Fondazione Studi
Consulenti del Lavoro
Consiglio Nazionale dell'Ordine

con il patrocinio di

FEDERPRIVACY

PRIVACY E GESTIONE DEL PERSONALE

A cura di

NICOLA BERNARDI
Presidente di Federprivacy

Introduzione di

GINEVRA CERRINA FERONI
Vice Presidente del Garante per la protezione dei dati personali

TeleConsul

Finito di stampare nel mese di settembre 2021 da
Rotostampa Group Srl
via Tiberio Imperatore, 23 – Roma

CAPITOLO 1
Trattamenti di dati personali nella gestione delle risorse umane

di Nicola Bernardi

Sommario: 1. Delimitazione del contesto dei trattamenti dei dati personali - **2.** Determinazione del ciclo di vita dei dati personali - **3.** Individuazione delle risorse (asset) utilizzate nelle operazioni di trattamento.

Una qualsiasi impresa o altra organizzazione che deve rispettare le prescrizioni del Regolamento UE 2016/679 e la normativa correlata in materia di privacy, prima ancora di pensare alle misure di sicurezza da adottare per proteggere i dati, deve conoscere quali sono le informazioni che effettivamente tratta, e per questo è fondamentale aver svolto a monte un'accurata attività di mappatura generale dei dati.

Infatti, nessun Titolare può sostenere di essere adeguato alla normativa sulla protezione dei dati senza conoscere bene quali informazioni tratta, per quali finalità le tratta, in quale contesto le tratta, come le tratta, e dove le conserva. Basti pensare ad esempio quanto sarebbe arduo rispondere ad una richiesta di accesso ai dati da parte di un interessato se il Titolare del trattamento neanche sapesse quali dati di costui effettivamente tratta, e se si trovano su archivi cartacei o supporti digitali che possono essere ubicati sia dentro che fuori dalla sede in cui svolge la propria attività.

In particolar modo con il **principio di responsabilizzazione** (c.d. accountability) introdotto dal GDPR, il Titolare del trattamento deve essere in grado di poter dimostrare in qualsiasi momento che le attività di trattamento rispettino gli obblighi e i requisiti della normativa, e per far questo è necessario fare un censimento per determinare il perimetro dei dati, le cui risultanze permetteranno anche di tenere correttamente un aggiornato registro delle attività di trattamento svolte sotto la propria responsabilità in conformità all'art. 30 del Regolamento europeo.

All'epoca dell'introduzione della Legge 31 dicembre 1996, n. 675, che è stata la prima nell'ordinamento italiano a disciplinare la protezione dei dati personali, effettuare una mappatura generale dei trattamenti poteva risultare un'attività relativamente facile, sia perché in molte realtà la più grande mole di dati personali si concentrava sul personale, sia perché la maggior parte di tali dati aziendali si presenta-

vano ancora in forma cartacea ed erano spesso riposti in archivi fisici come armadi e cassettiere, e la necessità di proteggerli poteva essere soddisfatta semplicemente mettendoli sotto chiave.

Ma soprattutto, la **società digitalizzata** così come la conosciamo oggi, era ancora ad uno stato primordiale, e ancora non si ponevano le molte criticità che nel corso degli anni sono progressivamente fioccate una dopo l'altra influendo anche sui dati riguardanti la gestione del personale, che sempre più spesso vengono trattati attraverso moderni strumenti tecnologi che nella maggior parte dei casi sono connessi ad Internet.

E nel contesto dello scopo per cui è stato scritto questo libro, occorre tenere in speciale considerazione che i dati inerenti le persone fisiche trattati nella gestione delle risorse umane e nell'amministrazione del personale richiedono tipicamente un elevato livello di sicurezza, non solo a causa degli importi delle retribuzioni dei dipendenti che devono essere mantenuti riservati, ma anche perché spesso contengono **informazioni c.d. sensibili** che rientrano nelle particolari categorie di dati contemplate nell'art. 9 del Regolamento europeo, cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, informazioni relative alla salute o alla vita sessuale, oltre ai dati genetici, i dati biometrici e quelli che rivelano l'orientamento sessuale.

