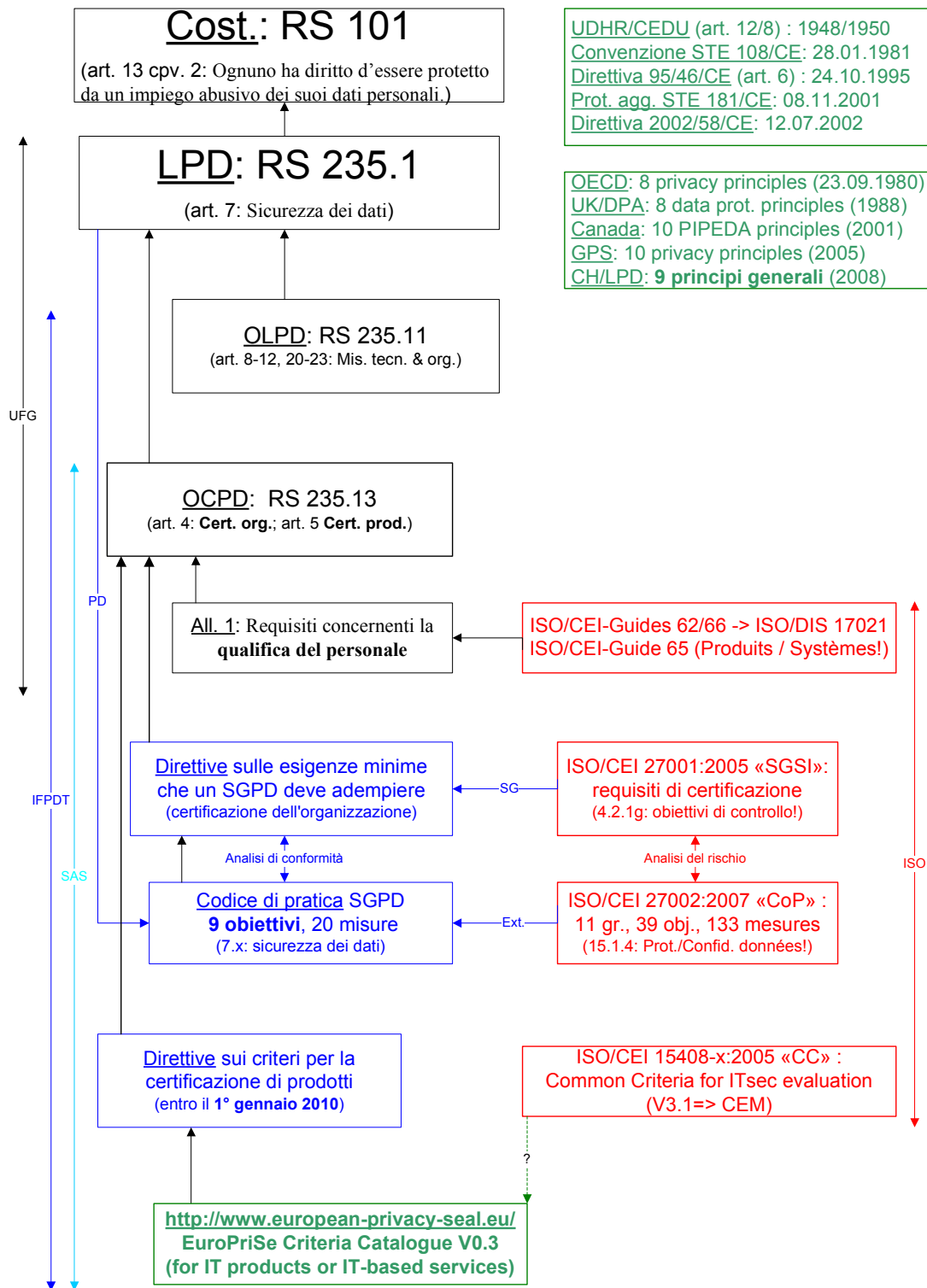




Commento esplicativo alle «direttive sulle esigenze minime che un sistema di gestione della protezione dei dati deve adempiere»

