Rev.	Data	Motivo Revisione	Preparato da Referente Schema	Verificato da Presidente CSI/Resp. Tecnico	Approvato da A.U./ Presidente
04	03/09/2020	Inserimento modifiche ai par. 2.2, 2.3,4.3, 5.3, 5.5	R. Giannetti	V. Guzzo	D. Gilormo
03	17/04/2020	Aggiornamento alla UNI PdR 66:2019 e nuovi documenti applicabili. Modificato logo.	R. Giannetti	V. Guzzo	D. Gilormo
02	11/05/2018	Inserimento commenti di Accredia	R. Giannetti	F. Banfi	R. De Pari
01	05/03/2018	Aggiornamento alla Circolare Tecnica ACCREDIA n°03/2018 del 13/02/2018	R. Giannetti	F. Banfi	R. De Pari
00	19/01/2018	Prima emissione	R. Giannetti	F. Banfi	R. De Pari

INDICE

1. SCOPO E CAMPO DI APPLICAZIONE

1.1 Definizione dei requisiti professionali

2. DOCUMENTI

2.1 Documenti di base
2.2 Documenti applicabili
2.3 Documenti di riferimento

3. DEFINIZIONI E ACRONIMI

4. REQUISITI SPECIFICI PER LA CERTIFICAZIONE DEI PROFESSIONISTI PRIVACY

4.1 Struttura del registro AICQ SICEV
4.2 Requisiti minimi
4.3 Domanda per accedere al processo di Certificazione
4.4 Rinnovo, sorveglianza e mantenimento della Certificazione
4.4 Responsabile Gruppo di Audit
4.5 Passaggio a Lead Auditor Data Protection
4.6 Trasferimento da un differente Organismo di Certificazione

5. ESAME PER LA CERTIFICAZIONE AICQ SICEV

5.1 Argomenti di esame
5.2 Materie di esame
5.3 Criteri di valutazione
5.4 Commissione esaminatrice
5.5 Decision Maker

ALLEGATO 1: Requisiti minimi e materie d'esame

ALLEGATO 2: Fac-simile Modello di presentazione esperienza lavorativa del candidato

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente Regolamento ha lo scopo di definire i requisiti minimi per la concessione della certificazione delle competenze per le seguenti figure professionali:

1. **Valutatore *privacy***
2. ***Data Protection* Auditor**
3. ***Data Protection* Lead Auditor**

operanti nell'ambito del trattamento e della protezione dei dati personali e per il mantenimento e il rinnovo della medesima.

In modo particolare, detto Regolamento si pone l'obiettivo di descrivere e differenziare:

- **Il profilo di Valutatore *Privacy* secondo la norma UNI 11697:2017**
- **Il profilo di Auditor/Lead Auditor *Data Protection* secondo lo Schema ISDP©10003**

Il presente Regolamento si applica sia ai candidati che abbiano presentato domanda di certificazione sia ai Valutatori privacy e sia agli Auditor/Lead Auditor *Data Protection* (ISDP©10003) già iscritti ai Registri.

1.1 Definizione dei profili professionali

Per **Valutatore Privacy** si intende un profilo che risponde a specifici requisiti di conoscenza, abilità, competenza e formazione ai sensi della norma UNI 11697:2017, che può effettuare **audit di 1^ e 2^ parte** e "*controlla la conformità del trattamento di dati personali a leggi e regolamenti applicabili".*

Nello specifico ha competenze, abilità e conoscenze specificate come da *§ 5.4 UNI 11697.*

Per **Auditor *Data Protection*** (ISDP©10003) si intende un profilo che risponde a specifici requisiti di conoscenza, abilità, competenza e formazione ai sensi della norma UNI 11697:2017 e dello schema di certificazione ISDP©10003 (*ai sensi della norma IS/IEC 17065:2012*), che può effettuare **audit di 1^, 2^ e 3^ parte**, "*controlla la conformità del trattamento di dati personali a leggi e regolamenti applicabili*" ed è in grado di attuare le politiche di valutazione dell'adeguatezza di un sistema di analisi e controllo dei principi e delle norme di riferimento in ambito del trattamento dei dati personali.
Nello specifico, ha il compito di supportare il Lead auditor nella conduzione degli audit. Partecipa alla predisposizione dei piani di verifica, alla stesura delle check list e dei rapporti di verifica eseguiti dal Lead auditor.