Per tali motivi, chi gestisce i dati del personale deve resistere alla tentazione di fare una valutazione approssimativa dei dati che presume sommariamente di trattare, ma deve invece diligentemente identificare e catalogare tutti i trattamenti, partendo da quelli che gestisce per i processi di ricerca e selezione del personale, includendo poi tutti quelli che tratta per finalità di assunzione, esecuzione del contratto di lavoro, gli adempimenti degli obblighi stabiliti dalla legge o dai contratti collettivi, quelli della pianificazione e organizzazione del lavoro, quelli su parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, nonché quelli trattati per finalità di cessazione del rapporto di lavoro.

Per evitare di impostare l'**attività di mappatura** in modo superficiale, da cui deriverebbe poi un quadro non rispondente alla realtà rispetto agli effettivi impatti in materia di privacy sulla gestione del personale di un'organizzazione, preliminarmente è consigliabile fare una ricognizione generale su tutti i possibili fronti che possono comportare dei trattamenti di dati, che in molti casi sono di facile individuazione, (ad esempio, Libro Unico del Lavoro, certificati medici, buste paga, iscrizioni sindacati, ecc.), mentre in altri potrebbero risultare meno evidenti. Inoltre, se nella maggior parte dei casi tali trattamenti di dati personali sono pienamente leciti, in altri casi dalla mappatura potrebbe emergere che alcuni trattamenti potrebbero

avvenire in modo non conforme alla normativa sulla protezione dei dati proprio a causa della mancanza di consapevolezza da parte del Titolare.

Potrebbe perciò essere opportuno **porsi** tutta **una serie di domande**, come quelle che a titolo di esempio si riportano di seguito, e che potrebbero essere incluse in una propria **check-list**:

- ✓ I computer aziendali registrano le attività di navigazione su internet dei dipendenti?
- ✓ Nel sito web aziendale esiste una sezione (ad esempio, "Lavora con noi") attraverso la quale è possibile ricevere candidature?
- ✓ I processi di ricerca e selezione del personale vengono affidati anche all'esterno (ad esempio, agenzie/head hunter/ecc.) oppure gestiti tramite piattaforme online specializzate?
- ✓ Per svolgere l'attività di gestione del personale utilizzo un servizio di cloud computing che potrebbe comportare un minor controllo dei dati e/o un loro trasferimento in paesi terzi?
- ✓ Le buste paga vengono consegnate ai dipendenti in formato digitale attraverso una piattaforma online che consente di scaricarle, o avvalendosi di un'altra procedura informatica?
- ✓ Nel parco degli automezzi utilizzato dai dipendenti ed altri collaboratori vi sono veicoli su cui sono installati sistemi di geolocalizzazione GPS o satellitari?
- ✓ Vi sono registri di automezzi aziendali che sono assegnati a specifici dipendenti, e dal cui numero di targa è possibile risalire all'identità dell'utilizzatore?
- ✓ Esiste un regolamento che disciplina l'utilizzo dei social network a cui i dipendenti ed altri collaboratori si devono attenere quando comunicano e/o condividono informazioni di lavoro all'esterno?
- ✓ L'ufficio risorse umane gestisce schede valutative o report riguardanti le performance dei dipendenti?
- ✓ L'azienda gestisce rimborsi spese dei dipendenti da cui è possibile desumere i loro spostamenti e gli acquisti effettuati?
- ✓ L'azienda effettua o commissiona attività di controllo medico o somministrazione di terapie mediche sui dipendenti?
- ✓ Ci sono lavoratori che sono stati dotati di dispositivi elettronici (ad esempio, braccialetti intelligenti/rilevatori di uomo a terra/ecc.) in grado di localizzare chi li indossa e certi loro comportamenti?

