REGOLAMENTO SPECIFICO PER LA CERTIFICAZIONE DELL'ESPERTO IN DATA PROTECTION SYSTEM

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

Sommario

1. SCOPO E CAMPO DI APPLICAZIONE 3
2. RIFERIMENTI NORMATIVI E DOCUMENTI APPLICABILI 3
3. TERMINI, DEFINZIONI E ACRONIMI 4
4. COMPITI, ATTIVITÀ E REQUISITI DELLA FIGURA PROFESSIONALE DELL'ESPERTO IN DATA PROTECTION SYSTEM 4
5. PAGAMENTO DELLE QUOTE 7
6. DOMANDA DI CERTIFICAZIONE 7
7. ANALISI DOCUMENTALE E ACCETTAZIONE DEL CANDIDATO 8
8. CONDUZIONE DELL'ESAME 8
8.1 Commissione d'esame 8
8.2 Struttura dell'esame 9
8.2.1 Prova teorica 9
8.2.2 Prova pratica 10
8.2.3 Valutazione complessiva delle prove e delibera 10
9. RILASCIO DEL CERTIFICATO 11
10. MANTENIMENTO E RINNOVO DEL CERTIFICATO 11
10.1 Mantenimento e sorveglianza 11
10.2 Rinnovo 12
11. CODICE ETICO E DEONTOLOGICO 12
12. RIESAME DELLO SCHEMA DI CERTIFICAZIONE 13

1. SCOPO E CAMPO DI APPLICAZIONE

Lo scopo del presente documento è di descrivere le responsabilità, le attività e le modalità operative adottate da TÜV Thüringen Italia per l'attività di valutazione e Certificazione della figura professionale dell'**Esperto in Data Protection System (EDP)**, in conformità con la norma UNI CEI EN ISO/IEC 17024:2012 e lo Standard TÜV Thüringen Italia STA.604 - Esperto in Data Protection System– Requisiti di competenza.

Il presente Regolamento Specifico si applica ai processi di Certificazione delle competenze per lo Schema 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, e ne definisce:

- I requisiti
- Il processo di Certificazione (modalità di esecuzione dell'esame e di rilascio del Certificato)
- Modalità e prassi per il mantenimento e il rinnovo della Certificazione

Per ulteriori informazioni riguardo i requisiti degli Schemi di Certificazione vedere RG.01- Regolamento Generale per la Certificazione di Persone del TÜV Thüringen Italia, presente sul sito web TTI.

2. RIFERIMENTI NORMATIVI E DOCUMENTI APPLICABILI

- **UNI CEI EN ISO/IEC 17024: 2012**- Valutazione della conformità - Requisiti generali per organismi che eseguono la certificazione di persone.
- **CEN Guide 14** - Linee guida di indirizzo per le attività di normazione sulla qualificazione delle professioni.
- **STA.604** - Esperto in Data Protection System – Requisiti di competenza.
- **Reg (CE) n. 765/2008** del Parlamento Europeo e del Consiglio del 09/07/2008 che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che regola e abroga il regolamento (CEE) n.339/93.
- **RG.601**- Regolamento Generale per la Certificazione di Persone del TÜV Thüringen Italia.
- **MGQ.600 -** Manuale del Sistema di Certificazione delle Competenze di TÜV Thüringen Italia, secondo la norma ISO/IEC 17024: 2012.
- **L. 14/01/2013 n° 4** - Disposizioni in materia di professioni non organizzate.
- **L. 03/02/1989 n. 39** e successive modifiche ed integrazioni.
- **Decreto del Presidente della Repubblica 07/08/2012 n. 137** – Regolamento recante riforma degli ordinamenti professionali, a norma dell'articolo 3, comma 5, del decreto- legge 13/08/2011 n. 138 convertito con modificazioni dalla legge 14/09/2011 n. 148.
- **D.Lgs 16/01/2013 N° 13** - Definizione delle norme generali e dei livelli essenziali delle prestazioni per l'individuazione e validazione degli apprendimenti non formali e informali e degli standard minimi di servizio del sistema nazionale di certificazione delle competenze, a norma dell'articolo 4, commi 58 e 68, della legge 28 giugno 2012, n. 92.
- **Decreto del Ministero della Giustizia 08/02/2013 n. 34** – Regolamento in materia di società per l'esercizio di attività professionali regolamentate nel sistema ordinistico, ai sensi dell'articolo

10, comma 10, della legge 12/11/2011 n.183.

