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

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 (326 download) (compreso l'allegato con le FAQ)
- Linee Guida Valutazione-Impatto WP 248 (270 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.

L’accreditamento ISO 17020 per gli organismi abilitati secondo il DPR 462/2001

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”) si troveranno presto ad affrontare **l’accreditamento UNI CEI EN ISO/IEC 17020:2012** (“Valutazione della conformità – Requisiti per il funzionamento di vari tipi di organismi che eseguono ispezioni”) reso obbligatorio dal Ministero dello Sviluppo economico.

Sono coinvolte oltre 230 organizzazioni collocate prevalentemente al Nord Italia (oltre la metà degli organismi) con un fatturato che – per la maggior parte di essi (oltre il 60%) – si posiziona al di sotto dei 500.000 euro.

Le attività svolte da tali organismi sono strettamente correlate alla **Sicurezza ed Igiene sul Lavoro delle aziende** che devono eseguire le **verifiche di messa a terra degli impianti elettrici** (ogni 5 anni o con frequenza biennale in determinate situazioni) servendosi dei verificatori di organismi abilitati secondo il DPR 462/2001.

L’obbligo di accreditamento ISO 17020 comporterà sicuramente un aggravio dei costi fissi per gli organismi che vorranno rimanere su un mercato che ha visto negli ultimi anni una forte concorrenza sui prezzi. Come per altri servizi obbligatori per legge, le Imprese spesso scelgono di rivolgersi a coloro i quali offrono il prezzo più basso, pur soddisfando i criteri minimi previsti dalla Legge. Tale sistema, ormai in uso in molte realtà, è sicuramente deleterio per il settore, spingendo gli organismi ad una lotta al ribasso dei prezzi, talvolta trascurando l’efficacia dei controlli e delle verifiche svolte.

Da questo punto di vista l’obbligo di accreditamento ACCREDIA è sicuramente un elemento positivo nell’accrescere l’affidabilità di tali servizi, strettamente correlati alla sicurezza delle persone che lavorano in azienda. Infatti le verifiche ACCREDIA, seppur onerose, potranno garantire un’applicazione più omogenea di metodi e procedure tecniche di verifica da parte degli organismi, a tutto vantaggio del mercato e della tutela della sicurezza delle aziende.

Indubbiamente l'adozione di un sistema di gestione conforme alla norma UNI CEI EN ISO/IEC 17020:2012 (si veda articolo sulla normaISO 17020) potrà risultare particolarmente impegnativo per piccole organizzazioni che non conoscono tale schema, soprattutto per quelle che non dispongono nemmeno di un **sistema di gestione per la qualità certificato ISO 9001**. Il sistema qualità, infatti, costituisce un "di cui" del sistema ISO 17020 da implementare.

Fanno eccezione Organismi di Ispezione di grandi dimensioni (TUV Italia, RINA, ecc.) che dispongono già della struttura organizzativa, delle competenze e dell'assetto documentale per affrontare questo nuovo accreditamento senza particolari scossono.

Gli Organismi più piccoli dovranno, quindi, accorparsi a formare Organismi più grandi e strutturati oppure accreditarsi per conto proprio.

Per ottenere l'accreditamento ISO 17020 gli organismi già certificati ISO 9001 dovranno integrare il loro sistema qualità per rispondere ai requisiti della norma ISO 17020 e dei **Regolamenti Accredia** (RG.01.01, RG.01.04) e **Linea Guida EA** (ILAC P10, ILAC P15), magari approfittando – se già non lo hanno fatto – dell'**adeguamento a ISO 9001:2015** della norma sulla qualità, per revisionare il sistema.

Per gli altri il lavoro sarà più lungo ed impegnativo, in quanto occorrerà adeguare il Manuale ed integrare le procedure esistenti.

Gli elementi più critici della ISO 17020 che dovranno essere affrontati dagli organismi abilitati secondo il DPR 462/2001 ritengo possano essere i seguenti:

- Valutazione dei rischi di imparzialità e gestione dell'indipendenza;
- Valutazione, qualifica e monitoraggio ispettori/verificatori;
- Pianificazione (predisposizione del piano di ispezione) e rendicontazione delle attività di verifica (emissione del rapporto di ispezione/verifica);
- Monitoraggio e controllo delle attività di verifica;
- Gestione rapporti contrattuali con i clienti (Regolamento, offerte e contratti);
- Gestione della taratura e controllo degli strumenti di misura;
- Gestione della formazione del personale esterno;
- Valutazione delle prestazioni, riesame di direzione e miglioramento.

Naturalmente occorrerà integrare la documentazione esistente (in misura maggiore se l'organismo non è certificato ISO 9001): manuale qualità, procedure, istruzioni operative, check-list e linee guida per lo svolgimento dell'attività.

Impatti del Regolamento Privacy sullo sviluppo software

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

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

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

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

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

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

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

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

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

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

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

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

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

Oggi molti applicativi, magari obsoleti, non permettono di implementare misure di sicurezza adeguate (password di lunghezza adeguata, password di complessità minima variate periodicamente, password trasmesse via internet con connessioni crittografate, gestione utenti, raccolta di dati minimi indispensabili, gestione dei

consensi, procedure di backup, ecc.) e in futuro il loro impiego diverrà non conforme alla normativa sulla privacy, ovvero non saranno più commercializzabili.

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

Come e quando migrare alla ISO 9001:2015?

Ad oggi sono molte le organizzazioni certificate ISO 9001:2008 che non hanno ancora adeguato il loro sistema di gestione per la qualità alla nuova ISO 9001:2015. Anche se il termine per effettuare il passaggio alla nuova norma è abbastanza lontano (15/09/2018) i tempi per effettuare una migrazione efficace ed efficiente non sono abbondanti per molte imprese, infatti sarebbe opportuno effettuare la migrazione in occasione di un **rinnovo della certificazione** oppure di una **visita di sorveglianza/mantenimento** al fine di contenere i costi di certificazione.

Questo perché in occasione degli audit di rinnovo l'Organismo di Certificazione già deve verificare tutti i processi dell'organizzazione e la documentazione di sistema, dunque i costi aggiuntivi sono minimi, se non addirittura nulli.

