Nuovo Decreto Legislativo n. 101 del 10 agosto 2018 – Codice Privacy emendato

Il Decreto Legislativo 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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)" è stato pubblicato in Gazzetta Ufficiale il 04/09/2018 ed entra in vigore dal 19/09/2018.

Il tanto atteso (da chi si occupa di GDPR e privacy in generale) documento normativo permette di inquadrare meglio la materia "protezione dati personali" nel panorama legislativo italiano dopo l'entrata in vigore del Regolamento UE 679/2016 (RGPD o GDPR).

Come previsto dalle letture delle precedenti versioni dello schema di Decreto, approvato dal C.d.M. lo scorso 8 agosto, il testo di legge non fuga molti dubbi che sono emersi dall'applicazione del GDPR in questi primi mesi (in realtà il Regolamento è noto da oltre due anni).

In particolare, non viene trattato il tema delle nomine dei Responsabili esterni del Trattamento (quando si rientra in questo caso? Che fare se la nomina viene rifiutata dal fornitore?), ma questo forse potrà essere argomento delle Linee Guida per le PMI del Garante Privacy, che di fatto riguarderanno la quasi totalità delle organizzazioni italiane per come è strutturato il nostro panorama industriale e dei servizi. Non vengono nemmeno fugati i molti dubbi circa l'applicazione di determinate misure di sicurezza o relativamente al concetto di "larga scala".

Purtroppo il concetto di *accountability* (responsabilizzazione) è lontano dall'animo degli imprenditori italiani, che hanno sempre necessitato di regole certe e ben definite: o bianco o nero, permesso o vietato. È come se nel Codice della Strada scomparissero i limiti di velocità e comparisse una regola generale che preveda che "in ogni strada ogni automobilista deve mantenere una velocità adeguata a garantire la sicurezza di persone e cose, minimizzando i rischi di provocare incidenti".

Oltre alle **misure di semplificazione per le PMI**, che il Garante Privacy italiano

dovrà emanare prossimamente (i tempi previsti sono piuttosto lunghi, visto anche che il GDPR è pienamente attuativo già da oltre tre mesi ed è stato pubblicato nel 2016), farà certamente piacere a molte organizzazioni sapere che tra le **disposizioni transitorie e finali**, contenute all'art. 22 del nuovo D.Lgs 101/2018, è invece previsto che *"per i primi otto mesi dalla data di entrata in vigore, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative (…), della fase di prima applicazione delle disposizioni sanzionatorie". Dunque, fino al 19 maggio 2019 il Garante sarà clemente? Cosa significa? Vuol dire che non ci saranno sanzioni, se non nei casi più gravi (o che costituiscono violazioni della normativa sulla privacy già da tempo), fino a maggio 2019, ma non si può dire ufficialmente per non subire la reprimenda della UE?*

Il nuovo D. Lgs 101/2018 in realtà va a modificare il vecchio D. Lgs 196/2003 che, però, vede abrogati la maggior parte dei suoi articoli e, di fatto, viene riscritto tenendo conto delle prescrizioni del GDPR Europeo. In pratica il D. Lgs 101/2018 è poco leggibile, se non si dispone di una versione del D. Lgs 196/2003 modificata e integrata. Ampiamente criticabile è la scelta di novellare il Codice Privacy (D. Lgs 196/2003 con le sue successive modifiche ed integrazioni intercorse negli anni) anziché abrogarlo in toto ed emanare un nuovo Decreto.

Tutto ciò non fa che rendere il panorama normativo in materia di privacy sempre più complesso, oltre che ancora fluido. Si pensi anche ai provvedimenti del Garante Privacy preesistenti all'entrata in vigore del Regolamento 679/2016, che sono stati ritenuti ancora validi, fatto salvo che il Garante stesso potrà modificarli per aggiornarli alla normativa attuale.

Ma veniamo ai punti salienti trattati dal nuovo Decreto Legislativo 101 del 2018:

- Inquadramento dei compiti di interesse pubblico che riguardano i trattamenti dei dati personali, attività della Pubblica Amministrazione e tutto ciò che concerne i trattamenti di dati personali effettuati dagli apparati Statali e dalla Sanità Pubblica. Nel GDPR tali situazioni erano correttamente rimandate a regolamentazioni nazionali.
- Chiarimenti sulle modalità di trattamento di particolari categorie di dati, quali dati relativi alla salute, dati genetici e dati biometrici.
- Definizione più dettagliata dei criteri di applicazione delle sanzioni ed introduzione delle sanzioni penali (solo per situazioni molto gravi).
- Introduzione dei soggetti "designati" al trattamento dei dati personali, con particolari compiti e responsabilità, non solo soggetti "istruiti" e non più "responsabili interni al trattamento".
- Disposizioni per settori specifici (anche semplificazioni per la gestione dei curriculum ricevuti dalle organizzazioni).
- Regole per il settore delle comunicazioni elettroniche e per il giornalismo.
- Conferimento di poteri al Garante per la Protezione dei Dati Personali per l'aggiornamento di provvedimenti e disposizioni varie, comprese le misure semplificate per le PMI e la definizione dei ruoli nei confronti di ACCREDIA

relativamente alla certificazione.
- Criteri di applicazione delle sanzioni.

In conclusione il percorso di rinnovamento del “sistema privacy” non si è ancora concluso e le problematiche attuative, soprattutto per le organizzazioni che trattano in modo significativo dati personali, anche appartenenti alle “particolari categorie di dati” individuate dal GDPR, restano abbastanza complesse, soprattutto a fronte di un meccanismo sanzionatorio incerto che potrebbe portare a parecchie contestazioni. Vedremo come il Garante potrà svolgere il gravoso compito demandatogli dal Governo.

Decreto Legislativo 101/2018 - Modifiche al Codice Privacy (39 download)

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.

