Prime esperienze di applicazione del GDPR

Il GDPR è divenuto pienamente attuativo dal 25 maggio scorso, anche se in realtà era stato pubblicato due anni prima, però il processo di adeguamento delle imprese italiane al GDPR è ancora in corso. Questo perché da un lato, come è consuetudine nel nostro Paese, le Imprese affrontano le scadenze legislative solo all'ultimo momento, non preoccupandosi di capire prima quanto tempo è necessario per l'adeguamento legislativo. Dall'altro anche le Istituzioni (Stato Italiano e Garante Privacy) stanno impiegando molto più tempo del previsto per rendere completo, ed auspicabilmente di chiara interpretazione, il panorama legislativo in materia di protezione dei dati personali.

Il fatto che molti punti del GDPR non sono di facile interpretazione e, anzi, gli approcci sono talvolta differenti, non ha fatto altro che rallentare il percorso di adeguamento.

Tra gli effetti collaterali di questo lento percorso di adeguamento c'è la difficoltà di interfacciarsi con i soggetti esterni all'impresa o allo studio professionale, perché il mondo perfetto in cui i miei clienti ed i miei fornitori sono già adeguati al GDPR – e lo hanno interpretato in modo uniforme – al momento non esiste, e non si sa quando ci si arriverà.

Passiamo ad esaminare le principali problematiche – e possibili soluzioni – delle prime applicazioni del GDPR in organizzazioni di diverso tipo e dimensioni.

1) **Informative e consensi**

L'informativa è lo specchietto delle allodole della nuova normativa sulla privacy; non bisogna credere che basta trovare un modello di informativa, magari gratuitamente dal web o da amici e colleghi, per aver risolto il problema privacy: uno su mille ce la fa! Solo pochi singoli (ditte individuali, professionisti singoli) senza dipendenti possono accontentarsi della nuova informativa.

Inoltre, l'informativa ha un contenuto che non può essere redatto in modo completo solo partendo da un modello standard e conoscendo l'art. 13 (e seguenti) del Regolamento UE 679/2016; occorre conoscere come funzionano i flussi di trattamento dei dati personali nell'organizzazione. Magari attraverso un'assessment ed una *gap analysis* approfondita, soprattutto nelle organizzazioni più complesse.

Infine, c’è il problema di come comunicare l’informativa agli interessati. Occorre analizzare bene requisiti normativi, processi gestionali ed esigenze organizzative per scegliere le modalità più opportune. Probabilmente un’informativa pubblicata su una pagina web ed una e-mail ai clienti (effettivi e potenziali) e fornitori, che comunica l’aggiornamento dell’informativa privacy, reperibile al sito www…. è la soluzione migliore nella maggior parte delle organizzazioni, soprattutto se operano B2B.

2) **Responsabili esterni del trattamento**

Il GDPR ci dice di identificare i soggetti esterni all’organizzazione che trattano per “suo conto” dati personali e di designarli come responsabili del trattamento attraverso un atto a valenza contrattuale.

In primo luogo occorre stabilire quali fornitori (e non solo) operano come responsabili del trattamento perché trattano dati personali di cui l’organizzazione è titolare del trattamento: società e studi che forniscono servizi contabili e fiscali, società e studi che forniscono servizi di elaborazione buste paga e consulenza del lavoro, società che forniscono servizi informatici (servizi di assistenza sistemistica, fornitori di software gestionale ed applicativo, fornitori di servizi cloud, ecc.) sono solo alcuni candidati… occorre anche qui capire come si svolgono le varie attività internamente ed esternamente ed è necessario valutare l’affidabilità del fornitore in termini di garanzie relative alla protezione dei dati personali.

Per gestire correttamente questo punto bisogna essere in due ed essere d’accordo sulla nomina di responsabile del trattamento e sui relativi obblighi contrattuali del responsabile.

Questa attività di “regolarizzazione” dei responsabili del trattamento è spesso lunga e non priva di ostacoli, anche per l’inerzia dei fornitori in questione a rispondere a semplici questionari nei quali si va a chiedere loro quali misure di sicurezza sono state implementate al loro interno (ad es. nella gestione operativa dello studio e/o nel software). Se poi il fornitore non accetta la nomina a responsabile del trattamento (e dei relativi obblighi contrattuali) perché si sente titolare autonomo o semplice soggetto autorizzato a trattare dati personali, ecco che il processo di adeguamento al GDPR si complica enormemente. Se si prende spunto dai sistemi di gestione qualità ISO 9001 si comprende che i fornitori dovranno essere “qualificati” per fornire la nostra organizzazioni e situazioni nelle quali il fornitore tiene “in scacco” il cliente in tema di privacy sono da evitare.

3) **Registro delle attività di trattamento**

È un adempimento non solo formale (praticamente l’unico richiesto alla stragrande maggioranza delle organizzazioni), ma sostanziale: per redigere il registro dei trattamenti (del titolare e del responsabile) bisogna conoscere quali dati personali

vengono trattati, in quali processi dell'organizzazione e con quali modalità. Anche in questo caso occorre un'analisi dei processi dell'organizzazione precisa e puntuale. Effetto collaterale di questa attività di mappatura dei flussi di dati dell'organizzazioni potrebbe essere quello, gradito, di individuare gestioni di dati ridondanti e inefficienti, da eliminare in prospettiva, non solo di privacy.