Per **Lead Auditor *Data Protection*** (ISDP©10003) si intende un profilo con una rilevante esperienza di audit di 3^ parte maturata anche su altri Schemi di Certificazione (ISO 9001 e ISO 27001) in coerenza ai requisiti specifici minimi identificati al Par. 4.1.
Nello specifico, ha competenze nella:

- Programmazione e pianificazione di audit relativamente alla *Data Protection*
- Verifica della efficace attuazione dei requisiti relativamente alla *Data Protection*
- Verifica dell'adeguatezza dei sistemi di analisi e controllo dei principi e delle norme applicabili relativamente alla *Data Protection*

2. DOCUMENTI

2.1 Documenti di base

- RG 01 – Regolamento Generale per la certificazione delle competenze dei valutatori, dei responsabili e dei supervisori dei gruppi di valutazione di Sistemi di Gestione, di prodotto e dei valutatori operanti in incognito
- Schema Internazionale per la Protezione dei Dati Personali **ISDP©10003 -** Criteri e regole di controllo per la certificazione dei processi per la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione degli stessi
- 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
- UNI/PdR 66:2019 Raccomandazioni per la valutazione di conformità ai requisiti definiti dalla UNI 11697:2017 “Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali – Requisiti di conoscenza, abilità e competenza”
- GDPR - *General Data Protection Regulation* Reg. EU 679/2016
- Direttiva NIS UE 2016/1148 (presente nei documenti di riferimento)
- Regolamento UE 2014/910 EIDAS (presente nei documenti di riferimento)
- Regolamento UE 2019/881 Cybersecurity Act

Nota 1 - Se non esplicitamente citata, l’edizione valida dei sopracitati documenti è l’ultima emessa.

2.2 Documenti applicabili

- RG 02 – Regolamento Generale per la qualificazione dei corsi di addestramento sulle metodologie di esecuzione delle verifiche ispettive (audit) dei sistemi di gestione e degli audit in incognito
- Manuale del Sistema di Gestione per la Qualità di AICQ SICEV e relative Procedure
- D. Lgs. 196/2003 – Codice in materia di protezione di dati personali novellato dal D. Lgs. 101/2018
- Provvedimenti Garante della Privacy italiano
- D. Lgs. 81/2008 – Tutela della Salute e della Sicurezza nei Luoghi di Lavoro
- D. Lgs. 65/2018 – Attuazione Direttiva (UE) NIS 2016/1148

Nota 2 - Se non esplicitamente citata, l’edizione valida dei sopracitati documenti è l’ultima emessa.

2.3 Documenti di riferimento

- UNI ISO 31000 – Gestione del rischio – Principi e linee guida
- ISO/IEC 27000 - Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
- UNI CEI ISO/IEC 27001 - Tecnologie informatiche Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni - Requisiti
- UNI CEI ISO/IEC 27002 - Tecnologie informatiche Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni –Raccolta di prassi sui controlli per la sicurezza delle informazioni
- ISO/IEC 27017:2015 Information Technology - Security Techniques - Code of practice for information security controls based on ISO/IEC 27002 for Cloud Services.
- ISO/IEC 27018 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27021 Information technology -- Security techniques – Competence requirements for information security management systems professionals
- UNI ISO 31000 “Gestione del rischio - Principi e linee guida”
- UNI CEI ISO/IEC 29100 - Tecnologie informatiche - Tecniche per la sicurezza - Quadro di riferimento per la privacy

- ISO/IEC 29101 **-** Information technology -- Security techniques -- Privacy architecture framework
- ISO/IEC 29134 - Information technology -- Privacy impact assessment – Guidelines
- ISO/IEC 29151 - Information technology -- Security techniques -- Code of practice for personally identifiable information protection
- 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 - Metodologia per la costruzione di profili professionali basati sul sistema e-CF
- 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 EN ISO 19011: 2018. Linee guida per gli audit dei sistemi di gestione
- UNI CEI EN ISO/IEC 17021-1 Requisiti per gli organismi che forniscono audit e certificazioni di sistemi di gestione
- ISO 28591 Sequential sampling plans for inspection by attributes
- ISO/IEC 25012 Data quality model
- ISO/IEC 25024 "Measurement of data quality"
- Direttiva UE 2016/680 Criminal Offences Penalities
- Direttiva UE 2016/1148 NIS
- Regolamento UE 2014/910 EIDAS
- D. Lgs. 231/01 – Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica
- Lg. 300/70 Statuto dei lavoratori & Jobs Act
- Guidelines pubblicate da Articolo 29 Data Protection Working Party
- Guidelines pubblicate da Comitato Europeo per la protezione dei dati (Edpb)

Nota 3 - Se non esplicitamente citata, l'edizione valida dei sopracitati documenti è l'ultima emessa.

3 DEFINIZIONI E ACRONIMI

Per le definizioni valgono quelle riportate nei documenti di paragrafo 2.

4. REQUISITI SPECIFICI PER LA CERTIFICAZIONE DEI VALUTATORI PRIVACY E DEGLI AUDITOR/LEAD AUDITOR PRIVACY

4.1 Struttura dello Schema di Certificazione AICQ SICEV

AICQ SICEV intende gestire la certificazione delle figure professionali operanti come Valutatore privacy ai sensi della norma UNI 11697 e Auditor/Lead Auditor sulla Protezione dei Dati Personali (Privacy) nel rispetto dei requisiti dello Schema internazionale per la protezione dei dati personali ISDP©10003 e della citata norma UNI 11697

Lo Schema di Certificazione prevede le seguenti figure professionali:

- **Valutatore Privacy**
- **Auditor/Lead Auditor *Data Protection* ISDP©10003**

4.2 Requisiti minimi

Con riferimento a quanto indicato nel paragrafo 5.1 del Regolamento Generale RG 01, e a quanto definito nel precedente paragrafo, i requisiti minimi per il percorso di certificazione risultano strettamente legati al profilo selezionato.