Organismi che effettuano verifiche ai sensi del DPR 462/2001: cosa serve per l'accreditamento ACCREDIA

Come ormai noto gli **organismi abilitati alle verifiche secondo il D.P.R. 462/2001** ("Regolamento di semplificazione del procedimento per la denuncia di installazioni e dispositivi di protezione contro le scariche atmosferiche, di dispositivi di messa a terra di impianti elettrici e di impianti elettrici pericolosi") hanno l'**obbligo di accreditamento UNI CEI EN ISO/IEC 17020:2012** ("Valutazione della conformità – Requisiti per il funzionamento di vari tipi di organismi che eseguono ispezioni") in base alle disposizioni del Ministero dello Sviluppo Economico e dagli accordi stipulati da quest'ultimo con ACCREDIA.

Con un'apposita circolare – la 29 del 2017 – l'Ente unico di accreditamento, facendo seguito alle precedenti comunicazioni, ha reso noto le modalità particolari di espletamento di tali pratiche. Oltre a ciò sono stati stabiliti alcuni requisiti aggiuntivi o integrativi della ISO 17020, della Linea Guida ILAC P15 e dei Regolamenti Accredia per l'accreditamento degli Organismi di Ispezione che operano in questo settore particolare.

Relativamente alle procedure di accreditamento, gli Organismi (OdI) sono stati suddivisi in due gruppi, in base alla data di scadenza dell'abilitazione. Il primo gruppo doveva presentare domanda di accreditamento ad ACCREDIA entro il 30 novembre 2017, il secondo dovrà farlo entro il **30 giugno 2018**.

Ciò non significa che gli Organismi dovranno essere pronti ad essere accreditati ISO 17020 entro tali date, ma semplicemente che abbiano presentato domanda. Ma cosa significa ciò in pratica?

Oltre alla compilazione della domanda (che include solo informazioni societarie), reperibile sul sito ACCREDIA, gli organismi dovranno presentare una serie di documenti riepilogati nel seguito:

- Manuale del Sistema di Gestione;
- Nome, titolo di studio e Curriculum vitae del Responsabile Tecnico e del suo

Sostituto;
- Organigramma nominativo con compiti e responsabilità;
- Statuto;
- Ultimo bilancio disponibile con revisione contabile indipendente;
- Polizza Assicurativa;
- Regolamento o documento equivalente per la gestione delle attività di ispezione per le quali è richiesto l'accreditamento;
- Elenco controllato degli Ispettori ed Esperti e relativi curricula vitae;
- Elenco delle Procedure, istruzioni operative e altri documenti applicabili alle attività dell'Organismo;
- Procedura di qualifica degli Ispettori o documenti equivalenti;
- Copia tipo dei Piani di Ispezione;
- Elenco dei Soggetti (organizzazioni o persone) in possesso di Rapporti di Ispezione rilasciati dall'Organismo (in questo visto che si tratta di Organismi che operano da tempo nel settore, credo sia sufficiente un elenco recente dei clienti per i quali sono state effettuate ispezioni come organismo abilitati dal Ministero).

Anche se l'elenco potrebbe spaventare, occorre ricordare che si tratta di Organismi che già operano con abilitazione Ministeriale in questo settore e dovrebbero già disporre di molte delle informazioni sopra elencate in forma documentata.

Probabilmente gli interventi più consistenti sulla documentazione già esistente si dovranno apportare al Manuale del Sistema di Gestione (in pratica un Manuale Qualità), predisposto in accordo alla ISO 17020 alla Procedura di Qualifica degli Ispettori e al Regolamento.

Riguardo agli altri documenti occorre fare alcune precisazioni in base a quanto contenuto nella Circolare Accredia n. 29/2017, anche con riferimento alla Direttiva del'11 marzo 2002:

- Nello Statuto non devono figurare attività in potenziale conflitto di interessi;
- Oltre al Bilancio d0esercizio è richiesta una **revisione contabile indipendente** (non più richiesta nell'ultima edizione della ISO 17020:2012);
- La Polizza Assicurativa per Responsabilità Civile Professionale deve coprire anche l'attività degli ispettori esterni (che, quindi, non devono sopperire con la propria polizza RC professionale) e deve avere un **massimale di 1, 55 milioni di euro**;
- Responsabile Tecnico (o Direttore Tecnico) e suo Sostituto devono soddisfare appositi requisiti di competenze e devono essere **dipendenti, titolari o soci operativi operanti in esclusiva per l'Organismo** (tale requisito non è imposto per i Sostituti del Direttore Tecnico dalla ISO 17020);
- Anche gli ispettori – interni ed esterni – devono soddisfare appositi requisiti di competenza e devono operare, per le attività di verifica oggetto di accreditamento, **in esclusiva** per l'Organismo.

La Circolare Accredia sopra menzionata specifica altri aspetti maggiormente restrittivi rispetto alla ISO 17020 ed alla ILAC P15:2016, in particolare:

- Gli strumenti di misura, gestiti sotto controllo dell'Organismo, devono soddisfare particolari requisiti di conferma metrologica (si veda al riguardo anche la Linea Guida ILAC P10);
- Gli ispettori non possono svolgere attività potenzialmente in conflitto di interesse – quali progettazione, installazione, manutenzione e commercializzazione di impianti elettrici – non solo relativamente all'oggetto ispezionato, ma rispetto a tutti gli oggetti simili (ovvero ogni impianto elettrico);
- Sono richieste all'OdI apposite dichiarazioni sul possesso e l'impiego di adeguati dispositivi di protezione individuale (D.P.I.).

Una volta presentata la domanda occorrerà attendere l'esame preliminare e la formulazione del preventivo da parte di ACCREDIA; una volta accettata l'offerta di ACCREDIA, l'Ente procederà all'esame documentale, che potrà comportare la richiesta di documenti integrativi. In caso di esito positivo di tale esame si procederà alla pianificazione della verifica ispettiva in sede ed alla verifica in accompagnamento presso i luoghi ove vengono svolte le verifiche degli impianti secondo il DPR 462/2001.

