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.

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 (561 download) (compreso l'allegato con le FAQ)
- Linee Guida Valutazione-Impatto WP 248 (300 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?

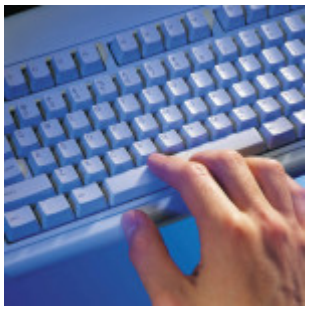
La probabilità di essere sanzionati a seguito di ispezioni del Nucleo Privacy della GdF è estremamente bassa, un po' più alta per organizzazioni che trattano dati particolarmente critici (la valutazione è fatta in base al numero delle ispezioni avvenute negli ultimi anni).

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 (117 download)

Beni ammissibili Piano Industria 4.0 (113 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 (96 download)

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.

La Business intelligence per la PMI

In questi ultimi tempi si è parlato spesso di **Big Data** e dell'utilità dell'analisi degli stessi per ottenere informazioni utili alla gestione di varie organizzazioni, anche al fine di prendere decisioni strategiche.

La **Business Intelligence** (BI) è un insieme di modelli, metodi e strumenti che permette la raccolta, l'aggregazione, l'analisi e la presentazione di informazioni, il tutto per generare conoscenza volta al miglioramento di attività e servizi. I Big Data in sé non generano valore, se non vengono analizzati con strumenti di Business Intelligence, appunto.

Viceversa la BI non serve solo ad analizzare i Big Data, ma anche per analizzare ed interpretare i dati – di entità inferiore – che sono contenuti nei sistemi informativi aziendali, a volte differenti fra loro, e che non sono integrati o comunque interconnessi, al fine di ottenere informazioni omogenee e realmente utili.

La Business Intelligence si suddivide in due aree:

- **Datawarehouse**, il cui scopo è di raccogliere, integrare, aggregare e presentare i dati;

- **Data Mining**, il cui scopo è di analizzare, interpretare e scoprire eventuali informazioni interessanti.

Datawarehouse

È un sistema per gestire e raccogliere in modo permanente e aggiornabile i dati provenienti da fonti diverse. Rappresenta il livello intermedio fra i sistemi **OLTP** (*On Line Transaction Processing*), che elaborano dati dettagliati e aggiornati da brevi transazioni ripetitive, e i sistemi **OLAP** (*On Line Analytical Processing*), che fungono da supporti alle decisioni compiendo complesse elaborazioni su notevoli quantità di dati storici con varie possibilità di aggregazione. L'OLAP crea, inoltre, una rappresentazione tridimensionale chiamata "***Data Cube***", che facilita la visualizzazione dei risultati.

Data Mining

È un sistema che si pone come gradino intermedio fra *Datawarehouse* e generazione della conoscenza. Permette di scoprire una serie di informazioni intrinseche e non banali contenute in basi di dati anche di notevoli dimensioni. Queste informazioni possono poi essere utilizzate a scopi gestionali o decisionali. Le attività principali del sistema riguardano l'individuazione di dipendenze fra eventi e di classi nella popolazione con una loro descrizione. Esiste anche la possibilità di riconoscere eccezioni, per esempio frodi o false richieste. Esistono svariate applicazioni della disciplina, per esempio nei mercati finanziari, nella valutazione di rischi e frodi, nella determinazione di meccanismi d'acquisto, nelle analisi di mercato via web e nel marketing, per esempio nel *clustering*.

Applicazioni della Business Intelligence

Le applicazioni e le opportunità della BI spaziano in diversi settori, sia a livello aziendale, sia nella Pubblica Amministrazione, senza dimenticare applicazioni sportive (es. analisi di dati statistici su partite di calcio, analisi dei dati della telemetria in Formula 1, ecc.).

La disciplina della BI comprende anche algoritmi specifici per l'analisi dei dati come l'algoritmo "A priori" e gli algoritmi di clustering "K-means" e "Simple Lincage Hierarchical Clustering". Inoltre la teoria prevede – prima di procedere all'analisi dei dati – una integrazione degli stessi ed una "pulizia preliminare" (*data cleaning*), per evitare che dati errati o poco significativi alterino i risultati delle analisi.