- **L. 28/06/2012, n. 92**, comma 59 et al.
- **L. 28/06/2012, n. 92**, comma 59 et al.
- 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, DEFINZIONI E ACRONIMI

Le definizioni cui si fa riferimento nel presente Regolamento sono mutuate dalla norma ISO/IEC 17024:2012 e dallo Standard STA.601 - Tecnico per la Pianificazione di Progetti Finanziati – Requisiti di competenza.

Acronimi:

- **TTI** – TÜV Thüringen Italia;
- **EDP** - Esperto in Data Protection System
- **AUN** – Amministratori TTI;
- **SCP**– Sistema di Certificazione delle Competenze di TTI;
- **RCP** – Responsabile Certificazione delle Persone;
- **RS** – Responsabile di Schema;
- **CTS** – Comitato Tecnico Scientifico;
- **COE** – Commissione d'Esame;
- **CdE** – Centro d'Esame;
- **SOGE** – Sistema Online per la Gestione degli Esami.

4. COMPITI, ATTIVITÀ E REQUISITI DELLA FIGURA PROFESSIONALE DELL'ESPERTO IN DATA PROTECTION SYSTEM

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'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.

Le competenze ed abilità richieste alla figura professionale del EDP, necessarie allo svolgimento della propria professione vengono definite e valutate da un punto di vista procedurale (input-output).

Le **fasi** sequenziali 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:

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	Conoscenza delle possibili minacce alla sicurezza;

			documenti professionali per 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

I **requisiti di base** di cui deve essere in possesso l'EDP sono i seguenti:

- 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.

Per quanto riguarda le **conoscenze**, l'EDP deve possedere le seguenti:

- 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

Le **abilità** richieste all'EDP sono di seguito descritte:

- 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

5. PAGAMENTO DELLE QUOTE

Le tariffe relative al processo di Certificazione, sorveglianza e rinnovo sono riportate sul sito web di TTI o disponibili su richiesta specifica. Le tariffe devono essere versate nei tempi e nelle modalità di seguito previste:

- **Richiesta di iscrizione, esame documentale e partecipazione all'esame** – entro 10 giorni lavorativi precedenti alla data dell'esame per cui si richiede l'iscrizione.
- **(Ove prevista) Emissione Certificato ed iscrizione Registri** – entro e non oltre 10 giorni dall'avvenuta comunicazione del superamento dell'esame.

Eventuali variazioni del tariffario sono prontamente comunicate agli Iscritti al Registro di pertinenza. Sarà AMZ a gestire il pagamento delle quote.
In caso di ritiro del Richiedente dall'iter certificativo, per gravi motivi scritti non imputabili a TÜV Thüringen Italia, verrà/verranno restituita/e solo la/e quota/e inerenti le fasi dell'iter non ancora svolte.

6. DOMANDA DI CERTIFICAZIONE

Il Richiedente deve effettuare l'iscrizione al processo di Certificazione di TTI accedendo al SOGE, al link **certificazione.tuv-thuringen.it**, creando un account personale ed iscrivendosi alla categoria "Espero nell'organizzazione e gestione di eventi" selezionando la sessione di suo interesse.
Successivamente è tenuto a:

- Versare la prima quota e caricare **copia della contabile** nel SOGE nella sezione "Pagamento tariffa di iscrizione".
- Fornire la documentazione ai fini dell'analisi documentale.