Le «direttive sulle esigenze minime che un sistema di gestione della protezione dei dati deve adempiere» concretizzano la delega dell'ordinanza sulle certificazioni in materia di protezione dei dati (art. 4 cpv. 3 OCPD; RS 235.13), che rinvia alle norme internazionali su installazione, gestione, monitoraggio e miglioramento di sistemi di gestione, in particolare alle norme ISO 9001:2000 e 27001:2005. Nel mettere a disposizione uno strumento già conosciuto ed utilizzato dagli specialisti, l'IFPDT si è basato sui requisiti dei sistemi di gestione concentrandosi sulla protezione dei dati piuttosto che sulla sicurezza dell'informazione.

Per fornire un quadro della situazione può essere utile posizionare queste direttive nell'ordinamento giuridico svizzero, a fianco dei fondamenti europei sulla protezione dei dati e delle corrispondenti norme ISO, senza dimenticare che l'IFPDT deve emanare le «direttive sui criteri specifici in materia di protezione dei dati da esaminare nell'ambito della certificazione di un prodotto» (art. 5 cpv. 3 OCPD) entro il 1° gennaio 2010:



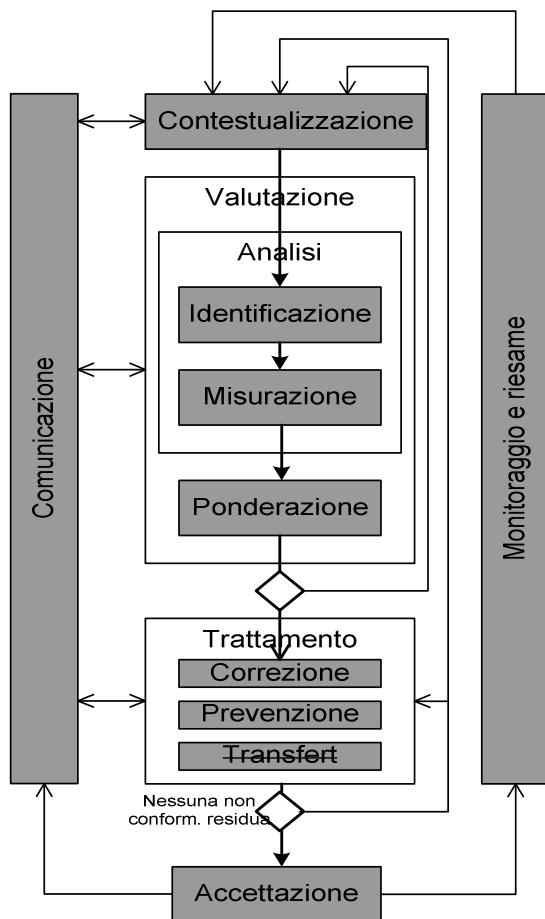
Per prima cosa si è trattato di riprendere dall'ISO 27001 i requisiti generici dei sistemi di gestione, a loro volta tratti dall'ISO 9001 per la gestione della qualità, come riportato nell'appendice informativa C dell'ISO 27001. L'importanza data alla protezione dei dati è sottolineata da un'analisi di non conformità che completa l'analisi dei rischi e in particolare dall'interpretazione di determinate clausole relative all'elaborazione e alla documentazione del sistema di gestione della protezione dei dati (SGPD).

La principale difficoltà è consistita nel porre l'accento sulla protezione dei dati piuttosto che sulla mera sicurezza dell'informazione. Fortunatamente l'art. 7, che riguarda le esigenze di sicurezza dei dati stabilite nella LPD, permette di considerare la protezione dei dati un obiettivo che ingloba quello della

sicurezza dell'informazione indicato nell'ISO 27001. Dunque si intende definire un sistema di gestione della protezione dei dati che prescriva tra l'altro una *politica del SGPD*, una *selezione di misure per il trattamento delle non conformità*, una *dichiarazione di applicabilità* delle misure realizzate con una spiegazione della ragione dell'esclusione di altre, un *piano di trattamento delle non conformità*, un *controllo/revisione delle violazioni alla protezione dei dati o degli eventuali incidenti e misure di correzione o prevenzione per migliorare il SGPD*.