I tempi previsti da Accredia per effettuare la verifica ispettiva sono di circa 3 mesi dal ricevimento della domanda. Vista la numerosità degli Organismi che dovranno richiedere l'accreditamento entro giugno 2018, però, si può supporre che tali tempi si allunghino; comunque ogni singolo Organismo deve cercare di completare positivamente l'audit di ACCREDIA e la successiva delibera del Comitato di Accreditamento entro la scadenza della propria abilitazione, dopodiché potrà formulare al MISE la richiesta di rinnovo (o estensione) dell'accreditamento, che verrà naturalmente accolta solo in presenza di accreditamento ISO 17020.

Si vedano i precednti articoli su:

- accreditamento ISO 17020 degli organismi di ispezione abilitati secondo il DPR 462/2001 e
- la norma UNI CEI EN ISO/IEC 17020:2012

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.

Il GDPR per la privacy nella sanità privata

Mancano ormai solo 8 mesi all'attuazione del nuovo Regolamento UE 679/2016 sulla Protezione dei Dati Personali (o *General Data Protection Rule*, GDPR), pubblicato nel maggio 2016, che diverrà pienamente attuativo il 25 maggio 2018. Esso apporta importanti novità alla Legge sulla Privacy italiana attualmente in vigore, il D. Lgs 196/2003 e s.m.i., ed impone un diverso modo per affrontare la privacy nelle organizzazioni che trattano dati sanitari, i quali costituiscono una particolare categoria di "dati sensibili" (ora definiti "dati particolari" dal GDPR).

In questo articolo ci occuperemo delle regole per la privacy dei dati sanitari secondo il GDPR, ma non di ciò che attiene alla Sanità Pubblica, quali Ospedali, ASL, ambulatori pubblici, ecc., i quali dovranno sottostare alle medesime regole, ma con adempimenti leggermente diversi (ad es. la figura del DPO o *Data Protection Officer* è obbligatoria sempre) e con l'identificazione del titolare del trattamento che investe un'entità della Pubblica Amministrazione. Da un certo punto di vista lo Stato ha mezzi adeguati per affrontare, speriamo nel modo corretto, l'adeguamento al GDPR.

Invece, per quanto riguarda la Sanità Privata, le cose sono un po' diverse ed a volte l'organizzazione interna non contempla competenze e tecnologie adeguate per far fronte al nuovo Regolamento 679/2016. Parliamo di organizzazioni di piccole e medie dimensioni, che vanno dalle Farmacie ai Poliambulatori di analisi diagnostiche, alle Cliniche e Case di Cura Private.

Alcuni adempimenti nelle organizzazioni private che si occupano di servizi sanitari sono da interpretare, in quanto la norma europea non fornisce indicazioni così precise su alcuni aspetti, ma pone l'accento sulla "responsabilizzazione" del titolare del trattamento, ovvero sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento, cioè misure tecniche ed organizzative adeguate.

Ci troviamo così di fronte ad un problema di competenze: il titolare del trattamento di queste organizzazioni della Sanità Privata è la società stessa che gestisce la struttura (a volte il singolo professionista), quindi tutte le responsabilità

ricadono, di fatto, sul legale rappresentante della stessa, il quale normalmente si occupa di tutt'altro (medico, farmacista o manager amministrativo) e non sa quali misure adottare per tutelarsi, non solo dalle possibili sanzioni (fino al 4% del fatturato annuo), ma anche da eventuali richieste di risarcimento danni di pazienti che non sentissero adeguatamente tutelata la propria privacy.

Gli elementi da considerare nella gestione della privacy in una organizzazione sanitaria privata sono diversi: la gestione dei documenti su supporto cartaceo o analogo (es. lastre di esami diagnostici), la gestione dei documenti su supporto digitale, la gestione delle informazioni elaborate dai sistemi informatici, la gestione delle informazioni trasmesse verbalmente…

Coloro che hanno gestito la privacy in passato con l'aiuto di un avvocato – che gli ha preparato lettere di nomina incaricati, informative e consensi – e di una società di consulenza informatica – che gli ha gestito la sicurezza dei dati (antivirus, backup, ecc.) – dovranno modificare il proprio approccio in quanto la nuova privacy del GDPR richiede un approccio più sistemico ed orientato alla valutazione dei rischi.

I principi introdotti dal GDPR – in particolare il principio di liceità del trattamento, di integrità e di riservatezza, di limitazione delle finalità… – devono essere recepiti interpretandoli nel modo corretto, declinandoli nella propria realtà; non esistono più regole ben definite (password di almeno 8 caratteri, antivirus aggiornati con una certa frequenza, ecc.).

I passi fondamentali che un'organizzazione sanitaria privata dovrebbe affrontare per adeguarsi al GDPR sono i seguenti:

- Analisi dei processi dell'organizzazione;
- Mappatura dei trattamenti di dati personali;
- Identificazione di ruoli e responsabilità per il trattamento;
- Predisposizione del Registro dei trattamenti di dati personali;
- Valutazione dei rischi sui trattamenti di dati;
- Valutazione di impatto per quei trattamenti che lo richiedono;
- Definizione delle misure organizzative per la protezione dei dati personali;
- Definizione delle misure tecniche per la protezione dei dati personali;
- Predisposizione delle procedure per il trattamento dei dati e loro documentazione.

In questo percorso si incontrano alcuni elementi particolarmente significativi, la cui gestione richiede molta attenzione ed una corretta interpretazione del Regolamento 679/2016:

- La formulazione dell'**informativa** e dei **consensi** al trattamento da parte degli interessati;
- La progettazione, implementazione e gestione della **sicurezza delle informazioni**

(non solo informatica);
- Gestione degli **applicativi informatici** e dei rapporti con i relativi fornitori;
- Rapporti con i **responsabili del trattamento esterni**;
- Eventuale **nomina del DPO** o RPD (Responsabile del Trattamento dei Dati);
- Modalità di effettuazione della **valutazione dei rischi** e necessità del c.d. *Data Impact Assessment* (DIA).