1. **Domanda di Certificazione** firmata e datata;
2. **Copia del Titolo di Studio** (diploma di studi di secondo grado livello EQF4);
3. **Copia di un Documento di Identità** (fronte e retro);
4. **Curriculum Vitae**, firmato dal Richiedente e datato;
5. **Attestato di 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.

La documentazione va caricata nella propria pagina personale sulla piattaforma online (SOGE) e deve contenere esclusivamente documenti non modificabili (PDF, .jpg o .png, documenti scannerizzati, ecc.) di dimensione massima di 32MB per documento e deve seguire le indicazioni per rinominare i documenti.

La validità delle fasi della Certificazione fino al superamento dell'esame è di **6 mesi** dalla data di inizio del processo di Certificazione, che coincide con la data di firma della domanda di Certificazione. Qualora non porti a termine il processo di Certificazione (ovvero non ottenga il Certificato), decorsi i sei mesi il Candidato dovrà presentare nuovamente la domanda di Certificazione e svolgere nuovamente tutte le fasi del processo di Certificazione.

7. ANALISI DOCUMENTALE E ACCETTAZIONE DEL CANDIDATO

La documentazione inviata dal Richiedente viene sottoposta alla disamina della COE, o del RS, allo scopo di verificare il soddisfacimento dei prerequisiti applicabili (vedere per dettagli il Regolamento Generale - RG.601).
A seguito dell'analisi documentale da parte della COE il RS effettua il riesame di tutta la documentazione del Richiedente e, qualora l'esito sia positivo, delibera l'accettazione del Richiedente come Candidato all'esame. La delibera viene notificata al Candidato via posta elettronica o attraverso il SOGE, da parte del RS. In occasione della comunicazione dell'esito dell'analisi documentale, il RS comunica le istruzioni per l'esame.

8. CONDUZIONE DELL'ESAME

Le informazioni riguardanti il calendario e la sede di svolgimento della prova d'esame sono indicate nel documento "Calendario Esami", presente nel sito web TTI. Si garantisce la comunicazione al Candidato della sede d'esame con un anticipo necessario per consentire di organizzarsi, prepararsi e recarsi presso la sede d'esame. TTI provvede ad accertarsi che per ogni Candidato esistano le condizioni di accessibilità alla sede stabilita per la sessione d'esame. Nel caso vengano segnalate particolari necessità da parte dei Candidati, TTI provvede a trovare una soluzione e a comunicare tale soluzione al Candidato, telefonicamente o via posta elettronica.

8.1 Commissione d'esame

La COE qualificata è selezionata dal RCP e ne possono fare parte:

- Tecnici Esperti del settore del Data Protection System, qualificati da TTI. La competenza tecnica degli Tecnici Esperti deve essere dimostrata tramite il possesso dei requisiti specificati nella procedura POI.609 – Commissioni d'esame. Nel caso di Commissari d'esame qualificati secondo il criterio di consolidata attività nel settore dell'organizzazione e gestione di eventi, al Candidato Commissario viene richiesta evidenza di almeno 10 anni di attività all'interno dei progetti europei. Ai Commissari viene inoltre richiesta evidenza di almeno 3 anni nel settore della valutazione e/o certificazione delle competenze.
- Una figura proveniente dalle Parti Interessate allo Schema di Certificazione, in qualità di potenziale datore di lavoro dei Candidati da certificare.
- Il RS, o persona delegata dal RCP come sorvegliante d'esame. In tal caso, l'attività del sorvegliante e l'andamento dell'esame devono essere supervisionati dal RS in collegamento via teleconferenza.

La COE deve dichiarare per iscritto di non avere conflitti di interesse con i Candidati da esaminare e di non essere stati loro docenti negli ultimi 2 anni.

Nel caso in cui un membro della COE rilevi durante la fase preparatoria dell'esame o nella fase iniziale della sessione d'esame l'insorgenza di un possibile conflitto di interesse con uno o più Candidati, il Commissario deve astenersi dall'esame e provvedere immediatamente a segnalarlo al RCP di TTI il quale, dopo aver analizzato gli estremi del caso, intraprenderà le azioni necessarie per rimuovere le cause del conflitto.

