UNAGRACO.INFO

ANNO IV - numero 14 - Gennaio 2019

EDIZIONE SPECIALE

Il Convegno Nazionale

Bari 29 gennaio 2019

La Rivoluzione della Privacy per aziende e P.A

I commercialisti e i disagi della digitalizzazione

il numero uno di UNAGRAGO Diretto difende la Categoria e chiede risposte

di *Giuseppe Diretto**

Abbiamo atteso, abbiamo sperato, abbiamo mediato.
Oggi è finito il tempo dell'attesa.
Oggi è il momento di dire basta alle vessazioni ai danni di una intera Categoria e dei contribuenti.
Oggi è giunta l'ora che ognuno si prenda le proprie responsabilità e che il Ministero inizi a dare risposte concrete in termini di semplificazione (sempre attesa e mai arrivata), di diminuzione della pressione fiscale e del riconoscimento del credito d'imposta in favore dei commercialisti. Un credito d'imposta che sia non inferiore a tutti gli investimenti necessari per fornire i servizi dal Ministero stesso richiesti/imposti. È necessario senza alcun ulteriore differimento, un intervento in favore della nostra Categoria, pertanto a favore di tutti gli studi professionale per adeguare le nostre strutture con ogni genere di investimento necessario: dalla formazione del personale, dei collaboratori e dei clienti agli investimenti e aggiornamenti costanti di hardware e software. Attendiamo finalmente un "SI" alle continue istanze di cui continueremo a farci interpreti e promotori instancabili, oltre che chiari e concreti strumenti in favore della categoria che, ricordiamolo, assolve ad una vera e propria funzione sociale irrinunciabile e meritevole di rispetto. Siamo stati penalizzati come categoria dalla rivoluzione digitale che porta senza dubbio con sé grandi vantaggi, ma a cui ci sarebbe dovuti preparare con risorse nuove, tempo e criterio. Questa rivoluzione, invece, ha penalizzato proprio noi Commercialisti. Le nostre molteplici attività (consulenza amministrativa, gestionale, societaria, contabile, fiscale, revisione contabile, revisione legale, revisione enti locali, perizie, consulenze tecniche, liquidazioni, passaggi generazionali, ecc...) sono oggi fortemente compromesse a causa del tempo che ci viene sottratto dall'adeguamento richiestoci, anzi, imposto dalle esigenze fiscali del Governo, che evidentemente ci considera degli "addetti" alla compilazione delle dichiarazioni e non solo, e all'invio telematico; per noi, di contro, tutto questo è solo un aspetto, quasi un corollario,

Giuseppe Diretto

della realtà della nostra professione. Eravamo abituati alle poche pagine delle dichiarazioni dei redditi e dell'IVA, da depositare rigorosamente a mano o spedite a mezzo servizio postale.
Ci siamo sempre mostrati pronti ad eseguire rigorosamente le istruzioni ministeriali, pronti alle levatacce in fila innanzi agli Uffici Provinciali IVA o presso gli Uffici Comunali. In seguito le pagine sono diventate decine e decine, perché le informazioni inviate agli Uffici finanziari "erano insufficienti". E noi, eravamo pronti a leggere centinaia di pagine di istruzioni per compilare le centinaia di pagine che i modelli iniziavano ad accogliere, ma pronti anche a sobbarcarci i costi di carta, stampanti e inchiostro. Pur essendoci mostrati pronti a rispondere alle diverse esigenze non siamo riusciti a stare al passo con la folle corsa della digitalizzazione, mentre qualcuno, ancora una volta, decideva per noi e per le imprese, di lasciare a casa i vecchi modelli cartacei per transitare definitivamente verso i modelli F24 telematici dove i costi (in termini di tempo, risorse lavoro, carta, ecc.) erano e sono ben lungi dal concetto di semplificazione e maggiori economie. Il disagio è contingente. Semplificazione dunque sì, ma la semplificazione è ben altro, non solo un insieme di norme che demandano al "contribuente" e al commercialista le mansioni dei dipendenti degli Uffici ministeriali. Urgente, invece, è un intervento in favore della nostra categoria, pertanto a favore di tutti gli studi professionali per colmare le nostre giuste incapacità tecnico-informatiche, nonché per adeguare le nostre strutture con ogni genere di investimento necessario: dalla formazione del personale, dei collaboratori e dei clienti agli investimenti e aggiornamenti costanti di hardware e software. Nonostante questo siamo pronti ad affrontare più uniti che mai questa nuova rivoluzione digitale.

** Presidente Nazionale UNAGRACO*

UNAGRACO.INFO
Editore
Giuseppe Diretto
Direttore Responsabile
Alessia De Pascale

Redazione: Via Guido Dorso,75 - Bari
ANNO IV - N.14 - Gennaio 2019
Registrazione N.REG. Stampa 29 3963/2014
16/10/2014 Tribunale di Bari
Distribuzione gratuita

Il Convegno Nazionale UNAGRACO di Bari: le principali novità in materia di Privacy

Nella prima tavola rotonda un focus sugli adempimenti necessari per aziende e P.A

La prima tavola rotonda

Un Convegno Nazionale dall'alto contenuto tecnico fortemente voluto da UNAGRACO, quello che si è tenuto a Bari il 29 Gennaio 2019 nel The Nicolaus Hotel: numerosi ed illustri relatori hanno dato il proprio importante contributo al dibattito incentrato, nella prima tavola rotonda, sugli adempimenti e la privacy per aziende e P.A e sulla fondamentale attività della Guardia di Finanza in materia di Privacy.
A portare i saluti al consesso riunito nella sala conferenze il sindaco di Bari **Antonio Decaro**: "È importante essere qui ed è importante il confronto per far crescere la comunità, per rafforzarsi nelle rivendicazioni e per dare utili indicazioni anche ad Enti e Istituzioni", **Nicola Altiero**, Comandante Provinciale della Gdf Bari, **Luigi Pagliuca**, Presidente CNPR, **Elbano de Nuccio**, Presidente ODCEC Bari, **Giovanni Stefanì**, Presidente Ordine Avvocati di Bari e **Roberto Masciopinto**, Presidente Ordine Ingegneri Bari.
L'apertura dei lavori è spettata a **Francesco Avolos**, Presidente UNAGRACO Bari e a **Giuseppe Diretto**, Presidente Nazionale UNAGRACO che hanno dato avvio ai preziosi interventi di esperti del settore privacy di grande prestigio. La prima relazione è stata quella dell'Avvocato barese **Daniela Bataloni**, esperta in privacy che si è soffermata a parlare di innovazione nella Pubblica Amministrazione: «senza una normativa potrebbero naufragare le strategie di rinnovamento con ripercussioni sociali ed economiche. Dunque, la normativa pone le basi per una democrazia dell'innovazione, nel senso che deve essere a beneficio di tutti. Pertanto, sarà necessario che le norme accompagnino ed agevolino il processo di innovazione nella P.A. mediante la diffusione di processi semplificati e tecnologie digitali rivolte a conseguire sistemi diretti al cittadino, il quale deve trarre vantaggio dalle tecnologie digitali in termini di servizi, celerità, conoscenza attraverso, appunto, gli strumenti di comunicazione con lo Stato. Ad ogni buon conto, occorre riflettere sulla non facile realizzazione della dematerializzazione e digitalizzazione e alle difficoltà che permeano la materia. In proposito, le difficoltà di applicazione principalmente operative, derivano dalle innumerevoli modifiche che hanno subito le norme nel susseguirsi degli anni come ad es. il Codice dell' Amministrazione Digitale frutto di numerosissimi interventi, oltre alla vastità delle leggi in materia che devono anche integrarsi ed essere applicate nelle loro differenti finalità come, per esempio, la L. 241/90 sul procedimento amministrativo e di diritto di accesso ai documenti amministrativi, il Regolamento UE

2016/679 del Consiglio e del Parlamento Europeo del 27 Aprile 2016 e Decreto legislativo n. 101 del 10 Agosto 2018; il D.Lgs. n. 33/2013 con il correttivo D.Lgs. 97/2016 riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, il codice dei contratti ecc. Ciò detto, non sempre appaiono comprensibili gli step fondamentali che possano concretizzarsi nel conseguimento degli obiettivi di innovazione che avrebbero indiscutibili effetti innovativi, di rinnovamento e di trasformazione. In questo scenario, la trasparenza dell'azione amministrativa è diretta a rendere cittadini e imprese sempre più informati, coscienti, consapevoli dei meccanismi di funzionamento della Pubblica Amministrazione. Lo strumento giuridico in questione risulta idoneo a rendere più partecipe la collettività alle scelte della PA, comprendendone l'operato, le scelte, divenendo la trasparenza anche strumento di prevenzione della corruzione di cui alla legge 6 novembre 2012, n. 190. Tuttavia, il principio della trasparenza non deve essere inteso in senso assoluto e senza alcun limite o vincolo. Per quanto attiene il trattamento dei dati personali, inoltre, il GDPR UE 2016/679 al Considerando 4 evidenzia: "....Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità.....". Ciò detto, la presente normativa andrà contemperata con quelle esistenti e il principio dell'accountability sarà basilare in tal senso. La trasparenza nel GDPR , distinta dalla Trasparenza prevista dal Decreto Trasparenza, è tra i principi di maggior rilevanza (art. 5, co. 1, a) ed è elemento costitutivo della "responsabilizzazione"; non a caso, la prescrizione della trasparenza, oltre alle sanzioni civili di risarcimento del danno, è assistita dalla sanzione amministrativa di cui all'art. 85 co 5 GDPR che è la più pesante. Nel GDPR, quindi, non basta fare "informativa" ma occorre realizzare la trasparenza e il titolare dovrà dare prova del rispetto della trasparenza stessa. Concludendo, i diritti fondamenti delle persone, a cui attengono anche la riservatezza e la protezione dei dati personali, segnano il passo delle evoluzioni

Dott. Francesco Avolos
Presidente UNAGRACO Bari

Dott. Giuseppe Diretto
Presidente Nazionale UNAGRACO
Vice Presidente ODCEC Bari

Gen. Nicola Altiero
Comandante Provinciale della Gdf Bari

tecnologiche e rappresentano nuovi scenari di convivenza "digitale ". In tal senso deve essere rivolta la normativa, ovvero, regolare l'innovazione continua dei servizi della PA che impone scenari di democrazia basati sull'utilizzo delle tecnologie e deve tener conto dei nuovi problemi che questa evoluzione pone alla società». Ne è seguito l'intervento di **Marcella Caradonna**, Presidente ODCEC Milano, che ha focalizzato il suo intervento sul ruolo del commercialista come team leader delle professionalità necessarie per un corretto adempimento degli obblighi della normativa: «Come è noto, infatti, la tutela dei dati sensibili deve avvenire attraverso la predisposizione di un sistema di procedure con anche il ricorso a tecnologie che riducano quanto più possibile il rischio di diffusione o utilizzo dei dati stessi per usi differenti da quelli per cui la persona ha fornito le informazioni. Perché il sistema sia realmente efficace deve essere costruito sulle specifiche caratteristiche dell'ente. È, quindi, indispensabile conoscere l'organizzazione della impresa, il suo funzionigramma e le dinamiche interne al fin di identificare i punti critici da sottoporre a controllo. In questo contesto il commercialista assume un ruolo chiave poiché è la figura che maggiormente conosce gli aspetti indicati e può ottimizzare il lavoro».