Negli audit di sorveglianza richiedere l'adeguamento alla ISO 9001:2015 potrebbe essere un po' più oneroso, ma per quelle organizzazioni che hanno la scadenza del certificato oltre la data limite per l'adeguamento (14 settembre 2018) questa è l'occasione migliore per passare alla nuova norma.

Visto che ormai il 2016 è passato, resta di fatto poco più di un anno e mezzo, ovvero solo una o due visite dell'Organismo di Certificazione – a seconda dei casi – per effettuare il passaggio, che comunque dovrà avvenire durante un audit svolto con

congruo anticipo rispetto alla data limite sopra indicata, per consentire all'Ente di sbrigare tutte le pratiche necessarie per il rinnovo del certificato in ISO 9001:2015.

Le organizzazioni che avranno la visita dell'Organismo di Certificazione nella seconda parte dell'anno avranno solo una occasione per rinnovare il loro certificato secondo queste modalità.

Rimandare eccessivamente può portare a costi aggiuntivi, infatti sarebbe necessario richiedere una visita straordinaria nell'estate 2018 (probabilmente prima della chiusura per ferie di agosto) per rinnovare in tempo il certificato, consci del fatto che lasciare scadere il certificato vorrà dire perdere di fatto la certificazione ISO 9001 e, quindi, dover intraprendere l'iter dal principio per riottenere la certificazione di qualità. In questi casi sicuramente ci sarebbero costi aggiuntivi.

Ma quale sono le ragioni dell'evidente attendismo di molte imprese nell'effettuare il passaggio? Le principali motivazioni possono probabilmente riassumersi nelle seguenti:

- Posticipare i costi di adeguamento (organismo di certificazione, consulenza, impegno interno,…);
- Incertezza sul mantenimento della certificazione oltre la scadenza del certificato;
- Incertezza sul futuro dell'organizzazione;
- Timore sull'impatto dell'adeguamento nell'organizzazione interna.

Sicuramente la prospettiva nel breve termine di molte piccole imprese è sui processi primari essenziali (produzione, commerciale) e viene evitato tutto ciò che porta impegno e costi su altri processi, soprattutto in realtà sottodimensionate in termini di risorse. Evidentemente non è stata adeguatamente compresa la portata di questa norma e del **sistema di gestione per la qualità come reale strumento di gestione**, **di controllo e di miglioramento di tutta l'azienda**. Un po' di paura nell'affrontare un cambiamento normativo non indifferente come quello del 2008 completa il quadro di parecchie organizzazioni.

Le interpretazioni sbagliate sulla nuova norma ISO 9001:2015 non mancano, da quelle eccessivamente "terroristiche" (requisiti molto più difficili da soddisfare) a quelle eccessivamente semplicistiche (si può buttare via il manuale e tutte le procedure ed anche rottamare il responsabile qualità).

Le linee guida UNI-Conforma, la linea guida ISO/TS 9002:2016 da poco pubblicata ed altri documento potrebbero aiutare nella corretta interpretazione dei requisiti.

L'approccio corretto – a mio parere – dovrebbe essere quello di pianificare l'adeguamento per tempo, allocando le risorse necessarie al progetto. Purtroppo

molte organizzazioni chiedono e continueranno a chiedere "*quanto costa passare alla nuova norma*?", "*quanto tempo ci si mette?*". A queste domande non c'è una risposta univoca corretta e rivolgersi al tal consulente piuttosto che ad altri solo perché promette costi e tempi inferiori è un grave errore che molti imprenditori commetteranno.

Costi e **tempi** per l'adeguamento dipendono da svariati fattori:

- Il sistema qualità è stato mantenuto aggiornato alla realtà aziendale oppure è obsoleto, modificato solo a fronte di rilievi dell'organismo di certificazione?
- I processi sono adeguatamente descritti oppure sono delineati in modo minimale e generico?
- Vengono sistematicamente calcolati e monitorati indicatori idonei a misurare le prestazioni dei processi oppure sono gestiti solo pochi indici standard poco aderenti alla realtà aziendale?
- La Direzione vuole semplicemente mantenere il certificato con il minimo sforzo oppure vuole sfruttare questo strumento per tenere sotto controllo l'organizzazione e cercare di migliorare?

Dalle risposte a queste domande si può capire meglio il lavoro che sarà da fare.

Situazioni con organizzazioni vicine alle prime parti delle domande sopra riportate sarebbero difficilmente certificabili secondo la nuova norma ISO 9001:2015, ma probabilmente lo saranno ugualmente ingannando se stesse. Il risparmio di tempi e costi nell'adeguamento potrà essere pagato in futuro mantenendo prassi obsolete e non efficienti, contrarie al vero spirito della norma.

Il tanto vituperato appesantimento della norma sulla certificazione di qualità, soprattutto dal punto di vista documentale, in realtà non esiste, a maggior ragione ora che bisogna "mantenere le informazioni documentate che servono". Il problema che molti detrattori della ISO 9001 non si rendono conto che molte evidenze (informazioni documentate) servono anche a cautelarsi quando qualcosa va storto (gestione dei rischi).

Di fatto molte piccole e medie imprese italiane sono lontane dai principi ispiratori della nuova norma sui sistemi di gestione per la qualità, ma non è detto che per ottenere la certificazione serva essere completamente in linea con essi, il percorso di miglioramento potrebbe essere più lungo, la verifica di passaggio alla ISO 9001:2015 potrebbe evidenziare molti rilievi, ma pian piano le carenze potranno essere eliminate e l'azienda potrà essere condotta su principi di gestione migliori di quelli attuali, secondo standard internazionali riconosciuti.

