La norma UNI 11697:2017 e la figura del DPO

Lo scorso dicembre – dopo lunghe discussioni – è stata pubblicata la norma UNI 11697:2017 "Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali – Requisiti di conoscenza, abilità e competenza", inerente la definizione dei requisiti relativi all'attività professionale dei soggetti operanti nell'ambito del trattamento e della protezione dei dati personali (compreso il DPO), da questi esercitata a diversi livelli organizzativi (pubblico o privato).

L'UNI dichiara che "*La norma definisce i profili professionali relativi al trattamento e alla protezione dei dati personali coerentemente con le definizioni fornite dall'EQF e utilizzando gli strumenti messi a disposizione dalla UNI 11621-1 Attività professionali non regolamentate – Profili professionali per l'ICT – Parte 1: Metodologia per la costruzione di profili professionali basati sul sistema e-CF*".

La norma, anche dopo la sua uscita, è stata fonte di animate discussioni fra gli esperti del settore e, soprattutto, è stata vivacemente contestata da chi ritiene che non esponga in modo chiaro e preciso i requisiti professionali delle figure in oggetto oppure definisca delle figure professionali favorevoli a certi profili piuttosto che altri.

Le figure professionali delineate dalla norma UNI sono le seguenti:

1. **Data Protection Officer** (DPO), figura di supporto al titolare o responsabile del trattamento nell'applicazione e per l'osservanza del Regolamento (UE) 2016/679, in conformità all' art. 37 (Designazione del Responsabile della protezione dei dati), art. 38 (Posizione del Responsabile della protezione dei dati) e art. 39 (Compiti del Responsabile della protezione dei dati).
2. **Manager Privacy**, figura che assiste il titolare nelle attività di coordinamento di tutti i soggetti che – nell'organizzazione – sono coinvolti nel trattamento di dati personali (responsabili, incaricati, amministratori di sistema, ecc.), garantendo il rispetto delle norme in materia di privacy e il mantenimento di un adeguato livello di protezione dei dati personali.
3. **Specialista Privacy**, figura di supporto appositamente formato (è richiesta una formazione minima di 24 ore), che collabora con il Manager Privacy e cura la corretta attuazione del trattamento dei dati personali all'interno dell'organizzazione, svolgendo le attività operative che, di volta in volta, si rendono necessarie durante tutto il ciclo di vita di un trattamento di dati personali.

4. **Valutatore Privacy**, figura dotata di una apposita formazione (minima di 40 ore) che si caratterizza per la sua terzietà sia nei confronti del Manager che dello Specialista Privacy; egli esercita una attività di monitoraggio (audit) andando ad esaminare periodicamente il trattamento dei dati personali e valutando il rispetto delle normative di settore emanate.

Concentriamoci sulla figura del DPO o RPD. La norma definisce una **descrizione sintetica** del profilo, una **missione**, dei **risultati attesi**, dei **compiti principali**, delle **competenze,** delle **abilità e delle conoscenze.**

Per ognuna delle competenze assegnate seguenti è definito un livello di competenza:

- Pianificazione di Prodotto o di Servizio
- Sviluppo della Strategia per la Sicurezza Informatica
- Gestione del Contratto
- Sviluppo del Personale
- Gestione del Rischio
- Gestione delle Relazioni
- Gestione della Sicurezza dell'Informazione
- Governante dei sistemi informativi

Tra le **Abilità** (Skill) stabilite che deve possedere il DPO si segnalano:

- Contribuire alla strategia per il trattamento e per la protezione dei dati personali
- Capacità di analisi
- Capacità organizzative
- Pianificazione e programmazione
- Saper analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi
- Saper anticipare i cambiamenti richiesti alla strategia aziendale dell'information security e formulare nuovi piani
- Saper applicare gli standard, le best practice e i requisiti legali più rilevanti all'information security
- Garantire che la proprietà intellettuale (IPR) e le norme della privacy siano rispettate
- egoziare termini e condizioni del contratto
- Preparare i template per pubblicazioni condivise
- Progettare e documentare i processi dell'analisi e della gestione del rischio
- Essere in grado di seguire e controllare l'uso effettivo degli standard documentativi aziendali

Invece tra le **Conoscenze** (Knowledge) possedute dal DPO vi sono:

- I principi di privacy e protezione dei dati by design e by default I diritti degli interessati previsti da leggi e regolamenti vigenti Le responsabilità

connesse al trattamento dei dati personali
- Norme di legge italiane ed europee in materia di trattamento e di protezione dei dati personali
- Norme di legge in materia di trasferimento di dati personali all'estero e circolazione dei dati personali extra UE
- Le metodologie di valutazione d'impatto sulla protezione dei dati e PIA
- Le norme tecniche ISO/IEC per la gestione dei dati personali
- Le tecniche crittografiche
- Le tecniche di anonimizzazione
- Le tecniche di pseudonimizzazione
- Sistemi e tecniche di monitoraggio e "reporting"
- Gli strumenti di controllo della versione per la produzione di documentazione
- I rischi critici per la gestione della sicurezza
- I tipici KPI (key performance indicators)
- Il ritorno dell'investimento comparato all'annullamento del rischio
- la computer forensics (analisi criminologica di sistemi informativi)
- La politica di gestione della sicurezza nelle aziende e delle sue implicazioni con gli impegni verso i clienti, i fornitori e i sub-contraenti
- Le best practice (metodologie) e gli standard nella analisi del rischio
- Le best practice e gli standard nella gestione della sicurezza delle informazioni
- Le norme legali applicabili ai contratti
- Le nuove tecnologie emergenti (per esempio sistemi distribuiti, modelli di virtualizzazione, sistemi di mobilità, data sets)
- Le possibili minacce alla sicurezza
- Le problematiche legate alla dimensione dei data sets (per esempio big data)
- Le problematiche relative ai dati non strutturati (per esempio data analytics)
- Le tecniche di attacco informatico e le contromisure per evitarli