Analogamente, ai Candidati viene comunicata l'identità della COE prima dello svolgimento degli esami e viene chiesto loro di comunicare a TTI, nella persona del RS, qualsiasi eventuale conflitto di interesse.

La COE deve essere presente almeno mezz'ora prima dell'inizio della sessione d'esame al fine di verificare gli ambienti nel quale si svolgerà l'esame ed effettuare il riconoscimento dei Candidati. In tal modo viene garantita una ragionevole disposizione dei Candidati nella stanza prevista per lo svolgimento dell'esame, al fine di assicurare la riservatezza e la trasparente conduzione dell'esame.
I Candidati vengono disposti in modo da dare garanzia di assenza di interferenze fra loro e in modo che le prove scritte e orali possano essere svolte in totale sicurezza ed imparzialità e con la necessaria comodità.

I Candidati devono fornire alla segreteria TTI notizia di loro particolari necessità connesse allo svolgimento delle prove d'esame, in questo caso, il RCP valuta le eventuali misure di intervento.

8.2 Struttura dell'esame

L'esame deve realizzarsi con metodi adeguati a valutare il possesso delle conoscenze e delle competenze da parte del singolo Candidato e a tal scopo è costituito da:

1. Prova scritta teorica con domande a risposta chiusa. Per ogni domanda vengono proposte tre risposte, delle quali una sola è corretta. Le opzioni errate non danno punteggio negativo.
2. Prova scritta pratica: analisi e/o sviluppo di un tema o di un caso di studio.

La durata complessiva dell'esame è di quattro ore, comprendenti prova teorica e pratica. La sequenza di svolgimento delle prove può essere definita di volta in volta dalla COE.
Gli argomenti su cui vertono le prove sono quelli definiti nel paragrafo 4 del presente Regolamento Specifico.

In qualsiasi fase dell'esame è proibito utilizzare telefoni cellulari o comunque strumenti di comunicazione elettronica di qualunque tipo che, se posseduti, dovranno essere tenuti rigorosamente spenti o consegnati alla COE. Durante l'esecuzione delle prove scritte non può essere consultabile alcun documento scritto o elettronico privato. Dispositivi personali quali computer, smartphone o tablet devono essere segnalati alla COE ed è proibito il loro utilizzo.
L'inosservanza di questo punto comporta l'allontanamento dall'aula e l'annullamento della prova.

8.2.1 Prova teorica

La **prova teorica** ha lo scopo di valutare il livello di conoscenze possedute dal Candidato sul settore della organizzazione e gestione di eventi.

- La prova teorica si svolge in una sala esami attrezzata appositamente per garantire il corretto e trasparente svolgimento dell'esame e previamente verificata da auditor qualificati da TTI.
- La prova teorica viene precedentemente elaborata dal CTS sotto supervisione del RS e successivamente inserita nella banca dati online (SOGE) dal RS.
- La prova teorica viene effettuata dal Candidato utilizzando come supporto un computer fornito da TTI (o da un ente esterno che TTI ha qualificato come Centro d'Esame). Il Candidato svolge la prova che è contenuta nel SOGE, accedendo alla banca dati con i medesimi *Username* e *Password* esclusivi con cui ha effettuato l'iscrizione all'esame di Certificazione.
- La prova teorica prevede 20 domande a risposta multipla (3 opzioni di cui una sola corretta) che il SOGE seleziona in modo casuale dalla banca dati. Le domande hanno tutte lo stesso peso. Le risposte errate non danno punteggio negativo.