Vediamo di chiarire un paio di punti relativamente alle organizzazioni sanitarie private.

La nomina del DPO (RPD) è obbligatoria:

1. se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
2. se le attività principali del titolare o del responsabile consistono in **trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala**;
3. se le attività principali del titolare o del responsabile consistono nel **trattamento su larga scala di categorie particolari di dati** o di dati personali relativi a condanne penali e reati.

Se è evidente che non siamo nel caso (a), probabilmente nemmeno nel caso (b), occorre riflettere bene sul caso (c).

I dati sanitari ricadono senz'altro nelle particolari categorie di dati definite dal GDPR e resta solo da capire cosa significa "su larga scala". Le interpretazioni ufficiali (Regolamento e Linea Guida sui RPD del GdL Articolo 29) ci indicano che i pazienti trattati da un singolo medico di famiglia non rientrano nel concetto di "larga scala". Analogamente si potrebbe pensare per una Farmacia o un piccolo ambulatorio privato, ma salendo di dimensione nelle organizzazioni è evidente che questa condizione trova applicazione.

Altra questione è quella relativa alla necessità di istituire un **Registro dei Trattamenti**: qui l'obbligo si ha per organizzazioni con più di 250 addetti oppure in presenza di rischio per diritti e libertà degli interessati per trattamenti non occasionali di dati sensibili o giudiziari. In questo caso le nostre organizzazioni della sanità privata ricadono quasi tutte nell'obbligo di trattamento, fermo restando che è comunque opportuno, per il principio di responsabilizzazione (*accountability*) del titolare del trattamento, creare e gestire tale Registro.

Esiste, infine, la possibilità, per i titolari del trattamento che vorranno garantirsi maggiormente dai rischi inerenti la privacy, di ottenere la certificazione del proprio processo di gestione di dati sanitari (per ora solo lo Schema di Certificazione ISDP©10003:2015 di INVEO, accreditato da ACCREDIA).

Il valore del vero audit interno

La nuova norma ISO 9001:2015 ripropone al punto 9.2, praticamente senza modifiche significative rispetto alla precedente edizione della norma, il requisito relativo all'Audit interno. La ISO 9001:2015 probabilmente pone maggiore enfasi sulla necessità di intraprendere tempestivamente le azioni finalizzate al trattamento dei rilievi (correzioni, azioni correttive o quant'altro) e certamente recepisce l'approccio basato sui rischi (*Risk Based Thinking*), per il quale la pianificazione e la conduzione degli audit interni dovrà riflettere la necessità di monitorare più frequentemente e più approfonditamente i processi maggiormente a rischio per il perseguimento degli obiettivi aziendali. Però in questo articolo l'aspetto che vorrei sottolineare è un altro: qual è il valore aggiunto di un "vero" audit interno?

La domanda, forse un po' provocatoria, vuole evidenziare il fatto che gli audit interni "finti" servono a poco, se non a coprire il punto della norma in occasione degli audit dell'ente di certificazione e nulla più.

Ormai lo hanno capito anche gli auditor degli Organismi di Certificazione: numerose aziende – che vivono male il loro sistema qualità – poco prima della visita di sorveglianza o rinnovo della certificazione si ritrovano ad adempiere a questo requisito di norma e per varie ragioni (risparmiare tempo e costi, incompetenza, indisponibilità del personale da auditare, urgenza di sbrigare la pratica…) preferiscono registrare audit interni fasulli – ovvero non svolti realmente – piuttosto che effettuare una vera verifica sulla corretta attuazione dei processi aziendali.

Tale pratica, molto diffusa anche da parte di consulenti compiacenti, spesso non sfugge ad un attento auditor dell'Organismo di Certificazione, che però non può o non vuole infierire sull'azienda, spesso anche per mancanza di evidenze oggettive che possano comprovare la falsità dei rapporti di audit.

In realtà predisporre un rapporto di audit interno fittizio, magari con tanto di check-list compilate, è tempo perso, anche se molti responsabili qualità credono di aver risparmiato tempo (e rogne) rispetto a condurre un vero audit.

Il vero audit, infatti, permette di capire cosa effettivamente viene svolto secondo le regole (procedure, specifiche del cliente, norme, ecc.) e cosa no, se i processi sono condotti in modo efficace e, soprattutto, efficiente, se il personale opera secondo i compiti assegnati e così via.

Certamente non svolgere gli audit e far risultare che tutto va bene talvolta permette al responsabile qualità o altro auditor incaricato, di evitare conflitti interni con i responsabili dei vari reparti(che così potranno continuare a fare quello che pare a loro) o con soggetti troppo permalosi se qualcuno osa sindacare il loro operato. Ma tutto ciò giova realmente all'azienda?

La Direzione, o meglio l'alta Direzione della norma ISO 9001, preferisce vedere dei rapporti di audit fasulli che sono dei "percorsi netti" pur di liberarsi di torno questo adempimento oppure preferisce sapere quali sono i reali problemi dell'azienda?

Un audit ben fatto, condotto da personale competente e imparziale (ovvero non solo indipendente dai responsabili dei processi verificati, ma anche in grado di giudicare in modo imparziale quello che rileva, senza farsi condizionare da chi ha di fronte) porta del grande valore aggiunto all'azienda, perché permette di capire quali sono i problemi attuali dell'organizzazione e quali potrebbero essere quelli futuri; ad esempio rilevare, durante un audit, che non viene controllato il prodotto acquistato, non registrandone nemmeno le informazioni che ne garantiscono la rintracciabilità, potrebbe portare guai all'azienda in caso di richiesta di risarcimento danni da parte del cliente per prodotto difettoso provocato dal prodotto/servizio acquistato presso il fornitore, impedendo anche di potersi rivalere sul fornitore che ha causato la non conformità. Il vero audit, dunque, tutela l'azienda e permette di fronteggiare possibili rischi di vario genere e natura.