Fra le competenze richieste determinate dalla norma emergono profili afferenti a:

- Consulenti direzione
- Consulenti ed esperti di sistemi di gestione della sicurezza delle informazioni (famiglia delle norme ISO 27000)
- Auditor di sistemi di gestione
- Esperti di Risk Management
- Consulenti/esperti sulle normative attinenti alla privacy ed alla protezione dei dati personali (leggi, normative, disposizioni del Garante, ecc.)

Inoltre sono richieste conoscenze legali sulla contrattualistica, competenze sulla sicurezza informatica (tecniche di attacco, crittografia, ecc.) e sui sistemi informatici e relativi database.

Pur con le dovute precisazioni relative al fatto che il candidato DPO dovrà ricoprire un ruolo le cui caratteristiche dipendono fortemente dall'organizzazione in cui dovrà andare a operare, è evidente che prevalgono le competenze gestionali/manageriali e quelle relative alla sicurezza delle informazioni, piuttosto che quelle legali. Per quanto possa essere contestata, la norma chiaramente individua soggetti più vicini all'ingegnere dell'informazione che all'esperto legale come possibile DPO/RPD. Sicuramente le competenze legali eventualmente mancanti a un profilo molto vicino all'ingegnere dell'informazione sono più facilmente colmabili, anche attraverso consulenze specifiche, rispetto ad altre situazioni in cui il potenziale DPO si trova a dover colmare il gap di competenza relativo ai sistemi di gestione della sicurezza delle informazione, al risk management, alle basi di dati e magari anche alla *cybersecurity*.

Sicuramenteci sono in giro illustri avvocati esperti di *info security* e *data protection*, magari anche consulenti ed auditor ISO 27001, ma tutti coloro che si propongono per il ruolo di DPO con competenze essenzialmente giurisprudenziali saranno adatti a ricoprire il ruolo di DPO?

Naturalmente queste considerazioni valgono se si pensa di affidare il ruolo di DPO ad un'unica figura, con l'eventuale supporto di un team di esperti nelle varie discipline.

Chiaramente ogni organizzazione o ente pubblico che vorrà selezionare il proprio DPO potrà decidere come meglio crede in base ai compiti e le caratteristiche identificate per il DPO dal Regolamento UE 679/2016, ma la norma UNI 11697, volontaria, dice questo.

Chi è il DPO?

Chi è realmente il Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO), figura prevista dal Regolamento UE 679/2016 (GDPR)?

Forse sarebbe meglio rispondere anche ad altre domande:

- Cosa fa il DPO?
- Quali requisiti deve possedere?
- A chi serve il DPO?

Il Garante italiano per la Protezione dei Dati Personali e le **Linee-guida del WP243**, sviluppate dall'apposito Gruppo di Lavoro Articolo 29 a livello europeo, ci vengono in aiuto, ma non bastano a disperdere il polverone che si sta facendo da ogni parte attorno a questa figura.

Si legge da varie fonti di "Corsi specialistici per DPO", "Esami per qualifiche da DPO", "migliaia di posti di lavoro come DPO" e così via. È tutto al vero?

Vediamo anzitutto **quali sono i requisiti di un DPO** o RPD che dir si voglia.

Il Responsabile della Protezione dei Dati (RPD o DPO), nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. Possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.
2. Adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che il RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali.
3. Operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio (RPD/DPO esterno).

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della Protezione dei Dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

Leggendo queste righe si evince che non possono esistere corsi per DPO che qualifichino per questo ruolo, né elenchi o albi. Ovviamente tutti i "corsi per DPO" possono essere più o meno validi per svolgere questa mansione in futuro, ma non forniscono la "patente" per farlo.

Le competenze del DPO (insieme di livello di istruzione, conoscenze, capacità/abilità ed esperienza…) devono svariare fra **competenze legali**, **informatiche** ed **organizzativo-gestionali**. Naturalmente il RPD deve conoscere bene il Regolamento UE 679/2016, ma anche il D.Lgs 196/2003 che costituisce tuttora la normativa sulla privacy italiana da oltre 13 anni ed i vari provvedimenti del Garante italiano su videosorveglianza, Amministratori di Sistema, ecc..

Quali saranno le competenze prevalenti? Fino a che livello un DPO deve sapere di sicurezza informatica?

Sicuramente sono più importanti competenze di base consolidate a 360° negli ambiti legale, informatico e gestionale, piuttosto che essere esperti di una materia e non conoscere nulla delle altre. Infatti il DPO non dovrà configurare un firewall (attività che potrà delegare a tecnici sistemisti), ma dovrà sapere cos'è e conoscere i suoi principi di funzionamento.

Per capire quali competenze precise dovrà possedere il DPO occorre comprendere che il DPO è **un ruolo** da ricoprire in una determinata organizzazione, dunque sarà importante che il DPO conosca discretamente i processi gestionali dell'organizzazione in cui dovrà operare ed in funzione del tipo di organizzazione dovrà possedere requisiti minimi differenti. Per esempio il DPO di un Ospedale o di una organizzazione della Sanità Privata non dovrà necessariamente avere le stesse competenze del DPO di un Comune, di un Ufficio Giudiziario o di una Società che sviluppa software per la profilazione di utenti. Quindi ad ognuno il suo DPO.

