Esperto in Data Protection System – Requisiti di competenza

STA.604

Il presente standard si prefigge lo scopo di definire i requisiti relativi all'attività professionale dell'Esperto in Data Protection System, ovvero la figura professionale esperta nel supportare il Responsabile per la protezione dei dati personali (Data Protection Officer) e/o il Manager Privacy nel mettere a punto le idonee misure tecniche e organizzative ai fini del trattamento dei dati personali.

TESTO ITALIANO

00	26/06/2018	Emissione	RQCP	RCP
Revisione	**Data**	**Motivazione**	**Preparato da**	**Approvato da**

INDICE

1. SCOPO E CAMPO DI APPLICAZIONE

Lo standard definisce i requisiti relativi alla professione di **Esperto in Data Protection System** (abbreviato EDP). La figura è il primo livello del profilo di Professionista nel Trattamento e nella Protezione Dati Personali e corrisponde al livello 4 nel sistema EQF – *European Qualifications Framework* (Figura 1).

Figura 1

L'Esperto in Data Protection System è una risorsa le cui competenze permettono di operare per migliorare il sistema di gestione per la sicurezza delle informazioni, in collaborazione con il manager privacy e con la direzione. La figura è in grado di guidare e informare enti pubblici e privati ad uniformarsi al Regolamento Europeo e alle altre disposizioni relative alla protezione dei dati. È inoltre in possesso di tutti gli strumenti professionali e trasversali per verificare che la nuova normativa e le policy delle aziende siano correttamente attuate ed applicate dai committenti.

L'Esperto in Data Protection System è un professionista che possiede un'adeguata conoscenza della nuova normativa Europea e delle prassi di gestione/protezione/trattamento dei dati personali nazionali e europei, in grado di adempiere alle proprie funzioni in piena indipendenza e in assenza di conflitti di interesse operando come dipendente, oppure come lavoratore autonomo e che cooperi con l'autorità di controllo, che informi e consigli chi gestisce il trattamento dei dati sulle eventuali criticità e sulle possibili azioni di miglioramento.

L'EDP cura la corretta attuazione del trattamento dati personali, è la figura che svolge le attività operative che si rendono progressivamente necessarie durante tutto il ciclo di vita di un trattamento di dati personali collaborando con una figura manageriale (quale, per esempio, il manager privacy competente). È un professionista che svolge il suo lavoro in tutti gli ambiti in cui vengono trattati dati di persone fisiche, partecipando alla verifica, alla creazione e al mantenimento di un sistema di gestione e tutela dei dati in base alle necessità dello specifico contesto. La professione può essere svolta sia in un rapporto di collaborazione come dipendente che in termini di lavoro autonomo, collocandosi presso Imprese, Enti pubblici o privati o Pubbliche Amministrazioni.

L'EDP può essere occupato ad esempio come:

- Responsabile della protezione dei dati
- Referente privacy
- Consulente privacy

Le attività dell'EDP vengono identificate in termini di competenza, a partire da compiti e attività specifiche, in conformità al Quadro Europeo delle Qualifiche (EQF). Una competenza esprime la

capacità di compiere una serie di processi che trasformano un input in un preciso output. Compiti e attività sono espressi in modo da facilitare i processi di valutazione delle competenze.

2. RIFERIMENTI NORMATIVI E DOCUMENTI APPLICABILI

Il presente standard rimanda a disposizioni contenute in altre pubblicazioni. Tali riferimenti normativi sono di seguito elencati.

- UNI 11506 Attività professionali non regolamentate - Figure professionali operanti nel settore ICT - Requisiti per la valutazione e certificazione delle conoscenze, abilità e competenze per i profili professionali ICT basati sul modello e-CF
- 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
- UNI 11621-2 Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 2: Profili professionali di "seconda generazione
- UNI EN 16234-1 e-Competence Framework (e-CF) - Framework comune europeo per i professionisti ICT in tutti i settori industriali - Parte 1: Framework (modello di riferimento)
- UNI CEI EN ISO/IEC 17024 Valutazione della conformità - Requisiti generali per organismi che eseguono la certificazione di persone
- UNI CEI EN ISO/IEC 27000 Tecnologie informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione - Descrizione e vocabolario
- UNI CEI EN ISO/IEC 29100 Tecnologie informatiche - Tecniche per la sicurezza - Quadro di riferimento per la privacy