Uno dei nodi di questa impostazione risiede nella procedura di gestione dei rischi su cui sono basate l'installazione e la gestione di un SGSI (sistema di gestione della sicurezza dell'informazione). Se una gestione dei rischi di questo tipo ben si adegua ad obiettivi volontari di sicurezza dell'informazione, non soddisfa però le esigenze legali della protezione dei dati. Un SGPD deve perciò assolutamente associare la gestione della conformità alla gestione dei rischi che a sua volta deve essere mantenuta per ragioni di sicurezza dei dati (cfr. principio/obiettivo/articolo 7).

In concreto, un metodo di **valutazione di non conformità** consiste in un'**analisi** di non conformità (individuazione delle fonti e misurazione della non conformità), cui segue una **ponderazione** di non conformità che in genere porta a due risultati: non conformità minore o maggiore. Si tratta quindi di passare al **trattamento** delle non conformità, cioè di porvi **rimedio (correzione)** adottando misure appropriate o di **evitarle (prevenzione)** rinunciando ad esempio al trattamento in questione, visto che non è possibile trasferire né accettare una non conformità (nessuna non conformità residua)!

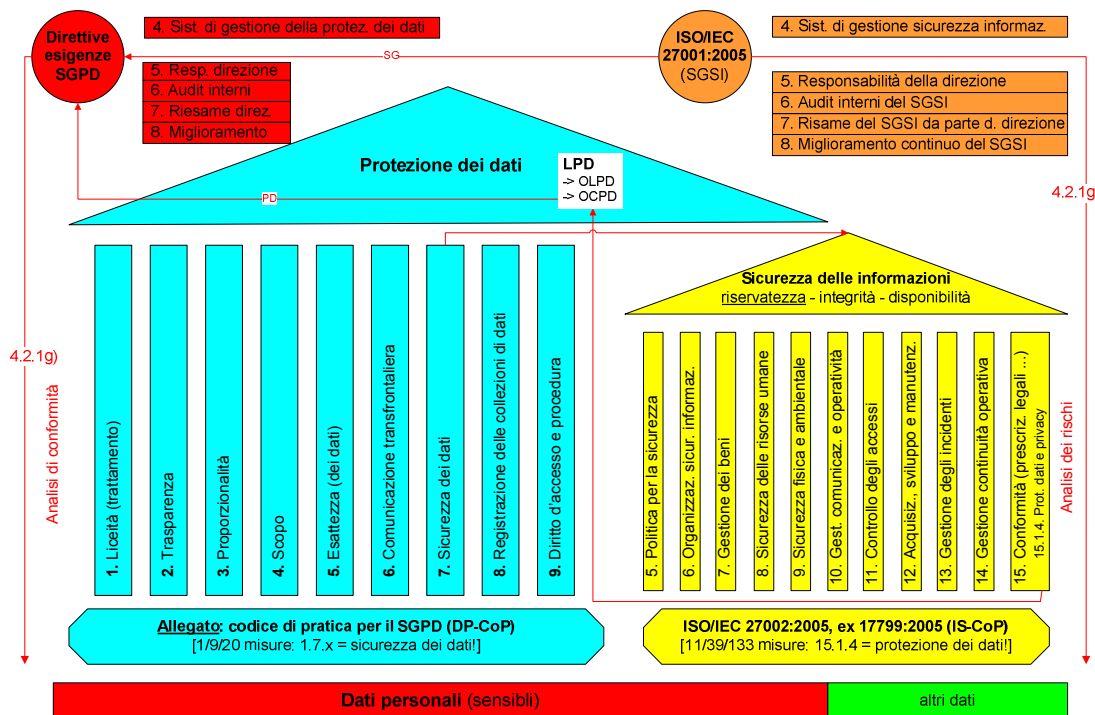


In un secondo momento, si è trattato di sostituire l'appendice normativa A dell'ISO 27001, costituita dall'indice della norma ISO/CEI 27002:2005, più conosciuta come «codice di pratica per la gestione della sicurezza dell'informazione», che comprende 15 capitoli, di cui gli ultimi 11 formano «gruppi di controllo» suddivisi in 39 «obiettivi di controllo» per un totale di 133 «misure di controllo» relative alla sicurezza dell'informazione. L'**importanza data alla protezione dei dati** è accennata solo alla misura 15.1.4 «protezione dei dati e privacy delle informazioni personali» che in sostanza prevede che «la protezione dei dati e la privacy devono essere assicurate, come richiesto nella legislazione, nei regolamenti e, se applicabili, nelle clausole contrattuali pertinenti». Nell'ottica della certificazione di un'organizzazione o di una procedura concernente la protezione dei dati, la misura 15.1.4, formulata in modo molto generale, deve essere precisata e suddivisa in obiettivi realizzabili con misure concrete

di protezione dei dati.