Infine sottolineiamo il fatto che il DPO deve essere indipendente dalle altre funzioni aziendali e dipendere solo dal titolare del trattamento, dunque in molte organizzazioni difficilmente una figura interna possiede questi requisiti.

Quindi, **quali sono i compiti del DPO**?

Il Responsabile della Protezione dei Dati dovrà, in particolare:

- **sorvegliare** l'osservanza del Regolamento, **valutando i rischi** di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- **collaborare** con il titolare/responsabile, laddove necessario, nel condurre una **valutazione di impatto** sulla protezione dei dati (DPIA);
- **informare** e **sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal Regolamento e da altre disposizioni in materia di protezione dei dati;
- **cooperare** con il Garante e fungere da **punto di contatto** per il Garante su ogni questione connessa al trattamento;
- **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento**.

Esaminando i suddetti punti emerge un ruolo un po' da **consulente** e un po' da **auditor**, ma con contorni non ben definiti. In base al tipo di organizzazione il DPO o RPD che dir si voglia dovrà svolgere compiti più o meno estesi, potrà essere supportato da un *team* di altre persone, interne o esterne all'organizzazione, che potranno essere specialisti in ambito informatico, legale o altro a seconda del settore di appartenenza. Ad esempio in una organizzazione sanitaria il DPO potrebbe essere supportato da esperti nel settore sanitario, ad esempio medici.

Anche un DPO esterno potrebbe assumere l'incarico avvalendosi di un *team* di collaboratori, anche per far fronte alle numerose richieste da parte degli interessati che potrebbero porre quesiti sulle modalità di trattamento dei propri dati personali.

Inoltre è da sottolineare il fatto che il DPO deve disporre anche di **autonomia** e **risorse sufficienti** a svolgere in modo efficace i compiti cui è chiamato ed è il titolare (o responsabile) del trattamento che ha l'onere di garantire ciò.

In definitiva il perimetro dei compiti del DPO andrebbe definito bene di caso in caso in apposito contratto o delega del titolare.

Si osserva che il GDPR impone al titolare o al responsabile del trattamento di pubblicare i dati di contatto del DPO e di comunicare i dati di contatto del DPO alle pertinenti autorità di controllo; dunque è un incarico ufficiale e pubblico, affinché tutti gli interessati al trattamento di dati personali effettuato dall'organizzazione possano contattare il DPO per richiedere informazioni sul trattamento dei dati che li riguardano.

Da ultimo, ma non di minore importanza: i DPO **non rispondono personalmente in caso di inosservanza del GDPR**, ma tale responsabilità ricade sempre e solo sul titolare o sul responsabile del trattamento.

Vediamo, infine, **in quali casi è previsto il DPO**, ovvero quando una organizzazione è obbligata a nominare un DPO.

Dovranno designare obbligatoriamente un RPD:

1. amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
2. tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
3. tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un RPD, è comunque possibile una nomina su base volontaria. Ma questa frase non farà effetto su quelle Società che pensano di nominare un DPO solo se strettamente obbligatorio per legge.

Si precisa che un gruppo di imprese o soggetti pubblici possono nominare un unico RPD.

Dunque un consulente esterno qualificato potrebbe assumere il ruolo di DPO, per così dire, in *outsourcing*, per diverse organizzazioni.

Gli esempi forniti nella Linea-guida del GdL Articolo 29 su chi effettivamente dovrà nominare un DPO in ambito privato forniscono qualche indicazione, ma non dirimono tutti i dubbi. Soprattutto il concetto di "larga scala" è molto dibattuto: preso atto che un medico di famiglia non tratta dati particolari (sanitari in questo caso) su *larga scala*, salendo sul gradino superiore di questa scala virtuale, quale soggetto, avente comunque un organico ridotto, tratta dati particolari su larga scala: un poliambulatorio privato, una clinica/ospedale privati, un Amministratore di Condominio, un fornitore di servizi di ristorazione collettiva?

Speriamo che non siano le sentenze a definire meglio la normativa che, qui come in altre parti, lascia ampio spazio all'interpretazione.

Da quanto esposto emerge una similitudine fra la figura del DPO – che deve proteggere i dati personali dell'individuo – e l'RSPP (Responsabile del Servizio Prevenzione e Protezione per la Sicurezza e Salute del Lavoro, secondo il D.Lgs 81/2009 e s.m.i.) – che deve garantire la sicurezza nei luoghi di lavoro -, con un distinguo, però: l'RSPP è responsabile anche legalmente in caso di incidente, mentre il DPO non è responsabile in caso di violazione dei dati personali.

Come sta la privacy ad un anno dall'attuazione del GDPR?

Il Regolamento (Ue) 2016/679, noto anche come **RGPD** (Regolamento Generale sulla Protezione dei Dati) o **GDPR** (*General Data Protection Regulation*), troverà piena attuazione esattamente fra un anno da oggi, il **25 maggio 2018**, ovvero al termine del periodo di transizione.

A seguito dell'interessante seminario svoltosi venerdì 19 maggio 2017 presso l'Ordine degli Ingegneri di Bologna sulle **possibili forme di certificazione in ambito Privacy**, è utile fare qualche riflessione sull'attuazione di questa nuova normativa nelle organizzazioni del nostro Paese.