In altri casi si rimanda ai seguenti riferimenti legislativi:

- Regolamento UE 2016/679 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)
- Decreto Legislativo 30/06/2003 n.196 "Codice in materia di Protezione dei Dati Personali"
- Linee Guida dell'European Data Protection Board (WP29)
- Linee Guida e Provvedimenti del Garante della Protezione dei Dati Personali

3. TERMINI E DEFINIZIONI

Ai fini del presente standard si applicano i seguenti termini e definizioni.

3.1 Qualifica: risultato formale di un processo di valutazione e convalida, acquisito quando un'organizzazione competente stabilisce che i risultati dell'apprendimento di una persona corrispondono a norme tecniche definite.
Nota 1 Definizione adattata del EQF, Allegato I, definizione a).

3.2 Risultati dell'apprendimento: descrizione di ciò che una persona conosce, capisce ed è in grado di fare al termine di un processo di apprendimento.

3.3 Valutazione dei risultati dell'apprendimento: metodi e processi utilizzati per definire la misura in cui una persona ha effettivamente conseguito una particolare conoscenza, abilità o competenza.

3.4 Competenza: comprovata capacità di utilizzare conoscenze, abilità e capacità personali in situazioni di lavoro o di studio e nello sviluppo professionale e personale, esercitabile con un determinato grado di autonomia e responsabilità.
Nota 1 Definizione adattata del EQF, Allegato I, definizione i).

3.5 Conoscenza: risultato dell'assimilazione di informazioni attraverso l'apprendimento. Le conoscenze possono essere teoriche o pratiche.

Nota 1 Definizione adattata dell'EQF, Allegato I, definizione g).

3.6 Abilità: capacità di applicare conoscenze per portare a termine compiti e risolvere problemi. Nota 1 Definizione adattata del EQF, Allegato I, definizione h).

3.7 Esperto in Data Protection System (EDP): figura professionale esperta nel supportare il Responsabile per la protezione dei dati personali (Data Protection Officer) e/o il Manager Privacy nel mettere a punto le idonee misure tecniche e organizzative ai fini del trattamento dei dati personali.

3.8 Sistema di Gestione della Sicurezza Informatica: consiste nel complesso delle attività gestite in maniera sistematica da un'organizzazione allo scopo di proteggere la sicurezza delle sue informazioni e degli asset che le contengono.

3.9 Indicatori: elementi che definiscono la modalità e i criteri in cui le evidenze (oggetti di osservazione) vengono valutate. Sono scritti sotto forma di sostantivo e consentono di cogliere, attraverso i relativi descrittori, il grado di padronanza di un soggetto in relazione ad una specifica competenza. Ogni indicatore deve avere un peso adeguato alla sua importanza relativa alla competenza complessiva.

3.10 Descrittori: elementi che definiscono il livello degli indicatori, da basilare a eccellente. In base al tipo dell'indicatore, i descrittori possono essere espressi con un semplice "sì" o "no", (presenza o assenza dell'evidenza), oppure possono specificare nel dettaglio qual è il livello atteso per ogni evidenza.

3.11 Oggetto dell'osservazione: processi/risultati che devono essere osservati, verificati, misurati e valutati. Può trattarsi di un prodotto finale o della performance richiesta per produrre un risultato atteso. Gli indicatori variano di conseguenza.

4. COMPITI E ATTIVITÀ SPECIFICHE DELLA FIGURA PROFESSIONALE

I compiti specifici dell'attività dell'Esperto in Data Protection System sono riferiti alle competenze. Nel presente Standard le competenze vengono definite e valutate da un punto di vista procedurale (input-output).