Queste basi scientifiche sono in forte espansione grazie alle sempre maggiori potenze di calcolo degli elaboratori e dei software di analisi, oltre alla sempre

maggiore disponibilità di dati che vengono raccolti dai sistemi informatici più svariati. La forza di Google è anche data dalla capacità che ha avuto l'azienda di Mountain View di analizzare in modo efficace i dati della navigazione e della ricerca sui siti web, inventando, di fatto, i *web analytics*.

BI e PMI

Le future possibilità di utilizzare questi sistemi per effettuare previsioni e le loro enormi potenzialità rendono facile pronosticare un loro ampio e sempre più efficace uso nel **controllo di gestione**, nella gestione della qualità e nell'analisi di scenari futuri presso imprese di ogni tipo e dimensione.

Ma oggi le PMI italiane possono trovare giovamento dalla business intelligence?

Il problema da un lato è **culturale**: nelle medio-piccole e piccole imprese italiane manca spesso la conoscenza della teoria (*drill-down*, *roll-up*, *data mart*, *datawarehouse*… sono tutti termini sconosciuti ai più) e degli strumenti di analisi dati. A ciò si può sopperire con la formazione del personale e con la consulenza di esperti in grado di aiutare l'azienda a capire quali informazioni si vogliono conoscere e come raccogliere gli indicatori necessari per supportare la Direzione nella gestione aziendale.

Per quanto riguarda gli strumenti, oggi non ci sono soltanto applicazioni di livello Enterprise, ovviamente molto costose, per analizzare i dati disponibili, ma esistono applicativi *free* o *open source* come **Microsoft Power BI** o **Qlik View** che permettono di integrare dati provenienti da diverse fonti (database SQL di software gestionali, fogli Excel, Database Access, ecc.) e di generare report e *dashboard* interattive con grafici e tabelle di dati molto utili per capire come sta andando l'azienda. Naturalmente bisogna saperli usare e conoscere come sono archiviati i dati nei Server (e spesso nei Client) dell'organizzazione.

Dall'altro lato molte PMI italiane **non hanno certo i Big Data** nei loro sistemi, ma forse neanche quei pochi dati organizzati da poterli analizzare. Questa carenza deriva dalla scarsa diffusione di sistemi informativi integrati nella PMI: quante (troppe) volte in azienda vi è un gestionale con il quale viene gestita la contabilità, gli ordini cliente e gli ordini di acquisto, poi ci sono fogli Excel per la programmazione della produzione, i controlli qualità vengono registrati su carta o su altri sistemi non integrati, le offerte non finiscono tutte nel gestionale, la rintracciabilità è gestita con moduli manuali e così via? Alla fine di tutto il **sistema qualità** richiede alcuni indicatori per il cui calcolo vengono impiegati tempo e risorse eccessive. Ne consegue che molti pensano che la qualità sia una perdita di tempo…

Oggi mediante i nuovi incentivi del Governo – con il super e iper-ammortamento per investimenti in **Industria 4.0** – molte PMI hanno l'opportunità di investire anche in strumenti di Business Intelligence che almeno renderanno più efficiente lo

svolgimento di alcune attività inerenti il **sistema qualità ISO 9001** ed il **controllo di gestione**, ma che se ben sfruttati possono essere integrati in altri sistemi (ad es. CRM) e potranno fornire molte informazioni agli imprenditori per rendere sempre più competitiva la propria azienda.

Effetti della Brexit sulla PMI

Ormai la Brexit, ovvero l'uscita della Gran Bretagna dalla UE, è ormai fatto certo, anche se i tempi non saranno immediati. Analizziamo, dunque, quali potranno essere gli effetti di questo avvenimento, oserei dire storico, sull'industria italiana che intrattiene rapporti commerciali diretti o indiretti con l'industria britannica.

In particolare, numerose imprese italiane hanno acquisito, soprattutto negli ultimi anni, alcuni clienti del Regno Unito, magari grazie ai **prezzi particolarmente competitivi**, grazie al cambio favorevole per la Sterlina nei confronti dell'Euro.