Operativamente la maggior parte dei sistemi qualità ISO 9001:2008 necessiterà delle seguenti attività:

- **Formazione del personale** sulla norma ISO 9001:2015;
- Identificazione e descrizione del **contesto dell'organizzazione**;
- **Valutazione dei rischi** di business (generali e specifici dei vari processi aziendali), attività che passa attraverso l'identificazione dei rischi, la loro ponderazione e la definizione delle misure da porre in essere per il loro trattamento;
- Revisione della **mappatura dei processi** (il livello di approfondimento dipende dallo stato del sistema qualità esistente);
- Rivalutare l'insieme di indicatori da monitorare (anche in questo caso dipende da cosa esiste attualmente);
- Revisione della **documentazione del sistema qualità** esistente: sicuramente il manuale qualità andrà per lo meno snellito, procedure e istruzioni saranno da aggiornare per riferimenti obsoleti, per recepire le azioni di trattamento dei rischi, per aggiornarle alla realtà aziendale e migliorarle in ottica di efficacia ed efficienza;
- Sottoporre ad **audit interno** il sistema di gestione per la qualità secondo le prassi abituali;
- Effettuare un **riesame della direzione** sul sistema di gestione per la qualità che recepisca i nuovi elementi.

L'eliminazione di documenti di tipo procedurale e il non tener evidenza documentale di talune attività (analisi del contesto, valutazione dei rischi, …) sono false semplificazioni, adatte solo a chi sa recitare senza leggere il copione, ovvero ad organizzazioni che hanno ben chiaro il proprio contesto organizzativo, i propri rischi, le azioni attuate per mitigarli, le procedure aziendali e tutte le prassi da adottare a tutti i livelli dell'organizzazione.

Le attività da completare potrebbero essere non eccessivamente impegnative e non tutte devono necessariamente essere completate prima della visita di certificazione.

Se in qualche caso l'impegno appare eccessivamente gravoso è perché probabilmente non è stato fatto nulla o quasi negli anni scorsi per mantenersi aggiornati. L'inadeguatezza della gestione attuale rispetto ai requisiti della norma ISO 9001:2015 e l'elevato gap da colmare per raggiungere la conformità con la nuova norma dovrebbe far riflettere la Direzione sul fatto che la gestione aziendale non è andata al passo coi tempi.

Esempi di questa situazione si possono trovare quando:

- risulta difficoltoso correlare strategie, politiche ed obiettivi aziendali;
- risulta estremamente impegnativo individuare e soprattutto calcolare indicatori idonei a misurare gli obiettivi e le prestazioni dei processi in termini di efficacia ed efficienza;

- emergono rischi importanti non adeguatamente gestiti;
- emergono carenze di risorse umane e delle relative competenze necessarie;
- emerge che la conoscenza organizzativa ed il know-how aziendale non è curato e tutelato adeguatamente;
- risultano carenze dal punto di vista tecnologico: hardware e software obsoleti, strumenti inadeguati, ecc.

In tutti questi casi la nuova norma ISO 9001:2015 può rappresentare un **valido strumento e stimolo per migliorare l'efficacia e l'efficienza interna**, molto più che costituire un obbligo certificativo.

La sicurezza delle informazioni in caso di calamità naturali e non naturali

In caso di catastrofi e calamità naturali quali terremoti, alluvioni, inondazioni, incendi, eruzioni vulcaniche, uragani oppure atti terroristici, uno dei danni collaterali dopo la perdita di vite umane e i danni materiali ad edifici ed infrastrutture, occorre considerare il blocco dei sistemi informativi che può rallentare notevolmente la ripresa delle normali attività.

Le metodologie da impiegare per prevenire e mitigar i danni che possono compromettere la ripresa delle attività dopo un evento catastrofico riguardano la tematica della business continuity (continuità operativa).

Nell'intervento presentato lo scorso 17/11 al Convegno EVENTI SISMICI: PREVENZIONE, PROTEZIONE, SICUREZZA, EMERGENZA, le cui slide sonono scaricabili in questa pagina, si sono presentate tutte le attività da porre in essere per controllare tali situazioni indesiderate, in particolare sono stati trattati i seguenti argomenti:

- business continuitymanagement
- normative ISO 22301, ISO 2001/27002 e ISO 27031 per la gestione della business continuity, con particolare riferimento ai sistemi informatici
- gestione dei rischi per la continuità operativa
- disaster recovery
- obiettivi ed indicatori di business continuity

- business continuity plan (piano di continuità operativa).

La sicurezza dei dati in caso di terremoto (185 download)

Nuova Specifica IATF 16949 per la qualità nell'automotive

Lo scorso 1° ottobre è stata pubblicata la nuova **specifica IATF 16949:2016**, revisione della Specifica tecnica ISO/TS 16949:2009 che, dunque, non è più norma ISO. Oltre a questo aspetto ci sono molte altre novità nella nuova specifica automotive, a cominciare dal **piano di transizione** alla nuova norma per i vecchi certificati ISO/TS 16949 e i nuovi certificati IATF 16949:2016, estremamente breve.

Infatti da ottobre 2017 non sarà più possibile certificarsi secondo il vecchio schema ISO/TS 16949 e a settembre 2018 tutti i vecchi certificati ISO/TS 16949 perderanno di validità se non migrati nel nuovo schema.

Ci si attendeva la revisione della ISO/TS 16949 del 2009, legata alla norma ISO 9001:2008 dopo la revisione 2015 della norma sui sistemi di gestione per la qualità, ma le modifiche sono state molto più significative che una semplice riproposizione dei requisiti secondo l'approccio della ISO 9001:2015.

La nuova specifica IATF 16949:2016 presenta in veste di requisito alcune prassi che erano diventate abituali nella catena di fornitura del settore automotive e rende obbligatorio il rispetto dei C.S.R. (*Customer Specific Requirments*) del cliente automotive, ma non solo.

Le principali novità riguardano sicuramente la gestione dei rischi (e non poteva essere altrimenti dopo l'uscita della ISO 9001:2015) e la gestione dei fornitori, molto più severa che in passato.

I punti principali di innovazione sono così riepilogati:

1. I **CSR** sono alla base di tutto il processo.
2. Le logiche automotive devono essere basate su logiche economiche (efficienza dei processi) e finanziarie.
3. La Specifica contiene requisiti aggiuntivi rispetto alla ISO 9001:2015, ma la suddetta norma non fa più parte del testo della specifica automotive, ma è solo richiamata.

