatizzati ex art. 22 GDPR
Le eccezioni al divieto di fondare su categorie particolari di dati decisioni in merito alla conclusione o all'esecuzione di un contratto o decisioni autorizzate dal diritto dell'Unione o dello Stato membro

La centralità del DPIA nei sistemi decisionali automatizzati (art. 35 c. 3 lettera a GDPR) e la designazione del DPO in forza della natura dei trattamenti da essi implicati (art. 37 c. 1 lettera b)

Avv. Rocco Panetta
Panetta & Associati

Milano, giovedì 25 ottobre 2018

II MODULO
DPIA E REGISTRO DEI TRATTAMENTI

LE LINEE GUIDA WP29 SULLA VALUTAZIONE DI IMPATTO

L'istituto del Data Protection Impact Assessment
Sedes materiae: l'art. 35 GDPR
Caratteristiche
Casi di obbligatorietà
La nozione di "rischio elevato"
L'assenza di rischio elevato e gli altri casi in cui la DPIA non è richiesta
L'assenza di una scala per misurare il rischio

La realizzazione del DPIA
Le tempistiche
I soggetti sui quali ricade l'obbligo di effettuarlo
Il metodo
DPIA e trasparenza: opportunità di pubblicazione di sintesi del DPIA

Come procedere quando non si riesce ad attenuare il rischio: il ruolo dell'Autorità di Controllo

I tool esistenti per eseguire il DPIA realizzati da Autorità di Controllo
L'esempio del tool elaborato dal CNIL

Avv. Adriano D'Ottavio
Chiomenti

Il DPIA e la valutazione della sua obbligatorietà come "occasione" di censimento dei trattamenti svolti. Le connessioni DPIA - Registro dei trattamenti e la corretta costruzione, compilazione e tenuta del Registro

Esempi di corretta tenuta di un Registro dei trattamenti

Avv. Sonia Piani
Esperta di Privacy Compliance

Milano, giovedì 8 novembre 2018

III MODULO
CONSERVAZIONE DEI DATI, PORTABILITÀ, TUTELA DELLO KNOW HOW AZIENDALE

LA CONSERVAZIONE DEI DATI

La definizione dei tempi di conservazione dei dati personali e di conseguente loro cancellazione al termine del periodo previsto per il trattamento
I riferimenti nel GDPR:
- il Considerando 39 (periodo di conservazione limitato "al minimo necessario"; definizione, da parte del titolare, di un termine per la cancellazione o per la verifica periodica);
- l'art. 5, lettera e (conservazione dei dati in forma idonea a consentire l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità del trattamento);
- l'art. 13 (e l'art. 14), comma 2, lettera a di entrambi (periodo di conservazione o criteri utilizzati per determinarlo quali informazioni necessarie per garantire un trattamento corretto e trasparente)

La necessità di dotarsi di una policy sulla cancellazione o l'anonimizzazione dei dati, una volta esaurite le finalità del trattamento
La conservazione dello stesso dato in più archivi aziendali per finalità diverse (e tempi di conservazione diversi)
Le soluzioni tecnicamente disponibili per gestire gli adempimenti di conservazione (e cancellazione)
Gli orientamenti del Garante sulla conservazione in particolari ambiti nel regime ante GDPR
La data retention dei dati di traffico telefonico e telematico
Il diritto di accesso dell'interessato ai dati conservati dal titolare, alla conoscenza del periodo di conservazione (o dei criteri per la relativa determinazione) e, in caso di trasferimento degli stessi a un paese terzo, dell'esistenza di garanzie adeguate

La scelta su dove (e come conservare)
Archivi cartacei, server interni, servizi di hosting: criteri guida della scelta e accountability

LE LINEE GUIDA SULLA PORTABILITÀ

Il diritto dell'interessato alla portabilità
La definizione di cui all'art. 20 GDPR
Gli approfondimenti delle LG sulle componenti principali di tale diritto
I rapporti tra portabilità e "vecchio" diritto di accesso
Trattamenti in relazione ai quali il diritto alla portabilità trova applicazione
I dati personali che debbono essere portabili

Avv. Rocco Panetta
Panetta & Associati

IL RISPETTO SOSTANZIALE DELL'OBBLIGO DI PORTABILITÀ

Gli obblighi in capo al titolare
L'obbligo per i titolari di informare gli interessati dell'esistenza di tale diritto: le informazioni da fornire previamente a riguardo
L'identificazione dell'interessato che chiede la portabilità: limiti, alla possibilità riconosciuta al titolare, di chiedere informazioni ulteriori per accertare l'identità dell'interessato
La tempistica entro cui ottemperare alla portabilità
Il diniego alla portabilità
La trasmissione diretta dei dati ad altro titolare: il limite del "tecnicamente fattibile"
Il formato di trasmissione dei dati
Il caso degli insiemi estesi o complessi di dati personali
La sicurezza dei dati portabili