- ✓ Esistono account di posta elettronica o altri profili utente che per qualche ragione sono rimasti attivi anche dopo la cessazione del rapporto di lavoro?
- ✓ All'interno del luogo di lavoro o anche in altre aree all'aperto adiacenti vi sono delle telecamere di videosorveglianza, e in tal caso sono dotati di sistemi intelligenti come le tecnologie di riconoscimento facciale?
- ✓ Sono installate o vengono utilizzate occasionalmente telecamere nascoste o altri dispostivi occulti a scopo difensivo contro sospetti dipendenti infedeli o prevenzione di furti?
- ✓ Il personale svolge attività lavorative anche da remoto? In tal caso utilizza dispositivi e strumenti aziendali o BYOD (Bring Your Own Device)?
- ✓ Come avviene la rilevazione delle presenze dei lavoratori? Vengono usati strumenti che prevedono l'utilizzo di dati biometrici come l'iride, l'impronta digitale, o il palmo della mano?
- ✓ I dipendenti ed altri collaboratori possono asportare dati personali aziendali memorizzandoli su chiavette usb o altri supporti di memoria removibili?
- ✓ Su pc ed altri dispositivi aziendali sono installati software in grado di controllare e/o monitorare le attività dei lavoratori?
- ✓ Se il datore di lavoro provvede ad alcuni dipendenti e/o collaboratori un cellulare aziendale, è in grado di visualizzare anche i tabulati delle telefonate effettuate per scopi personali?
- ✓ Chi tratta dati inerenti la gestione del personale li comunica solo nelle modalità espressamente autorizzate dalla direzione, o utilizza anche di propria iniziativa altre modalità e strumenti che possono risultare più pratici, come ad esempio app di messaggistica (WhatsApp/Telegram/Signal/ecc.) oppure piattaforme di file hosting per condividere dati con altri soggetti (Dropbox/WeTransfer/Google Drive/Onedrive/ecc.)?
- ✓ Vi sono dipendenti a cui è stata data una carta di credito aziendale dal cui estratto conto è possibile monitorare gli acquisti effettuati sia per motivi di lavoro che spese personali?
- ✓ I dipendenti che viaggiano per lavoro usano dispositivi elettronici o altri strumenti (Telepass/Viacard/ecc.) in grado di permettere al datore di lavoro di risalire agli itinerari percorsi?
- ✓ Sugli automezzi aziendali utilizzati dai dipendenti sono installati apparecchi antifurto o sistemi di controllo satellitari che geolocalizzano il veicolo o che monitorano gli stili di guida del conducente (ad esempio, scatola nera)?

L'attività di mappatura dei dati relativi alla gestione del personale dovrebbe quindi prevedere:

1) **identificazione delle attività di trattamento** effettuate e relativa descrizione di come vengono utilizzati e con quali finalità;
2) **definizione**, per ogni processo individuato, **di flussi informativi** e della natura qualitativa e quantitativa dei dati trattati;
3) identificazione e **classificazione della tipologia di dati trattati**, in particolare delle informazioni sensibili rientranti nelle categorie particolari di dati ai sensi dell'art. 9 del Regolamento europeo;
4) identificazione e **descrizione delle modalità** in cui il dato viene acquisito, elaborato, comunicato ed archiviato;
5) **descrizione delle articolazioni aziendali**, delle società esterne o dei professionisti interni e esterni che intervengono nel trattamento e di tutti gli altri attori che intervengono nel processo analizzato;
6) **identificazione dei legami logici** e delle interazioni **con altri processi** e con ulteriori attori che intervengono nel trattamento a cui sono comunicati/trasmessi i dati.

Per raggiungere i suoi scopi, un efficace processo di mappatura dei dati trattati nell'ambito della gestione delle risorse umane e dell'amministrazione del personale dovrebbe prevedere tipicamente **tre fasi** differenti:

1) delimitazione del contesto dei trattamenti dei dati personali;
2) determinazione del ciclo di vita dei dati personali;
3) individuazione delle risorse (asset) utilizzate nelle operazioni di trattamento.

1. DELIMITAZIONE DEL CONTESTO DEI TRATTAMENTI DEI DATI PERSONALI

Lo svolgimento di questa attività consente di **collegare i dati personali ai processi aziendali** che li utilizzano. In questo modo i dati sono ricondotti ad un contesto determinato.