Pertanto, per i requisiti minimi, si rimanda alle tabelle specifiche riportate nell'ALLEGATO 1.

4.3 Domanda per accedere al processo di Certificazione

Il candidato che vuole accedere al processo di certificazione dovrà presentare idonea documentazione, ovvero la Domanda di esame di certificazione comprensiva della documentazione indicata dal regolamento RG03, e dichiarare di non avere in corso altre richieste di certificazione per il medesimo profilo.

Oltre alla documentazione richiesta, per la certificazione nel/i profilo/i professionale/i relativo/i al trattamento e alla protezione dei dati personali, il candidato dovrà produrre:

- Una dichiarazione ai sensi del DPR 445/2000 di affidabilità giuridica e onorabilità professionale
- Un modello di presentazione dell'esperienza/e lavorativa/e più significativa a fronte della specifica figura/e professionale/i per la quale/i richiede la certificazione/i (vedi allegato 2)

La dichiarazione ai sensi del DPR 445/2000 di affidabilità giuridica e onorabilità professionale dovrà riportare almeno le seguenti informazioni:

- essere nello stato di pieno godimento dei diritti civili;
- di non essere presente / non risultare a proprio carico alcun procedimento relativo a reati penali e civili.

4.4 Rinnovo, sorveglianza e mantenimento della Certificazione

La certificazione ha validità **quadriennale** e il suo mantenimento è subordinato all'esito positivo della sorveglianza effettuata dall'OdC con cadenza annuale.

Per la **sorveglianza e il mantenimento annuale**, il candidato dovrà produrre la seguente documentazione:

1. almeno un incarico/attività/contratto di lavoro attraverso il quale si dimostri di aver operato nell'ambito dei compiti richiamati dalla Norma UNI 11697 e dallo Schema di certificazione ISDP©10003 per la figura professionale dell'Auditor/Lead Auditor ISDP©10003.
2. La dimostrazione tramite evidenze (attestati/contratti/registri partecipazione e similari) di partecipazione ad attività di formazione/convegni/docenze/relazioni/gruppo di lavoro normativo o tecnico, durante l'anno, finalizzate al mantenimento delle competenze specifiche per la certificazione posseduta, per almeno 8 ore;
3. Una autodichiarazione" ai sensi degli artt. 46 e 76 del D.P.R. 445/2000 contenente:
   - le attività svolte, rispetto ai punti 4 e 5 della norma UNI 11697:2017, specifiche nel campo della protezione dati, durante l'anno;
   - l'elenco completo dei corsi dei corsi di aggiornamento, partecipazione a convegni, seminari, relazioni, docenze inerenti agli argomenti relativi al settore della privacy;
   - la presenza di eventuali reclami relativi all'attività certificata;
   - la presenza di eventuali contenziosi legali in corso relativi all'attività certificata;
   - pagamento regolare delle quote annuali dovute all'Organismo di certificazione.

Il candidato in sostituzione delle esperienze, della partecipazione a corsi di aggiornamento ed altre evidenze può presentare una dichiarazione ai sensi del DPR 445/2000 dove vengono elencate esperienze specifiche, partecipazione a corsi o effettuazione di docenza specifica in ambito protezione dei dati e/o sicurezza delle informazioni necessarie a determinare i requisiti di accesso (vedere allegato 2 e UNI 11697). In caso di presentazione dell'autodichiarazione sopracitata, è richiesto all'iscritto, in aggiunta, l'indicazione di uno o più nominativi/referenze che AICQ SICEV si riserva di contattare per verificare la veridicità di quanto dichiarato.

Nel caso in cui siano presenti reclami o contenzioni legali sarà valutata da parte di AICQ SICEV la relativa gestione. L'attività di sorveglianza può avere come esito il mantenimento, la sospensione o la revoca della certificazione a fronte della valutazione in merito alla completezza, congruità della documentazione presentata nonché gestione di eventuali reclami e/o contenziosi legali.