A prendere la parola successivamente è stato **Giuseppe Diretto**, Presidente Nazionale UNAGRACO, che ha focalizzato l'attenzione della platea, avviando un'importante riflessione sulla dimensione della privacy, ossia quali e quanti soggetti hanno il dovere di garantire la protezione dei dati personali: « Per provare a dare queste dimensioni bisogna sfatare qualche mito che, negli anni, si è fatto largo nel pensiero comune e, soprattutto, bisogna pensare che, rispetto al vecchio Codice Privacy, sono cambiate almeno due cose: non ci sono schemi precostituiti per proteggere i dati personali né indicazioni prescrittive; tutto è sulle spalle di titolari e responsabili che dovranno essere in grado di valutare i rischi per i diritti e le libertà fondamentali delle persone fisiche; titolare e responsabile devono saper spiegare in modo chiaro, convincente e documentato le scelte che hanno fatto in termini di misure di sicurezza, sia

tecniche (tipicamente informatiche) sia organizzative (per esempio, dislocazione di archivi cartacei). Dunque, i miti da sfatare. Eccoli. Spesso, si sente dire che bisogna proteggere solo i dati sensibili e, quindi, chi non tratta questo tipo di dati non deve curarsi di rispettare le relative norme. Prima di sfatare questo mito bisogna chiarire che i dati sensibili non esistono più nelle definizioni del GDPR; esistevano, invece, nella vecchia versione del Codice Privacy (Dlgs. 196/2003). Erano i dati riguardanti la salute, l'orientamento sessuale, l'orientamento religioso, e così via. Molti, invece, attribuivano l'aggettivo sensibile a dati personali che non rientravano nella definizione del Codice ma che ritenevano di dover trattare con delicatezza: reddito annuo, punteggio ad un concorso, ecc. Chiarito questo equivoco, conviene sottolineare due aspetti: non è vero che occorre proteggere solo i dati sensibili che il GDPR, oggi, chiama particolari categorie di dati personali; tutti i dati devono essere protetti se riferiti (o riferibili) ad una persona fisica. Quindi occorre proteggere i dati anagrafici, le fotografie, l'indirizzo e mail, ecc. a meno che non siano trattati in ambito strettamente personale; il primo paragrafo dell'art. 9 del GDPR dice che è vietato trattare le particolari categorie di dati personali (gli ex dati sensibili); per fortuna, tuttavia, che lo stesso articolo, al secondo paragrafo, fornisce alcune deroghe che consentono il trattamento. Quindi, la platea di soggetti che devono porre attenzione alla protezione dei dati personali è molto estesa e. di fatto, riguarda tutti gli operatori economici ma anche la maggior parte degli operatori sociali (ONLUS, associazioni religiose, ecc.).

Dott. Luigi Pagliuca
Presidente CNPR

Dott. Elbano de Nuccio
Presidente ODCEC Bari

Avv. Giovanni Stefanì
Presidente Ordine Avvocati di Bari

Ing. Roberto Masciopinto
Presidente Ordine Ingegneri Bari

Un altra frase che, spesso viene ripetuta dagli operatori è "Non sono interessato dalla normativa sulla privacy perché non eseguo operazioni di trattamento". Anche questo è un falso mito perché, leggendo il GDPR, al punto 2, paragrafo 1 dell'art. 4, vengono esemplificate le operazioni di trattamento tra le quali, per esempio, c'è la semplice consultazione oppure la conservazione. Chi, tra gli operatori economici, non svolge questo tipo di operazioni? Tutti abbiamo un archivio, seppur minimo, di documenti che contengono dati personali. Spesso, si sente dire che è interessato alla protezione dei dati personali sono chi li tratta con strumenti elettronici. Anche questa è una falsa credenza: il GDPR, ma anche il Codice Privacy, non fa distinzione tra dati personali trattati informaticamente e dati personali contenuti in documenti cartacei. E, oggi, non basta, come qualcuno continua a credere, l'applicazione delle misure minime di sicurezza contenute nell'allegato B del vecchio Codice Privacy. Oggi occorre una valutazione del rischio piuttosto profonda per ogni processo di trattamento. Questo, per esempio, ha indotto il Garante per la Protezione dei Dati Personali a rivedere i codici deontologici allegati al vecchio Codice Privacy. Questa operazione non è stata solo di ridenominazione da codici deontologici in regole deontologiche (come previsto dal Dlgs. 101/2018) ma ha, di fatto, cancellato ogni riferimento a prescrizioni che potevano indurre il titolare del trattamento ad un mero comportamento adempitivo. Oggi il titolare del trattamento deve avere un comportamento continuamente proattivo per limitare i rischi per i diritti e le libertà degli interessati. Quest'ultimo falso mito, che circola ancora in molti uffici, fornisce l'occasione per approfondire un aspetto del principio di responsabilizzazione (accountability) che costituisce la vera novità del GDPR. Il principio è apertamente

espresso al paragrafo 2 dell'art. 5. "Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)". Molti si sono soffermati sulla parte che obbliga il titolare (o il responsabile) del trattamento ad applicare il GDPR ed a saperlo comprovare. Certamente, il titolare deve garantire un ciclo continuo di impegno nell'applicazione del GDPR e deve documentare il suo percorso. Ma pochi si sono soffermati sull'aggettivo competente (responsible nella versione inglese) che, invece, è centrale nell'interpretazione del singolo articolo oltre che dell'intero GDPR. L'aggettivo competente, in italiano, ha una doppia semantica: vuol dire "capace, esperto, professionale, adeguato" ma anche "che ne ha il compito esclusivo, che rientra nella sua peculiare sfera d'azione". Quindi, il titolare del trattamento dei dati personali è il dominus nell'applicazione del GDPR secondo una professionalità da acquisire direttamente (molto di rado) o indirettamente (affidandosi a specialisti della materia). E basta leggere proprio il paragrafo 1 dell'art. 5 per rendersi conto che la professionalità richiesta è di un livello quasi sconosciuto, almeno in Italia. L'analisi dei processi di trattamento, infatti, deve allargarsi ad ambiti giuridici, informatici ed organizzativi. In fondo, è proprio questo approccio a 360° che fa del GDPR l'occasione per riesaminare i processi che ogni operatore sviluppa nell'ambito della propria attività; un'attenta attività di analisi, finalizzata a condurre il percorso di conformità sulla privacy, può indurre a rivedere i processi operativi e, in molti casi, a renderli più efficienti. Tutto questo ci dice che la protezione dei dati personali deve estendersi su tanti aspetti della vita di un'organizzazione e che la sua taglia sembra essere una XXXL».

Dott. Giovanni Lucatuorto
DPO Azienda Ospedaliero Universitaria Policlinico di Bari

Giovanni Lucatorto, DPO Azienda Ospedaliero Universitaria Policlinico di Bari che ha iniziato la sua analisi partendo dal considerando n° 85, nel quale si citano le potenziali conseguenze di un data breach: «Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. È necessaria, quindi, una premessa prima di affrontare un tema particolarmente complesso proprio in ambito sanitario, nel quale si trattano informazioni più intime dell'individuo. L'Art. 4 del GDPR fornisce le definizioni di alcuni termini. In particolare al punto 1 si fornisce il significato di dato personale: "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale . Ai punti 13 – 14 e 15 del citato Art. 4 si forniscono le definizioni dei dati genetici, di quelli biometrici e di quelli relativi alla salute. 13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; (C34); 14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; (C51)
15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; (C35); Inoltre l'art. 4 al punto n° 12 fornisce il significato di «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati; (C85). Tutto ciò premesso aiuta a porre in primo piano l'obiettivo principale del GDPR: la protezione della persona fisica a cui si riferiscono i dati personali e la libera circolazione di tali dati. È noto che le strutture sanitarie devono garantire il godimento almeno di due diritti fondamentali costituzionalmente riconosciuti: l'Art. 32 e l'art. 2. L'Art. 32 recita: La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività, e garantisce cure gratuite agli indigenti. Nessuno può essere obbligato a un determinato trattamento sanitario se non per disposizione di legge. La legge non può in nessun caso violare i limiti imposti dal rispetto della persona umana. L'Art. 2 recita: La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale. (Il diritto alla riservatezza, quale diritto della personalità dell'individuo vede il suo fondamento giuridico proprio nell'Art. 2 della Costituzione). Pertanto nelle attività svolte quotidianamente le strutture sanitarie devono operare contemperando i citati due diritti senza evidentemente sbilanciarsi o da un lato o dall'altro. Il cittadino, nel nostro caso l'assistito, affida alla struttura sanitaria la sua persona e le sue informazioni più

intime affinché i professionisti sanitari possano ripristinare un bene inestimabile: la salute. Proprio in questo particolare momento della vita dell'individuo, il livello di attenzione sui suoi dati deve essere particolarmente elevato, in quanto la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso illecito ai dati personali dell'individuo può compromettere irrimediabilmente la reputazione, può discriminarlo, può esporlo a furti o usurpazione di identità o anche a perdite finanziarie o peggio a danni materiali e fisici. A titolo meramente esemplificativo si riporta un evento accaduto ad un giovane campano al quale non gli è stato concesso un mutuo in quanto l'ente creditizio è venuto a conoscenza di un potenziale problema di salute del suo cliente. Il comportamento della banca evidentemente ha discriminato il giovane. Ma altrettanto grave potrebbe essere la modifica, accidentale o illecita di un parametro vitale di un valore di un dispositivo sanitario o di un esame di laboratorio. Quanto brevemente esposto, ripercorre uno dei principi cardini del GDPR secondo il quale si deve garantire la Confidenzialità, l'Integrità e la Disponibilità dei dati. A tal proposito il GDPR all'art. 33 prescrive dei precisi adempimenti in caso di violazione dei dati personali ed in caso appunto di perdita della Confidenzialità, Integrità e Disponibilità del dato. La predisposizione di una procedura per la gestione delle violazione è stata una delle priorità indicate dall'Autorità Garante per la Protezione dei Dati Personali. A scopo informativo, con tale procedura si forniscono le istruzioni operative da adottare in caso di una violazione sospetta o certa di un dato personale. La procedura deve essere indirizzata a tutti coloro che trattano dati personali per conto del titolare ai quali è necessario fornire delle indicazioni su degli ipotetici incidenti. E' fondamentale precisare che una violazione di un dato personale può riguardare un dato conservato su un supporto cartaceo o informatico. Effettuata questa prima analisi si apre l'istruttoria necessaria per comprendere l'entità dell'incidente e a seconda del tipo dei supporti interessati si costituisce un team composto da soggetti con competenze diverse. In pratica se l'incidente si è verificato su un dato trattato informaticamente si dovrà interpellare il responsabile dell'ufficio informatico e l'amministratore di sistema al fine di valutare le misure tecniche ed organizzative adottate e la tipologia dell'atto perpetrato. Mentre se il dato compromesso è su un supporto cartaceo si dovranno valutare le misure fisiche ed organizzative adottate e di conseguenza valutare l'inosservanza di quale misura ha causato l'evento avverso. Infine, a titolo esemplificativo, se è stato perso un dispositivo elettronico o un supporto di memorizzazione il team di valutazione dell'incidente dovrà individuare il livello di rischio e di compromissione dei dati e, per esempio, l'adozione di tecniche crittografiche atte a ridurre il rischio di perdita della confidenzialità dei dati. Pertanto la prima fase dell'istruttoria parte con la segnalazione, al titolare e al RPD, di colui il quale ha avuto il sospetto o la certezza di aver riscontrato una violazione. Dopo una tempestiva prima analisi, al fine di individuare la presenza o meno di una violazione, si procede con l'apertura di una segnalazione all'Autorità Garante per la Protezione dei Dati Personali. Dopo lo svolgimento di tutta l'istruttoria, in caso di una violazione dei dati, a seconda dell'entità del danno, si procede con la comunicazione agli interessati e all'Autorità di controllo indicando i dati compromessi e le misure poste in essere per mitigare le conseguenze ed evitare il ripetersi nel futuro. Tutta l'attività istruttoria è agevolata dalla presenza di un registro delle attività di trattamento, dal quale è evidenziabile la tipologia dei dati trattati, le modalità e le misure di sicurezza adottate. Pertanto concludendo, si invita a riflettere che un "maltrattamento" di un dato personale può causare danni irreparabili alla persona fisica a cui si riferiscono i dati».