L'esplorazione dei dati trattati da un Titolare nell'ambito della gestione delle risorse umane e dell'amministrazione del personale può essere effettuata ponendosi le seguenti domande:

- Che tipo di dati personali sono trattati?
- Chi è il Responsabile dei dati all'interno dell'organizzazione?
- Per quali finalità i dati sono trattati?
- A chi si riferiscono i dati trattati?
- A chi sono comunicati i dati trattati, dentro e fuori l'organizzazione?

2. DETERMINAZIONE DEL CICLO DI VITA DEI DATI PERSONALI

Il ciclo di vita dei dati personali include **tutte le operazioni di trattamento dei dati**, che da un lato sono collegate alle persone autorizzate a compierle e dall'altro alle persone o altri soggetti esterni dell'organizzazione che possono venire a conoscenza di tali dati.

Si riportano di seguito alcune domande che possono aiutare a comprendere il ciclo di vita delle varie tipologie di dati personali che sono oggetto di trattamento:

- Chi può acquisire i dati personali che dovranno essere trattati?
- Chi può registrare i dati e in che formato saranno registrati?
- I dati sono strutturati, e se sì come?
- Per quanto tempo dovranno essere conservati i dati?
- Chi sono i soggetti che potranno accedere ai dati, modificarli, estrarli, e cancellarli?
- A quali altri soggetti saranno comunicati i dati trattati, e con quale modalità?
- I dati saranno trasferiti all'estero? A quali soggetti? Vi è una valida base giuridica per effettuare il trasferimento?
- I dati saranno a loro volta collegati ad altri dati personali? di che genere?

3. INDIVIDUAZIONE DELLE RISORSE (ASSET) UTILIZZATE NELLE OPERAZIONI DI TRATTAMENTO

Ogni operazione di trattamento di dati utilizza una o più risorse (asset) di supporto. Perciò, identificare tali strumenti è di primaria importanza perché ogni risorsa può avere delle vulnerabilità che possono essere causa di violazione dei dati, sia da parte di soggetti malintenzionati che a causa di errore umano da parte dello stesso personale addetto a trattarli.

Quindi, conoscere le risorse di supporto è il primo passo per individuare anche le vulnerabilità e i rischi sui dati per cui individuare adeguate misure di sicurezza. Di seguito **si riportano a titolo di esempio vari tipi di risorse** che possono essere usate per trattare dati nella gestione delle risorse umane e nell'amministrazione del personale:

- Locali, armadi, cassettiere, archivi, ecc.
- Pc client e server, stampanti, tablet, smartphone, fax, fotocopiatrici
- Sistemi di videosorveglianza, sistemi di controllo accessi e rilevazione presenze, sistemi GPS e satellitari in grado di geolocalizzare il personale
- Software, applicazioni, servizi di cloud computing, siti web, app, ecc.

- Reti cablate, reti wireless, ecc.
- Strumenti cartacei e documenti stampati come cedolini paga, *curricula*, registri degli infortuni, registri per le visite mediche, ecc.
- Canali di trasmissione come posta elettronica, intranet, workflow, ecc.

Di seguito alcune domande che possono essere d'aiuto per individuare le risorse utilizzate per trattare dati personali:

- Quali strumenti/risorse consentono di acquisire dati personali?
- Quali strumenti/risorse consentono di registrare i dati raccolti?
- Quali strumenti/risorse consentono di strutturare i dati trattati?
- Quali strumenti/risorse consentono di conservare i dati trattati?
- Quali strumenti/risorse consentono di accedere ai dati trattati e/o di modificarli o cancellarli?
- Quali strumenti/risorse consentono di cancellare i dati trattati?
- Quali strumenti/risorse consentono di comunicare i dati trattati?
- Quali strumenti/risorse consentono di trasferire i dati trattati?
- Quali strumenti/risorse consentono di estrarre i dati trattati?
- Quali strumenti/risorse consentono di connettere i dati trattati ad altri?