4. È presente una sezione specifica (Allegato B) che fornisce le linee guida ed indicazioni sulle modalità da attuare per gestire alcuni processi/attività in assenza di una specifica del cliente. I *tool* da poter utilizzare per la gestione di SPC, MSA, FMEA, APQP, ecc. **sono solo quelli indicati nell'Allegato B** (es. Manuali AIAG, ANFIA, VDA, ecc.).
5. Viene introdotta la **sostenibilità aziendale dei fornitori**.
6. **Responsabilità Sociale d'Impresa**: si deve predisporre ed attuare un sistema di gestione che prevenga le frodi, la corruzione ed altri reati (è esplicitamente richiesto un codice etico/di condotta). Naturalmente quelle imprese che già dispongono di un modello organizzativo secondo il D.Lgs 231 dovranno solo integrarlo nel sistema qualità.
7. I **fornitori** devono avere un processo sequenziale stabilito di crescita che ha come obiettivo finale il **conseguimento della certificazione IATF 16949**. Sono coinvolti tutti i fornitori della catena di fornitura del prodotto e relativi componenti/materie prime/lavorazioni esterne.
8. Viene introdotta la **gestione del rischio d'impresa** facendo esplicito riferimento alla ISO 31000 (oltre che alla ISO 19011 ed alla ISO 9001 stessa).
9. La logica di tutto il sistema è la ***business continuity***, ma il focus si sposta dal *manufacturing* (aspetto compreso anche nella precedente versione della specifica) a tutti i processi aziendali che possono generare interruzioni dell'operatività.
10. Compaiono requisiti specifici per il **software inserito nel veicolo**, con necessità di validazione dello stesso.
11. Il **set minimo di indicatori** da misurare nel sistema di gestione è riportato nella Specifica IATF.
12. Occorre garantire sempre più la **sicurezza del prodotto**.

In conseguenza delle modifiche, sostanzialmente tutte aggiuntive di requisiti, le giornate di verifica degli Organismi di Certificazione dovrebbero aumentare.

Molti aspetti dovranno essere chiariti dalle *Rules* di prossima pubblicazione e da eventuali Linee Guida nell'applicazione e nella verifica dei nuovi sistemi IATF 16949.

La nuova specifica mira a garantire la continuità operativa e la sostenibilità di tutta la catena dell'automotive e gli obiettivi economici potranno essere raggiunti e migliorati solo attraverso l'efficienza che potrà accrescere i margini, normalmente molto ridotti, anche se applicati a volumi di produzione elevati e continuativi.

Inoltre nella nuova IATF 16949:2016 sono citati per la prima volta strumenti e metodologia spesso adottate nell'automotive, quali la *lean production*, il *Problem Solving*, i 5S, ecc.

Anche i software impiegati per il controllo qualità e per la gestione della qualità dovranno essere validati e saranno sottoposti a verifica da parte degli auditor

dell’Organismo di Certificazione.

Infine i tempi di transizione sono estremamente ridotti:

- Dal **Marzo 2017** gli Organismi di Certificazione potranno certificare secondo la nuova specifica IATF 16949:2016.
- Le nuove certificazioni potranno essere emesse secondo la ISO/TS 16949:2009 solo fino a **Settembre 2017**
- Le transizioni alla nuova specifica IATF 16949 dalla vecchia ISO/TS 16949, per le aziende già certificate, termineranno con gli audit di **Maggio 2018** per consentire alle aziende di risolvere eventuali non conformità entro la scadenza di tutti i vecchi certificati ISO/TS 16949, fissata per il **14 Settembre 2018**.

La verifica dei progetti ai fini della validazione: nuove opportunità per i professionisti? – parte II

La regolamentazione della verifica dei progetti relativi ad appalti pubblici ai fini della validazione non è stata modificata sotanzialmente dall’uscita del nuovo Codice Appalti. Nel presente articolo, che segue la prima parte già pubblicata (La verifica dei progetti ai fini della validazione: nuove opportunità per i professionisti? parte I) su questo sito esaminiamo gliaspetti tecnici e gestionali che caratterizzano il servizio di verifica del progetto per Organismi di Ispezione e Società o Studi di Ingegneria.

Aspetti tecnci e procedurali della verifica

Cosa si intende per verifica del progetto

La verifica del progetto è trattata all’art. 26 del Codice degli Appalti. Essa è finalizzata ad accertare la conformità del progetto esecutivo o definitivo rispettivamente, al progetto definitivo o al progetto di fattibilità. La verifica accerta in particolare:

a) la completezza della progettazione e la rispondenza all’art. 23 del codice;

b) la coerenza e completezza del quadro economico in tutti i suoi aspetti;

c) l’appaltabilità della soluzione progettuale prescelta;

d) i presupposti per la durabilità dell’opera nel tempo;

e) la minimizzazione dei rischi di introduzione di varianti e di contenzioso;

f) la possibilità di ultimazione dell’opera entro i termini previsti;

g) la sicurezza delle maestranze e degli utilizzatori;

h) l’adeguatezza dei prezzi unitari utilizzati;

i) la manutenibilità e la presenza del piano di monitoraggio delle opere, ove richiesto.

I criteri generali della verifica erano descritti all’art. 52 del DPR 207/2010, che però è stato abrogato insieme a tutto il CAPO II. In assenza di nuove disposizioni possono comunque essere ritenuti validi aspetti del controllo stabiliti dal DPR 207/2010:

- affidabilità;
- completezza ed adeguatezza;
- leggibilità, coerenza e ripercorribilità;
- compatibilità;

intendendosi per:

a) affidabilità:

- verifica dell’applicazione delle norme specifiche e delle regole tecniche di riferimento adottate per la redazione del progetto;
- verifica della coerenza delle ipotesi progettuali poste a base delle elaborazioni tecniche ambientali, cartografiche, architettoniche, strutturali, impiantistiche e di sicurezza;

b) completezza ed adeguatezza:

- verifica della corrispondenza dei nominativi dei progettisti a quelli titolari dell’affidamento e verifica della sottoscrizione dei documenti per l’assunzione delle rispettive responsabilità;
- verifica documentale mediante controllo dell’esistenza di tutti gli elaborati previsti per il livello del progetto da esaminare;
- verifica dell’esaustività del progetto in funzione del quadro esigenziale;
- verifica dell’esaustività delle informazioni tecniche ed amministrative

contenute nei singoli elaborati;
- verifica dell’esaustività delle modifiche apportate al progetto a seguito di un suo precedente esame;
- verifica dell’adempimento delle obbligazioni previste nel disciplinare di incarico di progettazione;

c) leggibilità, coerenza e ripercorribilità:

- verifica della leggibilità degli elaborati con riguardo alla utilizzazione dei linguaggi convenzionali di elaborazione;
- verifica della comprensibilità delle informazioni contenute negli elaborati e della ripercorribilità delle calcolazioni effettuate;
- verifica della coerenza delle informazioni tra i diversi elaborati;

d) compatibilità:

- la rispondenza delle soluzioni progettuali ai requisiti espressi nello studio di fattibilità ovvero nel documento preliminare alla progettazione o negli elaborati progettuali prodotti nella fase precedente;
- la rispondenza della soluzione progettuale alle normative assunte a riferimento ed alle eventuali prescrizioni, in relazione agli aspetti di seguito specificati:
- inserimento ambientale;
- impatto ambientale;
- funzionalità e fruibilità;
- stabilità delle strutture;
- topografia e fotogrammetria;
- sicurezza delle persone connessa agli impianti tecnologici;
- igiene, salute e benessere delle persone;
- superamento ed eliminazione delle barriere architettoniche;
- sicurezza antincendio;
- inquinamento;
- durabilità e manutenibilità;
- coerenza dei tempi e dei costi;
- sicurezza ed organizzazione del cantiere.

La verifica della documentazione da parte del soggetto preposto al controllo è effettuata sui documenti progettuali previsti per ciascun livello della progettazione (progetto di fattibilità tecnica ed economica, definitivo, esecutivo), così come era riportato nel Regolamento DPR 207/2010 stesso.

All’art. 50 (*Verifica della documentazione)* del DPR 207/2010 erano pure esplicitate – con riferimento agli aspetti del controllo sopra citati – le modalità di esecuzione delle verifiche come segue:

a) per le relazioni generali, è necessario verificare che i contenuti siano coerenti

con la loro descrizione capitolare e grafica, nonché con i requisiti definiti nello studio di fattibilità ovvero nel documento preliminare alla progettazione e con i contenuti delle documentazioni di autorizzazione ed approvazione facenti riferimento alla fase progettuale precedente;

b) per le relazioni di calcolo è necessario:

- verificare che le ipotesi ed i criteri assunti alla base dei calcoli siano coerenti con la destinazione dell'opera e con la corretta applicazione delle disposizioni normative e regolamentari pertinenti al caso in esame;
- verificare che il dimensionamento dell'opera, con riferimento ai diversi componenti, sia stato svolto completamente, in relazione al livello di progettazione da verificare, e che i metodi di calcolo utilizzati siano esplicitati in maniera tale da risultare leggibili, chiari ed interpretabili;
- verificare la congruenza di tali risultati con il contenuto delle elaborazioni grafiche e delle prescrizioni prestazionali e capitolari;
- verificare la correttezza del dimensionamento per gli elementi ritenuti più critici, che devono essere desumibili anche dalla descrizione illustrativa della relazione di calcolo stessa;
- verificare che le scelte progettuali costituiscano una soluzione idonea in relazione alla durabilità dell'opera nelle condizioni d'uso e manutenzione previste;

c) per le relazioni specialistiche si deve verificare che i contenuti presenti siano coerenti con:

- le specifiche esplicitate dal committente;
- le norme cogenti;
- le norme tecniche applicabili, anche in relazione alla completezza della documentazione progettuale;
- le regole di progettazione;

d) per gli elaborati grafici, è necessario verificare che ogni elemento, identificabile sui grafici, sia descritto in termini geometrici e che, ove non dichiarate le sue caratteristiche, esso sia identificato univocamente attraverso un codice ovvero attraverso altro sistema di identificazione che possa porlo in riferimento alla descrizione di altri elaborati, ivi compresi documenti prestazionali e capitolari;

e) per i capitolati, i documenti prestazionali e lo schema di contratto, si deve verificare che ogni elemento, identificabile sugli elaborati grafici, sia adeguatamente qualificato all'interno della documentazione prestazionale e capitolare; verificare inoltre il coordinamento tra le prescrizioni del progetto e le clausole dello schema di contratto, del capitolato speciale d'appalto e del piano di manutenzione dell'opera e delle sue parti;

f) per la documentazione di stima economica, si deve verificare che:

- i costi parametrici assunti alla base del calcolo sommario della spesa siano coerenti con la qualità dell'opera prevista e la complessità delle necessarie lavorazioni;
- i prezzi unitari assunti come riferimento siano dedotti dai prezzari della stazione appaltante aggiornati o dai listini ufficiali vigenti nell'area interessata;
- siano state sviluppate le analisi per i prezzi di tutte le voci per le quali non sia disponibile un dato nei prezzari;
- i prezzi unitari assunti a base del computo metrico siano coerenti con le analisi dei prezzi e con i prezzi unitari assunti come riferimento;
- gli elementi di computo metrico estimativo comprendano tutte le opere previste nella documentazione prestazionale e capitolare e corrispondano agli elaborati grafici e descrittivi;
- i metodi di misura delle opere siano usuali o standard;
- le misure delle opere computate siano corrette, operando anche a campione o per categorie prevalenti;
- i totali calcolati siano corretti;
- il computo metrico estimativo e lo schema di contratto individuano la categoria prevalente, le categorie scorporabili e subappaltabili a scelta dell'aggiudicatario, le categorie con obbligo di qualificazione e le categorie con divieto di subappalto ai sensi di quanto previsto dal nuovo Codice degli Appalti;
- le stime economiche relative a piani di gestione e manutenzione siano riferibili ad opere similari di cui si ha evidenza dal mercato o che i calcoli siano fondati su metodologie accettabili dalla scienza in uso e raggiungano l'obiettivo richiesto dal committente;
- i piani economici e finanziari siano tali da assicurare il perseguimento dell'equilibrio economico e finanziario;

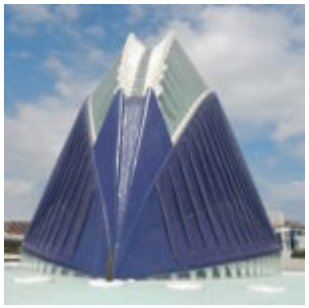
g) per il piano di sicurezza e coordinamento è necessario verificare che sia redatto per tutte le tipologie di lavorazioni da porre in essere durante la realizzazione dell'opera ed in conformità dei relativi magisteri; inoltre che siano stati esaminati tutti gli aspetti che possono avere un impatto diretto e indiretto sui costi e sull'effettiva cantierabilità dell'opera;

h) per il quadro economico è necessario verificare che sia stato redatto conformemente a quanto previsto dall'articolo 16 (ancora in vigore!) del DPR 207/2010;

i) accertare l'acquisizione di tutte le approvazioni ed autorizzazioni di legge previste per il livello di progettazione.