- Il Candidato deve evidenziare la risposta per lui corretta. Il candidato ha a disposizione 60 minuti di tempo per svolgere la prova.
- La COE, fornita di *Username* e *Password* esclusivi per l'accesso al SOGE, ha il compito di supervisionare lo svolgimento delle prove da parte dei Candidati.
- Indipendentemente dal risultato della prova teorica, il Candidato è comunque abilitato a sostenere la prova pratica. Al Candidato verrà comunicato il punteggio ottenuto, che saranno oggetto della ripetizione della prova teorica, da svolgersi entro un anno. TTI comunicherà data e luogo per la ripetizione della prova teorica.

8.2.2 Prova pratica

La **prova pratica** ha la finalità di verificare le competenze e abilità del Candidato.

- La prova pratica si svolge in una sala esami attrezzata appositamente per garantire il corretto e trasparente svolgimento dell'esame.
- Il candidato ha a disposizione 3 ore di tempo per svolgere la prova.
- La prova pratica viene precedentemente elaborata dal CTS con la supervisione del RS e successivamente inserita nella banca dati online dal RS.
- I contenuti della prova pratica vertono su concrete situazioni professionali dell'attività di data protection. Il Candidato si dovrà cimentare nell'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. Il Candidato deve dimostrare di possedere le conoscenze, le abilità e le competenze di cui al paragrafo 4 del presente Regolamento specifico, nonché di saperle adeguatamente applicare.
- La valutazione della prova pratica avviene sulla base della lista di riscontro di cui al §6.2 dello STA.604, figura 5.
- La COE ha il compito di supervisionare lo svolgimento delle prove da parte dei Candidati, forniti di *Username* e *Password* esclusivi, grazie ai quali potranno accedere alla prova pratica contenuta nel SOGE.

8.2.3 Valutazione complessiva delle prove e delibera

La valutazione della prova teorica viene effettuata automaticamente dal SOGE a fronte di una griglia di riferimento, sotto la supervisione della COE. La COE controlla l'andamento dei risultati e delle prestazioni dei Candidati durante tutto lo svolgimento dell'esame sul SOGE, tramite *Username* e *Password* personali.
La valutazione della prova pratica viene svolta dalla COE sul SOGE, valutando le prove consegnate dai Candidati a fronte della griglia di indicatori definita al §6.2 dello Standard STA.604.

La sufficienza per ognuna delle prove viene raggiunta totalizzando un punteggio uguale o superiore al **60%**.

I pesi sono i seguenti: la **prova teorica** pesa il 30%; la **prova pratica** pesa il 70% del totale.
Per ogni prova la sufficienza è:

- Prova teorica: 18/30
- Prova pratica: 42/70

L'esame s'intende superato al raggiungimento di un punteggio uguale o superiore al **60%** in ogni prova ed al **70%** del totale (prova teorica + prova pratica).

L'esito dell'esame verrà comunicato al Candidato dal RS tramite il SOGE, o via posta elettronica, entro dieci giorni lavorativi dalla data di svolgimento dell'esame. Il Candidato potrà conoscere l'esito dell'esame accedendo con *Username* e *Password* personali all'indirizzo **certificazione.tuv-thuringen**, all'interno della propria pagina.

L'**atto di delibera** viene effettuato dal RCP, coadiuvato da un esperto del settore del Data Protection

System (ALL.644).
Verificati gli esiti degli esami, nonché a fronte della previa analisi documentale e delle evidenze prodotte dal Candidato, delibera la Certificazione se ne ricorrono gli estremi, ovvero se i requisiti di Schema sono soddisfatti e l'esame di Certificazione è positivo.

Qualora il Candidato non superi l'esame di Certificazione, ovvero non ottenga il punteggio minimo uguale a 70/100, il Candidato ha la possibilità di ripetere l'esame entro tre mesi dalla data del primo esame. Il Candidato sarà tenuto a sostenere nuovamente solamente la/e prova/e d'esame relativamente alla/e competenza/e che non abbia superato. In tal caso resteranno valide le prime due fasi del processo di Certificazione (Richiesta d'iscrizione e Analisi documentale). Il Candidato è tenuto ad iscriversi nuovamente all'esame e ad effettuare il pagamento di una quota d'iscrizione all'esame come da tariffario.