Un audit reale può fornire anche molti spunti di miglioramento, se non altro per il fatto di esaminare i processi insieme al personale operativo che avrebbe l'opportunità di evidenziare possibili migliorie.

Un vero audit permette di rilevare delle anomalie, dei problemi, che poi dovranno essere risolti, affrontandoli in tempi ragionevoli. L'audit finto non rileva i problemi, ma questo non vuol dire che non ci sono!

Un vero audit ha bisogno di molto più tempo da parte dell'auditor e del personale intervistato, ma fornisce valore aggiunto, il finto audit non serve all'azienda, ma solo ad evitare rilievi in fase di verifica di certificazione/sorveglianza o rinnovo.

Spesso il finto audit è figlio di procedure finte: che cosa faccio a fare gli audit se dovrei verificare la conformità a procedure che non segue nessuno perché non rappresentano la realtà aziendale? A volte questo è un altro problema: il sistema di gestione per la qualità non è aderente alla realtà aziendale, dunque così com'è non serve a nulla.

Il vero audit va anche ad investigare sull'efficienza dei processi e sui relativi indicatori. Questi ultimi spesso sono deficitari (carenti o addirittura fasulli) per

monitorare i processi e dovrebbero essere messi in discussione dal bravo auditor. Ma anche quello degli indicatori poco pertinenti, imprecisi e non sistematicamente misurati è un altro problema di molti sistemi qualità.

Tutto questo, però, deve essere capito dalla Direzione, da chi governa l'azienda, dalla proprietà e forse alcuni non lo capiranno mai, ma se tutti coloro che lavorano in questo ambito operassero con l'obiettivo di far risaltare i vantaggi di possedere un vero sistema qualità, forse alcune aziende si farebbero un esame di coscienza e ripenserebbero al loro sistema qualità sotto un'ottica differente. Anche questo sarebbe un valore aggiunto di un vero audit interno.

Le regole applicative della UNI EN ISO 9001:2015

L'adeguamento delle aziende alla norma UNI EN ISO 9001:2015 prosegue a rilento con il solito approccio italiano "qual è la scadenza? Settembre 2018? Bene, cominciamo a pensarci a Giugno 2018 perché poi ci sono le ferie!"

Forse senza sapere che ben difficilmente si riuscirà a migrare in tempo utile, senza perdere la certificazione almeno per qualche mese; se non altro perché gli Organismi di Certificazione non avranno modo di gestire un'elevata mole di adeguamenti negli ultimi mesi del periodo di transizione. Oltre al fatto che se l'adeguamento non viene effettuato in occasione di un rinnovo o di una sorveglianza si spenderà di più.

Ma quali sono i **requisiti aggiuntivi per le aziende italiane** che vogliono recepire questa normativa? Sia in fase di transizione dalla vecchia norma ISO 9001:2008, sia come nuova certificazione di qualità?

Quali sono i contenuti dell'**Appendice C della UNI EN ISO 9001:2015 (versione italiana)** che dovrebbero aiutare le imprese del nostro Paese a recepire nel modo corretto questa norma?

Visto il tenore della nuova norma, infatti, noi italiani abbiamo bisogno di **regole più chiare**, espresse in termini di **obblighi e doveri** ("l'organizzazione DEVE"), senza troppe frasi del tipo "se ritenuto necessario", "quando necessario", "conservare informazioni documentate affinché si possa avere fiducia del fatto che…", "le informazioni documentate che l'organizzazione determina necessarie per…" e così via.

Vediamo sinteticamente quali sono queste regole applicative che dovrebbero agevolare anche il compito dell'auditor dell'Organismo di Certificazione, evitando inutili discussioni su cosa richiede la norma e cosa dovrebbe effettivamente essere presente per dimostrare la conformità del sistema di gestione per la qualità.

1. Se l'organizzazione migra dalla versione 2008 della ISO 9001 avrà un **Manuale Qualità** ed anche se esso non è espressamente richiesto dalla ISO 9001:2015 farà meglio a tenerselo. Naturalmente revisionandolo e rendendolo più snello, evitando inutili ridondanze con le procedure. Perché comunque il Manuale rappresenta il vertice della c.d. "piramide della documentazione", il documento di maggior sintesi che richiama documenti più di dettaglio (è un po' come il "*main program*" che richiama le varie "*subroutine*" dei programmi software). Del resto eliminando il Manuale, comunque dovremo documentare la Politica, i Processi ed altro…. dove li mettiamo se non nel manuale? Le aziende che pensano in futuro di certificarsi secondo la normativa del settore automotive IATF 16949:2016 considerino che tale standard richiede il manuale qualità.
2. Le **procedure** chi ce le ha se le tenga e chi è di nuova certificazione ci pensi bene a non predisporle. L'evoluzione dell'organizzazione aziendale negli ultimi 20-30 anni è andata sempre verso la definizione in forma documentata delle modalità di svolgimento delle attività, per definire regole precise che devono essere seguite da tutti, per evitare il caos ove ciascuno fa quello che gli pare. Se non ci sono procedure e istruzioni documentate nelle aziende italiane non solo si tende ad interpretare i processi in modo "personalizzato", secondo quello che il singolo ritiene meglio, ma i nuovi nell'incarico non hanno modo di imparare a ricoprire il ruolo perché l'addestramento è sempre scarso e non trovano regole scritte precise su cosa fare e cosa non fare. Ovviamente ci sono casi e casi: in determinate situazioni l'operatività è guidata dai sistemi informativi e, pertanto, non è facile portare a termine attività in modo diverso, per cui dettagliare troppo non serve.
3. L'**analisi del contesto dell'organizzazione** e la **valutazione dei rischi** sono da documentare. Infatti se suddette attività devono essere riesaminate periodicamente (ad esempio in occasione del riesame di direzione) come facciamo a ricordarci quello che abbiamo detto sull'argomento un anno o sei mesi fa se non scriviamo nulla? Quale imprenditore o Direttore Generale riesce ad analizzare il contesto interno ed esterno della propria organizzazione, identificare e valutare i rischi oralmente nello stesso modo a distanza di tempo, senza nemmeno tenersi una traccia scritta? Dal momento che poi le azioni pianificate per affrontare rischi ed opportunità devono essere documentate con tanto di responsabilità, tempi e valutazione dell'efficacia che senso ha

documentare le azioni, ma non i rischi che le hanno scaturite?