Ora, però, la Gran Bretagna sta per uscire dall'Unione Europea e si paventano nuovi ostacoli al commercio fra Europa dell'Unione e Regno Unito. Al momento non ci è dato sapere quali e quanti nuovi problemi sorgeranno negli scambi commerciali con la Gran Bretagna, in quanto le regole sono da riscrivere e ciò porterà via un po' di tempo.

Di certo c'è il consistente **calo della quotazione della Sterlina Britannica nei confronti dell'Euro** e ciò se da un lato favorisce il turismo e in generale i viaggi ed i soggiorni di lavoro verso la Gran Bretagna, dall'altro rende meno competitivi i prodotti italiani nei confronti dell'industria britannica. L'effetto si potrà avere non solo per clienti diretti inglesi, ma anche per la fornitura di prodotti a clienti che, a loro volta, forniscono imprese britanniche.

Perdere un 10% nel prezzo percepito dal cliente per un prodotto o per una commessa non è cosa di poco conto! Il cliente potrebbe rivalutare fornitori britannici a discapito dell'attuale fornitore italiano.

Per questo, al fine di **non perdere il cliente**, occorre che le imprese italiane che riforniscono – direttamente o indirettamente – clienti inglesi cerchino di mantenere la propria competitività non abbassando i prezzi per sopperire alla diminuzione di valore della Sterlina, ma puntando su **qualità del prodotto e del servizio**, oltre che sull'organizzazione interna, cercando di **rendere i propri processi più efficienti**.

Questo potrebbe essere ottenuto introducendo innovazioni nel processo produttivo, nella progettazione (ove presente) e nei processi di supporto, attraverso il miglioramento delle competenze del personale ed il ricorso a **sistemi informativi più moderni e performanti**, e perché no, ricorrendo anche ad **innovazioni tecnologiche** che rientrano nella sfera della cosiddetta "Industry 4.0".

Ottenere la certificazione ISO 9001 per chi non la possiede oppure migrare il sistema qualità alla ISO 9001:20015 sfruttando le opportunità di miglioramento fornite dalla nuova norma, o magari – per chi opera nel settore automotive – cercare di ottenere la certificazione ISO/TS 16949: queste sono alcune strade da percorrere per cercare di essere più competitivi ed apparire "più forti" nei confronti del cliente britannico che ha fatto della qualità il suo modus operandi ormai da decenni. E se per caso volesse venirci a visitare per fare un audit fornitore (si veda anche l'articolo "Il cliente straniero viene a fare un audit: che fare?") potremmo mostrare le capacità, l'organizzazione e l'affidabilità della nostra azienda.

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

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

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

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

Rispetto al precedente articolo pubblicato su questo sito il 27/04/2016, basato sulla traduzione della proposta di Regolamento approvata dal Parlamento Europeo a

dicembre 2015, di cui il presente articolo costituisce un aggiornamento, si rilevano alcune differenze nella traduzione del testo originale inglese in lingua italiana, rispetto all'attuale Codice privacy D.Lgs 196/2003:

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

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

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

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

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

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

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

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

- Viene regolamentato solo il trattamento di dati personali di persone fisiche (non giuridiche) per scopi diversi dall'uso personale.
- Resta una distinzione fra trattamento di dati personali comuni e trattamento di dati c.d. sensibili, anche se la definizione del D.lgs 196/2003 non viene utilizzata nel Regolamento UE 679, lasciando però la possibilità agli Stati membri di stabilire una disciplina particolare in merito.
- Restano gli obblighi di informare l'interessato sull'uso che verrà fatto dei suoi dati personali.
- Restano gli obblighi di ottenere il consenso per i trattamenti non necessari o per i trattamenti di particolari tipi di dati, ad esempio quelli idonei a rivelare lo stato di salute delle persone, le origini razziali, le idee religiose, ecc.