Gen. Gaetano Mastropierro
Comando Unità Speciali Gdf Roma

Tra i relatori anche **Gaetano Mastropierro** del Comando Unità Speciali Gdf Roma che ha approfondito con un importante contributo l'aspetto della protezione dei dati personali: «un tema che sta diventando sempre più centrale nella società contemporanea e, per effetto dei continue innovazioni tecnologiche, la sfera privata di ogni individuo diventa sempre più esposta a minacce di vario genere. Quotidianamente rendiamo pubblici i nostri dati personali attraverso l'utilizzo dei diversi dispositivi informatici nonché tramite gli oggetti di uso quotidiano sempre più connessi alla Rete. Tutto questo favorisce la divulgazione delle nostre abitudini, delle nostre preferenze e dei nostri stili di vita. L'acquisizione e l'illecito trattamento di tali dati può essere utilizzata in sostanza per definire la nostra reale personalità ed influenzare le nostre scelte in tutti gli ambiti. Emerge con chiarezza, quindi, quanto sia importante tutelare le persone rispetto al trattamento dei propri dati definiti il "petrolio" del nuovo millennio. Proprio in quest'ottica l'Unione Europea in data 4 maggio 2016, dopo anni di discussioni, proposte ed emendamenti, ha adottato il Regolamento Europeo 679 (GDPR), entrato in vigore il 25 maggio 2018. Uno dei temi di maggiore interesse e che ha creato un grande dibattito tra gli addetti ai lavori (e grande "apprensione" tra coloro che devono applicare la disciplina) è quello delle sanzioni irrogabili in materia di privacy. L'attenzione esasperata sulle norme che indicano la "reazione" dell'ordinamento, in ordine a determinati comportamenti non in linea con le prescrizioni dettate dal legislatore, potrebbe però essere riduttiva se finalizzata solo a conoscere le singole fattispecie in vista di un'applicazione meccanica e non ragionata di determinate sanzioni. In questi casi si correrebbe il rischio di non comprendere in profondità un "mondo" molto più articolato di quello che appare. In tale mondo interagiscono, infatti, differenti soggetti che, in

quanto portatori di interessi contrapposti, attivano dinamiche a volte molto complesse. Viene perciò richiesta, in tali circostanze, l'attenta e ponderata valutazione di ciascuna situazione alla luce dell'evoluzione tecnologica e delle tecniche/strumenti utilizzati per trattare i dati personali. I principi ispiratori di tutta la disciplina sulla protezione dei dati personali e la filosofia che ispira tutta la materia richiedono a tutti gli attori di questo settore (controllori e controllati) una particolare sensibilità nel saper individuare e cogliere gli aspetti sostanziali di una normativa che, diversamente dal passato, non prevede più il pedissequo rispetto di regole formali o l'adesione a requisiti minimi ma l'adeguamento a modelli organizzativi ed operativi finalizzati ad una reale e concreta protezione dei dati personali. Il GDPR richiede, infatti, un atteggiamento proattivo da parte dei destinatari degli adempimenti che devono essere in grado di modellare la disciplina in oggetto alle singole e diverse caratteristiche di ciascun contesto di riferimento. La nuova disciplina di cui al Regolamento UE 679/16 evita di imporre a priori regole eccessivamente astratte e lontane da chi in concreto si trova ad effettuare attività che coinvolgono dati personali, per introdurre, attraverso valutazioni, effettuate caso per caso, una disciplina che possa adattarsi alle esigenze di ciascuna realtà imprenditoriale per assicurare una tutela reale ed efficace dei dati personali. Proprio questi aspetti costituiscono i cardini sui cui definire sia i nuovi modelli di gestione sia i nuovi approcci ispettivi. Il cambiamento di prospettiva in questo senso richiede agli operatori del settore competenze nuove e di tipo trasversale in grado di affrontare le problematiche:non solo dell'area giuridica, oggetto di continua evoluzione e destinataria di contributi di differenti discipline relative ad ambiti strettamente collegati con la legislazione della protezione dei dati personali; ma anche dell'area gestionale, con riferimento agli assetti organizzativi, ai ruoli, alle funzioni, ai flussi informativi e alla gestione dei processi di lavoro; e dell'area informatica, avuto riguardo alle strategie di sicurezza aziendale, alle misure standard di protezione ed alle policies di business continuity e disaster recovery. In questi casi appare evidente quanto sia complesso sia il quadro di riferimento. Ma tutto ciò potrebbe non bastare. Nelle realtà organizzative più complesse potrebbero essere indispensabili anche ulteriori competenze riconducibili all'area delle capacità cc.dd. "personali". Quelle capacità che consentono, cioè, di dirigere e coordinare team multi-professionali. Saper lavorare in gruppo, disporre di appropriate doti di leadership, essere in grado di attivare adeguate forme di comunicazione e ascolto, padroneggiare tecniche di problem solving e decision making, sono infatti tutti tratti caratterizzanti di nuove figure professionali che devono sapersi muovere con duttilità in ambienti difficili ove elevate sono le resistenze che si oppongono al "cambiamento" verso nuovi modelli di gestione. Ovviamente il dato di partenza è quello giuridico perché permette di definire gli esatti ambiti di operatività materiale e territoriale delle norme nonché i principi di riferimento a tutela dei diritti degli interessati. Altrettanto importanti ed assolutamente innovativi in tale contesto si presentano altri aspetti come ad esempio: i richiami alla protezione dei dati personali mediante l'adozione di policies improntate ai criteri del risk management (gestione del rischi);l'introduzione del principio della responsabilizzazione (cd accountability); l'attenzione all'adozione di adeguate misure di sicurezza; l'innovativa previsione della designazione, in talune circostanze, del Responsabile della Protezione dei Dati Personali (Data Protection Officer). L'approccio verso l'area delle sanzioni come si può arguire deve caratterizzarsi da un ben più ampia "sensibilità" verso la realtà delle singole organizzazioni. Ovviamente ad ogni operatore, oltre all'indispensabile conoscenza delle singole fattispecie, viene richiesta l'adeguata conoscenza : degli organi di controllo (nazionali ed europei) delle attività ispettive svolte dai suddetti organi di controllo, con riguardo specifico ai vari poteri, agli strumenti operativi ed agli approcci ispettivi; dei procedimenti seguiti per la contestazione di violazioni e dei possibili rimedi amministrativi e giurisdizionali; dei rimedi risarcitori attivabili dagli interessati. Non a caso la privacy può definirsi come "paradigma della complessità"».

Avv. Antonio Matarrese
Partner di Lawapp.it - esperto in Privacy e DPO

Degno di grande interesse tecnico anche l'intervento dell'avvocato barese, **Antonio Matarrese**, esperto in privacy e DPO che si è soffermato sugli aspetti più importanti della materia: «Ogni realtà economica ha delle sue peculiarità specifiche, non ci sono quindi degli approcci ben precisi per analoghe attività; anche perché ciascuna realtà è guidata da "persone diverse" che inevitabilmente compiono sui dati dei trattamenti completamente diversi. In linea generale, tuttavia possiamo individuare delle macro attività che occorre necessariamente svolgere per "conoscere" la realtà alla quale ci approcciamo. L'attività preliminare, nonché la più complessa è l'attività conoscitiva. Molto spesso, infatti, entriamo in aziende o PA che non ci conoscono personalmente; altre volte magari conosciamo l'imprenditore, ma non i dipendenti dei singoli uffici. Quindi bisogna abbattere innanzitutto le barriere "psicologiche" di alcuni soggetti che non sono abituati a ricevere visite di consulenti "curiosi", ovvero soggetti che devono necessariamente compiere un numero elevato di domande per conoscere la realtà aziendale. L'ideale è iniziare a porre domande specifiche iniziando dal reparto amministrativo o da chi si occupa di privacy (reparto informatico o legale, ove siano presenti). Rivolgersi poi ai vari uffici più "delicati", ovvero qui settori che – per loro natura e per il contesto in cui operano – effettuano numerosi trattamenti su una discreta quantità di dati, come ad es. risorse umane, reparto marketing e comunicazione, IT, legale. Il consulente deve riuscire ad ottenere quanto meno una mappatura completa (pur se generica) del modus operandi dell'azienda e, se possibile, la documentazione al mo-

mento utilizzata. Individuare quindi le aree più critiche, cioè quelle che necessità di interventi immediati perché particolarmente esposti (o perché si stanno svolgendo trattamenti particolarmente illeciti); individuare gli eventuali gap da colmare, e iniziare a comprendere l'eventuale necessità di nomina del DPO. Potrebbe essere uno strumento utile dotarsi di una check list introduttiva, da far compilare facendosi supportare dai referenti aziendali competenti per settore; necessari sono in questa fase l'apparato amministrativo per l'individuazione dei responsabili del trattamento, ovvero qui soggetti che concorrono all'attività di trattamento dei dati (figure diverse però tra aziende private e PA); necessario è anche il responsabile IT per la precisa descrizione del patrimonio informatico e relative funzionalità: anche in questo caso pare una ovvietà, ma in moltissime realtà non è presente un vero e proprio censimento della struttura informativa (numero di pc fissi o portatili, presenza di altri device, i programmi scaricati sui singoli dispositivi, antivirus, ecc. ecc.). Dopo questa prima fase preliminare e conoscitiva si passa all' "incubo" di ogni realtà, ovvero l'Analisi dei trattamenti: questa attività si caratterizza proprio dalla necessità di censire con attenzione tutti i trattamenti di dati personali effettuati, tramite le cc.dd. "interviste" con i responsabili dei vari processi aziendali; individuare gli eventuali trasferimenti di dati personali verso paesi extra UE e verificare il rispetto delle disposizioni di cui agli artt. da 44 a 49 del GDPR; raccogliere tutte le informazioni e la documentazione necessaria per la compilazione del registro dei trattamenti (es. applicazioni, servizi esternalizzati, sistemi di controllo dei dati, durata della conservazione dei dati. ecc.). L'errore che può derivare da una scarsa conoscenza della materia è quella di volere immediatamente il "registro dei trattamenti". Ciò tuttavia non è possibile, perché tale documento costituisce proprio l'elaborato finale, ove vanno raccolti e registrati i trattamenti censiti, con le relative ulteriori informazioni che spesso l'azienda non conosce o quantomeno non ha sotto il proprio diretto controllo (ad es. le categorie dei soggetti interessati, i soggetti a cui i dati vengono comunicati o diffusi, la durata di ogni singolo trattamento, ecc.).