Attualmente esistono alcuni documenti ufficiali che permettono di comprendere meglio come declinare i requisiti del GDPR nella propria organizzazione, tra i quali:

- Linee Guida all'applicazione del RGPD del Garante Privacy italiano
- Linee guida sui responsabili della protezione dei dati (RPD) WP 243 (235 download) (compreso l'allegato con le FAQ)
- Linee Guida Valutazione-Impatto WP 248 (243 download) .

Al momento, però, le indicazioni fornite non sono in grado di fugare tutti i dubbi sull'applicazione del GDPR, anzi!

Il GDPR dà spazio a integrazioni dei requisiti in esso riportati per regolamentare situazioni specifiche per tipo di dati trattati e particolari legislazioni nazionali, sarà compito del Garante Italiano definire eventuali disposizioni integrative che avranno valore di Legge.

Esaminando i concetti principali del GDPR, quali **responsabilizzazione** (*accountability*) del titolare e del responsabile del trattamento, ***privacy by design***, ***privacy by default***, **valutazione di impatto**, **valutazione dei rischi** e "misure di sicurezza adeguate", è facile individuare molti punti di debolezza di numerose organizzazioni italiane che, per mentalità, non sono abituate ad affrontare il problema della protezione dei dati personali con metodo e come una reale priorità. Per molti vertici aziendali la privacy è "solo una scocciatura" e il nuovo Regolamento un "ennesimo obbligo cui toccherà adeguarsi", ma non tanto prima della

scadenza. Come se bastasse fare quattro documenti per risolvere il problema per sempre (o per lo meno fino al prossimo cambiamento normativo)!.

Purtroppo questo "approccio" per essere conformi al GDPR deve cambiare, perché è una norma di stampo anglosassone (tipo "*common law*", a dispetto della Brexit) che richiede una **forte responsabilizzazione di coloro che ricopriranno il ruolo di titolari** (rappresentanti legali per le società) **e responsabili del trattamento**.

L'affidamento all'esterno di dati personali, anche solo per adempimenti legislativi, come la preparazione delle buste paga demandate allo Studio di Consulenza del Lavoro, devono richiedere un'attenta analisi del contratto con il soggetto esterno e verifica che esso soddisfi tutti i requisiti in termini di misure di sicurezza per la protezione dei dati.

Certamente per le PMI che trattano solo dati personali di dipendenti e collaboratori, oltre a nominativi di referenti di clienti e fornitori, l'adeguamento al GDP non sarà di particolare impatto, ma basta demandare all'esterno ad un servizio via web come la gestione del personale oppure avere un sito internet di *e-commerce* che raccoglie dati di utenti per rendere la gestione un pochino più complessa.

Viceversa le **organizzazioni che trattano dati particolari** (i.e. sensibili), soprattutto se poco strutturate e se gestiscono tali dati insieme a fornitori di servizi mediante internet, dovranno cambiare il loro atteggiamento sulla privacy e valutare attentamente i rischi che corrono. Soprattutto non credano che basti far scrivere un DPS o "riesumare" quello precedentemente redatto prima che il Governo lo abolisse: la carta (o i documenti digitali) non bastano, occorre la consapevolezza e la sostanza di applicazione di regole comportamentali, misure di sicurezza fisica e logica (sistemi informatici) ritenute adeguate (da chi?) e instaurare con fornitori e partner rapporti contrattuali che prendano in considerazione anche il trattamento dei dati personali e la loro tutela.

Recenti eventi come i *ransomware* del tipo *Wannacry* potrebbero far piangere veramente i titolari di trattamenti di dati sanitari, il cui valore per gli hacker potrebbe essere ben superiore dei 300 dollari in Bitcoin. Il ricatto potrebbe essere non del tipo "se rivuoi i tuoi dati paga", ma "se non vuoi che divulghi su internet i tuoi dati paga il riscatto"!. Ci sono stati già casi analoghi legati a ricatti a proprietari di diritti di serie TV americane molto più innocui.

Relativamente al ruolo del DPO, l'obbligo di nomina imposto dal Regolamento ricade in modo certo solo su Enti Pubblici, mentre le Organizzazioni che controllano in modo regolare e sistematico dati personali di interessati su larga scala e quelle che trattano dati particolari (traducibili con i dati sensibili del vecchio Codice Privacy, D.Lgs 196/2003) su larga scala o trattano dati relativi a condanne penali e reati non sono facilmente determinabili. Cosa significa "su larga scala"? Le indicazioni fornite hanno permesso di stabilire che un medico di base della Sanità

Italiana non tratta dati sanitari su larga scala, ma come considerare strutture superiori come Farmacie, Ambulatori medici Privati, Cliniche Private? Gli Studi Legali devono nominare un DPO?

Sicuramente le **competenze del DPO** dovrebbero comprendere competenze **legali** (conoscenza di normative e leggi applicabili alla materia ed ai dati trattati dall'organizzazione titolare del trattamento), competenze **informatiche** (non necessariamente particolarmente approfondite, per esse può rivolgersi a tecnici specializzati come sistemisti ed esperti di sicurezza informatica) e **gestionali-organizzative**.