Ci sono diverse interpretazioni nella composizione del Registro dei trattamenti, francamente non credo che le diverse interpretazioni possano costituire un rischio di *compliance* del registro dei trattamenti a fronte di ispezioni del Garante, dato che in fondo non esistono linee guida chiare sulle corrette modalità di alimentazione dei registri dei trattamenti (le recenti FAQ del Garante in merito non aiutano più di tanto).

Un registro completo anche di informazioni non necessariamente richieste dal GDPR, ma utili nella gestione dei dati personali (es. software gestionali ed applicativi che trattano i dati personali, funzioni aziendali autorizzate a trattare i dati, ecc.) risulta utile per comprendere come sono gestiti i dati personali.

Da ultimo, per completare i registri dei trattamenti occorre sapere per quali attività di trattamento l'organizzazione è titolare del trattamento e per quali è solo responsabile: e ciò si lega alle problematiche del punto precedente, anche in senso opposto, relativamente ai ruoli di titolare e responsabile del trattamento, o magari di contitolare.

4) **Misure di sicurezza tecniche ed organizzative**

La definizione delle misure di sicurezza adeguate è uno dei punti più difficili del GDPR. Propedeutica a questa attività c'è la valutazione dei rischi che incombono sui dati personali e soprattutto sulle persone fisiche cui si riferiscono.

Al di là della criticità o meno dei trattamenti effettuati dalle diverse organizzazioni occorre stabilire un livello minimo di sicurezza nei sistemi di protezione dei dati personali, coerente con gli standard nazionali ed internazionali e le *best practice* di sicurezza informatica. Il problema è che non esistono più le misure minime di sicurezza stabilite per legge, anche se alcune di esse (non tutte) rimangono valide a livello di standard minimo di sicurezza sostenibile davanti ad un Giudice. Infatti, dobbiamo pensare al caso peggiore: l'ispezione del Nucleo Privacy della Guardia di Finanza (magari a seguito di un *data breach*) e le richieste di risarcimento danni di un interessato che si ritiene danneggiato da una violazione dei suoi dati personali.

Allora occorre documentare lo stato dei sistemi informatici con riferimento alle misure di sicurezza implementate e documentare anche le misure organizzative attuare. È il minimo per dimostrare *l'accountability*, ma può essere solo un punto di partenza se le misure implementate non sono convincenti per essere sostenute nei confronti di terzi.

Nelle PMI talvolta la gestione sistemistica dei sistemi informatici è delegata ad un soggetto esterno (singolo professionista o società di servizi informatici). In questi casi il titolare dei trattamenti come minimo dovrebbe pretendere una descrizione dettagliata delle logiche di funzionamento dei sistemi e delle misure di sicurezza implementate, ma spesso il fornitore è restio a documentare una prassi non completamente sicura, implicitamente accettata dalla Direzione aziendale che non intendeva sobbarcarsi ulteriori costi per rendere maggiormente sicuri i sistemi.

Una misura di sicurezza (organizzativa) è costituita proprio dalla disponibilità di relazioni e dichiarazioni scritte da parte del fornitore di servizi IT.

Tra le misure organizzative di sicurezza rientrano anche nomine ad amministratore di sistema (secondo il provvedimento del Garante per la Privacy del 2008 ancora valido) di coloro che di fatto svolgono tali mansioni, contratti con fornitori che garantiscono sicurezze adeguate sui dati personali da essi gestiti, compresa una designazione a responsabile esterno del trattamento, la formazione del personale, procedure e istruzioni interne.

Su quest'ultimo aspetto risulta molto utile istituire una sorta di "Regolamento informatico interno", che descriva le regole da seguire da parte del personale quando utilizza i dispositivi ITC messi a disposizione dall'azienda e non solo. Tale Regolamento dovrebbe trattare – coerentemente con le misure di sicurezza effettivamente implementate – argomenti quali: gestione delle password, gestione delle postazioni di lavoro, gestione dei dispositivi portatili, misure di sicurezza da adottare in viaggio, modalità di utilizzo dei dispositivi elettronici assegnati (cosa si può fare e cosa no), regole da seguire nella navigazione internet e nell'utilizzo della posta elettronica e così via.

Tali disposizioni, oltre che per la protezione dei dati personali, sono utili alla Direzione aziendale per garantirsi in caso di atti illeciti commessi da un dipendente tramite strumenti ICT dell'azienda.

Tornando alle misure di sicurezza informatica implementate, le principali carenze che si rilevano, soprattutto nelle piccole e microimprese, sono legate all'utilizzo di antivirus *free* (che talvolta non lo sono per utilizzo a fini commerciali), indirizzi di posta elettronica gratuiti, piattaforme in cloud gratuite, servizi di trasmissione di file di grandi dimensioni, ecc. Come noto il termine "gratis" è estremamente gradito a molti piccoli imprenditori, ma per chi tratta dati personali, specie se di tipo sanitario o giudiziario, i sistemi gratuiti offerti anche da importanti *player* mondiali quali Google, Microsoft, ecc. potrebbero non rappresentare una misura di sicurezza adeguata. Se i dati personali sono critici dal punto di vista della riservatezza, sistemi che non la garantiscono a priori (il servizio gratuito è generalmente fornito in cambio dell'utilizzo dei dati) non costituiscono la scelta migliore. Inoltre la conservazione di dati personali in *cloud storage* che fisicamente risiedono fuori dalla UE è ammessa solo sotto determinate condizioni.

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 (845 download) (compreso l'allegato con le FAQ)
- Linee Guida Valutazione-Impatto WP 248 (324 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.