Dott.ssa Marcella Caradonna
Presidente ODCEC Milano

Dopo aver effettuato la mappatura, è necessario individuare i possibili ambiti di rischio che dovranno essere oggetto di valutazione. A tal riguardo, ancor prima di esaminare i rischi, occorre definire la "metodologia di analisi" dei rischi più adatta alla realtà organizzativa aziendale, con particolare riferimento ai sistemi informatici. Successivamente occorre: analizzare (per ogni trattamento o per trattamenti simili) sia i rischi connessi ai trattamenti effettuati senza l'utilizzo di strumenti elettronici, che quelli relativi alla configurazione dei sistemi informativi e ai software utilizzati; censire le attuali misure di sicurezza organizzative, fisiche e logiche; definire le misure di sicurezza necessarie a ridurre il rischio entro un livello di accettabilità (es. pseudonimizzazione, cifratura, ecc.; ma anche semplice chiusura degli armadi a chiavi). Infine è necessario avviare politiche di sensibilizzazione, prima, e di controllo, poi, ai principi di privacy by design e privacy by default (art. 25 GDPR); Sulla base dei risultati dell'analisi dettagliata dei flussi dei dati personali – sia all'interno che all'esterno dell'organizzazione aziendale – si potrà cominciare a: definire i contenuti dell'accordo con gli eventuali contitolari; individuare, dopo aver verificato il possesso dei requisiti previsti dall'art. 28 del GDPR, i responsabili del trattamento e definire i contenuti vincolanti del contratto o altro atto giuridico; individuare gli eventuali referenti interni per la gestione delle politiche aziendali in materia di protezione dei dati personali; definire un piano formativo. Solo a seguito dello svolgimento di queste attività, si potrà procedere a redigere il "primo" registro dei trattamenti. All'inizio ci si potrà concentrare solo su ciò che obbligatoriamente l'art. 30 del GDPR prevede; poi potrà via via ricomprendere tanti altri elementi utili per illustrare tutti i trattamenti sviluppati dalla struttura di riferimento, in modo da procedere oltre, con un approccio reale di accountability. Se dette attività sono state svolte correttamente, si passerà alla predisposizione dei documenti e quindi ad aggiornare la documentazione esistente per renderla conforme al GDPR (es. informative, moduli di consenso, eventuali accordi con contitolari, eventuali contratti o altri atti giuridici con i responsabili esterni, policy aziendali); predisporre la documentazione mancante; definire e integrare le procedure di incident management per la gestione dei data breach, implementare le procedure finalizzate ad agevolare l'esercizio dei diritti da parte degli interessati; definire le politiche di data retention. Solo dopo aver svolto tutte le precedenti attività è necessario soffermarsi nuovamente sulla figura del DPO: avremo infatti un quadro più completo della realtà ove stiamo operando per poter valutare se ci troviamo di fronte ad una ipotesi di obbligo di nomina. Alternativamente – pur in caso di assenza di obbligo – ci sia auspica che i nostri referenti aziendali abbiano acquisito una sensibilità maggiore per poter valutare se sia utile comunque dotarsi di un DPO (anche al fine di manutenere il lavoro che è stato compiuto).

In questo contesto, saremo in grado di redigere un ulteriore e più completo registro delle attività di trattamento, aggiungendo tutte le informazioni che prima non avevamo considerando anche che la norma indica un "contenuto minimo" del suo contenuto, ma nulla impedisce di implementare il registro di tutte le informazioni necessarie. Da ultimo sarebbe opportuno definire un sistema di controlli periodici (audit) che consentano il costante monitoraggio del livello di compliance con il GDPR. Ciò può essere necessario per tenere costantemente aggiornato il registro dei trattamenti

e per poter affrontare con immediatezze delle pericolosità che potrebbero essere venute fuori nel tempo o delle situazioni – pur già conosciute – ma che i responsabili aziendali hanno tralasciato o trattato con superficialità. Appare a chi parla molto importante redigere un report finale dell'attività di consulenza, che possa descrivere – anche in via sommaria quello che è stato fatto, ovvero il percorso che la realtà ha compiuto dall'inizio alla fine dell'attività di consulenza. Non sempre questo documento è facile da redigere, perché ci sono delle realtà assolutamente dinamiche che, nel corso del tempo necessario per la messa a norma (spesso passano mesi), mutano il loro aspetto e aumentano la gamma dei trattamenti in maniera impressionante; diventa quindi difficile effettuare una fotografia del "come eravamo e come siamo". Quanto all'impatto delle aziende con il GDPR, molte di primo acchito lo hanno visto con l'ennesimo adempimento in un certo senso "imposto" dall'apparato burocratico e che, come conseguenza immediata, comporta un dispendio di danaro.
Tuttavia ci sono sempre delle realtà virtuose. Di certo, alla prima visita, il mio interlocutore – alla domanda che tipo di trattamento di dati effettuate – ha sempre risposto: "pochissimi trattamenti, di dati ne trattiamo pochi". Naturalmente si può solo immaginare il mio imbarazzo nel dover invece spiegare che le cose non stanno (spesso) come ci si immagina, ma che la realtà è ben più complessa. La difficoltà iniziale è pertanto far comprendere cosa sono i trattamenti, dove essi avvengono, quali sono le criticità o i possibili rischi; tanto più se si considera che spesso non conosciamo il nostro interlocutore né le dinamiche della sua attività aziendale o quant'altro. Quindi si può affermare con certezza che il "percepito" è distante dal "reale". Molto spesso, inoltre, non solo in ambito di primo incontro, ma anche successivamente (nel corso stesso della consulenza) sono emersi dei trattamenti assolutamente non considerati al principio e che purtroppo non sono stati valutati per la elaborazione del preventivo. Secondo la mia personale esperienza, quindi, possiamo individuare tre tipologie di reazioni: ci sono le realtà che si sono dimostrate assolutamente "pronte" al cambiamento, ovvero quelle che già sapevano che la privacy era un elemento fondamentale e imprescindibile del business, ed hanno colto la palla al balzo per poter non solo mettersi a norma, ma anche per realizzare un set up delle funzioni aziendali ed un upgrade delle misure di sicurezza. Generalmente queste realtà hanno un management più giovane, già predisposto al tema privacy, che utilizza i social ed il web in maniera quotidiana ed ha quindi una sensibilizzazione maggiore rispetto ad altri. Naturalmente questi sono gli interlocutori migliori perché coinvolgono il consulente in tutte le attività e sono maggiormente predisposti ad accettare suggerimenti o soluzioni. Inoltre, inutile sottolineare che ove il management aziendale è più sensibile, anche i singoli operatori sono maggiormente motivati e meno resistenti al necessario cambiamento; ci sono poi le realtà con una reazione di tipo "medio": sono quelle dove, a seguito di un impatto iniziale timido, viene compresa l'importanza di un adeguamento e la necessità di approfondire l'argomento. Sono quindi contenti di aver conosciuto il consulente, apprezzano la loro figura, tuttavia sono poco collaborativi. Come sopra accennato, la parte più difficile della consulenza è proprio la parte iniziale, quella conoscitiva, dove ogni realtà deve inevitabilmente non solo mettersi a disposizione ma effettuare un self assessment. È a tal riguardo necessario comprendere che prima ancora che il consulente possa elaborare un assessment, la realtà aziendale e la PA devono effettuare un self assessment: solo infatti chi opera concretamente può realizzare cosa fa con i dati (descrivendo i trattamenti) e descrivere le varie dinamiche dell'attività effettuata. Si perché la prima domanda che porgo ai miei interlocutori quando effettuo l'intervista è: "Lei cosa fa nel corso della sua giornata lavorativa? Qual è la sua attività?" Ed è proprio in questo frangente che l'interlocutore medio incontra maggiori difficoltà, perché gli si chiede uno sforzo in più che non vuole compiere: quindi si all'attività del consulente, ma no ad un coinvolgimento personale (non solo per un discorso di invadenza del consulente, ma anche per l'adempimento stesso che evidentemente è ulteriori rispetto all'attività aziendale); da ultimo ci sono gli "indifferenti", ovvero le realtà dove il GDPR non è arrivato, non lo si conosce, ovvero pur avendone sentito parlare si ritiene che non sia applicabile alla propria realtà. Naturalmente dopo un primo approccio, in cui si comprende che la norma è applicabile trasversalmente, l'atteggiamento non cambia. Inutile evidenziare che in queste realtà è difficilissimo lavorare, il consulente fa una fatica enorme a svolgere il proprio compito anche perché, ad un management aziendale per nulla sensibile, corrisponde una realtà aziendale impenetrabile, poco affidabile dove qualsiasi sforzo compiuto sarà inevitabilmente reso vano dopo poco tempo. Appare evidente che il ruolo del consulente - soprattutto in questa ultima categoria - è molto molto importante: se infatti si vuole svolgere una consulenza di qualità, occorrono consulenti responsabili che sappiamo ben informare i propri clienti delle necessarie attività da compiere. Sottolineo questo aspetto perché mi è capitato di imbattermi in realtà che hanno scelto consulenti i quali hanno parlato di adempimenti facili, di modelli agevolmente adattabili ad ogni realtà, di soluzioni software che "fanno tutto". In sostanza, parrebbe possibile affrontare il GDPR con soluzioni pronte, pacchettizzate, anche senza l'ausilio di un consulente, ma magari con supporto del gestore del servizio informatico (che magari ha fatto un corso di 4 ore sull'argomento).
Chi conosce il GDPR sa che ciò non è possibile; affrontare la novità normativa non è affatto semplice, ci vogliono competenze elevate con diversi settori di specializzazioni (legale ed informatico più degli altri, a mio avviso). Non ci si può affatto improvvisare, non solo perché le norme sono molto complesse e rigorose, ma anche perché le sanzioni sono elevate. E' evidente a tal riguardo che si auspica che ci siano controlli in tutte le realtà, ove il GDPR è stato affrontato con superficialità affinché si possa definitivamente porre fine ad un approccio di questo genere che, non solo è poco professionale, ma non consenti al sistema di operare come dovrebbe, cioè come una macchina perfetta capace di non incepparsi in alcuno dei propri ingranaggi».

Il contributo di **Ilaria Rizzo**, DPO Comune di Bari, si è focalizzato, invece, sulla sua fondamentale esperienza sul Data Protection Officer negli enti locali: « Quando l'Amministra-

zione mi ha nominato Responsabile della Protezione dei Dati Personali del Comune di Bari ho da subito avvertito la delicatezza e l'importanza del ruolo soprattutto perché nel trattamento dei dati personali bisogna ridurre al minimo gli errori. Perché sono in ballo i diritti e le libertà fondamentali dei cittadini. Sotto tale profilo le Linee guida n. 243 del WP29 adottate definitivamente il 5 aprile 2017 ribadiscono un concetto fondamentale: gli interessati, ovvero le persone fisiche di cui si trattano i dati personali, sono bisognose di protezione soprattutto quando hanno un margine esiguo di decisione rispetto al trattamento dei loro dati. Ed è proprio quello che accade nel caso degli organismi pubblici: esistono norme che impongono ai soggetti pubblici di trattare dati personali dei cittadini. Questi ultimi non possono sottrarsi e, quindi, necessitano di una tutela maggiore che viene garantita, appunto, dal DPO. Il naturale corollario di questa circostanza è che il DPO, nelle pp.aa. deve conoscere le norme che regolano l'ambito pubblico. È un lavoro, quindi, molto più impegnativo del DPO in ambito privato per almeno un paio di motivi: il quadro normativo cambia continuamente e, poiché il GDPR impone la privacy by design, ogni variazione impone una revisione dei processi di trattamento, almeno per verificare che i cambiamenti negli aspetti operativi siano conformi ai principi previsti dalla protezione dei dati personali; l'ambito privato è meno vincolato dal quadro normativo; il soggetto privato si autodetermina e si auto-vincola per rispondere a logiche di mercato cioè decide autonomamente quali sono i processi di business e come condurli; quindi, non deve inseguire nessuno e, già in fase di progettazione, può modellare i processi di business affinché il trattamento dei dati personali rispetti i principi del GDPR e sia condotto, a regime, con maggiore semplicità.