Suddetti aspetti sono spesso riportati nei Disciplinari per il Servizio di Verifica delle Stazioni Appaltanti e, dunque, anche se non costituiscono più – almeno per il

momento – un requisito di legge, tornano ad essere prescrittivi perché imposti dal Committente.



In assenza di Disciplinari o Capitolati per la Verifica del Progetto restano comunque *best practice* e potrebbero essere affiancate dai contenuti della UNI 10721 che, mentre prima essendo normativa volontaria veniva in secondo piano rispetto ai requisiti di legge, oggi costituisce un valido criterio per determinare le modalità ed i criteri della verifica.

Altre parti del CAPO II abrogato del vecchio Regolamento non sono al momento state sostituite da prescrizioni equivalenti. In ogni caso le normative applicabili al controllo tecnico (ISO 17020, UNI 10721, UNI 10722,…) ed i regolamenti ACCREDIA definiscono le "regole del gioco" ed in particolare prevedono l'emissione di un Rapporto di Ispezione con caratteristiche e contenuti ben precisi.

Le responsabilità del soggetto preposto alla verifica

Il soggetto incaricato della verifica ha la responsabilità degli accertamenti previsti dal Codice, dalle Linee Guida ANAC e da eventuali successivi decreti attuativi del Codice, ivi compresi quelli relativi all'avvenuta acquisizione dei necessari pareri, autorizzazioni ed approvazioni, ferma restando l'autonoma responsabilità del progettista circa le scelte progettuali e i procedimenti di calcolo adottati.

La specifica delle responsabilità del soggetto preposto alla verifica e le relative sanzioni, presenti al CAPO I del DPR 207/2010 non sono specificatamente presente nel nuovo Codice, ma l'opera, come detto, non è conclusa.

I costi della verifica

Circa i compensi per l'attività di verifica oggi la determinazione dei compensi per i servizi di ingegneria ed architettura è stabilita dal Decreto ministeriale 17 giugno 2016 "*Approvazione delle tabelle dei corrispettivi commisurati al livello qualitativo delle prestazioni di progettazione adottato ai sensi dell'art. 24, comma 8, del decreto legislativo n. 50 del 2016*", dove nell'allegato sono stabiliti i criteri per la determinazione della tariffa professionale per il supporto al RUP per i servizi di verifica ai fini della validazione del progetto.

Questi compensi dovrebbero poi essere posti a base di gara e l'aggiudicazione dovrebbe avvenire secondo il criterio dell'offerta economicamente più vantaggiosa, ovvero il prezzo dovrebbe avere solo un certo peso nella determinazione dell'offerta migliore. In realtà gli aspetti relativi alla capacità tecnica e professionale del soggetto offerente (Organismo di Ispezione oppure società o studio di ingegneria), documentati attraverso un'offerta tecnica (Relazione organizzativo-metodologica) e

la descrizione di alcuni servizi svolti nell'ambito della verifica di progetti di opere dell'appalto potrebbero essere non sufficientemente premianti a fronte di ribassi di prezzo molto elevati.

È opportuno chiedersi che controllo si ha sul servizio di verifica se le offerte al ribasso sul prezzo superano soglie inimmaginabili (nella realtà si sono registrati ribassi persino oltre il 70/80% su bandi di gara al massimo ribasso secondo il vecchio Codice)?

Se il bando di gara non prevede il controllo sulle offerte troppo basse e le eventuali giustificazioni richieste ai partecipanti sono verificate in modo troppo comprensivo, si rischia di svilire eccessivamente l'attività di controllo che, quindi, non potrà essere efficace e garantire, non solo il committente, ma la collettività che utilizzerà le opere realizzate dopo averle finanziate. In questo caso il presunto risparmio della Pubblica Amministrazione porta ad un aumento del rischio di sostenere maggiori costi in fase esecutiva, a causa della cattiva qualità della progettazione o, peggio, di realizzare opere pubbliche non efficienti e dannose per la collettività (si pensi a strade pericolose, scuole scarsamente fruibili, edifici pubblici non mantenibili con efficienza, edifici che sprecano risorse energetiche, ecc.).

Modalità di svolgimento della verifica

Passiamo ad esaminare il processo di verifica del progetto da un punto di vista tecnico-gestionale.

L'attività di verifica del progetto inizia al momento di consegna degli elaborati oggetto del controllo all'Organismo di Ispezione (o Società/Studio di Ingegneria ove applicabile) incaricato della verifica.

La prima fase del servizio consiste normalmente nel controllo dei documenti consegnati con il duplice scopo di:

1. Verificare la congruenza degli elaborati consegnati con l'elenco degli stessi preparato dai progettisti relativamente a revisioni, date di emissione, argomenti, ecc..
2. Verificare la completezza formale della documentazione rispetto ai requisiti cogenti stabiliti per il livello progettuale di riferimento (progetto di fattibilità tecnica-economica, definitivo ed esecutivo).

Mentre la prima fase potrebbe far emergere che gli studi o società di ingegneria non producono un elenco degli elaborati validi congruente con gli elaborati costituenti il progetto stesso, la seconda rivela talvolta che i medesimi organismi di progettazione non hanno nemmeno prodotto un progetto "formalmente" conforme ai requisiti in termini di documenti minimi ed indispensabili. Tali requisiti minimi sono banalmente contenuti nel vecchio Regolamento DPR 207, i cui contenuti seguenti

restano attualmente in vigore:

- per il progetto preliminare (progetto di fattibilità tecnica-economica) i documenti di progetto sono descritti nella Sezione I – Art. 17 e segg. del DPR 207/2010;
- per il progetto definitivo i documenti progettuali descritti alla Sezione III – Art. 24 e segg. del DPR 207/2010;
- per il progetto esecutivo i documenti progettuali descritti alla Sezione IV – Art. 33 e segg. del DPR 207/2010.