Relativamente alle forme di **certificazione sulla privacy** che, beninteso, non esimono i titolari ed i responsabili del trattamento da essere passibili delle sanzioni previste dal Regolamento e dal Garante Privacy Italiano in caso di infrazioni, occorre distinguere fra diversi tipi di certificazione:

- Certificazione di prodotto o servizio, accreditata secondo ISO 17065, come ad es. lo schema ISDP 10003:2015 – *Criteri e regole di controllo per la Certificazione dei processi per la tutela delle persone fisiche con riguardo al trattamento dei dati personali – Reg. EU 679/2016*.
- Certificazione delle figure Professionali della Data Protection (DPO, "Auditor Privacy", "Privacy Officer" e "Consulente Privacy").
- Certificazione delle Aziende del *Data Protection Management System* in conformità al Codice di Condotta DPMS 44001:2016© ed al Reg. (UE) 679/2016.
- Certificazione del sistema di gestione della sicurezza delle informazioni secondo la ISO 27001:2013.

Premesso che la certificazione accreditata secondo il Regolamento UE 679/2016, così come esposta dall'articolo 43 dello stesso RGPD, trova attualmente riscontri solo in standard e certificazioni afferenti allo schema di accreditamento ISO 17065 (certificazioni di prodotto o servizio), emergono le seguenti considerazioni:

- Non si è ancora affermato un sistema di gestione della privacy riconosciuto che, sulla base della struttura HLS delle norme sui sistemi di gestione (ISO 9001, ISO 27001, ecc.), consenta di gestire la protezione dei dati con un approccio sistemico, basato sui processi e concetti come il *risk based thinking* e l'attuazione di azioni finalizzate ad affrontare i potenziali rischi sul trattamento di dati personali.
- Il ruolo del *Data Processor Officer* (DPO o RPD), come è definito dal Regolamento, non corrisponde ad una figura professionale specifica avente determinati requisiti di competenza (istruzione scolastica e post scolastica, conoscenze normative e tecniche, esperienza nell'ambito privacy, partecipazione a corsi di formazione, superamento di esami o abilitazioni). Il DPO è piuttosto "un ruolo" che potrebbe richiedere competenze differenti a seconda della realtà in cui opera e della criticità della protezione dei dati personali nell'organizzazione stessa.

- Tutti gli schemi e gli standard sopra indicati permettono di ridurre il rischio che il titolare del trattamento e gli eventuali responsabili incorrano in infrazioni nel trattamento di dati personali e, quindi, rischino infrazioni anche pesanti e/o gravi danni di immagine.

Per concludere, secondo il *risk based thinking*, quali rischi corrono le aziende che non sono adeguate al GDPR?

La probabilità di essere sanzionati a seguito di ispezioni del Nucleo Privacy della GdF è estremamente bassa, un po' più alta per organizzazioni che trattano dati particolarmente critici (la valutazione è fatta in base al numero delle ispezioni avvenute negli ultimi anni).

La probabilità di incorrere in sanzioni o in risarcimento danni a causa di istanze di interessati che si sentono danneggiati nella loro privacy oppure in caso di incidenti di dominio pubblico è un po' più alta.

L'impatto delle conseguenze nel caso si verifichino suddetti eventi negativi dipende dal tipo di organizzazione e dai dati trattati, può essere significativo o devastante a seconda dei casi.

Leggi anche l'articolo Impatti del Regolamento Privacy sullo sviluppo software.

Impatti del Regolamento Privacy sullo sviluppo software

Il Nuovo Regolamento Europeo sulla Privacy (GDPR), emanato lo scorso maggio ed in vigore entro fine maggio 2018, pone nuove questioni relativamente all'impiego di programmi software per l'elaborazione di dati personali, in particolare se si tratta anche di dati c.d. "sensibili" secondo la vecchia definizione del D. Lgs 196/2003.

Infatti il nuovo Regolamento Europeo sulla privacy ("Regolamento UE 2016/679 del Parlamento europeo") impone alle organizzazioni che intendono effettuare trattamenti di dati personali di "progettare" il sistema in modo tale che sia conforme fin da subito (**Privacy by design**) alle regole della privacy, spostando la responsabilità del corretto trattamento tramite strumenti informatici idonei sul titolare e sul

responsabile del trattamento, quando identificato.

Nella pratica una organizzazione, prima di impiegare un applicativo software per trattare dati personali dovrà verificare che esso sia conforme ai requisiti stabiliti dal Regolamento UE 679/2016, ovvero che presenti caratteristiche di sicurezza adeguate per mantenere protetti i dati personali, compresa l'eventuale pseudonomizzazione dei dati personali, quando necessaria, e la cifratura dei dati stessi.

Il Regolamento parla anche di "certificazione" della privacy, che può riferirsi ad un singolo o ad un insieme di trattamenti effettuati da un programma software, oppure da tutti i trattamenti effettuati da una organizzazione. In quest'ultimo caso siamo molto vicini alla certificazione del sistema di gestione ISO 27001, anche se in realtà il GDPR intende qualcosa di differente. Al proposito è stato approvato da ACCREDIA lo schema proprietario ISDP©10003:2015 (conformità alle norme vigenti EU in tema di trattamenti dei dati personali)che conente di certificare un prodotto, processo o servizio relativamente alla gestione dei dati personali, quindi anche un applicativo software che tratta dati personali.

Lo schema di certificazione ISDP 10003:2015 risponde ai requisiti di cui agli art. 42 e 43 del Regolamento 679/2016 ed è applicabile a tutte le tipologie di organizzazioni soggette alle norme vigenti in tema di tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati. Lo schema di certificazione specifica ai "Titolari" e "Responsabili" del trattamento, soggetti ai vincoli normativi vigenti nel territorio dell'EU, i requisiti necessari per la corretta valutazione della conformità alle norme stesse.