Tra gli elementi che cambiano vi sono sicuramente:

- La denominazione ed i ruoli degli attori: il titolare del trattamento rimane tale, **il responsabile del trattamento è ora responsabile in solido con il titolare per i danni derivanti da un trattamento non corretto**, l'incaricato rimane il soggetto che fisicamente tratta i dati, ma tale ruolo non è delegabile, se non attraverso uno specifico accordo contrattuale. Il responsabile può individuare un proprio rappresentante.
- I dati personali trattati devono essere protetti con misure organizzative e tecniche adeguate a garantirne la riservatezza e l'integrità.
- I diritti dell'interessato sono più ampi e maggiormente tutelati.
- Il responsabile del trattamento deve mettere in atto **misure tecniche ed organizzative** tali da consentirgli di dimostrare che tratta i dati personali in conformità al Regolamento. Tali misure devono seguire lo stato dell'arte e devono derivare dall'analisi dei rischi che incombono sui dati, secondo relativa gravità e probabilità.
- **Privacy by default**: devono essere trattati "per default" solo i dati necessari a perseguire le finalità del trattamento posto in essere dal responsabile dello stesso, ovvero non devono essere trattati dati in eccesso senza che una persona

fisica autorizzata lo consenta.

- **Privacy by design**: ogni nuovo trattamento di dati personali dovrà essere progettato in modo da garantire la sicurezza richiesta in base ai rischi a cui è sottoposto prima di essere implementato. Anche i sistemi informatici dovranno essere progettati secondo tale principio.
- Possono esserci più responsabili per un medesimo trattamento che risulteranno, pertanto, corresponsabili di eventuali trattamenti non conformi, ma dovranno stabilire congiuntamente le rispettive responsabilità.
- Le imprese **con sede al di fuori dell'Unione Europea**, che trattano dati personali di interessati residenti nella UE dovranno eleggere una propria organizzazione o entità all'interno della UE che sarà responsabile di tali trattamenti.
- Devono essere mantenuti **registri dei trattamenti** di dati effettuati con le informazioni pertinenti e le relative responsabilità. Tali registri non sono obbligatori per organizzazioni con meno di 250 dipendenti salvo che non trattino dati sensibili (secondo la definizione del Codice della Privacy attualmente in vigore) o giudiziari. Tale discriminante potrà essere meglio specificata da appositi provvedimenti del nostro Garante.
- Il responsabile del trattamento deve notificare all'autorità competente – e, in casi gravi, anche all'interessato – ogni **violazione dei dati** (*data breach*) trattati entro 72 ore dall'evento.
- Quando un trattamento presenta dei rischi elevati per i dati personali degli interessati (i casi specifici dovranno essere esplicitati dall'Autorità Garante), il responsabile del trattamento deve effettuare una **valutazione di impatto preventiva**, prima di iniziare il trattamento.
- Viene introdotta la **certificazione** del sistema di gestione della privacy (le cui modalità dovranno essere meglio definite tramite gli Organismi di Accreditamento Europei, ACCREDIA per l'Italia)..
- È richiesta la designazione di un **Responsabile della Protezione dei Dati** (*Data Protection Officer*) nelle Aziende Pubbliche e nelle organizzazioni che trattano dati sensibili o giudiziari su larga scala oppure che la tipologia di dati trattati e la loro finalità richieda il controllo degli incaricati al trattamento su larga scala.

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

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

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

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

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

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

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

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

Ora la privacy sarà meno materia per avvocati – se non per la stesura di contratti

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

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

Il "cookie" non è un biscotto

In questi giorni entra in vigore un provvedimento del Garante Privacy (si veda http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884) relativo alla necessità di informare gli utenti di ogni sito web il cui proprietario risiede in Italia – ed a raccogliere il relativo consenso in determinati casi – dell'utilizzo dei c.d. cookies da parte del sito stesso.

Il termine per l'adeguamento dei siti web è un anno dalla pubblicazione in Gazzetta Ufficiale del suddetto provvedimento, avvenuta il 03/06/2014.

Si ricorda che l'uso dei cookie rientra tra i trattamenti soggetti all'obbligo di notificazione al Garante ai sensi dell'art. 37, comma 1, lett. d), del Codice, laddove lo stesso sia finalizzato a "*definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti*", ma da tale obbligo sono esclusi – sulla base di quanto previsto dal provvedimento del Garante del 31 marzo 2004, che ha inserito espressamente, tra i trattamenti esonerati dal suindicato obbligo – quelli "*relativi all'utilizzo di marcatori elettronici o di*

dispositivi analoghi installati, oppure memorizzati temporaneamente, e non persistenti, presso l'apparecchiatura terminale di un utente, consistenti nella sola trasmissione di identificativi di sessione in conformità alla disciplina applicabile, all'esclusivo fine di agevolare l'accesso ai contenuti di un sito Internet".