Il presente Standard è uno schema composto da elementi connessi uno con l'altro come parti costitutive di un sistema. Tali elementi permettono di descrivere e definire il grado in cui un professionista possiede le competenze richieste, descritte come insieme di attività complesse che richiedono l'uso di elementi appresi, procedure, metodi e standard. Tali attività vengono descritte come processi seguendo una grammatica precisa, che permette di coprire ciascuno degli aspetti citati. La struttura complessiva seguita nella descrizione dell'EDP e è la seguente (Figura 2):

1. Definizione dell'input ("Partendo da…")
2. Descrizione dell'azione tramite verbo ("La persona…")
3. Individuazione degli oggetti da utilizzare ("Utilizzando…")
4. Individuazione di procedure, metodi, standard da utilizzare ("Applicando…")
5. Definizione dell'output ("Al fine di ottenere…")

INPUT	a.Partendo da + complemento oggetto	Competenze e compiti richiesti al professionista. Vengono riportati sotto forma di locuzioni
ATTIVITA' COMPLESSE	b.Il professionista + verbo c. Utilizzando + complemento oggetto (saperi, strumenti…) d. Applicando + complemento oggetto (procedure, standard, metodi…)	
OUTPUT	e. Al fine di ottenere + oggetto	

Figura 2

Le conoscenze e abilità sono parte integrante di ciascuna fase, nelle colonne "Utilizzando/applicando".

Le **attività (competenze)** del processo lavorativo dell'EDP sono:

1. Verificare un sistema di gestione privacy
2. Implementare un sistema di gestione privacy
3. Aggiornare un sistema di gestione privacy

Suoi **compiti** durante le fasi sopra esposte sono di seguito esposte (Figura 3):

FASE	INPUT	OUTPUT	ATTRAVERSO	UTILIZZANDO /APPLICANDO
1) Verificare un sistema di gestione privacy	Richiesta del cliente	Gap Analysis	Check list di domande per identificare i punti critici	Tecniche di audit; I metodi per analizzare le informazioni non strutturate e i processi di business
Mappare il flusso di dati	Gap Analysis	Mappa del flusso di dati	Utilizzo di tecniche di presentazione dei dati per tracciare la mappa dei dati in ingresso, in uscita e degli asset che li contengono	Conoscenza della normativa; I metodi per analizzare le informazioni non strutturate e i processi di business
Controllare esaustività e conformità dei documenti esistenti	Mappa del flusso di dati	Elenco di non conformità documentali	Seguire e controllare l'uso effettivo degli standard documentativi aziendali, evidenziarne le carenze e i punti critici	Norme di legge in materia di trattamento e protezione dei dati personali con particolare riguardo alle disposizioni di rango primario e secondario (regolamenti, provvedimenti, autorizzazioni, linee-guida e standard settoriali, altro) relative agli specifici ambiti di operatività
Valutare le criticità del reparto IT	Mappa del flusso di dati	Elenco delle criticità degli asset del reparto IT	Analizzare gli asset tecnologici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi	Conoscenza degli impatti tecnologici sulla protezione dei dati; Conoscenza delle reti informatiche e di telecomunicazione; Conoscenza delle specifiche funzionali di un sistema informativo
2) Implementare un sistema di gestione privacy	Elenco delle criticità e non conformità	Sistema di gestione privacy adeguato alla normativa	Implementazione delle best practice e gli standard nella gestione della sicurezza delle informazioni	Comprendere gli elementi guida del business che impattano i componenti dell'architettura (dati, applicazioni, sicurezza, sviluppo, etc)
Redigere un registro dei trattamenti	Elenco delle criticità	Registro dei trattamenti	Gli strumenti per la produzione, l'editing e la distribuzione di documenti professionali per	Conoscenza delle possibili minacce alla sicurezza;