Questa verifica di completezza formale non dovrebbe essere trascurata dai soggetti coinvolti (R.P., progettisti ed organismo di verifica) in quanto potrebbe inficiare la successiva validazione del progetto.

Questa fase, cosiddetta di "ricezione" o "controllo documenti", comprende un'identificazione fisica degli elaborati forniti su supporto cartaceo (etichettatura, timbro o altra forma di identificazione fisica come previsto dalla norma ISO 17020), un loro inserimento in apposito elenco informatizzato (*database*) e la generazione di un primo output dell'attività di controllo. In caso di problemi riscontrati sarebbe necessaria una risposta celere da parte dei progettisti per sanare le prime non conformità documentali. Teoricamente, se la situazione riscontrata fosse gravemente carente (assenza di numerosi elaborati essenziali), l'attività di verifica non potrebbe proseguire in modo proficuo fintantoché i progettisti non colmano le lacune evidenziate. La tradizionale urgenza delle Stazioni Appaltanti potrebbe aver imposto tempi di verifica ridotti, ma ogni impegno contrattuale di termini temporali per l'attività di verifica dell'Organismo (OdI o altri soggetti abilitati) nei confronti del Committente decade nel momento in cui il progetto non è formalmente completo.

Si iniziano a presentare in questa prima fase i primi problemi dovuti a contratti ed interessi contrastanti fra le parti, in gran parte dovuti ad una mancata osservanza dei requisiti di legge. Infatti la frequente assenza del documento preliminare alla progettazione (cfr. art. 15 comma 5 del DPR 207/2010, che resta ancora in vigore: «*Il responsabile del procedimento redige un documento preliminare all'avvio della progettazione…* » con le caratteristiche indicate ai commi 6 e 7) inficia in partenza il procedere del processo di progettazione e verifica secondo i principi della legge. È evidente che è responsabilità del committente della progettazione e del servizio di verifica (ovvero del responsabile del procedimento) garantire che siano presenti tutti gli input necessari al processo di progettazione e della sua verifica.

Se, come accade sempre più frequentemente, gli elaborati sono trasmessi al soggetto incaricato della verifica solo su supporto digitale, le cose anziché semplificarsi, si complicano. Infatti il formato digitale spesso non è gestito con adeguati crismi riguardo la sua integrità, la gestione delle revisioni e, soprattutto, l'autenticità. Proprio su quest'ultimo aspetto il Regolamento DPR 207, nella parte

ancora in vigore, prevede che «*Tutti gli elaborati devono essere sottoscritti dal progettista o dai progettisti responsabili degli stessi nonché dal progettista responsabile dell'integrazione fra le varie prestazioni specialistiche*.» (art. 15, comma 12) e tale requisito, in assenza di elaborato su supporto cartaceo debitamente firmato e timbrato, può essere garantito solo dalla firma digitale apposta secondo quanto previsto dalla nostra legislazione. Purtroppo l'impiego della firma digitale è molto raro nell'ambito della progettazione di opere di ingegneria civile o infrastrutturale.

In conclusione, l'attività dell'Organismo di verifica deve prevedere sia la gestione degli elaborati cartacei, sia la gestione dei *file* elettronici, con relativo dimensionamento degli archivi, nel primo caso, dello *storage* informatico, nel secondo, con un occhio alla sicurezza delle informazioni in entrambi i casi.

In questa prima fase l'Organismo di Ispezione individua anche il Gruppo di Ispezione (se non già stabilito in fase di offerta per il servizio, come prescrive la norma ISO 17020:2012), ovvero il team di ispettori che, per competenza, andranno a verificare i singoli elaborati. Per requisiti regolamentari (ACCREDIA) il gruppo di lavoro deve essere comunicato al committente prima dell'inizio della verifica; quest'ultimo ha facoltà di ripudiarlo, anche parzialmente, entro un termine stabilito (generalmente pochi giorni) per fondati motivi. Tale gruppo di ispezione dovrà essere guidato da un coordinatore o responsabile della verifica che sottoscriverà i rapporti di ispezione, fermo restando che, comunque, il rapporto conclusivo deve comunque essere sottoscritto anche dal responsabile tecnico (direttore tecnico) dell'organismo di verifica (ingegnere o architetto con esperienza professionale di almeno 10 anni, oltre ad altre competenze specifiche).

La seconda fase del servizio comprende l'assegnazione dei singoli elaborati agli ispettori e la pianificazione della qualità del servizio, ovvero il riesame e la trasformazione dei requisiti contrattuali in specifiche per la conduzione della verifica. La distribuzione degli elaborati dovrebbe essere supportata da un valido sistema informativo (software gestionale, archivi informatici o modulistica cartacea) per tenere sempre sotto controllo *chi* dovrà verificare *che cosa*.

Oltre agli ispettori competenti nelle rispettive discipline l'Organismo di Ispezione (o altro organismo abilitato alla verifica) deve assegnare alla commessa anche uno o più coordinatori che coordinino, appunto, il lavoro svolto dai vari ispettori.

Solo a questo punto inizia l'attività di verifica vera e propria, spesso supportata da check-list o istruzioni operative per cercare di ottenere una certa uniformità di giudizio (teoricamente lo stesso elaborato, verificato da due ispettori di pari competenze, dovrebbe produrre lo stesso esito della verifica).

Durante la verifica ogni ispettore necessita di un valido ed efficace strumento di registrazione dei rilievi in conformità ai requisiti normativi: qui le diverse metodologie adottate dai vari Organismi di Ispezione possono fare la differenza in

termini di efficacia (ottenere una rendicontazione puntuale e priva di errori formali) ed efficiente (minimizzare l'impiego delle risorse, soprattutto quelle per il coordinamento dell'attività), tanto più quanto più sono numerosi gli elaborati da verificare (alcuni progetti di infrastrutture ne possono comprendere migliaia di elaborati).

I sistemi adottati per la gestione della registrazione degli esiti della verifica possono variare da moduli in formato Word, Excel o simili che riportano tutte le osservazioni rilevate dall'ispettore, suddivise per elaborato, disciplina o ispettore, a vere applicazioni Web che permettono agli ispettori (la maggior parte dei quali consulenti) di registrare l'esito dell'attività di verifica – dovunque essi si trovino purché sia disponibile un collegamento a internet – in moduli appositamente predisposti nel sistema informativo dell'Organismo. Naturalmente quest'ultimo approccio implica numerosi vantaggi:

- consentire al personale incaricato del coordinamento di visualizzare i risultati della verifica man mano che vengono pubblicati dagli ispettori direttamente dal sistema informatico, evitando così di dover gestire centinaia ed a volte migliaia di *file* inviati per e-mail e contenenti i rilievi formulati dagli ispettori;
- permettere un immediato controllo dell'attività "in progress" anche dal punto di vista dei contenuti, soprattutto relativamente alle verifiche di congruenza incrociate fra ispettori di diverse discipline che, inevitabilmente, devono comunque esaminare elaborati comuni (relazioni generali, computi, …);
- consentire ai progettisti di fornire una risposta ai rilievi formulati dagli ispettori direttamente nel sistema informatico, garantendo maggior sicurezza rispetto ad ogni altro sistema;
- fornire la possibilità al committente (R.P.) di esaminare l'andamento dell'attività quasi in tempo reale, sempre attraverso il collegamento internet con accesso riservato al sistema informativo dell'organismo di verifica.

Questa fase del controllo termina con l'emissione di un primo rapporto di ispezione intermedio che riferisce al committente dell'esito della verifica sugli elaborati consegnati. Tale rapporto – redatto seguendo precise prescrizioni normative e regolamentari (ACCREDIA) – comprende un elenco di rilievi, talvolta classificati per livello di criticità. Tali rilievi dovranno essere presi in carico dai progettisti che dovranno adeguare il progetto secondo le prescrizioni indicate.

Si entra così, con la consegna del rapporto di ispezione al committente ed ai progettisti nella terza fase del processo di verifica del progetto ai fini della validazione. Possono essere emessi più rapporti, cosiddetti intermedi, che documentano gli esiti, anche parziali, dell'attività di verifica su tutti o parte degli elaborati consegnati.

Come già premesso, i progettisti dovrebbero rispondere puntualmente, rilievo per rilievo, alle osservazioni/non conformità formulate dall'Organismo di Ispezione e,

quindi, non c'è niente di meglio che un sistema informatico *web-based*, accessibile via internet in modo sicuro mediante apposite credenziali di autenticazione, per registrare le risposte dei progettisti. I sistemi che prevedono l'impiego di documenti di Office ovviamente non forniscono le medesime garanzie in termini di efficacia, efficienza e sicurezza dei dati (è difficile garantire che il progettista non abbia alterato il testo dell'osservazione o assicurare che il testo di alcun rilievo sia stato inavvertitamente cancellato o comunque alterato).

Questa fase di interazione con il progettista presenta numerose analogie con la fase in cui le organizzazioni con sistema di gestione certificato (o certificando) devono rispondere ad eventuali non conformità od osservazioni formulate dal proprio Organismo di Certificazione, il quale deve accettarle prima di procedere con l'iter di certificazione. Anche in queste situazioni i vari organismi hanno adottato metodologie diverse, dallo scambio di file di Office a sistemi web, ma la differenza fondamentale, rispetto alle verifiche sui progetti, sta nel fatto che i rilievi sono molto meno numerosi (alcuni progetti complessi possono far emergere centinaia di rilievi contro i pochi rilievi registrati dagli organismi di certificazione per ogni audit) e la controparte (organizzazione certificata rispetto all'organismo di progettazione) è normalmente più diligente nell'attuazione delle azioni correttive o delle correzioni delle non conformità.

Infatti, questa terza fase non fruisce in modo snello, perché spesso i progettisti non accettano – per motivazioni diverse – le osservazioni formulate dall'OdI e sono restii a modificare il progetto. Viceversa il responsabile del procedimento non esercita sempre il potere che avrebbe per pretendere la risoluzione completa di tutte le anomalie rilevate.

La quarta fase consiste nella riverifica da parte degli ispettori dell'Organismo degli elaborati revisionati e delle controdeduzioni dei progettisti. Al termine di questa fase per ogni rilievo l'Organismo incaricato della verifica deve determinare un **esito finale del progetto**, giudicando le risoluzioni proposte dai progettisti. Al proposito si ribadisce il fatto che la legge prevede che proprio che la verifica avvenga in contraddittorio con i progettisti.

Al termine di questa fase viene prodotto il **rapporto di ispezione conclusivo** che riepiloga tutte le risultanze della verifica (oppure le richiama da precedenti documenti, come previsto dalla ISO 17020) e formula un giudizio professionale conclusivo sulla conformità del progetto. Sulla base dell'esito del rapporto di ispezione finale il responsabile del procedimento provvederà alla validazione formale del progetto.

Conclusioni

Oggi la prevista apertura del mercato ai professionisti della progettazione (studi o società di ingegneria) ipotizzata con il Regolamento DPR 207 sembra non essersi concretizzata, da un lato per i numerosi vincoli imposti al servizio di verifica di

progetti pubblici, dall’altro per la situazione di crisi del comparto edilizio solo in parte dovuta al minor numero di opere pubbliche di cui è stata pianificata la realizzazione, oltre alla contrazione dei compensi posti a base di gara. Non da ultimo l’ingresso nel mercato dei servizi di verifica della progettazione necessita di discreti investimenti di risorse che, probabilmente, pochi soggetti sono in grado o ritengono opportuno sostenere. Resta comunque una opportunità in più per gli studi o società di ingegneria che hanno visto ridursi notevolmente le commesse di progettazione e direzione lavori nel comparto privato.

Le Stazioni Appaltanti, invece, avranno la possibilità di dotarsi un sistema di gestione qualità ISO 9001 ed eventualmente accreditarsi come Organismo di Ispezione ISO 17020 per svolgere internamente le attività di verifica previste dalla legge.