Avv. Ilaria Rizzo
DPO Comune di Bari - Direttore della Ripartizione Segreteria Generale

Per un DPO in ambito pubblico, le norme da rendere compatibili con il GDPR e con il Codice Privacy (recentemente aggiornato dal Dlgs. 101/2018) sono tante e richiedono, quindi, un approccio olistico: le norme sulla trasparenza, cioè il Dlgs. 33/2013, volte a favorire forme diffuse di controllo sulle pubbliche amministrazioni, sono una fonte continua di impegno nel bilanciamento tra la casa di vetro e la privacy delle persone; non a caso, il Garante per la Protezione dei Dati Personali è spesso impegnato ad esprimere pareri sulle istanze dei Responsabili della Prevenzione della Corruzione e della Trasparenza di enti locali a fronte di richieste di riesame proposte da soggetti che volevano esercitare l'accesso generalizzato (previsto dal comma 2 dell'art. 5) agli atti della pubblica amministrazione; e, non a caso, l'ANAC ha prodotto ed aggiornato apposite le linee guida, concordate con il Garante, sia sugli obblighi di pubblicità sia sull'accesso generalizzato; le norme anticorruzione che, spesso, costringono a trattamenti che sono piuttosto invasivi della privacy delle persone; le norme sulla scelta del contraente, di cui l Codice dei Contratti Pubblici, che, incrociate con il comma 1 dell'art. 28 del GDPR, diventano molto critiche già in fase di avvio delle procedure di gara; infatti, quando si tratta di mettere a gara un servizio nell'ambito del quale saranno trattati dati personali (per esempio, il servizio di gestione delle entrate comunali), il contraente dovrà essere designato come responsabile del trattamento e, quindi, dovranno essere valutate, già in sede di candidature, le "garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR". Significa che, per evitare la culpa in eligendo, bisognerà definire il disciplinare di gara richiedendo al candidato una specifica sezione della proposta tecnica volta a spiegare come proteggerà i dati che l'ente pubblico intende fargli trattare; le norme sulla digitalizzazione, di cui al Codice dell'Amministrazione Digitale (CAD); il DPO dovrà agire in stretto contatto con il Responsabile per la Transizione Digitale, figura prevista dall'art. 17 del CAD, che, tra le altre attività, ha compiti di "indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture"; le norme sulla tutela dei beni culturali, di cui al Dlgs. 42/2004 (Codice dei beni culturali e del paesaggio); non bisogna dimenticare che i dati personali sono ancora molto presenti sui documenti cartacei e che questa specifica normativa prevede, all'art. 10, comma 2, che sono beni culturali "gli archivi e i singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonche' di ogni altro ente ed istituto pubblico"; questo principio deve essere coniugato efficacemente con il principio di limitazione della conservazione previsto dal GDPR. A questo quadro normativo, di carattere generale, si aggiungono le specificità degli enti pubblici locali (Dlgs. 267/2000) che complicano il lavoro rendendolo, tuttavia, ancora più affascinante».

L'impatto della manovra economica 2019 su contribuenti, professionisti e imprese

I contributi dei relatori e degli esperti della seconda tavola rotonda

Sen. Gianmauro Dell'Olio
5 Commissione permanente (Bilancio)

Dott. Luigi Pagliuca
Presidente CNPR

Dott. Antonio Gigliotti
Direttore Fiscal Focus

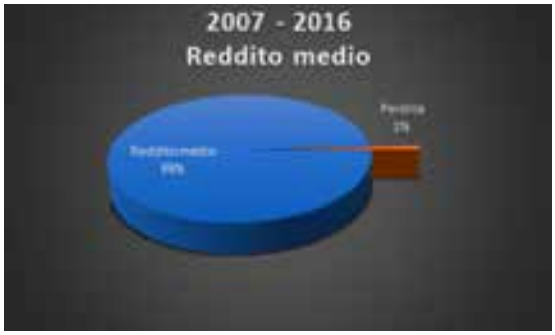
Giuseppe De Filippi
Vice direttore TG5

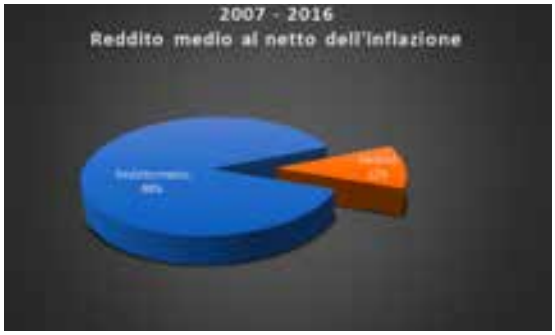
Illustri ospiti hanno portato il proprio contributo alla seconda tavola rotonda, moderata da Giuseppe De Filippi e dedicata all'impatto della manovra economica 2019 sui contribuenti, professionisti e imprese. Di grande spessore tecnico l'intervento di Luigi Pagliuca, Presidente della Cassa di previdenza dei Ragionieri: «Il commercialista rappresenta da sempre una figura centrale nell'economia del nostro paese. Dietro ogni imprenditore, ogni realtà economica, c'è sempre un commercialista, che offre un ruolo di supporto e di consulenza indispensabile. I valori e i principi generali a cui questi professionisti devono attenersi sono l'interesse pubblico, l'integrità, l'obiettività, la competenza, la diligenza, la qualità delle prestazioni, l'indipendenza, la riservatezza, il comportamento professionale. Quella del commercialista è una professione unica nel suo genere: tante competenze (economia aziendale, diritto di impresa, finanza, tributi, diritto societario e del lavoro, pubblica amministrazione), che coinvolgono settori molto diversi tra loro. La formazione interdisciplinare, vero e proprio vantaggio competitivo di questa figura professionale, consente al commercialista di avere una visione più completa delle problematiche dei propri clienti rispetto ad altre figure professionali. Nonostante ciò, la categoria non vive un momento felice. E sono i numeri ad illustrarci la situazione. Le difficoltà del momento, infatti, sono ben rappresentate dal dato relativo alle statistiche reddituali: se il reddito medio nominale, tra il 2007 e il 2016, è diminuito solo dell'1 per cento, lo stesso reddito medio al netto dell'inflazione si è ridotto del 12 per cento, come dimostrato dalle statistiche ricavate dal "Rapporto 2018 sull'Albo dei Dottori Commercialisti ed Esperti Contabili" elaborato dalla Fondazione Nazionale Commercialisti. Negli ultimi 10 anni non solo il potere di acquisto del reddito è diminuito, come già segnalato, ma il calo è ancora più evidente se si prendono in considerazione i redditi degli Under 40. Non solo sebbene la professione, in termini di numero di scritti, stia crescendo, tale crescita è in costante calo. In base alle risultanze del "Rapporto 2018 sull'Albo dei Dottori Commercialisti e degli Esperti Contabili" la linea di tendenza proietta "la crescita a popolazione zero" entro i prossimi 4 anni.

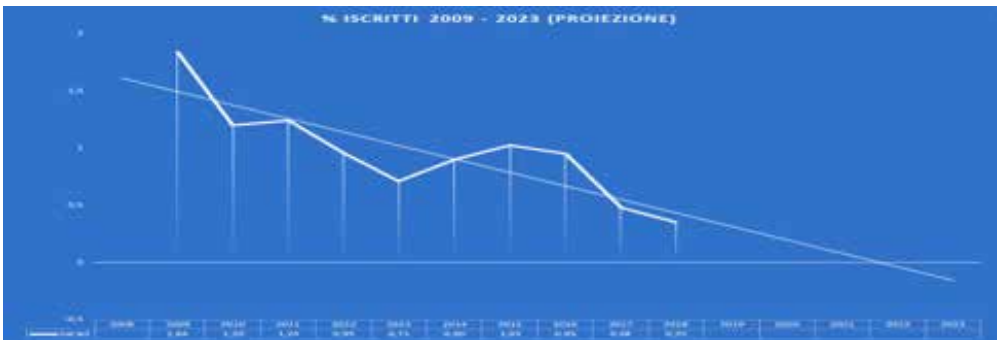
Sono dati allarmanti, che non vanno sottovalutati ma che anzi devono essere il punto di partenza per una riflessione condivisa sul futuro della nostra professione. Invertire la rotta è ancora possibile, ma il tempo a disposizione si riduce ogni giorno di più».

A seguire di grande rilevanza anche l'intervento di Antonio Gigliotti, direttore di Fiscal focus che si è soffermato sugli effetti della manovra economica 2019: «La Legge di Bilancio 2019 (Legge n. 145 del 30/12/2018 pubblicata sul S.O. alla G.U. n. 302 del 31 dicembre 2018), prevede numerose disposizioni di interesse fiscale tra conferme, proroghe, rimodulazioni, abrogazioni e novità. Per il "pacchetto casa", accanto alle ormai "tradizionali" detrazioni per gli interventi di recupero edilizio e risparmio energetico, si segnalano la proroga dell'agevolazione per l'acquisto di mobili ed elettrodomestici e del bonus verde. La legge di bilancio 2019, ha esteso l'ambito applicativo della cedolare secca sui canoni di locazione aventi ad oggetto le unità immobiliari classificate nella categoria catastale C/1. Questa condizione non è però sufficiente. È necessario anche che le unità immobiliari siano di superficie non superiore a 600 metri quadrati, escluse le pertinenze. Viene esteso il regime forfetario introdotto dalla Legge n. 190/2014 a coloro che nell'anno

precedente hanno conseguito ricavi o percepito compensi, non superiori a 65mila euro. Le modifiche sono così "invasive" che ne è conseguito un regime completamente nuovo. Tuttavia, nonostante il restyling, si realizza una sostanziale continuità tra il "vecchio" ed il "nuovo" regime. La Manovra 2019, ha modificato anche i criteri di utilizzo delle perdite di impresa da parte dei soggetti passivi Irpef. Le novità riguardano sia le imprese in contabilità semplificata, che determinano il reddito ai sensi dell'art. 66 del TUIR, ma anche le imprese in contabilità ordinaria. La novella è retroattiva trovando applicazione già dalla prossima dichiarazione dei redditi 2019, relativa al periodo di imposta 2018. Sono interessate dalla nuova misura anche le società di persone. Sono esonerati dall'obbligo dalla fattura elettronica i contribuenti "minimi", forfettari", piccoli produttori agricoli, pienamente operativo a partire dal 1° gennaio 2019, sia nei rapporti B2B che B2C. Accanto ai soggetti esonerati, possono essere individuate ulteriori categorie di contribuenti per i quali la normativa fiscale dispone non un esonero ma un divieto all'emissione della fattura in formato elettronico, ci riferiamo agli operatori sanitari per i quali il divieto opera in relazione alle spese sostenute dai contribuenti nel corso