			elencare i trattamenti in atto	
Condurre una valutazione d'impatto	Registro dei trattamenti	DPIA (Data Protection Impact Assessment)	Le metodologie di valutazione d'impatto sulla protezione dei dati e le procedure per creare una PIA	Le possibili minacce alla protezione dei dati personali; Le metodologie di valutazione d'impatto sulla protezione dei dati e PIA
Creare un piano di contenimento del rischio relativo alla sicurezza delle informazioni	DPIA (Data Protection Impact Assessment)	Documenti e sistemi adeguati alla normativa	Costruire un piano di gestione del rischio per fornire e produrre piani di azione preventivi	Conoscenze sui diritti degli interessati previsti da leggi e regolamenti; Applicare gli standard, le best practice e i requisiti legali più rilevanti all'information security
Creare politiche di contenimento del rischio	Documenti e sistemi adeguati alla normativa	Politiche di contenimento dei rischi	Applicare gli standard, le best practice e i requisiti legali più rilevanti all'information security	Analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi; Anticipare tutte le azioni necessarie a mitigare l'impatto dei cambiamenti (formazione, documentazione, nuovi processi)
3) Aggiornare un sistema di gestione privacy	Politiche di contenimento dei rischi	Sistema di gestione privacy aggiornato	Anticipare i cambiamenti richiesti alla strategia aziendale dell'information security e formulare nuovi piani	Seguire e controllare l'uso effettivo degli standard documentativi aziendali; Stabilire una comunicazione sistematica e frequente con clienti, utenti e stakeholder

Figura 3

5. CONOSCENZE, ABILITÀ E COMPETENZE RELATIVE ALL'ATTIVITÀ PROFESSIONALE

A partire dall'idea che la competenza esprime la capacità di compiere una serie di processi che trasformano un input in un preciso output, utilizzando conoscenze, abilità e capacità personali nella specifica situazione di lavoro, sono state identificate le competenze (e quindi conoscenze e abilità applicate) necessarie alla figura dell'EDP.

5.1 Conoscenze

L'Esperto in Data Protection System deve possedere le seguenti conoscenze:

- Conoscenza delle norme di legge italiane ed europee in materia di trattamento e protezione dei dati personali
- Conoscenza delle possibili minacce alla sicurezza
- I metodi per analizzare le informazioni non strutturate e i processi di business
- Comprensione dei processi aziendali
- Le strutture del database e l'organizzazione dei suoi contenuti
- Conoscenza delle responsabilità connesse al trattamento dei dati personali
- Conoscenza degli impatti tecnologici sulla protezione dei dati;
- Conoscenza delle reti informatiche e di telecomunicazione;
- Le metodologie di valutazione d'impatto sulla protezione dei dati e PIA
- Le possibili minacce alla protezione dei dati personali
- Conoscenze sui diritti degli interessati previsti da leggi e regolamenti

5.2 Abilità

L'Esperto in Data Protection System deve essere in grado di:

- Raccogliere la conoscenza interna ed esterna e i fabbisogni di informazione
- Seguire e controllare l'uso effettivo degli standard documentativi aziendali
- Analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi
- Rilevare punti critici e non conformità
- Analizzare il flusso di dati in ingresso e in uscita
- Verificare l'adeguatezza e la completezza dei documenti
- Analizzare le infrastrutture e la loro gestione
- Produrre i documenti, le politiche e le procedure necessarie all'adeguamento
- Elencare i trattamenti esistenti
- Esaminare le fonti del rischio connesso ai trattamenti
- Produrre documenti e sistemi per la gestione della sicurezza dei dati
- Individuare azioni di contenimento del rischio e dell'emergenza
- Aggiornare le procedure, le policy e i sistemi di gestione privacy

6. ELEMENTI PER LA VALUTAZIONE

6.1 Requisiti di accesso per l'Esperto in Data Protection System

Il Richiedente deve dare evidenza dei seguenti requisiti:

- Possesso di diploma di scuola media superiore (EQF IV) o laurea breve (EQF VI) preferibilmente a carattere giuridico, informatico o tecnico.
- Partecipazione ad un percorso formativo di almeno 400 ore nell'ambito della protezione dei dati personali che includa un tirocinio formativo della durata di almeno 200 ore in attività di tutela e gestione dei sistemi per la sicurezza delle informazioni o, in alternativa, esperienza professionale almeno biennale in attività di tutela e gestione dei sistemi per la sicurezza delle informazioni.