Completata l'attività di mappatura generale, che troverà la sua rappresentazione formale nel registro delle attività di trattamento ai sensi dell'art. 30 del Regolamento europeo ed in altri eventuali documenti a supporto, il Titolare avrà posto le basi per impostare il proprio modello organizzativo della gestione dei dati del personale, ed essere così in grado di svolgere le successive attività necessarie per soddisfare il complesso di prescrizioni dettate dalla normativa in materia di protezione dei dati personali.

Benché la **mappatura dei dati** sia un'**attività fondamentale** per impostare l'architettura e le politiche della propria organizzazione nella gestione delle informazioni aziendali e per la conformità al GDPR, occorre tuttavia considerare che, senza una **costante attività di monitoraggio periodico**, il perimetro dei dati può rapidamente sfuggire dal controllo a causa dei continui sviluppi tecnologici dai quali derivano degli impatti sui trattamenti di dati personali (come ad esempio una migrazione a un sistema di cloud computing), dai mutamenti delle attività aziendali che possono dar luogo a nuovi trattamenti non precedentemente mappati o farne cessare altri, oppure da eventuali fusioni societarie, incorporazioni, o qualsiasi altro cambiamento degli assetti organizzativi che vada a modificare il quadro ricavato dalla mappatura iniziale. Peraltro, se in fase di ispezione da parte dell'autorità di

controllo, il registro delle attività di trattamento non risultasse più adeguatamente aggiornato, o con il passare del tempo fosse diventato addirittura obsoleto, si configurerebbe una violazione degli obblighi dell'art. 83, par. 4, lett. a) del Regolamento europeo, che può comportare una sanzione amministrativa pecuniaria fino a 10.000.000 di euro, o per le imprese, fino al 2% del fatturato annuo.

È perciò opportuno prevedere nelle proprie procedure anche un'attività di monitoraggio per la **verifica** e l'**aggiornamento dei trattamenti di dati** personali effettuati dalla propria organizzazione, che può essere ricompresa tra i compiti attribuiti al Responsabile della Protezione dei Dati (Data Protection Officer) dall'art. 39, par. 1, lett. b) del GDPR in ordine alle attività di audit che questo svolge periodicamente per "*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*". Nei casi in cui non sia presente un DPO, il Titolare del trattamento potrà affidare tali compiti di monitoraggio ad un proprio Responsabile privacy interno o ad un consulente esterno.

CAPITOLO 14
Il Consulente del Lavoro: il duplice ruolo tra responsabilità e opportunità

di Nicola Bernardi

Sommario: 1. Responsabilità che ricadono sul Consulente del Lavoro - **2.** Non solo responsabilità, ma anche opportunità.

1. RESPONSABILITÀ CHE RICADONO SUL CONSULENTE DEL LAVORO

Come emerge dalla lettura di questo libro, nell'ambito della gestione del personale sono molteplici le responsabilità che ricadono sul Consulente del Lavoro in ordine alla tutela della privacy e al rispetto della normativa sulla protezione dei dati personali.

Per farsi un'idea generale di quanto siano importanti tali responsabilità, si pensi ad esempio al **segreto professionale** previsto dall'art. 6 della Legge 11 gennaio 1979, n. 12, e al dovere di riservatezza previsto dall'art. 9 del Codice Deontologico dei Consulenti del Lavoro, il quale impone al professionista di assicurare la riservatezza circa i dati e le notizie di cui venga a conoscenza in occasione della promozione o dell'esecuzione del rapporto professionale, e non solo per quanto lo riguarda in prima persona, ma anche per i trattamenti di dati effettuati da parte dei suoi dipendenti, dei soci, dei praticanti, e di tutti coloro che a vario titolo operano nel suo studio o comunque per suo conto.