Da ciò, pertanto, emerge che, mentre i **cookie di profilazione**, i quali hanno caratteristiche di permanenza nel tempo, **sono soggetti all'obbligo di notificazione**, i cookie che invece hanno finalità diverse e che rientrano nella categoria dei **cookie tecnici**, ai quali sono assimilabili anche i ***cookie analytics***, **non debbono essere notificati al Garante**.

Resta però l'obbligo di **informativa breve**, tramite *banner* nella *home page* del sito e in altre pagine, oltre che di **informativa estesa** facilmente reperibile nel sito stesso, anche tramite apposito link nel banner suddetto, relativamente all'uso dei cookie fatto dal sito web stesso.

Il mancato rispetto di tale provvedimento può comportare una sanzione da 6.000 a 36.000 euro e questo sta spaventando molto le organizzazioni che dispongono di un sito web, anche se con l'utilizzo di cookie minimale, spesso solo per raccogliere statistiche aggregate sulla consultazione del proprio sito. Questo non tanto perché è l'unico elemento di apparente non conformità al Codice della Privacy in molte organizzazioni, se non altro perché è un provvedimento recente, ma perché – a differenza di altri requisiti privacy per i quali sono previsti meccanismi sanzionatori equivalenti – in questo caso i tecnici dell'Ufficio del Garante Privacy possono verificare la presenza e la correttezza dell'informativa via internet, stando comodamente seduti alle loro scrivanie.

Dunque le imprese, **buona parte delle quali presentano altri aspetti di non conformità alla privacy**, non temono la poco probabile (viste anche le statistiche delle ispezioni effettuate nell'ultimo anno) ispezione del Nucleo Privacy della Guardia di Finanza, ma la più agevole verifica a campione sul proprio sito internet, disponibile pubblicamente e teoricamente soggetto anche a segnalazioni al Garante da parte di terzi senza troppa fatica.

In realtà i c.d. cookie di profilazione ("*I cookie di profilazione sono volti a creare profili relativi all'utente e vengono utilizzati al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dallo stesso nell'ambito della navigazione in rete*") sono quelli più insidiosi, sui quali il Garante richiede azioni di maggior tutela da parte dei gestori dei siti web (obbligo di informativa con consenso, notifica, ecc.), ma solo pochi siti ne fanno realmente uso.

Il problema, però, sta nella gestione inappropriata della privacy da parte di molte PMI, che non hanno il pieno controllo dei loro siti web (solo sito pubblicitario, vengono raccolte statistiche sulla consultazione, viene realizzato un servizio di e-commerce?).

Si tenga presente che è facile trovare risorse nel web (ad es. http://www.whois.com/whois/) in grado di scoprire a chi appartiene un determinato dominio, con tanto di ragione sociale o nome e cognome di una persona fisica. Così molti legittimi proprietari hanno demandato a società esterne la gestione del proprio sito, in alcuni casi abbandonandolo al suo destino, dimenticando, però, che ne restano responsabili di fronte alla legge.

Dunque non sapere "cosa fa il proprio sito web" è un rischio non trascurabile e può comportare responsabilità legali, oltre al fatto che è uno strumento di comunicazione e di marketing importantissimo che spesso andrebbe gestito meglio.

Maggiori informazioni su questi cookie, per evitare che diventino biscotti indigesti, si possono trovare in questo video https://www.youtube.com/watch?v=Mut-YXSExnw&feature=youtu.be

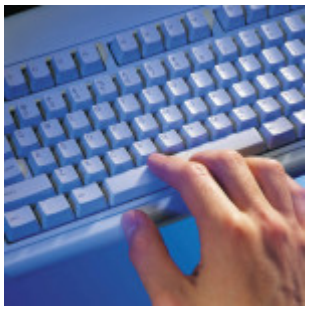
Ed a questi link

http://www.garanteprivacy.it/cookie

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167231

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2142939

La nuova edizione della norma ISO 27002 (seconda parte)



In questo articolo (cfr. precedente articolo) passiamo ad esaminare la seconda parte della norma La norma UNI CEI ISO/IEC 27002:2014 – *Raccolta di prassi sui controlli per la sicurezza delle informazioni* (che sostituisce la ISO 27002:2005).