4. La norma ISO 9001:2015 non richiede più il **Rappresentante della Direzione**, che in molte realtà coincideva con la figura del Responsabile Qualità (ce se diverso dal rappresentante della Direzione non era richiesto neanche prima): non ha nessun senso eliminare il Responsabile Qualità. Alcuni imprenditori che non hanno ben compreso la questione hanno cominciato a dire: "ma allora possiamo eliminare il responsabile qualità, con quello che costa!". In un mondo perfetto nel quale la Qualità è patrimonio di tutti e tutti applicano la norma in modo adeguato il Responsabile Qualità potrebbe effettivamente non servire, ma nelle nostre aziende italiane chi fa e fa fare le cose che servono per mantenere la certificazione senza il Responsabile Qualità? Oggi in molte realtà il Responsabile Qualità non solo svolge più attività di quelle di sua stretta pertinenza, ma costringe gli altri (responsabili di funzione, Direzione ed altri) a fare il loro dovere. Bisognerebbe alzargli lo stipendio, altro che eliminare la figura!
5. La norma prevede che sia l'organizzazione a determinare "cosa è necessario monitorare e misurare", come e quando farlo per ottenere risultati validi. Ora più di prima è necessario identificare **indicatori** pertinenti con gli obiettivi ed in grado di misurare l'efficacia – se non anche l'efficienza – dei processi. Le aziende non pensino che questa libertà possa permettere loro di decidere gli indicatori a loro convenienza: l'aumento di fatturato per il processo commerciale e il numero assoluto delle non conformità per la produzione non sono indicatori sufficienti a misurare suddetti processi e gli obiettivi di nessuna azienda.
6. La norma non prevede più le **azioni preventive**, ma le azioni finalizzate a migliorare l'efficacia e l'efficienza del Sistema e dei suoi processi sono state rinforzate. Le azioni preventive, ovvero quelle azioni finalizzate ad evitare il verificarsi di non conformità potenziali, sono solo un "di cui" delle azioni di miglioramento: chiamiamole così, non solo AP.

In conclusione la norma ISO 9001:2015 deve essere vista con lo spirito giusto dalle aziende italiane, dimenticandosi di quello che è stato fatto in passato, per evitare di buttare via tempo e denaro per un adeguamento forzoso che non porterebbe alcun vantaggio nel tempo all'impresa. Sarà compito anche degli auditor degli Organismi di Certificazione cercare di far capire alle aziende il reale significato di questa norma, ma bisognerà vedere se avranno tempo e voglia per farlo, soprattutto se osteggiati da rappresentanti dell'azienda e consulenti che affermeranno che la norma non richiede un manuale, non richiede delle procedure e non è prescrittiva per tante altre attività. Il rischio, in tal caso, è che l'auditor alzi bandiera bianca e dica "fate un po' quello che volete… se non avete capito voi a cosa servono certe cose…".

A proposito l'Appendice C della UNI ISO 9001:2015 italiana non esiste, ma è meglio far finta che le regola sopra esposte esistano veramente.

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 (500 download) (compreso l'allegato con le FAQ)
- Linee Guida Valutazione-Impatto WP 248 (294 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?

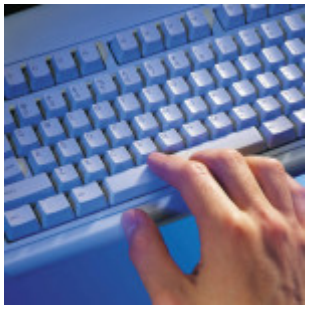
La probabilità di essere sanzionati a seguito di ispezioni del Nucleo Privacy della GdF è estremamente bassa, un po' più alta per organizzazioni che trattano dati particolarmente critici (la valutazione è fatta in base al numero delle ispezioni avvenute negli ultimi anni).

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.

Finanziamenti in innovazione per il miglioramento degli studi professionali



Il bando della Regione Emilia Romagna denominato "Progetti Ict per professionisti" (titolo completo "BANDO PER IL SOSTEGNO DI PROGETTI RIVOLTI ALL'INNOVAZIONE, LA DIGITALIZZAZIONE E L'INFORMATIZZAZIONE DELLE ATTIVITA' PROFESSIONALI A SUPPORTO DEL SISTEMA ECONOMICO REGIONALE") rappresenta un'ottima **opportunità di miglioramento dell'efficienza** interna per liberi professionisti, studi professionali, società di ingegneria e società fra professionisti (STP). Esso è finalizzato al **supporto di soluzioni ICT per le attività delle libere professioni** e l'implementazione di servizi e di soluzioni avanzate in grado di incidere significativamente sull'organizzazione interna, sull'applicazione delle conoscenze, sulla **gestione degli studi** e sulla **sicurezza informatica**.

I progetti finanziabili dovranno favorire lo **sviluppo dell'attività professionale**, **incentivare gli investimenti in nuove tecnologie**, **diffondere la cultura d'impresa**, **dell'organizzazione e della gestione/valutazione economica** dell'attività professionale.

Gli investimenti ammessi a contributo dovranno essere di almeno € 15.000, verranno finanziati a fondo perduto per il 40% del loro valore fino ad un massimo di € 25.000 erogati.

I termini per la presentazione sono racchiusi in due finestre temporali: maggio 2017 e 12 settembre – 10 ottobre 2017. Le spese dovranno avvenire entro il 31/12/2017.