Per il **rinnovo quadriennale** si applica quanto previsto nel paragrafo 11.2 di RG01, con le seguenti precisazioni:

a) Deve essere presentata la domanda di rinnovo corredata dalla documentazione richiesta per la sorveglianza annuale, come sopra riportato. Per quel che concerne la partecipazione a corsi/seminari/congressi di aggiornamento professionale, si richiede evidenza per le aree di miglioramento professionale e tecnico/legale/normativo in materia di protezione dei dati personali (in qualità di discente e/o docente) e per lo Schema di certificazione **ISDP©10003.** ~~I corsi devono essere riconosciuti da Inveo S.r.l. e/o AICQ SICEV o deve trattarsi di *workshop* dell'Autorità Garante (per un minimo di 8 ore/anno)~~. Per la certificazione dei **Valutatori privacy** (UNI 11697), gli attestati di partecipazione (o di docenza) devono fornire evidenza di aggiornamento/formazione specifica per un minimo di 24 ore nel triennio. ~~I corsi devono essere qualificati da AICQ SICEV (o da OdC equivalenti).~~

b) Deve essere fornita evidenza oggettiva della continuità di lavoro nel ruolo corrispondente al profilo specifico negli ultimi 4 anni. In particolare, si deve dare evidenza di aver effettuato almeno 9 audit completi, per una durata di almeno 18 giorni effettuati su più Organizzazioni o dipartimenti (per le Organizzazioni complesse)

c) in sede di rinnovo è prevista una prova scritta composta da domande a risposta multipla, strutturata come l'esame di certificazione (rimangono invariati anche i criteri per il superamento dell'esame). Nel caso in cui il candidato non superasse questa prima prova, può ripeterla in una sessione d'esami successiva (se la certificazione non è già scaduta), ripetendo la prova scritta composta da domande a risposta multipla ma con l'aggiunta dell'esame scritto sui casi di studio, strutturato come l'esame di certificazione (rimangono invariati anche in questo caso i criteri per il superamento dell'esame). In caso di esito negativo anche di questa seconda prova, è necessario effettuare un esame completo di prima certificazione (domande a risposta multipla, casi di studio e orale).

4.5 Passaggio a Lead Auditor Data Protection

L' Auditor *Data Protection* ISDP©10003 certificato ed iscritto al Registro potrà passare alla qualifica di Lead Auditor se soddisfa i requisiti della tabella di ALLEGATO 1.

4.6 Trasferimento da un differente Organismo di Certificazione

La richiesta di un trasferimento da un Organismo di Certificazione accreditato differente da AICQ SICEV può essere perfezionata in qualsiasi momento, presentando richiesta all'OdC subentrante, mediante la presentazione della domanda di trasferimento corredata dal certificato in corso di validità, dai documenti applicabili per la sorveglianza e dall'evidenza di chiusura di eventuali pendenze (economiche e tecniche) aperte con l'Organismo precedente.

Il candidato dovrà sostenere un esame orale con le stesse modalità previste per la certificazione dando evidenza di possedere i requisiti minimi richiesti dalla figura professionale per la quale intende farsi riconoscere la certificazione. Al completamento con esito positivo di questa istruttoria, AICQ AICEV deve deliberare l'emissione del proprio certificato e il candidato verrà inserito nel relativo registro professionale. Il certificato emesso manterrà la scadenza di quello precedente.

5. ESAME PER LA CERTIFICAZIONE AICQ SICEV

Gli esami vengono condotti secondo quanto definito al paragrafo 8 del Regolamento RG 01.

5.1 Modalità e argomenti di esame

L'esame di certificazione consiste di due esami scritti ed un esame orale.
Le due prove scritte sono finalizzate ad accertare le conoscenze e la corretta applicazione da parte dei candidati di quanto previsto nella casella "Conoscenze e abilità" delle tabelle in ALLEGATO 1. Tali prove consistono in:

- Un esame scritto per la valutazione delle conoscenze: 35 domande a risposta multipla. Tempo a disposizione 70 minuti.
- Un esame scritto su "casi di studio" finalizzati a verificare l'attitudine, le abilità, le competenze e le conoscenze del medesimo su questioni pratiche connesse al profilo professionale oggetto di certificazione: almeno due casi studio. Tempo a disposizione 20 minuti.

Le prove scritte vengono somministrate ai candidati separatamente. Non è consentito somministrare in un'unica prova di esame le due prove scritte. La correzione della prima prova scritta avviene durante lo svolgimento della seconda prova. Non è possibile, altresì, invertire l'ordine delle prove di esame, che sono rispettivamente: prima prova scritta per la valutazione delle conoscenze, seconda prova scritta per i casi di studio. All'esito positivo delle due prove scritte (superamento di entrambe), il candidato può essere ammesso alla prova orale.

Durante lo svolgimento dell'esame i due esaminatori devono essere contemporaneamente presenti alla sessione di esame. Almeno uno degli esaminatori deve essere fisicamente in presenza del candidato, mentre l'altro potrà essere presente in contemporanea, ma "da remoto", con l'uso di tecnologie IT. Non sono ammessi collegamenti solo telefonici. La valutazione è eseguita congiuntamente da almeno due esaminatori che rilasciano un solo giudizio risultante dalla media delle proprie valutazioni. Alla Commissione si può unire un tecnico dell'Organismo di Certificazione con funzioni di segretario o tecnico facilitatore nella compilazione dei verbali di esame.