12 Sicurezza delle attività operative

Questa area comprende ben 7 categorie:

- **Procedure operative e responsabilità (12.1)**: devono essere predisposte procedure per documentare lo svolgimento di una serie di attività inerenti la sicurezza,

occorre gestire i cambiamenti all'organizzazione e la capacità delle risorse (di *storage*, di banda, infrastrutturali ed anche umane), infine è necessario mantenere separati gli ambienti di sviluppo da quelli di produzione.

- **Protezione dal malware (12.2)**: un solo controllo in questa categoria (protezione dal malware) che prescrive tutte le misure di sicurezza da attuare contro il malware. Non solo antivirus per prevenire ed eliminare malware, ma anche azioni di prevenzione tecnica e comportamentali (consapevolezza degli utenti).
- **Backup (12.3)**: devono essere documentate ed attuate procedure di backup adeguate a garantire il ripristino dei dati in caso di perdita dell'integrità degli stessi e la continuità operativa (vedasi anche punto 17).
- **Raccolta di log e monitoraggio (12.4)**: devono essere registrati, conservati e protetti i log delle attività degli utenti normali e di quelli privilegiati (si ricorda che per apposita disposizione del Garante Privacy italiano i log degli accessi in qualità di Amministratore di Sistema devono essere mantenuti in modo "indelebile" per almeno 6 mesi), occorre inoltre mantenere sincronizzati gli orologi dei sistemi con una fonte attendibile.
- **Controllo del software di produzione (12.5)**: particolari attenzioni devono essere adottate nell'installazione ed aggiornamento del software di produzione (non solo per organizzazioni del settore ICT, banche o assicurazioni, ma anche per aziende manifatturiere!).
- **Gestione delle vulnerabilità tecniche (12.6)**: viene fornita dalla norma un'ampia guida attuativa sulla gestione delle vulnerabilità tecniche conosciute (occorre mantenere un censimento dell'hardware e del relativo software installato su ogni elaboratore, installare le *patch* di sicurezza in modo tempestivo, mantenersi aggiornati sulle vulnerabilità di sicurezza conosciute, ecc.), oltre alle indicazioni sulla limitazione nell'installazione dei software (è opportuno, infatti, ridurre al minimo la possibilità per gli utenti di installare applicativi software autonomamente, anche se leciti come le utility gratuite che, a volte, possono essere il veicolo di *adware* o altre minacce alla sicurezza).
- **Considerazioni sull'audit dei sistemi informativi (12.7)**: gli audit sui sistemi informativi dovrebbero avere un impatto ridotto sulle attività lavorative e le evidenze raccolte dovrebbero essere raccolte senza alterare i dati dei sistemi (accessi in sola lettura) e dovrebbero essere mantenute protette.

Questi elementi nella precedente versione della norma erano in gran parte all'interno della sezione 10 "*Communications and Operations Management*" (ma la gestione delle vulnerabilità tecniche era, invece, al paragrafo 12.6, per puro caso lo stesso della versione attuale della norma), il quale comprendeva anche i controlli del punto 13 seguente.

13 Sicurezza delle comunicazioni

Questa sezione contiene due sole categorie:

- **Gestione della sicurezza della rete (13.1)**: occorre adottare alcuni accorgimenti

per garantire la sicurezza delle reti interne (responsabilità, autenticazioni, ecc.); viene anche citata la ISO/IEC 27033 nelle sue parti da 1 a 5 sulla sicurezza delle reti e delle comunicazioni per ulteriori informazioni. Deve, inoltre, essere gestita la sicurezza dei servizi di rete, compresi i servizi acquistati presso fornitori esterni, e la segregazione delle reti (separazione delle VLan, gestione delle connessioni Wi-Fi, …).