9. RILASCIO DEL CERTIFICATO

Il RS renderà disponibile il Certificato, in formato digitale, nella pagina personale del Candidato sul SOGE. Contestualmente il RS inserisce i dati del professionista certificato e del relativo Certificato nei Registri online di TTI.
Il rilascio del Certificato avviene entro un mese dall'esito favorevole della delibera da parte del RCP.
La data di emissione del Certificato decorre dalla data di delibera della Certificazione.

10. MANTENIMENTO E RINNOVO DEL CERTIFICATO

La Certificazione delle competenze della figura professionale del EDP, ottenuta al termine del positivo esito dell'iter di Certificazione descritto nel presente Regolamento Specifico, ha la durata di **6 (sei) anni** a decorrere dalla data del rilascio del Certificato. La Certificazione deve pertanto essere riconvalidata allo scadere dei sei anni, al fine di riconfermare la competenza dell'EDP.

10.1 Mantenimento e sorveglianza

Al Candidato è richiesto il **mantenimento** di un elevato livello di conoscenza della materia e di abilità nella professione, tramite un processo di formazione continua specifica e qualificata.
Per il **mantenimento triennale** è necessario 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.

TTI effettua inoltre un'attività di **sorveglianza** sull'operato del professionista certificato attraverso la cogestione dei reclami, chiedendo al Valutatore Immobiliare di inoltrare a TTI gli eventuali reclami ricevuti. Si veda a riguardo il catalogo delle sanzioni previsto nel RG.01 - Regolamento Generale per la Certificazione di persone del TÜV Thüringen Italia, al paragrafo 8.

10.2 Rinnovo

In occasione del **rinnovo** il professionista dovrà fornire evidenza di avere operato nell'ottica dell'apprendimento permanente, secondo i seguenti criteri:

- Versare la quota per il rinnovo, come da tariffario presente sul sito web TÜV Thüringen Italia.
- Svolgimento di una prova pratica della durata di tre ore concernente le abilità e competenze descritte nel punto 4 del presente Schema, finalizzata inoltre a verificare il costante aggiornamento normativo del professionista certificato.

Per ulteriori informazioni riguardo i criteri per la Certificazione iniziale ed il rinnovo si veda il RG.01 - Regolamento Generale per la Certificazione di Persone del TÜV Thüringen Italia S.r.l.

11. CODICE ETICO E DEONTOLOGICO

Il EDP certificato e/o in iter di certificazione si impegna a rispettare i seguenti aspetti etici e deontologici, in linea con lo Standard TÜV Thüringen Italia STA.604 – Esperto in Data Protection System – Requisiti di competenza:

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. Il Esperto nell'organizzazione e gestione di eventi 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 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

Ciascun Esperto in Data Protection System ha il dovere di improntare i rapporti con coloro che hanno correlazione con la professione dell'Esperto in Data Protection System 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.

L'accettazione degli aspetti etici e deontologici qui sopracitati è obbligatoria ai fini del conseguimento della Certificazione.

12. RIESAME DELLO SCHEMA DI CERTIFICAZIONE

In occasione degli audit interni il RCP e il RS, congiuntamente al CTS, rivedono la documentazione di Schema per verificarne la corrispondenza alle normative, leggi, prassi professionali per garantire la validità delle specifiche professionali.
RCP e RS vigilano sull'uso delle prove d'esame garantendo adeguata varietà delle stesse, in modo da ridurre i rischi derivanti da un utilizzo ripetuto degli stessi materiali d'esame.
In funzione dei risultati degli esami e del monitoraggio periodico degli stessi, nonché in funzione di cambiamenti nella legislazione e nelle norme, è possibile rivedere la documentazione d'esame, la composizione delle prove, e i contenuti del presente Regolamento in generale anche prima della scadenza pianificata da TTI.