Il verbale di esame prevede la registrazione delle domande di esame somministrate con le prove scritte sostenute, e relativa correzione, e delle domande orali con relativa valutazione. Le registrazioni devono dare evidenza che siano state valutate, con domande scritte e orali, tutte le macro aree di competenza previste per le singole figure professionali oggetto di valutazione.

L'esame orale, della durata minima di 30 minuti, consiste in un colloquio finalizzato alla (vedere anche paragrafo 8.5 di RG 01):
- Simulazione di situazioni reali operative (per una durata di circa 10 minuti, inclusi nei minuti totali dell'esame orale);
- Analisi e valutazione di lavori effettuati per approfondire la valutazione delle abilità, delle conoscenze e della capacità relazionali del candidato;
- Approfondimento del grado di conoscenza degli elementi delle prove scritte;
- Approfondimento dell'ambito dell'esperienza professionale e delle informazioni presentate dai candidati;
- Valutazione dell'adeguatezza e del grado di aggiornamento delle esperienze specifiche operative;
- Verifica del modo di gestire i rapporti interpersonali dei Candidati.

Durante l'esame orale è inoltre previsto l'approfondimento della conoscenza dei concetti di "Privacy by design" e "Privacy by default", delle tecniche di anonimizzazione, pseudonimizzazione, DPIA, il

concetto di trattamento dei dati personali e i relativi fattori di rischio qualora tali argomenti non siano già stati oggetto di valutazione durante le prove scritte.

Durante lo svolgimento dell'esame i due esaminatori devono essere contemporaneamente presenti alla sessione di esame. Almeno uno degli esaminatori deve essere fisicamente in presenza del candidato, mentre l'altro potrà essere presente in contemporanea, ma "da remoto", con l'uso di tecnologie IT. Non sono ammessi collegamenti solo telefonici. La valutazione è eseguita congiuntamente da almeno due esaminatori che rilasciano un solo giudizio risultante dalla media delle proprie valutazioni. Alla Commissione si può unire un tecnico dell'Organismo di Certificazione con funzioni di segretario o tecnico facilitatore nella compilazione dei verbali di esame.

5.2 Materie di esame

Le materie di esame si basano sulle conoscenze previste nelle schede dell'ALLEGATO 1 ed in particolare:

- conoscenza specifica dello Schema **ISDP©10003 (*)**
- conoscenza terminologia dello Schema **ISDP©10003(*)**
- conoscenza specifica della terminologia della *Data Protection*
- conoscenze specifiche delle norme che regolamentano la *Data Protection*
- conoscenza delle norme UNI EN ISO 19011 e ISO/IEC 17021-1
- conoscenza dei requisiti generali della ISO/IEC 17065 (*)
- conoscenza della norma UNI ISO 31000

***Nota**: sono contrassegnate con un asterisco (*) le materie di esame applicabili ai soli Auditor/Lead Auditor ISDP©10003*

5.3 Criteri di Valutazione

Per superare l'esame il Candidato deve ottenere almeno un punteggio di 70% nelle singole prove.

Per il superamento della prova "caso di studio", il valore del punteggio complessivo attribuito è quello della media dei punteggi dei diversi casi di studio con il vincolo di aver ottenuto almeno5/10 per la peggiore delle risposte.

Qualora il Candidato non abbia concluso con esito positivo l'esame le eventuali singole prove superate rimangono valide per 12 mesi e l'esame può essere nuovamente sostenuto non prima di tre mesi dalla data della prova di esame non superata. Nei mesi intercorrenti tra l'esame non superato e la sua ripetizione, il candidato non può presentare domanda di certificazione ad altro Organismo di Certificazione, pena l'invalidazione dello stesso processo di certificazione.

5.4 Commissione esaminatrice

La commissione esaminatrice deve essere composta da almeno due membri e soddisfare nel suo insieme i seguenti requisiti:

a) conoscenza delle regole e criteri definiti dall'Organismo di Certificazione per l'esame di certificazione in coerenza con quanto richiamato dalla UNI CEI EN ISO/IEC 17024
b) il possesso della certificazione del profilo della norma UNI 11697 come da tabella della UNI/PdR 66:2019
c) competenza maturata, a seguito di esperienze lavorative di almeno 8 anni, in ambito giuridico con comprovata esperienza nell'ambito del trattamento dei dati personali e materie attinenti alla sicurezza delle informazioni con esperienza nell'ambito della protezione dei dati personali

Per i primi tre anni di operatività, in sostituzione del membro in possesso di una certificazione sotto accreditamento, l'Organismo può servirsi di *granparent* in possesso dei requisiti al punto a) e c).

I membri delle commissioni non possono essere stati docenti nei corsi di formazione dei candidati, salvo adottare specifiche misure di mitigazione dello specifico rischio di imparzialità.