6.2 Valutazione delle competenze

Per la valutazione delle competenze oggetto del presente standard è necessario tener presente che vanno seguiti determinati passaggi, a partire dalla descrizione delle competenze così come esposte in Figura 2. Il primo è quello di identificare l'oggetto di osservazione, ovvero cosa deve osservare l'esaminatore per capire se il processo è svolto dal professionista correttamente oppure no; il secondo è definire gli indicatori che permettono di valutare in maniera oggettiva l'evidenza definita, e quindi i relativi descrittori.

Il processo seguito dal presente standard per la valutazione delle competenze dell'EDP è riassunto nella seguente tabella (Figura 4).

• INDICATORI	Sostantivo che descrive i criteri per raccogliere l'evidenza
• PESO DELL'INDICATORE	Da 1 a 5
• DESCRITTORI	In una scala da 1 a 5, dove 1 è NO e 5 è SI, si descrive in che misura il professionista compie il compito richiesto
• OGGETTO DELL'OSSERVAZIONE	Due possibili categorie: di processo (performance) o di prodotto (risultato del compito complessivo)
• RISULTATO OTTENUTO	Punteggio massimo; Punteggio minimo;

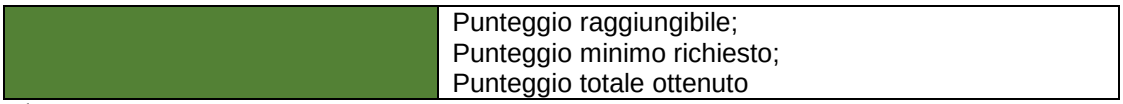

Figura 4

La valutazione delle competenze dell'EDP si basa sugli elementi definiti nella tabella che segue. Ad ogni fase dell'attività dell'EDP corrispondono degli input e degli output, a cui è associato un oggetto dell'osservazione e quindi un indicatore (Figura 5).

FASE	INPUT	OUTPUT	OGGETTO DI OSSERVAZIONE	INDICATORE	DESCRITTORE (1=no – 5=sì)
1) Verificare un sistema di gestione privacy	Richiesta del cliente	Gap Analysis	Elenco punti critici e non conformità	Rilevare	5=i punti critici e le non conformità sono stati rilevati in toto 4= i punti critici e le non conformità principali sono stati rilevati ma ne mancano alcuni 3= i punti critici e le non conformità sono presenti ma manca qualche elemento principale 2=mancano alcuni punti critici e non conformità principali 1=sono completamente assenti i punti critici e le non conformità principali
Mappare il flusso di dati	Gap Analysis	Mappa del flusso di dati	Il flusso di dati in ingresso e in uscita	Analizzare	5= la mappa è completa e contiene tutto il flusso di dati 4= la mappa è quasi completa ma manca qualche dettaglio 3= la mappa è poco dettagliata ma vengono individuati gli elementi principali 2= mancano alcuni elementi chiave del flusso di dati 1= mancano totalmente gli elementi del flusso di dati
Controllare esaustività e conformità dei documenti esistenti	Mappa del flusso di dati	Elenco di non conformità documentali	L'adeguatezza e la completezza dei documenti	Verificare	5= l'elenco rileva tutte le non conformità documentali 4= l'elenco rileva quasi tutte le non conformità documentali 3= l'elenco rileva le principali non conformità documentali 2= l'elenco manca di alcune non conformità fondamentali 1= mancano totalmente le non conformità richieste
Valutare le criticità del reparto IT	Mappa del flusso di dati	Elenco delle criticità degli asset del reparto IT	Le infrastrutture e la loro gestione	Analizzare	5= l'elenco rileva tutte le criticità del reparto IT 4= l'elenco rileva quasi tutte le criticità del reparto IT 3= l'elenco rileva le principali criticità del reparto IT 2= l'elenco manca di alcune criticità fondamentali 1= mancano totalmente le criticità richieste
2) Implementare un sistema di gestione privacy	Elenco delle criticità e non conformità	Sistema di gestione privacy adeguato alla normativa	I documenti e le politiche/procedure necessarie all'adeguamento	Produrre	5= i documenti principali sono tutti presenti e tutti completi 4=i documenti principali sono tutti presenti ma parzialmente completati 3= mancano alcuni dei documenti principali e sono parzialmente completati