dell'anno da trasmettere al Sistema Tessera Sanitaria ai fini della predisposizione della dichiarazione precompilata da parte dell'Agenzia delle Entrate. In prossimità dell'approvazione della Legge di Bilancio 2019 i commenti della stampa specializzata si sono concentrati sull'incremento della soglia dei ricavi e dei compensi per accedere al regime forfetario. Non è più previsto un limite per ogni categoria economica, ma la soglia è unica per tutti i soggetti, ed ammonta a 65.000 euro. La vera "rivoluzione" riguarda la cancellazione" delle altre condizioni per poter accedere al regime forfetario. Il Legislatore ha compreso che per produrre 65.000 euro di ricavi o di compensi il contribuente potesse avere necessità di avvalersi dell'aiuto di lavoratori dipendenti, collaboratori o anche di beni strumentali. Il Legislatore abrogato il limite di spesa, in precedenza pari a 5.000 euro, che in passato impediva l'accesso al regime forfetario. La verifica delle condizioni per poter determinare il reddito secondo i criteri forfetari all'uopo previsti deve essere effettuata con riferimento all'anno precedente. Si deve però tenere conto che le novità in rassegna sono applicabili sin dal 1° gennaio 2019. Conseguentemente se il contribuente ha sostenuto nell'anno 2018 spese per lavoro dipendente di importo pari a 15.000 euro e, in mancanza della nuova disposizione sarebbe stato obbligato ad uscire dal regime forfetario, a seguito della novità prevista dalla Legge di Bilancio 2019 potrà continuare a determinare il reddito con l'applicazione del coefficiente di redditività previsto specificamente per l'attività esercitata. Allo stesso modo è irrilevante l'ammontare dei beni strumentali utilizzati nell'attività al 31 dicembre dell'anno precedente. Se, ad esempio, il contribuente ha effettuato ulteriori acquisti dei predetti beni nell'anno 2018, superando, quindi, il "vecchio" limite di 20.000 euro, potrà continuare a beneficiare dell'applicazione del regime forfetario anche nell'anno 2019. Tra le novità introdotte, mediante la sostituzione integrale della lettera d) al comma 57 dell'articolo 1 della Legge 190/2014, il Legislatore ha riformulato le cause ostative all'applicazione del regime agevolato connesse alla detenzione di partecipazioni. Fino al 31 dicembre 2018, il regime forfetario era precluso dal contemporaneo possesso di partecipazioni in società di persone o associazioni professionali (articolo 5, TUIR), ovvero in Srl in regime di trasparenza (art. 116, TUIR). Dal 1° gennaio 2019, invece, la menzionata lettera d) del comma 57 preclude l'applicazione del regime nei confronti degli: "esercenti attività d'impresa, arti o professioni che partecipano, contemporaneamente all'esercizio dell'attività, a società di persone, ad associazioni o a imprese familiari di cui all'articolo 5 del testo unico (…), ovvero che controllano direttamente o indirettamente società a responsabilità limitata o associazioni in partecipazione, le quali esercitano attività economiche direttamente o indirettamente riconducibili a quelle svolte dagli esercenti attività d'impresa, arti o professioni". Per le prestazioni sanitarie da inviare al Sistema Tessera Sanitaria, ai sensi del D.L. 119/2018 come modificato dalla legge di bilancio 145/2018, vige il divieto di emissione di e-fattura. Sul punto l'Agenzia, nel corso del convegno del 15 gennaio, ha confermato che tale divieto vige anche nel caso in cui il paziente esprima opposizione all'invio dei dati al Sistema Tessera Sanitaria. Operativamente, un operatore del settore sanitario, per comprendere come emettere la fattura dovrà innanzi tutto verificare i seguenti punti: 1. La fattura è emessa verso una partita IVA (B2B)? Se la risposta è affermativa, si tratta di spesa non indicabile in Tessera sanitaria, pertanto la fattura deve essere emessa in formato elettronico; 2. La fattura ha per oggetto un'operazione che non rileva ai fini di TS, quale, ad esempio, la cessione di un bene strumentale oppure un'attività di docenza ad un convegno? Se la risposta è affermativa, si tratta anche in questo caso di spese da non trasmettersi al Sistema TS, pertanto la fattura deve essere emessa in formato elettronico. Se, invece, la fattura è emessa per prestazioni sanitarie effettuate a favore di un "privato", ovvero con indicazione del solo codice fiscale del cliente, e riguarda prestazioni che rientrano nel novero di quelle da comunicarsi al Sistema TS da parte dei soggetti interessati a tale adempimento, allora la fattura dovrà obbligatoriamente essere cartacea (anche nel caso di opposizione alla trasmissione dei dati da parte del paziente). Questo divieto vale per il solo anno 2019. La discriminante che porta al divieto di e-fattura è dunque quella che la fattura riguardi una prestazione che deve essere trasmessa al Sistema Tessera Sanitaria (o che dovrebbe essere trasmessa, fatto salvo il diritto per il paziente di opporsi). Specularmente, scatta l'obbligo di fattura elettronica laddove la fattura non sia trasmissibile al sistema TS poiché emessa da un soggetto non tenuto all'invio dei dati a tale sistema, quali gli odontotecnici. In questi casi, dunque, l'obbligo di emissione di fattura elettronica è pienamente operativo, posto che il dettato della norma (articolo 10

bis del D.L. 119/2018) dispone il divieto di e-fattura solo a carico dei "soggetti tenuti all'invio dei dati al Sistema tessera sanitaria". La Legge di Bilancio 2019 ha modificato completamente i criteri di utilizzo delle perdite di impresa da parte dei soggetti passivi Irpef. Le novità riguardano sia le imprese in contabilità semplificata, che determinano il reddito ai sensi dell'art. 66 del TUIR, ma anche le imprese in contabilità ordinaria. La novella è retroattiva trovando applicazione già dalla prossima dichiarazione dei redditi 2019. Il legislatore ha di fatto realizzato un perfetto allineamento della disciplina delle imprese soggette ad Irpef, con la disciplina del riporto a nuovo delle perdite dei contribuenti soggetti ad IRES. Per tale ragione, con la novella, viene rimosso il limite temporale del riporto a nuovo delle perdite che potranno essere riportate in avanti, ed utilizzate in compensazione, anche oltre cinque anni e senza alcun limite di tempo. Il legislatore non ha previsto una disciplina transitoria al fine di individuare le perdite "vecchie" che potranno essere portate in avanti senza limiti di tempo. Il riferimento potrà essere ragionevolmente rappresentato dalla Circolare dell'Agenzia delle entrate n. 53 del 2011. Secondo il predetto documento di prassi entrano nel "meccanismo" del riporto illimitato le perdite non prescritte nell'anno di prima applicazione della novità normativa (anno 2018). A tal proposito deve essere osservato come l'art. 1, comma 24 della legge n. 145/2018 preveda, in deroga allo "Statuto del contribuente" l'applicazione retroattiva della novella. In particolare, si dispone che "In deroga all'articolo 3, comma 1, della legge 27 luglio 2000, n. 212, le disposizioni di cui al comma 23 del presente articolo si applicano a decorrere dal periodo d'imposta successivo a quello in corso al 31 dicembre 2017". Per i contribuenti con periodo d'imposta coincidente con l'anno solare, la prima applicazione riguarderà il periodo d'imposta 2018. Conseguentemente sono utilizzabili senza limiti di tempo le perdite riferibili al periodo di imposta 2013 che avrebbero potuto essere utilizzate in compensazione con gli eventuali redditi relativi al periodo di imposta 2018. Quest'anno sarebbe stato, ove non fosse entrata in vigore retroattivamente la novella, l'ultimo anno di utilizzo delle perdite. Invece, in caso di mancata compensazione, le perdite riferibili al predetto periodo di imposta 2013 potranno essere utilizzate in avanti senza alcun limite temporale. I contribuenti in contabilità semplificata potranno iniziare ad effettuare la compensazione verticale, senza limiti di tempo, dalla prossima dichiarazione dei redditi relativa al periodo di imposta 2018. Tuttavia, inizialmente il legislatore ha previsto l'applicazione di un limite inferiore all'80 per cento. Tale misura si applicherà solo con decorrenza dal periodo di imposta 2021. In buona sostanza dal reddito conseguito nel periodo di imposta 2021, potranno essere considerate in diminuzione le perdite pregresse fino al limite massimo dell'80 per cento. La disposizione in commento prevede la possibilità di scomputo delle perdite in diminuzione dei redditi: nei periodi di imposta 2018 e 2019 in misura non superiore al 40 per cento dei redditi dichiarati; nel periodo di imposta 2020 in misura non superiore al 60 per cento dei redditi di impresa dichiarati; nel periodo di imposta 2021 e nei successivi, a regime, in misura non superiore all'80 per cento dei redditi dichiarati. La disposizione prevede anche la possibilità di "recuperare" le perdite maturate nel periodo d'imposta 2017, cioè nel primo anno di applicazione del regime di cassa, e non utilizzate a causa del "divieto" normativo secondo le disposizioni allora in vigore. Anche in questo caso la possibilità di utilizzo è graduale. In particolare, le predette perdite sono computate in diminuzione dei redditi conseguiti: nei periodi di imposta 2018 e 2019 in misura non superiore al 40 per cento dei medesimi redditi dichiarati; nel periodo d'imposta 2020 in misura non superiore al 60 per cento dei redditi di impresa dichiarati.

ISFORM
Istituto per la Formazione Manageriale

Con il patrocinio di:

UNAGRACO · CONFINDUSTRIA Bari e Barletta-Andria-Trani Giovani Imprenditori · OIBA Ordine degli Ingegneri della Provincia di Bari

5°edizione

Corso di **Alta Formazione Manageriale** per

DATA PROTECTION OFFICER
MANAGER PRIVACY
PRIVACY SPECIALIST

Ruolo e compiti della nuova figura prevista dal Regolamento 2016/679/UE

Corso qualificato CEPAS
iscritto al n°154 del Registro dei Corsi Qualificati

Chi è il DPO

Dal 25/05/2018, a seguito dell'entrata in vigore del Nuovo Regolamento Europeo in materia di Protezione dei Dati, tutte le amministrazioni e gli enti pubblici; tutte le aziende la cui attività principale consiste in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; tutti i soggetti la cui attività principale consiste nel trattamento di dati particolari, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici, dovranno obbligatoriamente dotarsi di un Responsabile della Protezione dei dati. Il Data Protection Officer è un professionista con particolari competenze in campo informatico, giuridico, di risk management e di analisi dei processi. E' anche dotato di qualità manageriali ed organizzative affinchè sia in grado di assistere il Titolare del trattamento per l'adozione di adeguate misure tecniche ed organizzative.Informa e fornisce consulenza al Titolare o al Responsabile del trattamento, in merito agli adempimenti previsti dal GDPR. Il DPO svolge un ruolo chiave nella promozione della cultura della protezione dei dati all'interno dell'azienda, contribuisce a sorvegliare il rispetto dei principi fondamentali previsti dal regolamento, a garantire i diritti degli interessati, ad attuare il principio della privacy by design e by default, a notificare le violazioni dei dati personali e coopera e funge da punto di contatto con l'Autorità di controllo.

Obiettivi

Il corso **ISFORM di Alta Formazione Manageriale** è pensato per formare consulenti e referenti privacy per le aziende nel settore pubblico e privato o liberi professionisti, che intendano ricoprire il ruolo di **Data Protection Officer** *(Responsabile della protezione dei dati)*, **Manager Privacy** e **Privacy Specialist**, in conformità al **GDPR** (*Nuovo Regolamento Europeo*) entrato in vigore lo scorso 25 Maggio 2018. Il Corso per il "Data Protection Officer" fornirà ai partecipanti una preparazione manageriale completa e multidisciplinare secondo quanto previsto dal Regolamento UE per la protezione dei dati personali.

Destinatari

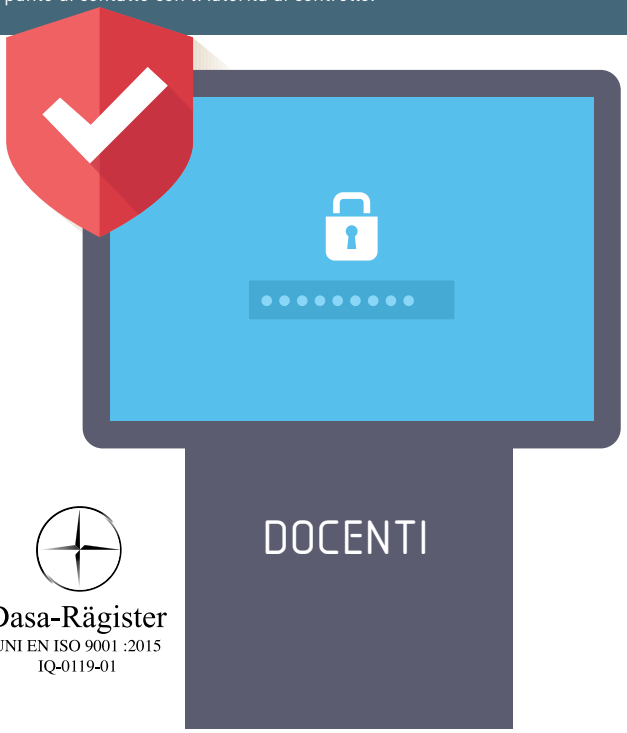
Dipendenti e dirigenti aziendali (pubblici o privati), commercialisti, ingegneri, informatici, neo laureati, legali d'impresa, consulenti che ricoprono o intendano ricoprire il ruolo di:

- DATA PROTECTION OFFICER **80 ORE** (moduli da 1 a 6)

Sedi

Edizione Bari: *The Nicolaus Hotel, Via Cardinale Agostino Ciasca, 27 - 70124 Bari*
Edizione Roma: Piazza san Bernardo, 106 – 00185 Roma