5.5 Decision maker

L'Organismo di Certificazione ha adottato dei criteri di qualifica del *Decision Maker* per assicurarsi che possieda adeguate competenze che comprendono i seguenti criteri:

- Conoscenza dei processi di delibera dell'OdC
- Conoscenza generale della norma UNI 11697

A seguito della predisposizione della delibera di certificazione la responsabilità di emettere il certificato di conformità rimane alla Direzione dell'organismo di Certificazione.

ALLEGATO 1 – Requisiti minimi e materie d'esame

Profilo professionale: VALUTATORE PRIVACY

Definizione sintetica del profilo: "Esamina periodicamente il trattamento dei dati personali, valutando il rispetto di leggi e regolamenti applicabili e approva le misure necessarie a eliminare eventuali non conformità rilevate, mantenendo una posizione indipendente da chi svolge attività manageriali e operative" *(§ 5.4 UNI 11697*)

Le conoscenze ed abilità di carattere generale dell'auditor devono assicurare che egli:

(a) esegua gli audit in modo coerente mediante:
- l'applicazione corretta di principi, procedure e tecniche di audit (UNI EN ISO 19011)
- il rispetto dei tempi
- l'individuazione delle priorità e degli aspetti significativi da verificare
- la raccolta efficace di informazioni
- l'utilizzo di documenti di lavoro per le registrazioni
- la predisposizione dei rapporti di audit
- la comunicazione chiara ed efficace

(b) comprenda il campo dell'audit e applichi i criteri dell'audit;

(c) conosca le norme cogenti, e le procedure applicabili e documentate

(d) conosca il contesto operativo dell'organizzazione: i processi aziendali, le strutture e le funzioni;

sia consapevole dei requisiti applicabili all'organizzazione oggetto dell'audit: leggi e regolamenti, contratti e altri requisiti sottoscritti dall'organizzazione.

REQUISITI MINIMI	
Grado di istruzione	Diploma di scuola media superiore.
Esperienza lavorativa specifica	Minimo **sei anni** di esperienza professionale specifica continuativa con incarichi o progettazione di modelli privacy o almeno quattro anni di lavoro all'interno di un team privacy. Il valutatore privacy dovrà dimostrare di aver eseguito almeno 10 audit di 1^ e/o 2^ parte. Per un periodo transitorio di 3 anni possono essere considerati validi gli audit eseguiti sui Sistemi di Gestione per la Sicurezza delle Informazioni o la dimostrazione di almeno quattro attività di audit preliminare, gap analisi, *assessment* documentale, nell'ambito del trattamento e della Protezione dei Dati Personali.
Formazione ed addestramento	Attestato di superamento corso di 40 ore per "Valutatore Privacy", riconosciuto da AICQ SICEV (o da OdC equivalenti) Altra tipologia di formazione potrà essere vagliata dalla commissione esaminatrice che valuterà la documentazione fornita. La documentazione dovrà almeno evidenziare le materie studiate e la tipologia della verifica finale effettuata. Al fine di poter acquisire la certificazione come Auditor/Lead Auditor ISDP©10003, i valutatori privacy certificati secondo la Norma UNI, dovranno acquisire un attestato di superamento corso "Auditor Privacy ISDP©10003" della durata di 16 ore.

REQUISITI MINIMI	
Lingue Straniere (su richiesta)	Capacità di esercitare la professione in lingua straniera attraverso colloquio e redazione di elaborati in tale lingua. Tale conoscenza può essere dimostrata da dichiarazioni rese da Istituti di formazione linguistica pubblici, privati o dalla Società di appartenenza del Candidato. AICQ SICEV si riserva di verificare durante la prova orale le reali conoscenze del candidato. Il livello minimo atteso è il B2, secondo quanto definito dalla Comunità Europea (QCER/CEFR da A1 a C2)

MATERIE DI ESAME

Durante gli anni di esperienza specifica, il Candidato deve aver operato e aver maturato una conoscenza approfondita su:

Norme/Framework Sistemi di Gestione Privacy

- *UNI CEI ISO/IEC 27001*
- *UNI EN ISO/IEC 25012-24*
- *UNI EN ISO/IEC 9001*
- *ISO IEC 17021-1 (per la parte di competenza) – Valutazione della conformità – Requisiti generali per gli organismi operanti la certificazione dei sistemi di gestione.*
- *UNI EN ISO 19011 - Linee guida per gli audit dei Sistemi di Gestione*
- *ISO 31000 - Risk Management*

Inoltre, deve avere conoscenza delle seguenti norme:

- *ISO/IEC 27000*
- *UNI CEI ISO/IEC 27002*
- *ISO/IEC 27017*
- *ISO/IEC 27018*
- *UNI CEI ISO/IEC 29100*
- *ISO/IEC 29101*
- *ISO/IEC 29134*
- *ISO 22301 - Business Continuity*

Nota – se non diversamente specificato vale l'ultima revisione disponibile delle sopracitate norme.