Questo fine viene raggiunto con il «**codice di pratica per la gestione della protezione dei dati**» i cui obiettivi e misure figurano sinteticamente al punto 5 delle «**Direttive sulle esigenze minime che un sistema di gestione della protezione dei dati deve adempiere**» e sono riportate integralmente nel relativo allegato. In altre parole, il «codice di pratica per la gestione della protezione dei dati» rappresenta per le direttive SGPD quello che la norma ISO 27002 rappresenta per la norma ISO 27001.

Seguendo l'esempio dell'OCSE e di altri Paesi quali l'Australia, il Canada e la Gran Bretagna, abbiamo ritenuto i «**9 principi generali della legge sulla protezione dei dati**» come obiettivi essenziali del «codice di pratica per la gestione della protezione dei dati». Attualmente questi obiettivi vengono attuati con 20 misure concrete di protezione dei dati che riassumono in maniera non esaustiva i principali requisiti di cui nella legge e nella relativa ordinanza. Al fine di facilitare la lettura e la comprensione dell'appendice, ogni misura è strutturata secondo lo standard ISO 27002 (misura, applicazione ed altre informazioni). Allo stesso modo in cui la misura 15.1.4 rinvia i SGSI ai SGPD, bisogna sottolineare che il 7° obiettivo «Sicurezza dei dati» con le relative misure rappresenta il rinvio dei SGPD ai SGSI. Tra le 133 misure dell'ISO 27002 sono dunque state scelte le più pertinenti per la sicurezza dei dati nell'ottica della protezione dei dati.



Ovviamente non è possibile imporre una certificazione SGSI al fine di ottenerne una certificazione SGPD. Perciò l'organo certificante deve valutare e decidere caso per caso il livello di riconoscimento della certificazione SGSI preesistente, in particolare per quel che riguarda i requisiti di «sicurezza dei dati». Se si tratta di un accreditamento del SAS, invece, è molto probabile che l'accREDITAMENTO SGPD sia previsto come estensione di quello SGSI (ISO 27001), dato lo stretto ed esplicito nesso con i requisiti di questa norma.

Per gli operatori interessati (accreditamento, certificazione, certificati, audit, controlli etc.), è necessario sottolineare che l'attuale stretto nesso con le norme internazionali ISO 27001 e 27002 si rivela sensato e proficuo, dato l'elevato grado di riconoscimento e diffusione sul mercato mondiale nonché il prezioso apporto terminologico, strutturale e sistematico. Il contesto normativo è già, o lo sarà presto, ampliato da guide supplementari quali l'ISO 27003 sull'implementazione di un SGSI, l'ISO 27004 su metrica e misurazione, l'ISO 27005 sulla gestione dei rischi, l'ISO 27006 sui requisiti per l'accREDITAMENTO e l'ISO 27007 sugli audit per i SGSI, cui si potrà fare riferimento per i SGPD.