DISPONIBILE LA VERSIONE E-LEARNING



Dasa-Rägister
UNI EN ISO 9001 :2015
IQ-0119-01

Avv. Daniela BATALONI
Avvocato in Bari - Esperto in privacy

Lino FORNARO
Esperto in Sicurezza delle Informazioni e Privacy - Evolumia Srl

Dott. Giuseppe GIULIANO
Funzionario Dipartimento Attività Ispettive e Sanzioni del Garante per la Protezione dei Dati Personali - ROMA

Dott. Giovanni LUCATORTO
Data Protection Officer - Azienda Ospedaliero Universitaria Policlinico di Bari

Dott. Francesco MALDERA
Esperto di protezione dei dati personali e dei processi di digitalizzazione Data Protection Officer – Già dirigente nella Pubblica Amministrazione di strutture di audit e sicurezza, di governo dei sistemi informativi e di servizi al cittadino

Avv. Antonio MATARRESE
Avvocato in Bari e Milano - Partner di LawApp - esperto in Privacy e DPO

Avv. Sandra MELILLO
Avvocato del Foro di Brindisi, esperto in diritto penale d'impresa

Dott.ssa Loredana ROSSIELLO
Esperta in privacy e DPO certificata

Coordinatore

Dott. Giuseppe DIRETTO
Commercialista – Vice Presidente Ordine Dottori Commercialisti Bari - Presidente Nazionale UNAGRACO

La Gallery del Convegno

Il direttivo UNAGRACO

La platea

Il sindaco di Bari Antonio Decaro al Convegno UNAGRACO

Gli ospiti del Convegno

L'UNAGRACO, l'ODCEC di Roma e con la collaborazione di **ISFORM &Consulting srl - Istituto per la formazione manageriale** presenta:

Master per Consulente aziendale GARE E APPALTI PUBBLICI

(Edizione base – Edizione avanzata)

Destinatari

Il Master è rivolto ad avvocati, commercialisti, ingegneri, imprenditori, dirigenti, funzionari, amministratori, responsabili di uffici tecnici e tutti coloro che intendano ricoprire il ruolo di consulenti aziendali in materia di Appalti pubblici.

Obiettivi

Alla luce della Nuova Riforma in materia di Appalti Pubblici e in virtù dell'elevato livello di specializzazione della normativa che disciplina la contrattualistica pubblica, i professionisti devono far fronte a nuove conoscenze e approfondire le dinamiche e le procedure di gara ed esecuzione dei contratti. Il Master, dunque, si propone di formare consulenti in grado di gestire correttamente problematiche connesse ad aspetti procedurali ed economici sempre più complessi per accompagnare le imprese in questo processo e diventarne punto di riferimento. L'obiettivo è di trasferire delle competenze professionali a riguardo e di approfondire la nuova normativa introdotta dal D.Lgs. n. 50 del 2016, come modificato dal Decreto correttivo D.Lgs. n. 56/2017, e alla luce dei numerosi provvedimenti attuativi (cd. "soft law", costituita da Linee guida e Decreti), emanati dall'ANAC e dal Ministero delle Infrastrutture, per offrire agli operatori del settore e a quanti intendono specializzarsi nella materia, strumenti di aggiornamento e analisi necessari ad affrontare e gestire al meglio le principali novità.

Docenti

Dott. Alfredo G. Allegretta
Magistrato TAR Puglia

Dott. Franco Aschi
Dottore Commercialista e Revisore Contabile, esperto in gare

Dott. Alessandro Quarta
Capo Area Gestione Progetti e Fund Raising dell'Università del Salento

Avv. Carmine Rucireta
Avvocato amministrativista, patrocinante presso le Magistrature superiori

Testimonianze

Direttore della Ripartizione Infrastrutture, Viabilità e Opere Pubbliche Comune di Bari

Direttore della Ripartizione Stazione Unica Appaltante, Contratti e Gestione Lavori Pubblici Comune di Bari

Sedi

Edizione Bari:
The Nicolaus Hotel, Via Cardinale Agostino Ciasca, 27 - 70124 Bari

Edizione Roma:
Piazza san Bernardo, 106 – 00185 Roma

Coordinatore Didattico

Dott. Giuseppe Diretto
Commercialista -
Vice Presidente Ordine Dottori Commercialisti Bari -
Presidente Nazionale UNAGRACO

La Cena di Gala

La cena di gala al The Nicolaus Hotel di Bari - 28 gennaio 2019

Un momento della serata

Le commissioni UNAGRACO

Lo stand ISFORM

Fatturazione Elettronica?

OPEN vi offre la soluzione più efficiente e sicura al costo più contenuto.

Fattura Elettronica, Il portale per la gestione completa del ciclo attivo e passivo comprensivo di conservazione a norma. **Non importa quante fatture dovrete gestire complessivamente** (dato imponderabile): **OPEN** vi propone la tariffazione ad anagrafica, con documenti illimitati, così saprete in partenza, senza sorprese, quanto spenderete.

Dal 2014 abbiamo gestito la fatturazione elettronica verso la Pubblica Amministrazione di più di 8.000 studi per un volume complessivo di quasi 10 milioni di fatture elettroniche PA. **Insomma, questa è una bella garanzia!**

Per saperne di più contatta lo 0171.700700

OPEN Dot Com
Società dei Dottori Commercialisti

www.opendotcom.it

Sanità digitale e Privacy

di *Giovanni Lucatorto**

Sacrificare la libertà e la dignità degli individui a favore dell'innovazione tecnologica? Privarsi dei benefici offerti dalla sanità digitale e quindi di una migliore qualità di vita per gli assistiti cronici a favore di una maggiore riservatezza? È necessario contemperare almeno due diritti costituzionalmente riconosciuti. L'art. 32 della Costituzione che sancisce il diritto alla salute e l'art.2 della Costituzione che sancisce i diritti fondamentali dell'individuo (riservatezza). Questa rappresenta la sfida più impegnativa a cui la sanità pubblica e privata dovrà rispondere con delle strategie mirate al bilanciamento di interessi tra due diritti costituzionalmente riconosciuti. È evidente, però, che alla competizione dovranno partecipare attivamente, insieme alle strutture sanitarie, le aziende produttrici di software e dei dispositivi sanitari che dovranno tutelare, fin dalla progettazione, i diritti e le libertà delle persone fisiche secondo il principio della Privacy by Design. L'incremento della longevità e dell'aspettativa di vita derivano da un costante miglioramento delle condizioni di vita e dai progressi della medicina. Questo aspetto, a prima vista, rappresenta indubbiamente un elemento positivo che, però, senza un'adeguata programmazione sanitaria potrebbe rappresentare una delle maggiori criticità per il futuro delle strutture sanitarie. Gli amministratori regionali e il management delle strutture sanitarie devono garantire costantemente un elevato livello qualitativo nonostante le limitate risorse economiche, strutturali ed umane a disposizione. Con l'incremento della popolazione di anziani gli ospedali saranno alle prese con la gestione della cosiddetta "cronicità" a cui, per un principio cardine dell'economia essendo le risorse limitate, non si avrà un corrispondente incremento delle risorse. Il livello tecnologico raggiunto e la riduzione dei costi dell'hardware rappresenta un'opportunità da cogliere per portare, quanto più possibile, l'ospedale a casa degli assistiti, decongestionando gli ospedali e le strutture sanitarie in genere con la finalità di garantire all'assistito una migliore qualità di vita, un'assistenza efficiente ed efficace ed un monitoraggio costante del "cronico". Tutto ciò è già possibile utilizzando quella che si chiama Sanità Digitale. Numerosissime sono le soluzioni software ed i dispositivi elettronici, indossabili e non, che acquisiscono le informazioni sulla salute dell'individuo. Altrettanto numerose sono le sperimentazioni, condotte con successo, affinché il monitoraggio dei cronici si effetti direttamente a casa e solo in caso di necessità l'assistito è invitato a recarsi presso la struttura sanitaria. Alla domanda Sanità Digitale sì?La risposta non può che essere positiva però salvaguardando i dati personali dell'individuo. Cerchiamo insieme di comprendere perché è importante proteggere le informazioni riguardanti la sfera personale. È necessario riflettere sul motivo per cui proliferano numerosi portali e APP per smartphone la cui utilità è talvolta discutibile. Chiediamoci anche il perché per alcuni semplici giochini è necessario registrarsi donando i nostri dati personali. Per non parlare delle informazioni che quotidianamente forniamo su di un piatto d'argento proprio ai social network. "Se non paghi il prodotto, non sei il cliente: sei il prodotto venduto". Questa definizione, coniata da un utente del community weblog MetaFilter, inquadra alla perfezione i servizi offerti da alcuni big della rete come Google, Facebook, LinkedIn, Twitter, ecc. Queste società offrono servizi gratuiti in cambio dello "sfruttamento" dei nostri dati. Gli utenti affidano a tali società una straordinaria quantità di informazioni personali che rappresentano, per le imprese cosiddette OTT "Over The Top": che forniscono attraverso internet servizi e messaggi pubblicitari personalizzati, un'importante fonte di introiti. Queste imprese non hanno una propria infrastruttura, agiscono al di sopra dei servizi presenti in rete, da cui il termine over the top.

Giovanni Lucatorto

Il Data Dollar Shop

Una preoccupante sperimentazione, sul valore attribuito ai dati personali, è stata effettuata a Londra sulla East London in Old Street dove un negozio ha posto in vendita le opere e i gadget dello street artist Ben Eine. Al momento del pagamento delle opere però gli addetti ai lavori hanno chiesto i Data Dollar ossia foto, video o altri dati personali presenti negli smartphone o nei tablet degli acquirenti. Dopo lo stupore iniziale della "novità" i clienti hanno acconsentito allo scambio. Sui nostri smartphone giornalmente si producono numerosissime "impronte" della nostra vita privata, si lasciano costantemente le tracce dei luoghi frequentati, si acconsente ai software di leggere le nostre email per poi ricordarci degli appuntamenti, ecc. Il patrimonio informativo presente nei dispositivi elettronici, cellulari, tablet, pc, cresce in modo esponenziale e l'aspetto più preoccupante è proprio l'inconsapevolezza del valore di tali informazioni. Non si attribuisce il giusto valore alle tracce che si lasciano su internet mentre si naviga, quando si utilizzano i motori di ricerca e quando si effettuano degli acquisti dai siti di e-commerce. Anche un innocuo Like espresso sui social potrebbe esporre alla rete una preferenza, una convinzione politica, religiosa, sessuale, ecc. Pertanto i portale web e le APP che apparentemente sono gratuite, in realtà sono pagate con i dati personali degli utenti. Dall'esperimento effettuato, si evince che gli utenti dei dispositivi elettronici non attribuiscono alla protezione dei propri dati personali ed al valore delle proprie informazioni il giusto rilievo. Nell'ultimo decennio si è assistito ad una rapidissima pervasività di internet e dei dispositivi elettronici (pc, smartphone, tablet, smartwatch, ecc.) a cui non vi è stato un adeguato incremento della consapevolezza della potenza, delle opportunità e dei "pericoli" forniti da tali strumenti.