Per maggiori informazioni su questo schema di certificazione si veda la pagina del sito Inveo
http://www.in-veo.com/servizi/certificazioni-inveo/isdp-10003-2015-data-protection.

Ricordiamo anche che all'art 25, coma 2 il Regolamento sancisce che:

Il titolare del trattamento mette 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.

Rappresenta **la c.d. Privacy by default**: devono essere trattati "per default" solo i dati necessari a perseguire le finalità del trattamento posto in essere dal responsabile dello stesso, ovvero non devono essere trattati dati in eccesso senza che una persona fisica autorizzata lo consenta.

La certificazione introdotta all'Art. 42 può servire a dimostrare l'adozione di misure tecniche ed organizzative adeguate.

L'impatto di queste regole sugli **applicativi software** utilizzati per trattare anche dati personali è notevole: una organizzazione di qualsiasi dimensione che adotta un sistema informatico gestionale che tratta dati personali non in modo conforme al Regolamento UE 679/2016 di fatto rischia di essere sanzionata perché non ha adottato misure di sicurezza adeguate. Le responsabilità ricadono, in questo caso, sul titolare del trattamento e sul responsabile del trattamento, ove presente.

Dunque prima di adottare un nuovo software che gestisce archivi contenenti dati personali (a maggior ragione se vengono gestiti dati sanitari o altri dati c.d. "sensibili") titolari e responsabili del trattamento devono valutarne la **conformità alla normativa sulla privacy** e questo può essere al di fuori delle competenze di chi decide l'acquisto di un applicativo software (responsabili EDP, Direttori Generali, ecc.), soprattutto nelle piccole e medie imprese o nelle strutture sanitarie di modeste dimensioni (es. Cliniche ed ambulatori privati).

La casistica di software che ricadono in questa sfera è vastissima, si va dai comuni ERP che trattano anche dati del personale, ai software per la gestione delle paghe, ai programmi per la gestione delle *fidelity card*, ai software impiegati in strutture sanitarie o quelli utilizzati dagli studi legali.

Oggi molti applicativi, magari obsoleti, non permettono di implementare misure di sicurezza adeguate (password di lunghezza adeguata, password di complessità minima variate periodicamente, password trasmesse via internet con connessioni crittografate, gestione utenti, raccolta di dati minimi indispensabili, gestione dei consensi, procedure di backup, ecc.) e in futuro il loro impiego diverrà non conforme alla normativa sulla privacy, ovvero non saranno più commercializzabili.

Da un lato i progettisti e gli sviluppatori di applicativi software dovranno considerare fra i requisiti di progetto anche quelli relativi alla normativa privacy, dall'altro le organizzazioni che adotteranno applicativi software (o che già li stanno utilizzando) saranno responsabili della loro eventuale non conformità al Regolamento Privacy. Sicuramente una certificazione di tali applicativi o un assessment indipendente potrà sollevare il titolare del trattameto dalle rsponsabilità (cfr. principio dell'*accountability)* connesse all'adozione di un software che non tratta i dati in conformità al GDPR.

Nuovo Regolamento UE sulla Privacy: cosa cambia per le imprese?

Lo scorso 4 maggio è stato pubblicato sulla gazzetta ufficiale della Comunità Europea il "**Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE** (regolamento generale sulla protezione dei dati)" e dopo 20 giorni dalla sua pubblicazione è divenuto legge europea, pertanto a partire dal 25 maggio 2016 decorrono i due anni di transitorio per l'applicazione del nuovo Regolamento.

Nella pagina Documenti di questo sito è possibile scaricare il testo ufficiale (ora anche per gli utenti non registrati).

Il Garante per la Protezione dei dati personali ha pubblicato un'apposita guida (http://194.242.234.211/documents/10160/5184810/Guida+al+nuovo+Regolamento+europeo+in+materia+di+protezione+dati).

Rispetto al precedente articolo pubblicato su questo sito il 27/04/2016, basato sulla traduzione della proposta di Regolamento approvata dal Parlamento Europeo a dicembre 2015, di cui il presente articolo costituisce un aggiornamento, si rilevano alcune differenze nella traduzione del testo originale inglese in lingua italiana, rispetto all'attuale Codice privacy D.Lgs 196/2003:

- Viene mantenuto il "Titolare del trattamento" (*Data Controller*);
- Viene mantenuto il "Responsabile del Trattamento" (*Data processor*);
- Viene abolito l'Incaricato del trattamento.

Il nuovo Regolamento introdurrà una legislazione in materia di protezione dati uniforme e valida in tutta Europa, affrontando temi innovativi – come il diritto all'oblio e alla portabilità dei dati – e stabilendo anche criteri che da una parte responsabilizzano maggiormente imprese ed enti rispetto alla protezione dei dati personali e, dall'altra, introducono notevoli semplificazioni e sgravi dagli adempimenti per chi rispetta le regole. Il Regolamento UE 679/2016, però, non sarà l'unica fonte legislativa per regolamentare la protezione dei dati personali, infatti le Autorità dei singoli Stati Membri – e quindi il Garante della Privacy per l'Italia – potranno integrare i contenuti del Regolamento dettagliando meglio alcuni aspetti che al momento appaiono poco chiari, introdurre linee guida generali e di settore, regolamentare aspetti particolari, ecc.