- *Leggi e provvedimenti:*
- D. Lgs. 196/2003 – Codice in materia di protezione di dati personali novellato dal D. Lgs. 101/2018
- GDPR General Data Protection Regulation 2016/679
- Provvedimenti, pronunce e/o linee guida pubblicate dal Garante e/o Garanti Europei (presente tra i documenti applicabili)
- Guidelines pubblicate da Articolo 29 Data Protection Working Party
- Guidelines pubblicate da Comitato Europeo per la protezione dei dati (Edpb)
- Regolamento UE 2019(881 Cybersecurity Act
- Normative e leggi settoriali
- *Competenze e-CF assegnate, Conoscenze e* Abilità (Skill): così come richiesti dalla UNI 11697

Profilo professionale: AUDITOR E LEAD AUDITOR *DATA PROTECTION* ISDP©10003

Definizione sintetica del profilo:

AUDITOR: ha il compito di supportare il Lead auditor nella conduzione degli audit. Partecipa alla predisposizione dei piani di verifica, alla stesura delle *check list* e dei rapporti di verifica eseguiti dal Lead auditor.

LEAD AUDITOR: ha il compito di condurre gli audit. Predisposizione i programmi e i piani di verifica, le *check list* e i rapporti di verifica.

Le conoscenze ed abilità di carattere generale di Auditor e Lead Auditor devono assicurare che egli:

(e) esegua gli audit in modo coerente mediante:
- l'applicazione corretta di principi, procedure e tecniche di audit (UNI EN ISO 19011 - 17021-1)
- il rispetto dei tempi
- l'individuazione delle priorità e degli aspetti significativi da verificare
- la raccolta efficace di informazioni
- l'utilizzo di documenti di lavoro per le registrazioni
- la predisposizione dei rapporti di audit
- la comunicazione chiara ed efficace

(f) comprenda il campo dell'audit e applichi i criteri dell'audit;

(g) conosca le norme cogenti, la procedura ISDP©10003 e le procedure applicabili e documentate

(h) conosca il contesto operativo dell'organizzazione: i processi aziendali, le strutture e le funzioni;

(i) sia consapevole dei requisiti applicabili all'organizzazione oggetto dell'audit: leggi e regolamenti, contratti e altri requisiti sottoscritti dall'organizzazione.

REQUISITI MINIMI	**AUDITOR DATA PROTECTION ISDP©10003**	**LEAD AUDITOR DATA PROTECTION ISDP©10003**
Grado di istruzione	Diploma di scuola media superiore. Dopo un periodo transitorio di tre anni, sarà necessaria la laurea triennale.	
Esperienza lavorativa specifica	Esperienza documentata continuativa in almeno una delle seguenti attività: ▪ DPO con almeno un anno di esperienza ▪ Auditor in Organismi di Certificazione per la norma UNI CEI ISO IEC 27001 con almeno 4 anni ▪ Audit interni documentati per almeno due anni ▪ Tre anni complessivi con incarichi o progettazione di modelli privacy o almeno quattro anni di lavoro all'interno di un team privacy. ▪ Esecuzione di n° 3 audit completi, nell'ambito della data protection, per una durata complessiva di 6 giorni. Per un periodo transitorio di 3 anni possono essere considerati validi gli audit eseguiti sui Sistemi di Gestione per la Sicurezza delle Informazioni o la dimostrazione di almeno quattro attività di audit preliminare, gap analisi, *assessment* documentale, nell'ambito del trattamento e della Protezione dei Dati Personali. Compensazioni ulteriori per il periodo transitorio: • Iscrizione a Collegi ed Ordini (requisito sostitutivo di un anno di esperienza lavorativa specifica) • Appartenenza a corpi militari dello stato con il grado di ufficiale o sottufficiale (Guardia di Finanza, Carabinieri) 0,5 anni ogni 5 anni di servizio.	Esperienza documentata continuativa in almeno due delle seguenti attività specifiche quali: ▪ DPO con almeno 3 anni di esperienza ▪ Lead auditor in Organismi di Certificazione per la norma UNI CEI ISO IEC 27001 con almeno 4 anni di esperienza ▪ Audit interni documentati per almeno quattro anni ▪ Esecuzione di n° 3 audit completi documentati per una durata di 10 giorni di audit effettuati su più organizzazioni o dipartimenti (per le organizzazioni complesse). Per un periodo transitorio di 3 anni possono essere considerati validi gli audit eseguiti sui Sistemi di Gestione per la Sicurezza delle Informazioni o la dimostrazione di almeno quattro attività di audit preliminare, gap analisi, *assessment* documentale, nell'ambito del trattamento e della Protezione dei Dati Personali. NOTA BENE: Tale deroga non viene presa in considerazione nel passaggio tra auditor a lead auditor
Formazione ed addestramento	Attestato di superamento corso "Auditor Privacy ISDP©10003". La formazione deve prevedere in totale un minimo di 40 ore.	Attestato di superamento corso "Auditor Privacy ISDP©10003". La formazione deve prevedere in totale un minimo di 40 ore.