Dati personali in cambio di 2 euro

L'esperimento londinese citato non è una vera e propria novità, diversi anni fa a dicembre del 2013 la società Telefonica, in collaborazione con la Fondazione Bruno Kessler e DISI Università di Trento avviarono uno studio attraverso il quale un gruppo di sessanta persone accet-

tarono di concedere tutte le informazioni personali riguardanti le abitudini quotidiane, i gusti, le telefonate, le pagine web ed i luoghi visitati per la modica cifra di 2 euro. Quindi il Data Dollar Shop non è una "novità". Rappresenta una fondamentale lezione al fine di far incrementare la consapevolezza che per poter usufruire di un servizio apparentemente gratuito, in realtà lo si sta pagando con una moneta più preziosa, i dati personali. La registrazione ai servizi on line è un'azione che si compie in assoluta naturalezza e incoscienza anche più volte al giorno. Ognuno di noi si è serenamente registrato su una molteplicità di portali e di APP per le quali quasi certamente nessuno ha la percezione e la traccia, ormai, di tali registrazioni. Considerate le innumerevoli registrazioni effettuate abbiamo lasciato, come Pollicino, una scia di sassolini e di informazioni personali utili però non a colui a cui si riferiscono ma a coloro che forniscono i servizi on line. Il Presidente dell'Autorità Garante per la Protezione dei dati Personali, Antonello Soro, nella relazione sulle attività svolte nel 2014 dall'Autorità ha evidenziato come "tutto ruota intorno ad una raccolta onnivora di dati la cui vulnerabilità degli stessi rappresenta la vulnerabilità delle nostre persone". Ed ha anche evidenziato che nella società digitale "noi siamo i nostri dati". Nel discorso il Presidente Soro ha sottolineato che proprio dalle vulnerabilità "occorre partire per ricercare nuove e più efficaci forme di tutela delle nostre libertà". E così dalla telemedicina alle consultazioni politiche on-line; dalla giustizia telematica al fascicolo sanitario elettronico; dalla videosorveglianza ai social network, "non c'è dimensione della vita, privata e pubblica, che non presupponga un trattamento di dati personali e non richieda solide garanzie". Ma "garantire la sicurezza è sempre più difficile, considerato l'aumento esponenziale della criminalità informatica". Con l'entrata in vigore del Regolamento Europeo per la Protezione dei Dati Personali – GDPR 2016/679 la tutela della privacy non è più una prerogativa di istituzioni e governi democratici ma è affidato nelle mani dei titolari e responsabili del trattamento che acquisiscono e trattano dati degli individui che si rivolgono ad essi. Si rende opportuno chiarire che il Titolare è il rappresentare legale pro tempore della struttura sanitaria, mentre i responsabili del trattamento sono anche le aziende fornitrici di software e servizi di manutenzione delle banche dati ai quali, il corpus normativo vigente in tema di protezione dei dati personali, detta chiari ed inequivocabili adempimenti affinché sia garantita un'adeguata protezione ai dati personali trattati. Il mutato quadro normativo rappresenta un cambiamento epocale nel modo di considerare la protezione dei dati personali, intesa come attività preliminare orientata al soddisfacimento dei requisiti normativi fin dalla fase di progettazione. Si parla di Privacy by design, principio introdotto da Anna Cavoukian, Privacy Commissioner dell'Ontario (Canada), che fu adottato nel 2010 nel corso della 32ma Conferenza mondiale dei Garanti privacy. Con il Regolamento Europeo sulla Protezione dei Dati (GDPR 2016/679) si armonizza a livello europeo la regolamentazione in tema di protezione dei dati personali. Il nuovo corpus normativo cambia veste e da un approccio formale si passa ad un approccio sostanziale. Numerosi sono gli adempimenti in capo ai titolari ed ai responsabili del trattamento ai quali però è lasciato ampio margine decisionale, in quanto il termine chiave del regolamento è l'accountability e l'adeguatezza delle misure adottate al fine di proteggere i dati personali trattati. L'elevato valore dei dati personali e la bassa attenzione dedicata ancora alla Cyber security ed alle sue conseguenze richiede un notevole impegno proprio dalle aziende che progettano soluzioni software e hardware. L'Art. 25 comma 1 del GDRP 2016/679 "Protezione dei dati fin dalla progettazione (by Design) e protezione per impostazione predefinita (by default)" attribuisce delle precise responsabilità ai titolari ed ai responsabili del trattamento. Pertanto per qualunque nuova implementazione che tratti i dati personali, i titolari ed i responsabili devono mettere in atto misure tecniche e organizzative adeguate: "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso". Inoltre i trattamento devono soddisfare i principi dettati dall'Art. 5 del GDPR 2016/679 della liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, dell'esattezza, della limitazione della conservazione, dell'integrità e riservatezza e della responsabilizzazione . Nell'Art. 25 comma 2 sono esplicitati gli obblighi dei titolari e dei responsabili i quali per impostazione predefinita (Privacy by Default) mettono in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica. La sicurezza del trattamento è disciplinata dall'Art. 32 il quale recita: "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio". Nel valutare l'adeguato livello di sicurezza, si deve tener conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'aspetto altrettanto innovativo del Regolamento Europeo sulla Protezione dei Dati (GDPR 2016/679) è rappresentato dal principio di "Accountability" disciplinato dall'Art. 24 mediante il quale ai titolari ed ai responsabili è affidato il compito: "tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, di mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento. Dette misure devono essere riesaminate e aggiornate qualora necessario". In conclusione, quindi, che sia benvenuta la Sanità Digitale con tutti i benefici purché sia dedicata particolare attenzione alla protezione dei dati personali. Il furto o la diffusione dei dati sanitari potrebbero ledere pesantemente la dignità dell'individuo discriminandolo.

**DPO Azienda Ospedaliero Unversitaria Policlinico di Bari*

La portabilità: più vicina di quello che si crede

di *Francesco Maldera**

Sembra incredibile ma, nell'anno in cui è diventato definitivamente applicabile il GDPR, nato anche per impedire che qualcuno faccia soldi sui dati personali, è sorta un'organizzazione (che si autodefinisce banca) che vuole favorire l'arricchimento utilizzando i diritti nati (proprio col GDPR) per tutelare i dati personali.
Chiariamo il concetto. Questa organizzazione, operante tramite un sito web, vorrebbe recuperare i nostri dati personali da tutte le piattaforme alle quali li abbiamo ceduti gratuitamente (con un nostro precedente consenso) e, poi, lasciare a noi, per il suo tramite, la facoltà di rivenderli alle stesse piattaforme. Si tratta di recuperare i dati personali ceduti a social network, carte fedeltà, newsletter, ecc.
La questione, tuttavia, non è così semplice.
Per cominciare, questa presunta banca cita il diritto alla portabilità (art. 20 del GDPR) come leva principale del proprio modus operandi. Questo, per fare l'esempio di un famoso social network, significa che si abbandona Facebook e che i dati transitano tutti su una cassetta di sicurezza della banca: quanti utenti sono disposti a questa operazione? Cioè, quanti utenti sono disposti a stare anche un solo giorno senza Facebook? E, poi, siamo sicuri che Facebook o altre piattaforme sono disposte a riammetterci a fronte del pagamento di una somma?
Inoltre, c'è qualche dubbio sul fatto che possa esserci un intermediario (in questo caso la banca) tra noi (interessati) e la nostra piattaforma (titolare del trattamento). Il comma 6 dell'art. 12 del GDPR prevede che "[..] qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato." Questo significa che il titolare ha il diritto di verificare a che titolo e su quale base formale (delega, procura, ecc.) la banca chiede di ottenere i dati per nostro conto. Non basta che questa organizzazione dica che abbiamo creato un account presso di lei.
Infine, questa organizzazione, potenzialmente, potrebbe raccogliere milioni di dati personali, anche quelli riguardanti la salute, gli orientamenti sessuali, ecc. Quindi, il trattamento che effettua ricade nelle fattispecie per le quali è obbligatoria una valutazione d'impatto sulla protezione dei dati (DPIA). È stata fatta? Con quali esiti? Sul sito non ce n'è traccia.
Tutto questo, in ogni caso, ci fornisce l'occasione per riflettere più attentamente su alcune fattispecie interessanti rispetto al diritto alla portabilità che è una delle novità più rilevanti del GDPR. L'art. 20 prevede che
L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e


Francesco Maldera

b) il trattamento sia effettuato con mezzi automatizzati.
La riflessione più interessante riguarda i dati personali che i clienti forniscono ai professionisti, per esempio ai commercialisti, per la tenuta della contabilità e per gli adempimenti tributari. I dati possono essere contenuti nei contratti, nelle fatture, ecc.; il loro trattamento, certamente, avviene, ormai in quasi tutti gli studi commerciali, in modalità automatizzata. Quindi, questo tipo di dati soddisfano certamente il requisito al punto b) del paragrafo 1 dell'art. 20. Sembra, inoltre, che i dati soddisfino anche il requisito del punto a); infatti, i dati sono forniti a seguito di un contratto che, in molti casi, è verbale ma perfettamente valido secondo la normativa civilistica italiana. Questo vuol dire che il cliente potrà tranquillamente invocare nei confronti del commercialista il diritto alla portabilità cioè chiedere al professionista di far transitare tutto ciò che lo riguarda, e che è stato in passato elaborato nel corso della prestazione professionale, ad un altro professionista. Questa operazione deve concludersi, secondo l'art. 12 del GDPR, entro un mese con possibilità di proroga (motivata) di altri due mesi; un eventuale inadempimento rispetto all'esercizio di tale diritto prevede una sanzione fino a venti milioni di euro.
In realtà, il rapporto tra cliente e commercialista dovrebbe rientrare, secondo il GDPR, nel rapporto tra titolare del trattamento e responsabile del trattamento cioè il commercialista tratta i dati personali per conto del cliente. Questo richiederebbe che il cliente si tutelasse secondo le previsioni dell'art. 28 che, per la verità, prevede un comportamento altamente proattivo nei confronti del professionista e, di contro, non prevede alcuna tutela direttamente esercitabile.
Non si può escludere, quindi, che qualche cliente, per tutelarsi, possa invocare l'esercizio dell'art. 20. Questa ipotesi, peraltro, diventa ancora più probabile proprio in questo momento storico in cui il processo di fatturazione si svolge interamente nei luoghi digitali condivisi tra cliente e commercialista.
Appare necessario, quindi, che ogni professionista organizzi la propria attività in modo che possa rispondere in maniera corretta, e senza sanzioni, all'esercizio del diritto alla portabilità.

* *Esperto di protezione dei dati personali e dei processi di digitalizzazione - DPO*

La nuova figura dell'esperto contabile

di *Fedele Santomauro**

Negli ultimi 10 anni l'Italia ha visto un tasso di disoccupazione giovanile estremamente elevato. La crisi del 2008, il blocco del turn over nel pubblico impiego e lo skill mismatch sono alcune tra le principale cause che hanno visto i giovani del nostro Paese toccare punte di disoccupazione di oltre il 40%. Ancora oggi i dati ci dicono che i giovani che non studiano e non lavorano, i NEET, sono più di 2 milioni. In questo contesto si inserisce la nuova figura dell'esperto contabile, che oggi è il risultato di un percorso professionale rapido e dinamico, capace di creare giovani preparati ad affrontare il mondo del lavoro con capacità, competenze e professionalità. È una professione giovane e per giovani. L'esperto contabile, come molti altri professionisti, si trova di fronte a forti cambiamenti di scenario nel mondo del lavoro. La trasformazione tecnologica in atto, fondata sull'intreccio di digitalizzazione e automazione delle relazioni socio-economiche, espone il lavoro a profondi cambiamenti. Come in tutti i processi di cambiamento, il lavoro, e la società nel suo complesso, si trovano a fronteggiare rischi ma anche grandi opportunità. Riteniamo che l'Italia debba cogliere al meglio tutte le sfide del futuro. Un futuro mai così prossimo. Per farlo, deve puntare sulle sue forze migliori: i giovani, il loro talento, le loro energie. La figura dell'esperto contabile si inserisce in questo percorso di rinnovamento, contribuendo alla formazione di una figura professionale giovane, dinamica, competente. A trarne beneficio saranno i nostri giovani, le nostre imprese, la nostra economia e tutto il sistema-Paese.

* *Consigliere d'Amministrazione*
Cassa di Previdenza dei Ragionieri

Fedele Santomauro

Oltrelidea - www.oltrelidea.it

UNAGRACO
Unione Nazionale Commercialisti ed Esperti Contabili
Via delle Cave di Pietralata n.14 - 00157 ROMA
Tel. +39 06 811.751.02 - Fax. +39 06 811.519.78
info@unagraco.org - www.unagraco.org

Sponsor

GRUPPO24ORE

Foto di Fonte Silvia Meo