E quando un'azienda o un ente affida i dati personali dei propri dipendenti al Consulente del Lavoro, oltre ad espletare tutti gli adempimenti burocratici riguardanti la gestione e l'amministrazione del personale, egli non può sottrarsi alla responsabilità di rispettare anche la disciplina sulla protezione dei dati personali dettata dal GDPR e dalla normativa correlata, e non solo perché si esporrebbe al rischio di pesanti sanzioni amministrative e di potenziali azioni di rivalsa da parte dei suoi clienti nel caso essi fossero multati dall'autorità di controllo per violazioni commesse dal professionista, ma anche perché la stessa deontologia richiede al consulente di essere preparato e regolarmente aggiornato con particolare riferimento ai settori nei quali svolge l'attività, e quand'anche non possedesse le conoscenze di tali materie, si dovrebbe addirittura astenere dall'accettare incarichi che sappia di non poter svolgere con la necessaria competenza o per i quali non sia in grado di assicurare un'organizzazione adeguata.

E proprio riguardo la necessità di soddisfare i **requisiti di adeguatezza** dell'**organizzazione delle attività** del proprio studio, il professionista dovrà egli stesso rispettare diligentemente le varie prescrizioni del GDPR, ad esempio relativamente alle autorizzazioni al trattamento di dati personali dei suoi collaboratori, alla loro istruzione ed il loro aggiornamento in materia, alla tenuta di un **registro delle attività di trattamento** svolte sotto la propria responsabilità ai sensi dell'art. 30 del Regolamento europeo, all'analisi dei rischi sui dati e quando previsto alla valutazione d'impatto ai sensi dell'art. 35, alla protezione dei dati mediante l'adozione di misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio nel rispetto dell'art. 32, dotandosi quando richiesto anche di un Responsabile della Protezione dei Dati (DPO).

Indubbiamente, i temi della tutela della privacy e della protezione dei dati personali costituiscono una disciplina complessa che richiede notevoli sforzi per acquisire e mantenere le dovute conoscenze e competenze, le quali però, una volta conseguite, possono essere sfruttate dal Consulente del Lavoro non solo come mero destinatario che deve sottostare alle prescrizioni, ma anche come professionista qualificato in grado di offrire ulteriori servizi che possono rappresentare un valore aggiunto per la propria clientela, oppure anche per accrescere la propria competitività sul mercato allargando la propria cerchia di clienti.

I temi della privacy e della protezione dei dati personali costituiscono infatti una medaglia con due diverse facce per il Consulente del Lavoro, non attribuendo a questo solo gravose responsabilità nell'esercizio delle proprie attività, ma presentando anche importanti opportunità professionali, che non sempre sono colte da chi è immerso nella routine dell'amministrazione del personale e della gestione delle risorse umane.

Basti pensare che secondo le stime dell'Osservatorio di Federprivacy, fin dall'approvazione del Regolamento UE 2016/679 erano state previste solo in Italia 75.000 nuove opportunità professionali nei successivi anni in cui le imprese e tutte le organizzazioni avrebbero dovuto adeguarsi e mantenersi conformi alla normativa europea sulla protezione dei dati, e al momento della stesura di questo libro i dati forniti dal Garante per la privacy rilevavano già oltre 60.000 nomine di "data protection officer" notificate all'Autorità.

Tali opportunità, che si incastrano in uno scenario di mercato delle professioni in cui la domanda è generalmente superiore all'offerta per carenza di esperti effettivamente preparati sulla materia, possono essere particolarmente a portata di mano per il Consulente del Lavoro, che è il professionista per eccellenza a cui aziende ed altre organizzazioni già si rivolgono per affidare nelle sue mani i dati personali dei propri dipendenti, ed anche perché quella sulla protezione dei dati personali è

una normativa specificamente applicabile alle persone fisiche, soggetti di cui il Consulente del Lavoro è già abituato a occuparsi proprio per le sue peculiarità professionali.

Anche se non vi sono particolari preclusioni sull'esercizio delle attività professionali negli ambiti della protezione dei dati personali, in quanto esse non sono riservate ad una specifica professione protetta da un albo o da un collegio, e peraltro il Garante ha chiarito che allo stato attuale neanche esistono titoli abilitanti o attestati formali che determinano l'idoneità per svolgere il ruolo di Responsabile della Protezione dei Dati, è però evidente che il profilo del Consulente del Lavoro presenta un fisiologico vantaggio iniziale rispetto a molte altre categorie professionali che ruotano intorno al mondo imprenditoriale, che però poco o niente riguardano così da vicino le persone fisiche.