					2= sono presenti solo alcuni documenti principali e alcuni non sono completi 1= mancano i documenti principali e non sono completi
Redigere un registro dei trattamenti	Elenco delle criticità	Registro dei Trattamenti	I trattamenti esistenti	Elencare	5=il registro contiene tutti gli elementi essenziali ed è completo 4= il registro contiene tutti gli elementi essenziali ma manca qualche trattamento 3=il registro contiene parte degli elementi essenziali e qualche trattamento 2= il registro manca di qualche elemento essenziale e di qualche trattamento 1= il registro manca di tutti gli elementi essenziali e della maggior parte dei trattamenti
Condurre una valutazione d'impatto	Registro dei Trattamenti	DPIA (Data Protection Impact Assessment)	Le fonti del Rischio connesso ai trattamenti	Esaminare	5=la DPIA è completa e sono esaminati tutti gli elementi connessi al rischio 4= la DPIA contiene tutti gli elementi essenziali ma manca qualche trattamento 3= la DPIA contiene parte degli elementi essenziali e qualche trattamento 2= la DPIA manca di qualche elemento essenziale e di qualche trattamento 1= la DPIA manca di tutti gli elementi essenziali e della maggior parte dei trattamenti
Creare piano di contenimento del rischio relativo alla sicurezza delle informazioni	DPIA (Data Protection Impact Assessment)	Documenti e sistemi adeguati alla normativa	Documenti e sistemi di gestione	Produrre	5=i documenti sono tutti presenti e contengono le informazioni necessarie 4= i documenti principali sono presenti e contengono le informazioni necessarie 3= i documenti sono parzialmente presenti e contengono le informazioni principali 2= mancano alcuni dei documenti principali e alcune delle informazioni principali 1= mancano tutti i documenti principali e le informazioni sono frammentate
Creare politiche di contenimento del rischio	Documenti e sistemi adeguati alla normativa	Politiche di contenimento dei rischi	Azioni di contenimento del rischio e dell'emergenza	Individuare	5=sono state indicate tutte le azioni di contenimento del rischio e dell'emergenza 4= le azioni principali dii contenimento del rischio e dell'emergenza sono state indicate 3= le azioni principali di contenimento sono state parzialmente indicate 2=non sono state adottate alcune delle principali azioni di contenimento 1=non è stata adottata nessuna delle azioni di contenimento
3) Aggiornare un sistema di gestione privacy	Politiche di contenimento dei rischi	Sistema di gestione privacy aggiornato	Le procedure, le policy e i sistemi	Aggiornare	5=sono state aggiornate tutte le procedure, le policy e i sistemi 4= sono state aggiornate le procedure, le policy e i sistemi principali

					3= sono state aggiornate alcune delle procedure, policy e sistemi principali 2= sono state aggiornate alcune procedure, policy e sistemi 1=non sono state aggiornate le procedure, policy e sistemi

Figura 5

La valutazione de professionisti avverrà utilizzando le seguenti metodologie:

1. Valutazione dei prerequisiti:
    a) Titolo di studio conseguito dal Richiedente, che deve essere non inferiore a diploma di istruzione secondaria superiore, rilasciato a seguito di un corso di durata quinquennale oppure quadriennale integrato dal corso annuale previsto per legge o da un titolo estero dichiarato equipollente.
    b) Curriculum Vitae e dei documenti allegati, comprovanti le attività formative e lavorative specifiche dichiarate dal Richiedente.
2. Prova scritta teorica con domande a risposta chiusa. Per ogni domanda vengono proposte tre risposte, delle quali una sola è corretta. Le opzioni errate danno punteggio negativo.
3. Prova scritta pratica: analisi e/o sviluppo di un tema o di un caso di studio per verificare l'applicazione di singole competenze in ambiti specifici relativi alla data protection e riguardanti la verifica, l'implementazione e l'aggiornamento dei sistemi di protezione dei dati.