Prof. Avv. Pierluigi Perri
Università Statale di Milano

I DATI COSTITUENTI KNOW HOW

Come e perché la gestione e la protezione dei dati personali secondo GDPR può costituire un valore aggiunto anche ai fini della tutela del know how
Cos'è know how e cosa sono i segreti commerciali, anche alla luce del D. Lgs. n. 63/2018
I data base commerciali come know how
La migliore protezione dai dipendenti infedeli e la migliore tutelabilità in sede giudiziale quale know how di un database manutenuto conformemente a GDPR
La definizione di procedure per il controllo della tracciatura del dato: i contratti di data concession agreement con i fornitori per l'imposizione di obblighi di segretezza
Le tutele giudiziali del know how nel D. Lgs. n. 63/2018

Avv. Gianluca De Cristofaro
LCA Studio Legale

Milano, giovedì 22 novembre 2018

IV MODULO
SICUREZZA E DATA BREACH

APPLICAZIONE DELLE LINEE GUIDA SUL DATA BREACH

La nozione di violazione dei dati personali
La definizione nel GDPR e nelle Linee Guida
I tipi di violazioni dei dati personali
Le possibili conseguenze di una violazione dei dati personali

La notifica del breach all'Autorità di controllo (art. 33 GDPR)
Quando notificare

- I requisiti di cui all'articolo 33
- Quando un titolare diventa "consapevole" della violazione
- Cosa succede nei casi di contitolarità
- Gli obblighi del responsabile

La trasmissione delle informazioni all'Autorità di controllo
- Le informazioni da rendere
- L'importanza della previsione di cui all'art. 33 comma 4: la possibilità di fornire informazioni in fasi successive al breach "senza ulteriore ingiustificato ritardo"
- Le notifiche ritardate

Le violazioni transfrontaliere e le violazioni negli stabilimenti extra-UE
Le condizioni nelle quali non è richiesta la notifica

La comunicazione all'interessato (art. 34 GDPR)
Quando informare l'interessato
Le informazioni da fornire
Le condizioni al ricorrere delle quali non è richiesta la comunicazione

La valutazione del rischio e il rischio elevato
Il rischio come trigger per la notifica
I fattori da considerare nel valutare il rischio

Accountability e conservazione dei record
La documentazione dei breaches
Il ruolo del responsabile della protezione dei dati
Gli obblighi di notifica nell'ambito di altri testi normativi (Regolamento eIDAS, Direttiva NIS)

Prof. Avv. Alessandro Del Ninno
LUISS Guido Carli di Roma
Studio Legale Tonucci & Partners

IMPATTI SULLA SICUREZZA CONSEGUENTI ALL'APPLICAZIONE DEL D. LGS. N. 65/2018 (RECEPIMENTO DIRETTIVA NIS)

Il campo di operatività del Decreto e i settori impattati
La scelta "minimalista" del Legislatore interno riguardo agli ambiti di applicazione del Decreto
I settori impattati: energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali; motori di ricerca, servizi cloud e piattaforme di commercio elettronico
Gli effetti del passaggio da misure tecnico-organizzative "minime" a misure "adeguate" alla gestione dei rischi e alla prevenzione degli incidenti informatici: un cambio di filosofia in linea con il GDPR
Il ruolo delle future Linee Guida del Gruppo di Cooperazione quale standard di compliance per l'adeguatezza
Il mantenimento dell'ancoraggio a misure tecnico-organizzative minime per la PA (che non svolga servizi tra quelli ricadenti nei settori di applicazione della NIS): possibili problematiche operative conseguenti al contestuale assoggettamento al GDPR (e alle sue misure "adeguate")?
Gli obblighi di notifica degli incidenti rilevanti
Le sanzioni previste
I prossimi step per la piena attuazione del D. Lgs. "NIS": l'aggiornamento del Piano nazionale per la protezione cibernetica e la sicurezza informatica

Dott. Tommaso Stranieri
DCL Data CompLetence Lab
Data Protection Officer del Network Deloitte

Note organizzative e condizioni

Luogo e data dell'evento
Milano, 11 ottobre 2018
Milano, 25 ottobre 2018
Milano, 8 novembre 2018
Milano, 22 novembre 2018

Sede dell'evento
Baglioni Hotel Carlton
Via Senato, 5 - Milano

Orario dei lavori
9.00 - 13.00 14.30 - 17.30

Quota di partecipazione
Una giornata: € 1.100 + Iva
(Early Booking): **€ 880** + Iva

Due giornate: € 2.050 + Iva
(Early Booking): **€ 1.640** + Iva

Tre giornate: € 2.900 + Iva
(Early Booking): **€ 2.320** + Iva

Quattro giornate: € 3.700 + Iva
(Early Booking): **€ 2.960** + Iva

La quota di partecipazione include la consegna del materiale didattico in formato elettronico, la partecipazione alla colazione di lavoro e ai coffee breaks, la possibilità di presentare direttamente ai relatori domande e quesiti di specifico interesse.

Modalità di iscrizione
L'iscrizione si intende perfezionata al momento del ricevimento del modulo di iscrizione integralmente compilato. Il numero dei posti disponibili è limitato e la priorità d'iscrizione è determinata dalla data di ricezione del modulo. Si consiglia pertanto di effettuare una preiscrizione telefonica per verificare la disponibilità.