2. NON SOLO RESPONSABILITÀ, MA ANCHE OPPORTUNITÀ

Per il Consulente del Lavoro che sa quindi fare di necessità virtù quando si deve comunque rimboccare le maniche per studiare la materia, si prospettano varie opportunità professionali, come ad esempio quella di assumere l'incarico di "Data Protection Officer" (figura a cui è dedicato specificamente il Capitolo 3 di questo libro), quella di offrire alle imprese il servizio di consulenza e supporto in materia di protezione dei dati personali per adeguarsi o mantenersi conformi alla normativa vigente, quella di svolgere il ruolo di docente nei corsi di formazione che le imprese devono somministrare ai propri addetti per autorizzarli a trattare i dati personali in conformità al GDPR, ed anche fornire consulenza giuslavoristica in materia di privacy in ambito extragiudiziale, nonché assistenza e rappresentanza in sede di contenzioso con l'autorità di controllo o con gli organi ispettivi del Lavoro.

Poiché **non esistono titoli abilitanti** per operare come esperto in materia di privacy e protezione dei dati personali, ed anche l'art. 37 del Regolamento UE 2016/679 lascia una porta aperta prescrivendo come requisito per chi viene designato come Data Protection Officer il possesso della "*conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati*", per posizionarsi nel mercato delle professioni occorre essere in grado di documentare la propria formazione attraverso la partecipazione a corsi ed altri eventi formativi per dimostrare l'acquisizione delle competenze e il regolare aggiornamento in materia.

Anche se **non vi sono obblighi di possedere specifiche certificazioni**, nel corso degli anni si sono rivelate strumenti particolarmente utili quelle rilasciate da organismi indipendenti e imparziali basate sugli standard internazionali della Norma ISO/IEC 17024 "*Conformity assessment - General requirements for bodies operating*

certification of Persons", che permettono di offrire una garanzia preventiva al mercato, fornendo un rilevatore immediato e garantito a supporto del cliente, che può oggettivamente individuare i professionisti in possesso di determinate competenze e di un certo livello di preparazione. Tra le certificazioni più diffuse e riconosciute dal mercato italiano vi sono quella di "Privacy Officer e Consulente della Privacy" rilasciata dall'ente TÜV Süd sul disciplinare tecnico di Federprivacy, quella basata sugli standard nazionali della Norma UNI 11697: 2017, e la certificazione CIPP/E rilasciata dalla IAPP (International Association of Privacy Professionals), quest'ultima gradita in particolar modo dalle imprese multinazionali.

Un altro strumento utile ai professionisti che devono dimostrare le proprie credenziali in materia di privacy sono gli **attestati di qualità dei servizi** che vengono emessi dalle associazioni professionali iscritte presso il Ministero dello Sviluppo economico, ai sensi della Legge n. 4/2013 sulle professioni non organizzate in ordini o collegi. Tali attestati, rilasciati in formato cartaceo o mediante tesserino, consentono generalmente di verificare una serie di dettagli utili alla valutazione delle qualità professionali dell'associato, riguardanti ad esempio l'effettivo possesso di determinati requisiti, il suo aggiornamento professionale, l'eventuale copertura assicurativa, le certificazioni possedute, e l'impegno di rispettare un insieme di regole etiche da questo assunto al momento dell'iscrizione all'associazione.

Anche se può sembrare superfluo ricordarlo, a parte le varie modalità che il professionista può valutare di scegliere per dimostrare le proprie credenziali, ciò che fa veramente la differenza per affermarsi come esperto di privacy e protezione dei dati personali e per essere realmente in grado di cogliere le opportunità del settore è rappresentato dall'elevato livello di preparazione necessario, che si può ottenere solo dedicando tempo e fatica allo studio della materia, considerando che essendo trasversale e sempre in continua evoluzione, comprende temi giuridici, tecnici, informatici, ed anche organizzativi che devono essere seguiti costantemente.