Alcuni esempi, non certo esaustivi, di progetti che potranno essere finanziabili dal bando sono i seguenti:

- Acquisto di **software di gestione dello studio** che migliori l'efficienza dei processi organizzativi;
- Implementazione di sistemi di archiviazione digitale di documenti (**gestione documentale** compresa archiviazione sostitutiva o "a norma");
- Implementazione di sistemi di **sicurezza informatica**, compresi i loro test di adeguatezza, ad esempio per adeguarsi alle nuove misure di sicurezza richieste dal Regolamento UE 679/2016 sulla Protezione dei Dati Personali;
- Sviluppo di sistemi di collaborazione fra professionisti, anche attraverso l'impiego del *cloud*;
- Sviluppo di sistemi per migliorare la vendita on-line dei servizi (**sito internet**) e sistemi di supporto alla clientela (**CRM**);
- Implementazione di sistemi di **controllo di gestione**;
- Implementazione di **sistemi di gestione** aziendale (ISO 9001).

In questo ambito sarà ammesso a finanziamento l'acquisto di attrezzature, hardware, licenze software, servizi di supporto informatico, brevetti, accessori di carattere edilizio, consulenze specialistiche.

Questo bando potrebbe davvero aiutare molte piccole organizzazioni professionali (studi di ingegneria ed architettura, studi di commercialisti, avvocati, notai, studi medici, ecc.) a diventare più efficienti attraverso l'utilizzo di nuove tecnologie, soprattutto in realtà dove l'inefficienza è generata dalla scarsa conoscenza delle tecnologie informatiche.

Da ultimo le graduatorie per determinare l'ammissibilità del progetto premieranno i progetti più in linea con i criteri del bando e quelli maggiormente innovativi.

A questo link è possibile reperire maggiori informazioni.

Opportunità per le imprese con il Piano Industria 4.0

In questi mesi si sente parlare molto delle agevolazioni fiscali per le imprese relative al Piano Industry 4.0, promosso già dal Governo Renzi in autunno 2016. Cerchiamo, in questo articolo, di capire meglio quali sono le reali opportunità per le imprese ed i vincoli che la Legge pone per usufruire degli incentivi, anche per capire in quali situazioni conviene realmente investire in questa direzione, al fine di non trovarsi brutte sorprese ad investimenti effettuati.

Il focus del Piano Industria 4.0 è il **settore manifatturiero**, esso punta alla **digitalizzazione** delle imprese produttrici, anche se non sono completamente escluse le aziende di servizi. Il fine del Governo è quello di **incrementare gli investimenti nelle imprese**, che al momento latitano e vedono il nostro Paese indietro rispetto al resto d'Europa. La carenza di investimenti è molto probabilmente la principale causa della crescita bassa (in termini di "zero virgola"…) dell'Industria del nostro Paese, soprattutto se paragonata agli altri Paesi industrializzati dell'Europa.

Perché Industria 4.0? La prima rivoluzione industriale è avvenuta alla fine del 18° secolo con l'introduzione di potenza vapore per il funzionamento degli stabilimenti produttivi, la seconda rivoluzione industriale si colloca all'inizio del 20° secolo con l'introduzione dell'elettricità, dei prodotti chimici e del petrolio; la terza rivoluzione industriale è iniziata all'inizio degli anni '70 con l'utilizzo dell'elettronica e dell'IT per automatizzare ulteriormente la produzione (robot industriali e computer). Ora, invece, nella quarta rivoluzione industriale, il concetto fondamentale è la **connessione con un sistema di raccolta e gestione dei dati**, collegamento a internet, IoT o Internet delle Cose (utilizzo di macchine intelligenti, interconnesse e collegate ad internet) ed altro ancora.

L'elemento caratterizzante del piano di incentivazione, dunque, è la connessione, fra diversi dispositivi (macchina-elaboratore, macchina-macchina, macchina-internet, macchina-dispositivo mobile, ecc.).

Le **tecnologie coinvolte** nel piano Industry 4.0 sono le seguenti:

1. *Advanced Manufacturing Solutions* (Robot collaborativi interconnessi e rapidamente programmabili).
2. *Additive manufacturing* (Stampanti in 3D connesse a software di sviluppo

digitali).
3. *Augmented Reality* (Realtà aumentata a supporto dei processi produttivi).
4. *Simulation* (Simulazione tra macchine interconnesse per ottimizzare i processi).
5. *Horizontal/Vertical Integration* (Integrazione informazioni lungo la catena del valore dal fornitore al consumatore).
6. *Industrial Internet* (Comunicazione multidirezionale tra processi produttivi e prodotti)
7. *Cloud* (Gestione di elevate quantità di dati su sistemi aperti).
8. *Cyber- security* (Sicurezza durante le operazioni in rete e su sistemi aperti).
9. *Big Data and Analytics* (Analisi di un'ampia base dati per ottimizzare prodotti e processi produttivi).

Evidentemente l'elenco è disomogeneo, ma in ogni caso indica alle imprese quali sono le tecnologie abilitanti per usufruire delle agevolazioni.

Fra le voci più significative vi è l'integrazione orizzontale e verticale.

L'**integrazione verticale** va dall'acquisizione di dati a livello produttivo, attraverso sensori, all'elaborazione dati tramite software gestionali: è l'integrazione che parte dal MES (*Manufacturing Execution System*) al sistema di Controllo di Gestione.

Sono diverse le soluzioni di **integrazione orizzontale**, ad esempio possono passare attraverso la connessione con il fornitore per migliorare la *supply chain* comprendendo soluzioni per la collaborazione, il *planning*, l'*order management*, il *tracking* per la logistica, il *data analytics* e molto altro ancora.

Nel piano Industria 4.0 le **principali incognite** per le imprese possono essere così riepilogate:

- il rapporto costi/benefici dell'intervento;
- la mancanza di competenze digitali interne;
- la portata degli investimenti, che comunque rappresentano un costo che, ricordiamolo, viene finanziato solo se l'impresa è in utile;
- la carenza di standard digitali;
- l'incertezza sulla sicurezza dei dati (ad esempio nel caso della connessione attraverso *Internet of Things* e il *Cloud Computing*).