REQUISITI MINIMI	**AUDITOR DATA PROTECTION ISDP©10003**	**LEAD AUDITOR DATA PROTECTION ISDP©10003**
Lingue Straniere (su richiesta)	Capacità di esercitare la professione in lingua straniera attraverso colloquio e redazione di elaborati in tale lingua. Tale conoscenza può essere dimostrata da dichiarazioni rese da Istituti di formazione linguistica pubblici, privati o dalla Società di appartenenza del Candidato. AICQ SICEV si riserva di verificare durante la prova orale le reali conoscenze del candidato. Il livello minimo atteso è il B2, secondo quanto definito dalla Comunità Europea (QCER/CEFR da A1 a C2)	

MATERIE DI ESAME:

Durante gli anni di esperienza specifica, il Candidato deve aver operato e aver maturato una conoscenza approfondita su:

- Norme/Framework Sistemi di Gestione Privacy
- *UNI CEI ISO/IEC 27001*
- *UNI EN ISO/IEC 25012-24*
- *UNI EN ISO/IEC 9001*
- *ISO IEC 17021-1– Valutazione della conformità – Requisiti generali per gli organismi operanti la certificazione dei sistemi di gestione.*
- *UNI EN ISO 19011 - Linee guida per gli audit dei Sistemi di Gestione*
- *ISO 31000 - Risk Management*
- Schema internazionale per la protezione dei dati personali ISDP©10003 Criteri e regole di controllo per la Certificazione dei processi per la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione degli stessi.

Inoltre, deve avere conoscenze sulle seguenti norme:

- *ISO/IEC 27000*
- *UNI CEI ISO/IEC 27002*
- *ISO/IEC 27017*
- *ISO/IEC 27018*
- *UNI CEI ISO/IEC 29100*
- *ISO/IEC 29101*
- *ISO/IEC 29134*
- *ISO 22301 - Business Continuity*
- *UNI CEI EN ISO/IEC 17065 Valutazione della conformità. Requisiti per organismi che certificano prodotti, processi e servizi*

Nota – se non diversamente specificato vale l'ultima revisione disponibile delle sopracitate norme

Leggi e provvedimenti:

- D. Lgs. 196/2003 – Codice in materia di protezione di dati personali novellato dal D. Lgs. 101/2018
- GDPR General Data Protection Regulation 2016/679
- Provvedimenti, pronunce e/o linee guida pubblicate dal Garante e/o Garanti Europei (presente tra i documenti applicabili)
- ~~o~~ Guidelines pubblicate da Articolo 29 Data Protection Working Party
- ~~o~~ Guidelines pubblicate da Comitato Europeo per la protezione dei dati (Edpb)
- Regolamento UE 2019(881 Cybersecurity Act
- Normative e leggi settoriali

ALLEGATO 2 - Modello di presentazione esperienza in ambito Protezione dei Dati del candidato

Il presente Allegato propone un fac-simile dal quale il candidato, in fase di presentazione della domanda di certificazione per uno dei profili considerati nel presente regolamento, predisporrà un documento dove evidenzierà l'esperienza lavorativa che ritiene più significativa a fronte della specifica figura professionale. Il candidato può inserire anche più esperienze.
La discussione dell'elaborato presentato è necessaria per il superamento dell'esame orale, in considerazione del fatto che lo scopo generale è quello di mettere in grado la commissione esaminatrice di apprezzare le competenze sviluppate dal candidato nel progetto descritto.

ESPERIENZA LAVORATIVA DA DISCUTERE DURANTE L'ESAME ORALE

CANDIDATO: _____

PROFILO RICHIESTO:

- ❑ Valutatore Privacy (UNI 11697)
- ❑ Auditor Data Protection ISDP©10003
- ❑ Lead Auditor Data Protection ISDP©10003

PERIODO DI RIFERIMENTO: DATA di avvio (__/__/____) data di termine (__/__/____)

SETTORE ATTIVITÀ: _____

OGGETTO DELLA CONSULENZA/ATTIVITÀ GESTITA DAL CANDIDATO:

DENOMINAZIONE/BREVE DESCRIZIONE/OBIETTIVO/I DEL PROGETTO PIU' SIGNIFICATIVO A FRONTE DELLA SPECIFICA FIGURA PROFESSIONALE:

MODALITÀ ADOTTATE DAL CANDIDATO PER LA GESTIONE DELL'ATTIVITÀ DEL PROGETTO SOPRA DESCRITTO:

DESCRIZIONE DI MAGGIOR DETTAGLIO CHE COMPRENDA LE ATTIVITÀ, METODI E/O STRUMENTI UTILIZZATI DAL CANDIDATO, I PRINCIPALI DOCUMENTI E RISULTATI DI PROGETTO, LE CRITICITÀ RISCONTRATE, LE SOLUZIONI: