



**ORDINE DEGLI  
INGEGNERI**  
DELLA PROVINCIA  
DI CASERTA

2019

La protezione dei dati personali  
negli studi professionali: come  
orientarsi tra diritti e doveri



Gruppo di Lavoro DPO  
**ing. Pasquale Cantiello**  
**ing. Antonietta Perrone**  
**ing. Giuseppe Spera**  
**ing. Michaela Suppa**

06/03/2019

## **INDICE**

- 1. Privacy: normativa e novità**
- 2. Le misure minime organizzative per gli studi professionali**
- 3. Gestione degli archivi cartacei e Registro delle attività**
- 4. Le problematiche legate alla sicurezza della rete**
- 5. L'uso del Cloud Computing: la valutazione del livello di sicurezza nel trattamento dei dati**

**Il presente lavoro è stato approvato dal Consiglio dell'Ordine degli Ingegneri  
nella seduta di Consiglio del 06.03.2019 in rev.00 del 06.03.2019**

## 1. Privacy: normativa e novità

La necessità di individuare metodi per tutelare la riservatezza dei dati ha rappresentato per l'uomo una preoccupazione fin dall'antichità, basti pensare ai famosi cifrari di Cesare o alle scacchiere di Polibio, con cui già nel 150 a.C venivano utilizzati sistema crittografici per proteggere il contenuto di alcuni messaggi militari.

Le origini moderne della privacy, però, si fanno risalire a due giuristi di Boston, Samuel Warren e Louis Brandeis, che, con un saggio intitolato *The Right to Privacy*, proposero interessanti riflessioni su quali informazioni riguardanti la vita personale di un individuo potessero essere di pubblico dominio e quali, invece, dovessero essere tutelate dall'invasione altrui. Nel 1890, i due avvocati furono, infatti, impegnati in una causa contro alcuni giornali che si occuparono un po' troppo frequentemente delle indiscrezioni sulla vita matrimoniale della moglie dello stesso Warren.

Estratto dal saggio "The right privacy" - "Questa faccenda dei giornali che si occupano troppo della vita mondana di mia moglie non può continuare."

Facendo un ulteriore balzo in avanti, l'attuale giurisprudenza si è compiutamente occupata della tutela dei dati personali a partire dal trattato di Shengen del 14 giugno 1985, fino ad arrivare al 4 maggio 2016, data in cui è stato pubblicato il **Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**, nonché alla libera circolazione di tali dati, che ha abrogato la direttiva 95/46/CE

regolamento generale sulla protezione dei dati) **da cui era disceso il nostro D.Lgs. 196/2003.**

Con tale regolamento, attuato a partire dal **25 maggio 2018**, senza ulteriori atti di recepimento, da tutti gli Stati Membri, si è data piena attuazione al principio fondamentale, contenuto nella Carta di Nizza, del diritto di ogni persona al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni (art. 7), e il diritto alla protezione dei dati di carattere personale che la riguardano.

Art. 8 della Carta di Nizza

1. *Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.*
2. *Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.*
3. *Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.*

Il nuovo Regolamento Europeo, ha disciplinato e riordinato la materia sulla protezione dei dati personali quale diritto fondamentale dei cittadini, mirando ad una **armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea.**

Art. 1 par. 2 del Reg. UE 2016/679"Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali"

E' però necessario sottolineare che il Regolamento Ue 2016/679 in ogni caso non rappresenta l'unica fonte legislativa per regolamentare la protezione dei dati personali:

infatti tutte le singole Autorità degli Stati membri dell'Ue – come per l'Autorità Garante della Privacy per quanto riguarda l'Italia – avranno la facoltà di integrare i contenuti del Regolamento che, è bene chiarirlo fin da subito, è più un atto di indirizzo che un insieme di regole specifiche che devono essere applicate in determinate circostanze.

Con l'entrata in vigore del Regolamento Ue 2016/679, dunque, non sono affatto aboliti i Provvedimenti interpretativi e di prassi che sono stati emanati nel tempo da parte dell'Autorità Garante per la Tutela dei Dati Personali su temi quali: Videosorveglianza, Amministratori di Sistema, Fidelity Card, trattamenti di dati biometrici, eccetera. In buona sostanza, le autorizzazioni generali che sono state di anno in anno emanate dall'Autorità Garante italiana, ad es., resteranno valide almeno sino a quando non verranno sostituite da nuovi atti elaborati e promulgati alla luce delle norme introdotte dal Regolamento.

Il nuovo Regolamento istituisce, in particolare, un quadro normativo incentrato sui doveri e sulla responsabilizzazione del Titolare del trattamento (c.d. principio **accountability**, tradotto sommariamente nel termine di “responsabilizzazione”, in maniera più precisa vuol dire "dover rendere conto del proprio operato"). La nuova disciplina impone a tale soggetto di garantire il rispetto dei principi in essa contenuti, ma anche di essere in grado di provarlo, adottando una serie di strumenti che lo stesso GDPR indica, partendo da un'attenta valutazione di rischi e impatti.

In Italia, il legislatore nazionale ha completato il quadro regolamentare nazionale adeguando il Codice Privacy in

materia di dati protezione dei dati personali (d.lgs. n. 196/2003), alle disposizioni europee, in data 19 settembre 2018, con l'entrata in vigore del decreto legislativo 10 agosto 2018, n. 101 recante **“Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE/2016/679”** pubblicato in G.U. lo scorso 4 settembre 2018.

Il GDPR impone la costruzione di un assetto organizzativo ad hoc per la privacy, incentrato sull'istituzione della figura del **Data Protection Officer (DPO)**. Trattasi di una figura che deve essere obbligatoriamente designata in caso di trattamento effettuato da un'Autorità pubblica o un organismo pubblico, o se il Titolare o il Responsabile effettuano un trattamento che richiede un monitoraggio su larga scala, oppure se vengono eseguiti trattamenti su larga scala di particolari categorie di dati o dati relativi a condanne penali o reati.

L'obbligo di nomina del DPO non sussiste, pertanto, quando l'attività professionale è svolta in forma individuale mentre sussiste quando la stessa è svolta nell'ambito di uno Studio Associato Professionale.

Si può affermare che l'importanza del DPO è tale che la richiesta delle imprese – dai grandi gruppi alle Pmi alle imprese familiari – dei professionisti e del settore pubblico è **urgente e superiore alla disponibilità** di questi soggetti; tale necessità rappresenta per molti l'occasione giusta per intraprendere una nuova carriera lavorativa o implementare nuove conoscenze.

Il Regolamento 679/2016, a questo riguardo, indica come compiti del DPO quelli di:

- a) sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, tra le quali sono da ricomprendere l'attribuzione delle diverse responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- b) fornire, qualora venga richiesto, un parere relativamente alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- c) controllare che le violazioni dei dati personali siano documentate, notificate e comunicate.

Il DPO deve svolgere le sue funzioni valutando debitamente i rischi inerenti ai diversi trattamenti di dati personali, tenendo conto della loro natura, contesto, ambito di applicazione e finalità, definendo un ordine di priorità nell'attività svolta e concentrandosi sulle questioni che possono presentare maggiori rischi in termini di protezione dei dati.

La figura del DPO ha pertanto un taglio manageriale, indipendente, competente e in diretta relazione con i vertici aziendali. Si tratta di una figura professionale chiave e protagonista nell'ambito del trattamento dei dati personali, nuova sul mercato, che necessita di una preparazione specialistica e di una formazione continua ma anche di un'esperienza concreta sul campo per supportare adeguatamente le organizzazioni.

## 2. Le misure minime organizzative per gli studi professionali

Gli studi professionali, come le altre organizzazioni, non sono a digiuno degli adempimenti in materia di privacy, la normativa, infatti, è tutt'altro che recente; il legislatore italiano, si è occupato della tutela dei dati personali, già con il D.Lgs. 675/96 e poi con il D.Lgs. 196/2003. Sono quindi oltre 20 anni che i diritti e i doveri dei singoli, nella gestione delle informazioni che transitano nei nostri archivi, sono sotto la lente di ingrandimento. Tutti abbiamo già fatto i conti, in passato, con il Documento Programmatico della Sicurezza e, attraverso periodi di maggiore o minore attenzione alla problematica, ci siamo fatti carico di individuare le figure preposte al trattamento dei dati.

Ciò che però è fondamentale cambiato dalla vecchia stesura del codice della privacy al nuovo regolamento europeo è l'approccio, non più formale, all'argomento.

Il regolamento, infatti, ha spostato il fulcro del sistema privacy **dalla tutela dell'interessato alla responsabilità del titolare** e dei responsabili del trattamento (principio di **accountability**). Tale "assunzione" di responsabilità si concretizza attraverso l'adozione di un comportamento consapevole capace di mettere in atto strategie che anticipino gli eventi e permettano l'adozione di misure che siano frutto di una corretta valutazione del rischio e analisi delle tipologie di dati trattati; qualcosa, in buona sostanza, molto lontano dalla sterile acquisizione di consensi e dalla diffusione di informative.



Al Titolare pertanto non basta più adottare misure minime di sicurezza, bensì deve **dimostrare di avere svolto azioni attive per recepire il GDPR**, calandolo nella propria organizzazione in base ai rischi dei dati personali trattati. In particolare, il Titolare deve dimostrare di avere **impostato la data protection, di avere disegnato operation «a prova di privacy»** e di avere il **governo dei dati** trattati. Tale risultato si centra con la **conoscenza dei dati trattati** (Data Governance), dei processi in cui avviene il **trattamento** (governance dei processi) e delle applicazioni che lo sostengono, nonché **delle infrastrutture** che ospitano tali applicazioni (IT governance).

In tal senso anche il più semplice studio professionale assume la complessità di “Organizzazione”, intesa come “Azienda”, in cui ruoli e responsabilità devono essere chiaramente definiti e l’assetto organizzativo e strutturale analizzato come aspetto sostanziale e non marginale, strettamente legato alla deontologia a servizio del cliente.

Il professionista, attuando una vera e propria strategia di leadership, oggi, deve conoscere con esattezza il proprio contesto e dotarsi di una struttura, formata da attrezzature e risorse umane, capace di rispondere alle diverse esigenze che emergono da tali analisi.

Tale approccio impone dapprima una valutazione preliminare sulla categoria di dati trattati, sia che si tratti solo di dati personali o anche di dati sensibili, per poi individuare quali siano i soggetti preposti al trattamento dei dati medesimi, del loro ruolo e della loro responsabilità.

In base a quanto disposto dall'art. 5 del Reg UE, **i dati trattati devono essere quelli strettamente necessari e essi devono essere conservati solo per il tempo legato al conseguimento delle finalità**: la finalità e la durata del trattamento sono elementi indispensabili che devono essere riportati nel registro dei trattamenti che via via deve essere compilato, attraverso la verifica continua dei principi di correttezza, trasparenza e liceità; infine dovranno essere individuati gli ambiti di diffusione e comunicazione dei dati.

Solo dopo aver costruito i registri dei trattamenti, si potrà procedere con serenità alle nomine formali, ricordando che in uno studio professionale, il professionista rivestirà il ruolo di

titolare del trattamento, ovvero quel soggetto, persona fisica o giuridica che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento dei dati personali.

Il nuovo regolamento prevede anche l'individuazione di "contitolari": può essere questo il caso in cui vi sia uno studio associato e i professionisti operino determinando congiuntamente le finalità e i mezzi del trattamento.

Se possibile si consiglia sempre di definire individuali responsabilità e obblighi circa il trattamento dei dati personali, attraverso degli accordi interni.

ORGANIGRAMMA		
TITOLARE DEL TRATAMENTO		
Responsabile interno del trattamento dei dati	Incaricati del trattamento	Amministratore di sistema
Garantisce l'applicazione delle misure di sicurezza e delle regole per la gestione della privacy	Tratta i dati secondo policy, procedure e regole vigenti e su indicazioni ricevute dal titolare o dal responsabile interno di riferimento	E' responsabile della gestione ed eventuale manutenzione di impianti di elaborazione attraverso cui vengono effettuati trattamenti di dati personali, inoltre gestisce e si occupa della protezione dei dati
<p align="center"><b>responsabile esterno del trattamento dei dati</b></p> <p>Opera e tratta i dati per conto del titolare garantendo l'applicazione delle misure e regole di trattamento dei dati personali all'interno della società così come regolato nel contratto stipulato tra le parti</p>		

Terminata la fase della valutazione dei rischi e della stesura del registro dei trattamenti, sarà necessario predisporre quegli elementi o evidenze formali che permettono di responsabilizzare i vari elementi dell'organigramma aziendale: procedere alle nomine dei responsabili del trattamento e degli autorizzati.

E' importante ricordare che in molti casi il professionista diviene anche piattaforma di interscambio dei dati con altri professionisti, per adempiere a degli obblighi di legge o perché si avvale di servizi esterni (si pensi al fornitore del servizio di gestione informatica che da remoto effettua il backup aziendale).

In tal caso il professionista ha l'obbligo di acquisire informazioni circa la compliance aziendale dell'altra organizzazione.

### **3. Gestione degli archivi cartacei**

Anche se tutta l'attenzione sembra continuare ad essere incentrata sulla gestione dei dati informatici, non deve essere assolutamente trascurato l'aspetto della gestione degli archivi cartacei e, in generale, dell'adeguatezza della struttura anche dalla protezione fisica (incendio, intrusione, ecc.): la semplice raccolta di fascicoli relativi alla causa di un cliente o alla sua posizione retributiva o il cartiglio relativo ad una perizia estimativa, svolto senza l'ausilio di strumenti automatizzati, è pur sempre un trattamento di dati personali ai sensi dell'art.

4.2 del GDPR.

L'art. 32 prescrive al titolare del trattamento l'adozione di misure tecniche ed organizzative adeguate a garantire un livello di sicurezza corrispondente al rischio. L'efficacia di tali misure dovrà essere regolarmente verificata dal titolare del trattamento.

Art. 32 GDPR – Regolamento Generale sulla Protezione dei Dati (UE/2016/679)

1. 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, che comprendono, tra le altre, se del caso:

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Al pari delle procedure imposte da un qualsiasi sistema di gestione aziendale, deve essere definita la modalità di conservazione dei documenti per fare in modo che essi siano: rintracciati e individuati facilmente, se necessario.

Ricordiamo che la persona interessata deve poter richiedere la misura dell'oblio e noi, invece, dobbiamo essere in grado di distruggere i documenti in nostro possesso nel momento in cui non sia più necessario tenerli.

La rintracciabilità, l'identificazione la gestione dei tempi di trattenuta dei dati permette di ridurre drasticamente il rischio a cui il nostro studio può essere esposto.

In base all'identificazione delle categorie di dati trattati, è possibile seguire semplici regole di conservazione fisica:

- I documenti sensibili devono essere conservati in armadietti chiusi a chiave il cui accesso è limitato a un determinato numero di persone all'interno dell'azienda.
- I normali dati personali possono essere conservati in scaffalature a giorno con i faldoni, i contenitori a bottone, i tubi per i disegni, ecc., l'importante è che non siano in luoghi aperti al pubblico o non presidiati.

Da evitare, in ogni caso, di scrivere sulla costa dei faldoni dati personali come il nome del cliente, basta scrivere un codice identificativo o il nome del progetto.

In ogni studio professionale, come in ogni altro ambito lavorativo, è essenziale avere un distruggi-documenti, al fine di presentare delle evidenze oggettive nella propria organizzazione a sostegno delle procedure utilizzate per la distruzione definitiva dei dati che non hanno più ragione di essere presso la nostra struttura.

Per le caratteristiche fisiche dei luoghi, non vi sono regole precise ma, a seconda del livello di rischio che il titolare del trattamento stima in base ai dati trattati nel proprio studio, possono essere sufficienti alcune misure di sicurezza minime, come: porta blindata, grate alle finestre o, semplicemente, chiudere a chiave l'ufficio quando ci si assenta, o arrivare alla necessità di garantire l'esistenza di un sistema antifurto

Nel caso di studi associati o multiprofessionali, è opportuno che stampanti e fax vengano posizionati in luoghi presidiati e non accessibili al pubblico per evitare che vengano letti dati personali, anche del tutto casualmente.

In generale, la politica comportamentale del rispetto della privacy deve essere diffusa anche in forma scritta e a conoscenza di tutti.

#### 4. La Sicurezza delle Reti - Introduzione

La gestione degli archivi informatici rappresenta uno dei maggiori problemi connessi alla sicurezza, in quanto ormai tutti i computer sono collegati alla rete internet e quindi a rischio di **Attacchi Informatici**. Con il termine Attacco Informatico (o Cyber Attacco) si indica una qualunque manovra, che colpisce sistemi informativi, infrastrutture, reti di calcolatori e dispositivi elettronici personali finalizzati al furto, alterazione o distruzione delle informazioni o delle infrastrutture stesse.

Gli attacchi informatici possono essere classificati come:

- Intercettazione dell'informazione;
- Alterazione (Modifica non autorizzata) dell'informazione;
- Generazione non autorizzata dell'informazione;
- Interruzione dell'informazione;

Questi attacchi informatici in una rete “sicura” (o in un sistema informatico “sicuro”) sono impediti attraverso componenti HW e SW così da garantire le caratteristiche fondamentali dell'informazione riassunte di seguito (Triangolo CIA) :

- **Confidenzialità:** garantisce la privacy e riguarda la capacità di proteggere i dati da tutti gli individui che non sono autorizzati ad averli;
- **Integrità:** è la capacità di impedire che i dati vengano modificati in modo non autorizzato o indesiderato;
- **Disponibilità:** capacità di poter accedere ai dati quando ne abbiamo bisogno;

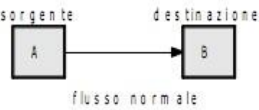
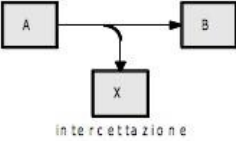
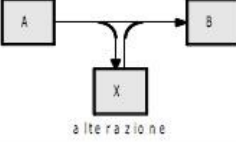
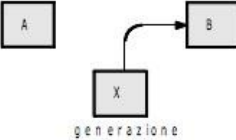
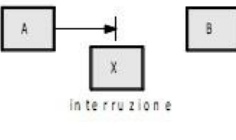


**Una Rete Informatica è sicura se garantisce:**

- **Autenticità del messaggio**
- **Triangolo CIA Informazione (Confidenzialità – Integrità - Disponibilità)**



Di seguito si riportano i tipi possibili di attacchi informatici con esempi di implementazione degli stessi

Attacco	Schema	Esempi del mondo reale
<p><i>Flusso normale dell'informazione</i></p>	 <p>The diagram shows a box labeled 'A' on the left and a box labeled 'B' on the right. Above 'A' is the word 'sorgente' and above 'B' is 'destinazione'. A horizontal arrow points from 'A' to 'B'. Below the arrow is the text 'flusso normale'.</p>	<p>Invio di un pacchetto IP            Invio di email            Accesso a una pagina web            Lettura di dati da un database</p>
<p><i>Intercettazione</i></p>	 <p>The diagram shows box 'A' on the left and box 'B' on the right. A horizontal arrow points from 'A' to 'B'. A third box 'X' is positioned below the arrow. A curved arrow branches off from the main arrow pointing to 'B' and points down to box 'X'. Below box 'X' is the text 'intercettazione'.</p>	<p>Sniffing di pacchetti di rete            Furto di informazione mediante crittoanalisi            Furto di informazione mediante analisi del traffico            Furto di informazione mediante covert channel</p>
<p><i>Alterazione</i></p>	 <p>The diagram shows box 'A' on the left and box 'B' on the right. A horizontal arrow points from 'A' to 'B'. A third box 'X' is positioned below the arrow. Two arrows branch off from the main arrow: one points down to box 'X', and the other points to box 'B'. Below box 'X' is the text 'alterazione'.</p>	<p>Modifiche non autorizzate a file o programmi            Attacchi "man in the middle"            Azioni di disturbo del canale di comunicazione</p>
<p><i>Generazione</i></p>	 <p>The diagram shows box 'A' on the left and box 'B' on the right. A horizontal arrow points from 'A' to 'B'. A third box 'X' is positioned below the arrow. An arrow points from box 'X' up to the main arrow between 'A' and 'B'. Below box 'X' is the text 'generazione'.</p>	<p>Masquerading            Spoofing            Intrusioni</p>
<p><i>Interruzione</i></p>	 <p>The diagram shows box 'A' on the left and box 'B' on the right. A horizontal arrow points from 'A' to 'B'. A third box 'X' is positioned below the arrow. A vertical line with a horizontal bar across it (representing a barrier or stop) is placed over the arrow between 'A' and 'B'. Below box 'X' is the text 'interruzione'.</p>	<p>Denial of service            Flooding, resource starvation, mail storm            Crashing di applicazioni            Sabotaggio linee di comunicazione            Danneggiamenti fisici</p>

## **5. L'uso del Cloud Computing: la valutazione del livello di sicurezza nel trattamento dei dati**

Il professionista moderno gestisce sempre più il rapporto con altri studi o con i propri clienti tramite la condivisione di documenti ed elaborati attraverso l'uso del cloud computing, i cui classici esempi di applicazione, universalmente utilizzati, sono: Dropbox, Google Drive, Gmail, iCloud, OneDrive o le varie photo libraries.

Il cloud computing è un modello nato per consentire un facile accesso a richiesta (on demand), tramite rete ad un pool condiviso di risorse di calcolo configurabili (server, unità di memoria, applicazioni e servizi) che possono essere rese disponibili prontamente ed analogamente rilasciate al termine dell'uso, con un impegno di gestione e di supporto minimo da parte del fornitore del servizio.

La sempre più ampia diffusione di questo sistema di interscambio in ambito lavorativo, va ricondotta oltre che alla facilità dell'adozione di tale modello, anche alla cosiddetta "elasticità", ovvero alla capacità del fornitore di aumentare rapidamente la potenza di calcolo o la capacità di memorizzazione al crescere delle richieste dell'utente e successivamente ridurre tali proprietà nel momento in cui l'utente ne richieda di meno.

Anche dal punto di vista dei costi, i vantaggi sono notevoli per l'utente, che può così avere a disposizione risorse hardware, software, applicazioni e servizi senza dover affrontare i costi per l'acquisto, la configurazione e la manutenzione continua di

hardware e software. Il modello di business tende a diventare analogo a quello delle utilities, ovvero una tariffazione a consumo come avviene per l'energia elettrica, l'acqua, il gas o la telefonia.

### **Ma quali valutazioni deve fare il professionista per scegliere un sistema compliant al regolamento europeo e alle norme in materia di privacy in generale?**

Come affrontare una scelta coerente con il livello di rischio legato alla tipologia di dati trattati? Capire quali sono i rischi per la sicurezza e per la privacy nel cloud computing e sviluppare delle soluzioni efficienti ed efficaci sono fattori critici e che non possono essere trascurati. Le caratteristiche architettoniche uniche sollevano diversi timori in tal senso.

Il cloud fornisce ad esempio l'accesso ai nostri dati, e **uno dei problemi è quella di essere certi che solo le entità effettivamente da noi autorizzate possano ottenerne l'accesso.** Quando utilizziamo ambienti cloud, stiamo delegando a terzi (il provider) la decisione sui nostri dati e sulla nostra piattaforma in un modo completamente nuovo rispetto a quanto di solito in uso in informatica. Diventa critico quindi avere meccanismi appropriati per impedire che un cloud provider possa utilizzare i dati (o consentirne a terzi l'utilizzo) in una qualche modalità su cui non ci sia stato un preventivo accordo. E' sicuramente improbabile che mezzi esclusivamente tecnici possano impedire completamente ai cloud provider l'uso inappropriato di tali dati, quindi occorrerà aggiungere ad essi anche degli strumenti "non tecnici" per raggiungere l'obiettivo. Il cliente dovrà innanzitutto instaurare un rapporto

di fiducia con il provider sia riguardo le sue capacità tecniche sia della sua stabilità economica. Il cloud provider deve essere ovviamente compliant con le norme sulla privacy ed in particolare con il nuovo regolamento Europeo 2016/679: il GDPR.

Ma ovviamente non è sufficiente che il provider soddisfi tali requisiti; le responsabilità sui dati trattati non possono essere delegate da cliente a provider. Entrambi dovranno condividere la responsabilità della sicurezza e della privacy in ambiente cloud, anche se il livello di condivisione varia in base ai diversi modelli di cloud computing:

- **Software as a Service:** il provider fornisce servizi ed applicazioni con caratteristiche integrate quasi del tutto preconfigurate ed in tal senso è maggiormente responsabile della corretta gestione dei dati del cliente.
- **Platform as a Service:** il provider fornisce l'ambiente su cui il cliente sviluppa e costruisce la propria applicazione. In questo caso il cliente è il primo responsabile per la corretta protezione dell'applicazione che ha sviluppato e che gira sui sistemi del provider. Quest'ultimo dovrà comunque garantire il necessario isolamento tra le applicazioni e gli spazi di lavoro dei diversi clienti.
- **Infrastructure as a Service:** rappresenta il modello più espandibile e fornisce quasi nessuna caratteristica di tipo applicativo. Ci si aspetta che il cliente si occupi della sicurezza del sistema operativo, delle applicazioni e dei dati. Dal punto di vista del provider, vanno comunque fornite delle caratteristiche di protezione ai dati anche se di livello più basso.

Dal punto di vista dei ruoli privacy nel Cloud Computing, è sicuramente ovvio che il titolare del trattamento dei dati è il cliente che utilizza il servizio cloud e, quindi, il titolare dello studio professionale, e ne decide le finalità e le modalità del trattamento.

Il ruolo del Provider può essere diverso: qualora questo si limiti alla mera conservazione dei dati può essere ritenuto responsabile del trattamento e dovrà essere designato tale con apposito contratto dal responsabile. Se però il cloud provider aggiunge un livello di trattamento dei dati per fini diversi da quelli del cliente diventa anch'esso titolare.

Occorre altresì precisare che a volte esiste un ulteriore attore nel modello descritto in precedenza. Non sempre il cloud provider dispone direttamente di data center di proprietà, ma si avvale di un soggetto terzo che fornisce l'infrastruttura fisica su cui vengono poi ospitati i dati. In tal caso tale soggetto entra a far parte della catena di responsabilità dei dati e, come tale, dovrà essere coinvolto negli accordi con il cliente che dovrà fornire il consenso al suo coinvolgimento e da esso nominato sub-responsabile del trattamento. In questo modo il cliente può essere sempre consapevole di tutti i soggetti coinvolti nel trattamento dei propri dati. Anche l'ubicazione fisica dei data center deve essere tenuta in conto, in particolar modo qualora questa non ricada in un paese dell'Unione Europea. Occorrerà verificare che il paese in questione fornisca gli adeguati livelli di protezione pari a quello europeo.

Concludendo questa breve introduzione alla problematica della sicurezza dei dati e della privacy in ambito cloud, è possibile

dire che il cloud computing rappresenta sicuramente un'opportunità per le aziende in particolar modo le PMI, consentendo loro un risparmio economico ed un abbattimento dei costi di investimento. **Tutto ciò a patto di servirsi di cloud provider che siano compliant alla normativa e di affidarsi a un professionista o al proprio DPO (qualora esista) per verificare il rispetto delle norme in materia di privacy. E al tempo stesso essere consapevoli che anche affidandosi a seri professionisti, il titolare resta sempre responsabile dei dati che tratta.**



100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100