Per il **mantenimento triennale** della Certificazione i professionisti devono fornire le seguenti evidenze:

- Pagamento della quota per il mantenimento, come da tariffario presente sul sito web TÜV Thüringen Italia.
- Evidenza oggettiva degli interventi eseguiti nell'ambito dell'esperienza specifica di lavoro per la quale si richiede la Certificazione di competenza: evidenze di svolgimento di attività lavorativa in ambito di conduzione o supporto agli audit, attività in ambito di verifica, gestione e aggiornamento dei sistemi di protezione dei dati, attività di docenza su tematiche attinenti o equivalenti.
- Copia di almeno un attestato di frequenza a corsi/seminari di formazione e di aggiornamento su tematiche attinenti allo Schema di Certificazione di interesse (EDP), pari ad almeno 16 ore annue.

Per il **rinnovo** della Certificazione ogni **sei anni** i professionisti devono versare la quota per il rinnovo e sostenere una prova scritta.

6.3 Organizzazione che effettua la valutazione

L'organizzazione che effettua la valutazione delle competenze deve:

- Possedere requisiti di indipendenza, imparzialità, trasparenza, assenza di conflitto d'interesse e competenza.
- Assicurare omogeneità delle valutazioni.
- Assicurare la verifica dell'aggiornamento professionale.

Tali requisiti sono da intendersi assolti da Organismi di Certificazione delle persone operanti in conformità alla norma UNI CEI EN ISO/IEC 17024.

APPENDICE INFORMATIVA
ASPETTI ETICI, DEONTOLOGICI E COMPORTAMENTALI APPLICABILI

1. **Correttezza e moralità**
   L'attività dell'Esperto in Data Protection System deve essere svolta nel rispetto delle disposizioni di legge vigenti, dei principi di correttezza e lealtà professionale e deve uniformare la propria condotta, anche nella vita privata, a principi di dignità e decoro.
   L'Esperto in Data Protection System rifiuta di accettare incarichi per i quali ritenga di non possedere adeguata preparazione, e/o quelli per cui ritenga di non avere adeguata potenzialità organizzativa/professionale per l'adempimento dell'incarico proposto, fatto salvo che, al fine di gestire alcuni aspetti dell'incarico, coinvolga appropriate figure professionali (previa autorizzazione del committente).

2. **Aggiornamento professionale continuo**
   L'Esperto in Data Protection System deve costantemente aggiornare la propria formazione professionale al fine di migliorare la qualità del servizio reso alla committenza.

3. **Indipendenza, infedeltà, incompatibilità**
   L'Esperto in Data Protection System è tenuto ad esercitare la professione garantendo assoluta indipendenza e assoluta imparzialità nell'esecuzione del mandato.
   L'Esperto in Data Protection System è tenuto a rifiutare incarichi qualora si verifichino situazioni di incompatibilità.

4. **Rapporti con il committente**
   I rapporti con il committente devono essere improntati a principi di massima chiarezza, lealtà e correttezza.
   L'Esperto in Data Protection System è tenuto ad accettare un incarico esclusivamente se possiede la certezza di poterlo svolgere e portare a termine con scienza, coscienza e diligenza, avendo costante cura di tutelare sempre l'interesse del proprio committente. In relazione a ciò, L'Esperto in Data Protection System deve costantemente tenere aggiornato il committente sull'evoluzione del proprio incarico, concordando con esso ogni decisione importante.
   L'Esperto in Data Protection System System deve definire chiaramente e preventivamente con il committente contenuti e termini dell'incarico professionale.
   L'Esperto in Data Protection System è tenuto a informare il committente circa tutti i potenziali casi di conflitto di interesse, ovvero nelle circostanze in cui l'attività prevista possa ingenerare sospetti di violazione delle disposizioni etico-deontologiche contenute nel presente codice di condotta.

5. **Rapporti con i colleghi**
   Ciascuno Esperto in Data Protection System ha il dovere di improntare i rapporti con coloro che hanno correlazione con la professione di Esperto nell'organizzazione e gestione di eventi Finanziati alla massima lealtà e correttezza professionale.

6. **Pubblicità**
   L'Esperto in Data Protection System ha la facoltà di diffondere la pubblicità del servizio che svolge, a mezzo stampa o per via telematica, purché questa sia improntata al buon gusto e purché non sia ingannevole.