- **Trasferimento delle informazioni (13.2)**: occorre stabilire ed attuare politiche e procedure per il trasferimento delle informazioni con qualsiasi mezzo (posta elettronica, fax, telefono, scaricamento da internet, ecc.), nel trasferimento di informazioni con soggetti esterni occorre stabilire accordi sulle modalità di trasmissione, le informazioni trasmesse tramite messaggistica elettronica dovrebbero essere adeguatamente controllate e protette (non solo e-mail, ma anche sistemi EDI, *instant messages*, *social network*, ecc.) e, infine, occorre stabilire e riesaminare periodicamente accordi di riservatezza e di non divulgazione con le parti interessate.

I 7 controlli di quest'area sono sicuramente molto dettagliati e migliorano, oltre ad aggiornare, la precedente versione della norma, includendo controlli (un po' sparsi nella versione 2005 della ISO 27002) che recepiscono le nuove modalità di comunicazione, tra cui i social network, professionali e non.

14 Acquisizione, sviluppo e manutenzione dei sistemi

Quest'area tratta la sicurezza dei sistemi informativi impiegati per le attività aziendali e comprende tre categorie:

- **Requisiti di sicurezza dei sistemi informativi (14.1)**: la sicurezza dei sistemi informativi- acquistati o sviluppati ad hoc – deve essere stabilita fin dall'analisi dei requisiti, deve essere garantita la sicurezza dei servizi applicativi che viaggiano su reti pubbliche (ad esempio attraverso trasmissioni ed autenticazioni sicure crittografate), infine occorre garantire la sicurezza delle transazioni dei servizi applicativi.
- **Sicurezza nei processi di sviluppo e supporto (14.2)**: devono essere definite ed attuate politiche per lo sviluppo (interno o esterno all'organizzazione) sicuro dei programmi applicativi, devono essere tenuti sotto controllo tutti i cambiamenti ai sistemi (dagli aggiornamenti dei sistemi operativi alle modifiche dei sistemi gestionali), occorre effettuare un riesame tecnico sul funzionamento degli applicativi critici a fronte di cambiamenti delle piattaforme operative (sistemi di produzione, database, ecc.) e si dovrebbero limitare le modifiche (personalizzazioni) ai pacchetti software, cercando comunque di garantirne i futuri aggiornamenti. Inoltre dovrebbero essere stabiliti, documentati ed attuati principi per l'ingegnerizzazione sicura dei sistemi informatici e per l'impiego di ambienti di sviluppo sicuri. Nel caso in cui attività di sviluppo software fossero commissionate all'esterno, dovrebbero essere stabilite misure per il controllo del processo di sviluppo esternalizzato. Infine dovrebbero essere eseguiti test di sicurezza dei sistemi durante lo sviluppo e test di

accettazione nell'ambiente operativo di utilizzo, prima di rilasciare il software.
- **Dati di test (14.3)**: i dati utilizzati per il test dovrebbero essere scelti evitando di introdurre dati personali ed adottando adeguate misure di protezione, anche al fine di garantirne la riservatezza.

Nel complesso i 13 controlli di questa sezione sono molto dettagliati e comprendono una serie di misure di sicurezza informatica ormai consolidate che riguardano tutti gli aspetti del ciclo di vita del software impiegato da un'organizzazione per la propria attività. Alcuni principi vanno commisurati ad una attenta valutazione dei rischi, poiché una stessa regola di sicurezza informatica (ad es. l'aggiornamento sistematico e tempestivo del software di base) potrebbe non garantire sempre l'integrità e la disponibilità dei sistemi (ad es. errori o malfunzionamenti introdotti dagli ultimi aggiornamenti di un sistema operativo).

15 Relazioni con i fornitori

Questo punto di controllo tratta tutti gli aspetti di sicurezza delle informazioni che possono legati al comportamento dei fornitori. Sono state individuate due categorie:

- **Sicurezza delle informazioni nelle relazioni con i fornitori (15.1)**: è necessario stabilire una politica ed accordi su tematiche inerenti la sicurezza delle informazioni con i fornitori che accedono agli asset dell'organizzazione; tali accordi devono comprendere requisiti per affrontare i rischi relativi alla sicurezza associati a prodotti e servizi nella filiera di fornitura dell'ICT (cloud computing compreso).
- **Gestione dell'erogazione dei servizi dei fornitori (15.2):** occorre monitorare – anche attraverso audit se necessario – e riesaminare periodicamente le attività dei fornitori che influenzano la sicurezza delle informazioni, nonché tenere sotto controllo tutti i cambiamenti legati alle forniture di servizi.