A tal proposito occorre ricordare che, con l'uscita del Regolamento 679 non vengono aboliti i provvedimenti del nostro Garante su Videosorveglianza, Amministratori di Sistema, fidelity card, biometria, tracciamento flussi bancari, ecc. Tali provvedimenti probabilmente verranno modificati e/o integrati dal Garante Privacy per aggiornarli ed eventualmente adeguarli alle prescrizioni del Regolamento Europeo 679.

Il Garante Privacy italiano potrà inoltre integrare il Regolamento UE 679 per disciplinare il trattamento di dati personali effettuato per adempiere obblighi di legge italiana e in particolari ambiti, ad esempio quello dei dati sanitari, oppure per definire in modo più dettagliato gli obblighi per le PMI (ovvero per le organizzazioni che occupano meno di 250 dipendenti, per le quali il regolamento 679 ha stabilito delle semplificazioni).

Ma quali sono le principali novità per le imprese nella gestione della privacy a fronte del Regolamento UE?

L'aspetto più significativo è sicuramente il cambio di approccio rispetto al Codice Privacy attualmente in vigore in Italia, ed in particolare all'Allegato B, ovvero al Disciplinare Tecnico delle Misure Minime di Sicurezza. Il nuovo Regolamento Europeo sulla privacy, infatti, non definisce requisiti specificati in termini precisi, come avviene per l'attuale normativa italiana sulla privacy, ma sposta la responsabilità di definire le misure di sicurezza idonee a garantire la privacy dei dati personali trattati sul titolare o responsabile del trattamento, dopo un'attenta analisi dei rischi.

Dunque non ci sono più misure minime, ma solo misure di sicurezza adeguate, progettate dal titolare o responsabile del trattamento dopo aver effettuato l'analisi dei rischi che incombono sui dati personali che si intende trattare. Sottolineiamo quest'ultimo aspetto: le misure di prevenzione vanno poste in atto prima di iniziare il trattamento.

Poiché a livello nazionale la legislazione italiana ed il Garante per la Protezione dei Dati Personali hanno seguito il percorso europeo, a partire dalla Direttiva Europea 46/95, a livello di principi sulla privacy non ci sono differenze significative tra normativa italiana e Regolamento Europeo. Infatti, alcune regole già imposte dal Codice Privacy e dalle successive disposizioni del Garante restano valide, anche se con contorni un po' meno definiti da criteri oggettivi. In sostanza:

- Viene regolamentato solo il trattamento di dati personali di persone fisiche (non giuridiche) per scopi diversi dall'uso personale.
- Resta una distinzione fra trattamento di dati personali comuni e trattamento di dati c.d. sensibili, anche se la definizione del D.lgs 196/2003 non viene utilizzata nel Regolamento UE 679, lasciando però la possibilità agli Stati membri di stabilire una disciplina particolare in merito.

- Restano gli obblighi di informare l'interessato sull'uso che verrà fatto dei suoi dati personali.
- Restano gli obblighi di ottenere il consenso per i trattamenti non necessari o per i trattamenti di particolari tipi di dati, ad esempio quelli idonei a rivelare lo stato di salute delle persone, le origini razziali, le idee religiose, ecc.

Tra gli elementi che cambiano vi sono sicuramente:

- La denominazione ed i ruoli degli attori: il titolare del trattamento rimane tale, **il responsabile del trattamento è ora responsabile in solido con il titolare per i danni derivanti da un trattamento non corretto**, l'incaricato rimane il soggetto che fisicamente tratta i dati, ma tale ruolo non è delegabile, se non attraverso uno specifico accordo contrattuale. Il responsabile può individuare un proprio rappresentante.
- I dati personali trattati devono essere protetti con misure organizzative e tecniche adeguate a garantirne la riservatezza e l'integrità.
- I diritti dell'interessato sono più ampi e maggiormente tutelati.
- Il responsabile del trattamento deve mettere in atto **misure tecniche ed organizzative** tali da consentirgli di dimostrare che tratta i dati personali in conformità al Regolamento. Tali misure devono seguire lo stato dell'arte e devono derivare dall'analisi dei rischi che incombono sui dati, secondo relativa gravità e probabilità.
- **Privacy by default**: devono essere trattati "per default" solo i dati necessari a perseguire le finalità del trattamento posto in essere dal responsabile dello stesso, ovvero non devono essere trattati dati in eccesso senza che una persona fisica autorizzata lo consenta.
- **Privacy by design**: ogni nuovo trattamento di dati personali dovrà essere progettato in modo da garantire la sicurezza richiesta in base ai rischi a cui è sottoposto prima di essere implementato. Anche i sistemi informatici dovranno essere progettati secondo tale principio.
- Possono esserci più responsabili per un medesimo trattamento che risulteranno, pertanto, corresponsabili di eventuali trattamenti non conformi, ma dovranno stabilire congiuntamente le rispettive responsabilità.
- Le imprese **con sede al di fuori dell'Unione Europea**, che trattano dati personali di interessati residenti nella UE dovranno eleggere una propria organizzazione o entità all'interno della UE che sarà responsabile di tali trattamenti.
- Devono essere mantenuti **registri dei trattamenti** di dati effettuati con le informazioni pertinenti e le relative responsabilità. Tali registri non sono obbligatori per organizzazioni con meno di 250 dipendenti salvo che non trattino dati sensibili (secondo la definizione del Codice della Privacy attualmente in vigore) o giudiziari. Tale discriminante potrà essere meglio specificata da appositi provvedimenti del nostro Garante.
- Il responsabile del trattamento deve notificare all'autorità competente – e, in casi gravi, anche all'interessato – ogni **violazione dei dati** (*data breach*) trattati entro 72 ore dall'evento.

- Quando un trattamento presenta dei rischi elevati per i dati personali degli interessati (i casi specifici dovranno essere esplicitati dall'Autorità Garante), il responsabile del trattamento deve effettuare una **valutazione di impatto preventiva**, prima di iniziare il trattamento.
- Viene introdotta la **certificazione** del sistema di gestione della privacy (le cui modalità dovranno essere meglio definite tramite gli Organismi di Accreditamento Europei, ACCREDIA per l'Italia)..
- È richiesta la designazione di un **Responsabile della Protezione dei Dati** (*Data Protection Officer*) nelle Aziende Pubbliche e nelle organizzazioni che trattano dati sensibili o giudiziari su larga scala oppure che la tipologia di dati trattati e la loro finalità richieda il controllo degli incaricati al trattamento su larga scala.

Proprio quest'ultimo punto, variato rispetto alle precedenti versioni del Regolamento, farà molto discutere, poiché non stabilisce criteri precisi ed oggettivi (cosa significa "su larga scala"?) per l'adozione di tale figura professionale, di competenze adeguate a garantire una corretta applicazione della normativa sulla privacy. Il Responsabile per la Protezione dei Dati dovrà essere correttamente informato dal Responsabile del Trattamento su tutte le attività che riguardano la privacy e dovrà disporre di risorse adeguate per svolgere il proprio compito e mantenere le sue competenze adeguate al ruolo che ricopre. Egli dovrà inoltre essere indipendente dalle altre funzioni dell'organizzazione e riferire solamente all'alta direzione.

La sicurezza dei dati – in termini di riservatezza, integrità e disponibilità – deve essere garantita in funzione del rischio che corrono i dati stessi, dei costi delle misure di sicurezza e dello stato dell'arte della tecnologia. Pertanto le password di almeno 8 caratteri variate almeno trimestralmente, l'antivirus aggiornato, il firewall e l'aggiornamento del sistema operativo potrebbero essere misure adeguate per determinati trattamenti, ma non per altri, oppure in determinate organizzazioni, ma non in altre, in ogni caso lo potrebbero essere oggi, ma non domani quando il progresso tecnologico (anche degli hacker e di coloro che minacciano i nostri dati) potrebbe renderle insufficienti.

Lasciando per il momento stare gli impatti che il nuovo Regolamento UE sulla privacy potrà avere per i colossi del web, quali Facebook, Google, ecc., è opportuno osservare che per le piccole e medie imprese italiane dovrà cambiare l'approccio

alla privacy, soprattutto per quelle organizzazioni che trattano dati sensibili o giudiziari. Occorrerà un cambio di mentalità: non serve più un po' di carte (informative, consensi, lettere di incarico, …) ed alcune misure minime di sicurezza specifiche (password, antivirus,…) per garantire il rispetto della legge. Poiché molti imprenditori vedono la privacy solo come un disturbo da gestire soltanto per non incorrere in sanzioni e, quindi, come una pratica da sbrigare nel modo più indolore possibile, ecco che il passaggio al nuovo Regolamento – che dovrà avvenire nei prossimi due anni – non sarò proprio una passeggiata.

Le responsabilità in capo al responsabile del trattamento (ex titolare del trattamento) sono maggiori e comunque più impegnative da gestire, soprattutto laddove il trattamento di dati venga delegato a fornitori (es. consulenti del lavoro, consulenti fiscali e legali, strutture esterne, ecc.) che dovranno inevitabilmente essere tenuti sotto controllo.

Non è che taluni principi fossero assenti dalla normativa italiana del 2003, ma – complice la crisi e le semplificazioni adottate da precedenti governi, soprattutto l'abolizione del DPS – hanno un po' sminuito l'importanza della privacy in azienda, anche perché – si sa come siamo fatti noi italiani – senza sanzioni esemplari non ci preoccupiamo di nulla… e sono stati molto rare le sanzioni comminate alle aziende, anche perché i controlli sono stati molto poco frequenti.

Paradossalmente ha spaventato di più la disposizione sui *cookie* perché la sua mancata applicazione è di fatto pubblica, mentre altre regole di fatto trascurate rimangono tra le muar delle organizzazioni di ogni dimensione.

L'indeterminatezza di alcune regole potrà essere colmata da disposizioni specifiche dei singoli Stati membri e/o da linee guida di settori specifici che potranno agevolare l'interpretazione della legge.

Ora la privacy sarà meno materia per avvocati – se non per la stesura di contratti che regolamentano i rapporti fra clienti e fornitori anche in materia di trattamento dati personali – e più materia per **esperti della sicurezza delle informazioni**. Infatti l'approccio del nuovo Regolamento Europeo sulla Privacy si avvicina, *mutatis mutandis*, a quello della norma UNI EN ISO/IEC ISO 27001 e della linea guida UNI EN ISO/IEC 27002.

L'adozione del nuovo Regolamento UE sarà, pertanto, più impegnativa per piccole organizzazioni che trattano molti dati c.d. sensibili o giudiziari, quali organizzazioni private nel campo della sanità (cliniche ed ambulatori privati, farmacie, …), studi di consulenza del lavoro, infortunistiche, studi legali, studi di consulenza fiscale, ecc., piuttosto che per aziende che trattano come unici dati sensibili i dati relativi ai propri dipendenti. Anzi saranno proprio queste ultime che dovranno pretendere da società e studi di consulenza esterna adeguate garanzie

per il trattamento dei dati di cui sono responsabili.