Su quest'ultimo punto il Piano Industria 4.0 ha pensato di introdurre il capitolo della Sicurezza delle Informazioni, anche relativamente ai dati gestiti in ambito IoT.

Per capire meglio il significato e la portata di tali incognite occorre precisare che – per chi ancora non lo sapesse – le agevolazioni sono costituite dall'**iper-ammortamento** (250% del valore del bene) e dal **super-ammortamento** (140% del valore del bene), che si applicano, nel primo caso, ai beni materiali acquistati, nel secondo anche ai beni immateriali.

L'elenco dei beni materiali e immateriali a cui è applicabile il super e iper ammortamento è stato ufficialmente pubblicato dal Ministero dello Sviluppo Economico (MISE) ed è scaricabile in allegato al presente articolo insieme alle **linee guida del MISE** stesso per l'applicazione delle agevolazioni.

Occorre precisare che per rientrare nel Piano Industria 4.0 ed usufruire degli incentivi occorre **acquisire almeno un bene materiale rientrante nell'elenco**, ovvero acquisire strumentazione atta a trasformare un'apparecchiatura/macchina preesistente in un "bene Industria 4.0" (caso del *revamping* di macchinari). In altre parole per poter usufruire del super ammortamento per l'acquisto di un bene immateriale, ad esempio un software, rientrante nelle categorie previste dalla Legge, occorre che **il soggetto beneficiario del finanziamento acquisti anche un bene materiale**; non è richiesto il collegamento fra bene materiale e beni immateriali acquistati per usufruire dell'agevolazione! Ad esempio, al limite un'impresa potrebbe acquistare un sistema di sensori per acquisire dati da una macchina produttiva (ad esempio temperature da un forno) ed applicare il super ammortamento all'acquisto di un sistema MES o *big data analytics* che non trattano i dati rilevati dalla macchina 4.0.

Tra i vincoli per poter usufruire dell'agevolazione vi è che l'investimento deve avvenire entro il 31/12/2017, con almeno un ordine ed un anticipo del 20% pagato entro il 31/12/2017 e con consegna del bene entro 30/06/2018. La **perizia giurata** di un ingegnere iscritto all'Albo o di un perito industriale è necessaria per investimenti superiori a 500.000 € per il singolo bene, negli altri casi è sufficiente una autodichiarazione del Legale Rappresentante dell'impresa.

È evidente che il fattore tempo gioca un ruolo fondamentale nella decisione ed effettuazione di investimenti che, soprattutto nel caso di PMI, normalmente richiedono una valutazione abbastanza lunga ed incerta. Visto poi che la Legge non è di chiarissima interpretazione (si attende in questo mese una Circolare interpretativa dell'Agenzia delle Entrate su molti aspetti ambigui), alcune imprese rischiano di effettuare investimenti che poi non risulteranno ammissibili, magari trascinati dalle indicazioni di venditori di macchine e apparecchiature. Al proposito va ricordato che l'autodichiarazione del Legale Rappresentante ha risvolti penali in caso di non ammissibilità del bene; dunque esiste la concreta possibilità che molte aziende **richiedano comunque la perizia giurata di un ingegnere abilitato** per garantire il vertice aziendale contro brutte sorprese (costo non iper-ammortizzabile e dichiarazione mendace). Buona prassi sarebbe rivolgersi, prima di effettuare l'investimento, ad un consulente che possa indirizzare l'azienda ed il management non competente nelle tecnologie da acquisire e verso investimenti che,

non solo siano ammissibili agli incentivi Industria 4.0, ma che **risultino realmente utili per l'azienda** nel medio-lungo periodo.

Fra i principali fattori inibitori nell'adottare le tecnologie incluse nel piano Industria 4.0 vi è sicuramente la scarsa cultura digitale delle PMI italiane e una mancanza di *leadership digitale* del management della PMI stessa.

Tra i processi che potrebbero trarre maggior vantaggio dall'implementazione di misure Industry 4.0 spiccano sicuramente le tematiche di **pianificazione, schedulazione e controllo avanzamento della produzione** e lo **sviluppo del prodotto/industrializzazione**.

Il Piano Industria 4.0 è un percorso di trasformazione, non solo tecnologico, ma anche organizzativo e gestionale. Il fine dell'impresa deve essere l'incremento del valore per il cliente, anche attraverso il miglioramento dell'efficienza aziendale, la fornitura di soluzioni innovative, la proposta di servizi innovativi e migliorativi rispetto allo standard.

Per iniziare un progetto di Industria 4.0 è importante effettuare una valutazione iniziale finalizzata all'obiettivo Industry 4.0 per capire **di cosa l'azienda realmente bisogno**, quali sono gli elementi di possibile **miglioramento** e le **opportunità** da poter cogliere, ma anche dei rischi connessi agli investimenti.

Si ribadisce che i benefici per beni materiali e immateriali devono essere connessi attraverso il soggetto beneficiario, non direttamente fra gli *asset* fisici e immateriali, ma chiaramente un piano Industry 4.0 coerente dovrà prendere in considerazione l'interconnessione fra gli uni e gli altri, solo così facendo si otterrà il massimo nel miglioramento dell'efficienza dei processi aziendali.

Si ricorda che il software deve essere incluso nell'allegato B per poter rientrare nell'incentivo, mentre per i software c.d. "*embedded*" prevale il riferimento al bene iper-ammortizzabile nel quale è contenuto. Tale bene deve appartenere ai beni dell'allegato A alla Legge.

Infine non è ancora chiaro quali costi accessori (consulenza finalizzata all'utilizzo del bene) siano iper e super ammortizzabili, al proposito si attende la Circolare di chiarimento dell'Agenzia delle Entrate.

Linea Guida MISE Industria 4.0 (112 download)

Beni ammissibili Piano Industria 4.0 (107 download)

Articolo 1 commi da 8 a 13 della legge 11 dicembre 2016 n 232 - Proroga con modificazioni della disciplina del c.d. super ammortamento e introduzione del c.d. iper ammortamento (93 download)