16 Gestione degli incidenti relativi alla sicurezza delle informazioni

L'area relativa agli incidenti sulla sicurezza delle informazioni (sezione 13 della precedente versione della norma) comprende una sola categoria (erano 2 nella precedente edizione):

- **Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti (16.1)**: devono essere rilevati e gestiti tutti gli incidenti relativi alla sicurezza delle informazioni (viene qui richiamata la ISO/IEC 27035 – *Information security incident management*), ma anche rilevate ed esaminate tutte le segnalazioni di eventi relativi alla sicurezza che potrebbero indurre a pensare che qualche controllo è risultato inefficace senza provocare un vero e proprio incidente e pure tutte le possibili debolezze dei controlli messi in atto. In ogni caso ogni evento relativo alla sicurezza delle informazioni va attentamente valutato per eventualmente classificarlo come

incidente vero e proprio o meno. Occorre poi rispondere ad ogni incidente relativo alla sicurezza delle informazioni in modo adeguato ed apprendere da quanto accaduto per evitare che l'incidente si ripeta. Infine dovrebbero essere stabilite procedure per la raccolta di evidenze relative agli incidenti e la successiva gestione (considerando anche eventuali azioni di analisi forense).

17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa

In quest'area (corrispondente al punto 14 sella precedente versione della norma) viene trattata la ***business continuity*** in 5 controlli suddivisi in due categorie:

- **Continuità della sicurezza delle informazioni (17.1)**: la continuità operativa per la sicurezza delle informazioni dovrebbe essere pianificata a partire dai requisiti per la business continuity, piani di continuità operativa (*business continuity plan*) dovrebbero essere attuati, verificati e riesaminati periodicamente.
- **Ridondanze (17.2)**: per garantire la disponibilità (e la continuità operativa) occorre prevedere architetture e infrastrutture con adeguata ridondanza.

Naturalmente sull'argomento esiste la norma specifica UNI EN ISO 22301:2014 – *Sicurezza della società – Sistemi di gestione della continuità operativa – Requisiti.*

18 Conformità

Questo ultimo punto di controllo (era il punto 15 nella ISO 27002:2005) tratta la gestione della cosiddetta "*compliance*", ovvero la conformità a leggi, regolamenti ed accordi contrattuali con i clienti. Sono identificate due categorie:

- **Conformità ai requisiti cogenti e contrattuali (18.1)**: occorre innanzitutto identificare i requisiti cogenti, quindi attuare controlli per evitare di ledere i diritti di proprietà intellettuale, proteggere adeguatamente le registrazioni che permettono di dimostrare la conformità a tutti i requisiti cogenti, in particolare devono essere rispettati leggi e regolamenti sulla privacy (in Italia il D.Lgs 196/2003 in attesa del nuovo Regolamento Europeo, ma nella norma viene citata come riferimento la ISO/IEC 29100:2011 "*Information technology – Security techniques – Privacy framework*"). Infine occorre considerare eventuali limitazioni all'uso dei controlli crittografici vigenti in alcune nazioni.
- **Riesami della sicurezza delle informazioni (18.2)**: dovrebbe essere svolto periodicamente un riesame indipendente sulla sicurezza delle informazioni dell'organizzazione, i processi di elaborazione delle informazioni e le procedure dovrebbero essere riesaminate periodicamente per valutarne la continua conformità ed adeguatezza alla politica ed alle norme ed infine dovrebbero essere eseguite delle verifiche tecniche della conformità dei sistemi informativi a politiche e standard di sicurezza (ad esempio *penetration test* e *vulnerability assessment*). Su quest'ultimo controllo si fa riferimento alla

ISO/IEC TR 27008 — *Guidelines for auditors on information security management systems controls*.