Modalità di pagamento
La quota di partecipazione deve essere versata prima dell'effettuazione dell'evento formativo tramite bonifico bancario intestato a:
PARADIGMA SpA, C.so Vittorio Emanuele II, 68 - 10121 Torino
P. IVA 06222110014
c/o Banco Popolare Società Cooperativa
IBAN: IT 78 Y 05034 01012 000000001359

Diritto di recesso e modalità di disdetta
Il recesso dovrà essere comunicato in forma scritta almeno sette giorni prima della data di inizio dell'evento formativo (escluso il sabato e la domenica). Qualora la disdetta pervenga oltre tale termine o qualora si verifichi di fatto con la mancata presenza al corso, la quota di partecipazione sarà addebitata per intero e sarà inviato al partecipante il materiale didattico. In qualunque momento l'azienda o lo studio potranno comunque sostituire il partecipante, comunicando il nuovo nominativo alla Segreteria Organizzativa.

Variazioni di programma
Paradigma SpA, per ragioni eccezionali e imprevedibili, si riserva di annullare o modificare la data dell´intervento formativo, dandone comunicazione agli interessati entro tre giorni dalla data di inizio prevista. In tali casi le quote di partecipazione pervenute verranno rimborsate, con esclusione di qualsivoglia onere o obbligo a carico di Paradigma SpA. Paradigma SpA si riserva inoltre, per ragioni sopravvenute e per cause di forza maggiore, di modificare l'articolazione dei programmi e sostituire i docenti previsti con altri docenti di pari livello professionale.

Crediti formativi
È stata presentata domanda di accreditamento dell'iniziativa ai diversi Ordini Professionali. Per verificare lo stato degli accreditamenti consultare l'area del sito internet www.paradigma.it dedicata all'evento.

Per ulteriori informazioni è possibile consultare il sito www.paradigma.it oppure contattare la Segreteria Organizzativa al numero 011.538686 o all'indirizzo di posta elettronica info@paradigma.it.

Modulo di iscrizione Mod. 3.4 rev. 3

L'iscrizione si intende perfezionata al momento del ricevimento da parte di Paradigma SpA, del presente modulo di iscrizione - da inviare via mail all'indirizzo **info@paradigma.it** - integralmente compilato e sottoscritto per accettazione. La Segreteria Organizzativa provvederà a inviare conferma dell'avvenuta iscrizione.

UNI EN ISO 9001:2008

Dati relativi all'evento

Percorso formativo Privacy

Milano, 11 ottobre 2018	❒ **AULA**	❒ **VIDEOCONFERENZA**
Milano, 25 ottobre 2018	❒ **AULA**	❒ **VIDEOCONFERENZA**
Milano, 8 novembre 2018	❒ **AULA**	❒ **VIDEOCONFERENZA**
Milano, 22 novembre 2018	❒ **AULA**	❒ **VIDEOCONFERENZA**

Dati relativi al partecipante

Nome Cognome

Azienda/Studio/Ente

Funzione aziendale/Professione

E mail

Telefono Fax

Dati per eventuale partecipante under 35

Nome Cognome

E mail

Dati per la fatturazione

Intestatario fattura

Indirizzo

Città CAP Provincia

P. Iva/C. F.

E mail per invio fattura

Dati per la fatturazione elettronica PA

Codice IPA Codice CIG

OdA Data OdA

Altri riferimenti

Per informazioni contattare

Referente

Telefono Fax

E mail

Data e Firma

Ai sensi dell'art. 1341 c.c. si approvano espressamente le condizioni di partecipazione riportate sul sito www.paradigma.it con particolare riferimento alle modalità di disdetta e alle variazioni di programma.

Data e Firma

Informativa Privacy
I dati forniti a **Paradigma SpA** sono raccolti e trattati, con modalità anche informatiche, esclusivamente per evadere la Sua richiesta di partecipazione all'intervento formativo e svolgere le attività a ciò connesse. I dati potranno essere trattati, per conto di **Paradigma SpA**, da dipendenti e collaboratori incaricati di svolgere specifici servizi necessari all'esecuzione delle Sue richieste. Il conferimento dei suoi dati, pur essendo facoltativo, si rende necessario per l'esecuzione del servizio richiesto.

Solo in caso di Sua autorizzazione i dati saranno inoltre conservati e trattati da **Paradigma SpA** per effettuare l'invio di materiale informativo relativo a prossime iniziative di **Paradigma SpA**. Lei potrà esercitare i diritti di cui all'articolo 7 del D. Lgs. n. 196/2003 (accesso, integrazione, correzione, opposizione, cancellazione) inviando una richiesta scritta a **Paradigma SpA** con sede in Torino, C.so Vittorio Emanuele II, 68, tel. 011.538686, fax 011.5621123. Letta l'informativa, acconsente all'utilizzo dei dati inseriti nel presente modulo per l'invio del materiale informativo?

❒ **SI** ❒ **NO**

Data e Firma