REQUISITI **(rif. UNI 11697:2017_appendice B,** Circolare Tecnica ACCREDIA **N.03/2018- UNI/PdR 66:2019)**	
Titolo di studio (apprendimento formale)	Laurea che includa discipline almeno in parte afferenti alle conoscenze del professionista privacy, legali o tecnico/informatiche[1)]
Formazione specifica (apprendimento non formale)	Corso di almeno 80 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni (rif nota* 2) . Il numero di ore complessive può essere raggiunto anche con più corsi di formazione o con l'effettuazione di docenza specifica. Ove i professionisti abbiano già seguito precedenti percorsi di formazione, non coincidenti con le indicazioni della norma UNI 11697, sarà cura di KHC effettuare una comparazione analitica tra il percorso già seguito dal candidato alla certificazione e il percorso illustrato nella norma medesima.
Esperienza lavorativa (apprendimento informale)	Minimo **6** anni di esperienza lavorativa legata alla privacy di cui almeno **4** anni in incarichi di livello manageriale (rif. nota* 3)
Equipollenza	Se in possesso di laurea magistrale l'esperienza lavorativa si riduce a **4** anni di cui **3** in incarichi di livello manageriale. Se in possesso di diploma di scuola media superiore, minimo **8** anni di esperienza lavorativa di privacy di cui almeno **5** anni in incarichi di livello manageriale.
Note* **(requisiti di accesso riferiti all'appendice B della UNI 10697)**	1) un laureato con laurea non afferente alle conoscenze del professionista privacy, legali o tecnico/informatico è da considerarsi equiparato a un diplomato di scuola media superiore. 2) è ammissibile la riduzione delle ore di formazione richieste fino a un massimo del 10% (30% per il Valutatore Privacy) in caso di possesso di certificazioni professionali riconosciute come attinenti alle conoscenze richieste al professionista privacy in questione. 3) gli incarichi di livello manageriale possono includere anche attività **rilevante svolta nell'ambito di attività di consulenza o di prestazioni d'opera condotta nell'ambito dell'esecuzione di ingaggi professionali**.
Competenze rif. §5.1 UNI 11697 - e-CF 3.0	A.4 Pianificazione di prodotto o di servizio; D.1 Sviluppo della strategia per la Sicurezza Informatica; D.8 Gestione del Contratto; D.9 Sviluppo del Personale; E.3 Gestione del Rischio; E.4 Gestione delle relazioni; E.8 Gestione della Sicurezza dell'Informazione; E.9 Governance dei sistemi informativi
Abilità rif. §5.1 UNI 11697	Contribuire alla strategia per il trattamento e per la protezione dei dati personali, gestire l'applicazione dei codici di condotta e delle certificazioni applicabili in materia di trattamento e protezione dei dati personali, capacità organizzative, capacità di comunicare, capacità di analisi, autogestione e controllo dello stress, capacità di controllo, capacità di autosviluppo, capacità di convincimento, capacità di gestione dei conflitti, iniziativa, idoneità alla negoziazione, pensiero prospettico, tenacia, atteggiamento costruttivo nella soluzione dei problemi, pianificazione e programmazione; *S1*- affrontare le esigenze della formazione continua (CPD) del personale per soddisfare le esigenze dell'organizzazione, *S5*- analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi, *S19*- anticipare i cambiamenti richiesti alla strategia

	aziendale dell'information security e formulare nuovi piani, *S21*- applicare azioni di contenimento del rischio e dell'emergenza, *S23*- applicare gli standard, le best practice e i requisiti legali più rilevanti all'information security, *S40*- coaching, *S52*- comunicare e pubblicizzare sia i risultati dell'analisi del rischio che i processi di gestione del rischio, *S55*- comunicare le buone e le cattive notizie per evitare sorprese, *S66*- costruire un piano di gestione del rischio per fornire e produrre piani di azione preventivi, *S91*- garantire che la proprietà intellettuale (IPR) e le norme della privacy siano rispettate, *S111*- identificare gap di competenze e skill gap, *S140*- negoziare termini e condizioni del contratto, *S153*- preparare i template per pubblicazioni condivise, *S156*- progettare e documentare i processi dell'analisi e della gestione del rischio, *S167*- raccogliere la conoscenza interna ed esterna e i fabbisogni di informazione, *S171*- rendere l'informazione disponibile, S172- rispondere alle esigenze di sviluppo professionale del personale per soddisfare le esigenze organizzative, *S176*- seguire e controllare l'uso effettivo degli standard documentativi aziendali, *S187*- sviluppare piani di risk management per identificare le necessarie azioni preventive.
Conoscenze rif. §5.1 UNI 11697	I principi di privacy e protezione dei dati by design e by default, i diritti degli interessati previsti da leggi e regolamenti vigenti, le responsabilità connesse al trattamento dei dati personali, le responsabilità connesse al trattamento dei dati personali, norme di legge italiane ed europee in materia di trattamento e di protezione dei dati personali, norme di legge in materia di trattamento e protezione dei dati personali per all'estero e circolazione dei dati personali extra UE/SEE, le metodologie di valutazione d'impatto sulla protezione dei dati e PIA, le possibili minacce alla protezione dei dati personali, tecniche e strumenti di comunicazione (relazione con Istituzioni, autorità, Forze dell'Ordine, enti locali e stampa), sistemi e tecniche di monitoraggio e "reporting", le tecniche crittografiche, le tecniche di anonimizzazione e de-anonimizzazione, le tecniche di pseudonimizzazione, le norme tecniche ISO/IEC per la gestione dei dati personali, i codici di condotta e le certificazioni applicabili in materia di trattamento e protezione dei dati personali; *K26*-gli strumenti di controllo della versione per la produzione di documentazione, *K49*- i metodi di sviluppo delle competenze, *K60*- i processi dell'organizzazione ivi inclusi le strutture decisionali, di budget e di gestione, *K67*- i rischi critici per la gestione della sicurezza, *K71*- i tipici KPI (key performance indicators), *K83*- il potenziale e le opportunità offerte dagli standard e dalle best practice più rilevanti, *K85*- il ritorno dell'investimento comparato all'annullamento del rischio, *K98*- l'impatto dei requisiti legali sulla sicurezza dell'informazione, *K108*- la computer forensics (analisi criminologica di sistemi informativi), *K115*- la politica di gestione della sicurezza nelle aziende e delle sue implicazioni con gli impegni verso i clienti, fornitori e i sub-contraenti, *K122*- la strategia dell'informazione nell'organizzazione, *K130*- le best practice (metodologie) e gli standard nella analisi del rischio, *K132*- le best practice e gli standard nella gestione della sicurezza delle informazioni, *K139*- le metodologie di analisi dei fabbisogni di competenze e skill, *K149*- le norme legali applicabili ai contratti, *K152*- le nuove tecnologie emergenti (per esempio sistemi distribuiti, modelli di virtualizzazione, sistemi di mobilità, data sets), *K158*- le possibili minacce alla sicurezza, *K161*- le problematiche legate alla dimensione dei data sets (per esempio big data), *K162*-le problematiche relative ai dati non strutturali (per esempio data analytics), *K180*- le tecniche di attacco informatico e le contromisure per evitarli.

Esame certificativo - PV (Procedura Valutativa) e completamento iter certificativo	
PV - Procedura Valutativa Con una commissione esaminatrice composta da due Commissari Superata la valutazione documentale, il candidato potrà accedere all'esame certificativo (PV), concordato con KHC preventivamente, composto da:	**Verifiche preliminari:** il candidato per essere ammesso all'esame certificativo (PV), deve soddisfare tutti i requisiti suddetti, in termini di: titolo di studio, esperienza lavorativa, formazione, inviando opportuna documentazione comprovante quanto dichiarato nel CV con "autodichiarazione" redatta in conformità agli artt. 46 e 76 del D.P.R. 445/2000 (rif. appendice B della UNI 11697:2017), in termini di titoli e attività, allegandoli alla Domanda di certificazione QI 300104a e Scheda descrittiva per l'esperienza lavorativa, ivi richiamata. Solo ad esito positivo della verifica documentale suddetta, KHC comunica al richiedente il suo status di candidato all'esame e la data della prima sessione disponibile. L'avvio dell'iter certificativo tramite la Domanda di certificazione, comporta da parte del candidato, la sottoscrizione ed il rispetto delle *Norme Deontologiche* e del *Regolamento e Manuale d'uso del marchio di Certificazione (consultabili sul sito www.khc.it)*. Le prove che costituiscono l'intero esame, nel loro insieme, devono ricoprire, per tutti i candidati, le abilità e conoscenze fondamentali richieste dalla norma UNI 11697. Per superare l'esame il candidato deve ottenere almeno un punteggio del **70**% nelle singole prove, rispetto al punteggio massimo previsto per ogni prova. Qualora il candidato non abbia concluso con esito positivo l'esame le eventuali singole prove superate rimangono valide per 12 mesi.
a) esame scritto per la valutazione delle conoscenze come previsto dal §5.1 della UNI 11697: *Le prove scritte sono somministrate ai candidati separatamente ed in sequenza: 1) test a risposta multipla, 2) casi di studio. La correzione della prima prova scritta avviene durante lo svolgimento della seconda prova. Solo a superamento*	1) **test a risposta multipla** - **40 domande** con quattro risposte di cui solo una esatta. **Tempo a disposizione massimo 80 min.** La prova si ritiene superata con un numero di risposte esatte pari o superiore a **28** ed un punteggio pari o superiore a **21/30** (con attribuzione di 0.75 punti per ogni risposta esatta e 0 per ogni risposta mancante o errata); Durante l'esame il candidato può consultare i seguenti documenti forniti dall'OdC : - norma UNI 11697:2017; - Regolamento (UE) 679/2016 e s.m.i.; - D.Lgs. 101/2018; - raccolta non commentata dei provvedimenti del Garante per la Privacy. 2) **tre casi di studio** - per la verifica dell'attitudine, delle abilità, delle competenze e le conoscenze del medesimo su questioni pratiche connesse al profilo professionale del DPO. **Tempo a disposizione massimo complessivo 30 min** (10 minuti massimo per caso di studio). La media dei 3 punteggi dei singoli casi di studio, per il superamento della prova, deve essere almeno pari al 70% del punteggio massimo attribuito ovvero un punteggio minimo di 21/30, con il vincolo di non aver ottenuto meno di 15/30 nella peggiore delle risposte fornite ai tre casi di studio.

delle prove scritte il candidato può essere ammesso alla prova orale.	Nota: le risposte errate** fornite dai candidati alle domande delle prove scritte non comporteranno alcuna penalizzazione. Ciò nonostante, tali risposte saranno oggetto di approfondimento tassativo in sede di esame orale, con un tempo di almeno 3' per ogni domanda da approfondire.
b) esame orale, per approfondire eventuali incertezze riscontrate nelle prove scritte e/o per approfondire il livello delle conoscenze acquisite dal candidato in tutte le aree previste dalla Norma UNI 11697 per *DPO*.	**Tempo a disposizione: minimo di 40 minuti,** per l'approfondimento di ciascuna domanda la commissione esaminatrice deve avere a disposizione mediamente 3 minuti e complessivamente non più di 60 minuti (il tempo aggiuntivo di esame destinato all'approfondimento delle domande errate nelle sessioni scritte deve essere di 3 minuti per il numero di domande errate). La prova si ritiene superata con un punteggio di almeno 21/30. L'esame orale inizia con l'approfondimento delle risposte errate della prova scritta**, ove presenti e comprende: 1) **simulazioni di situazioni reali operative** (es. casi di studio, role play richiamato al punto 6 della UNI 11697:2017)/domande situazionali per valutare, oltre alle abilità e competenze tecniche, anche quelle personali (per esempio competenze relazionali o comportamentali). Per simulazione si intende una riproduzione, anche parziale, di una situazione nella quale il candidato deve immedesimarsi, valutando tutti gli aspetti pertinenti al caso, al fine di esprimere un giudizio professionale su quello che dovrebbe essere il comportamento o la valutazione tecnica ritenuti più adeguati nella situazione rappresentata. Gli aspetti tecnici sono quelli relativi al contesto del trattamento; gli aspetti ambientali sono quelli relativi alle pressioni di varia natura che possono influenzare le decisioni o il comportamento della figura professionale della quale il candidato chiede la certificazione. 2) **analisi e valutazione di lavori effettuati**, presentando alla Commissione esaminatrice un elaborato redatto secondo un modello - Appendice A/Scheda descrittiva esperienza lavorativa, allegata alla Domanda di certificazione, relativo a una situazione lavorativa, considerata significativa dal candidato, rispetto all'esperienza lavorativa complessiva indicata nel CV, a fronte della figura professionale come DPO. La discussione di questo elaborato è parte integrante dell'esame orale. 3) **domande su tematiche complementari** a quelle dei test a risposta multipla, che siano rappresentative delle diverse aree di conoscenza (relazionali, giuridiche e tecniche) e di come questa è declinata nelle specifiche competenze. Durante l'esame orale è previsto l'approfondimento, per tutti i candidati, della conoscenza dei concetti di a) "Privacy by Design" e "Privacy by Default", b) delle tecniche di anonimizzazione, c) psedonimizzazionee, d) DPIA, e) il concetto di trattamento dei dati personali e i relativi fattori di rischio, nonchè in riferimento alle **aree di competenza - prospetto 1 UNI 11697** Ove in tale fase dovessero **emergere significative carenze teoriche o di competenza**, l'esame è considerato **non superato**.
Iter certificativo	A seguito del superamento dell'esame certificativo (ottenendo un punteggio del 70% nelle singole prove, rispetto al punteggio massimo previsto per ogni prova), come sopra indicato, l'evidenza del possesso dei requisiti come previsto dalla UNI 11697, il pagamento delle quote previste (consultabili sul sito rif. http://www.khc.it/certificazione/privacy/ ovvero quota di "presentazione domanda di certificazione" da saldare alla presentazione della Domanda di certificazione e quota di "accettazione domanda di certificazione" da saldare prima della svolgimento della PV), la delibera positiva da parte del Comitato di Delibera (CdA), si completerà l'iter certificativo con l'emissione del

	certificato e l'inserimento sul registro on-line KHC. Qualora il candidato non abbia concluso l'esame con esito positivo, le eventuali singole prove superate rimangono valide per 12 mesi e l'esame può essere nuovamente sostenuto non prima di tre mesi dalla data delle 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.
Durata della certificazione	4 anni (dalla data della delibera della certificazione/prima emissione del certificato) con sorveglianze annuali.
Sorveglianza annuale/ Mantenimento della certificazione	Nel periodo di validità della certificazione, per confermare la validità della certificazione, annualmente il professionista certificato prima della scadenza annuale (il riferimento è la data di inserimento a registro), deve inviare a KHC il modulo **"Autodichiarazione" QI 60 01 10** (ai sensi degli artt. 46 e 76 del D.P.R. 445/2000) scaricabile dal sito rif. http://www.khc.it/certificazione/privacy/, dove elencare: 1) **continuità dell'esperienza lavorativa** - ovvero le attività svolte, specifiche nel campo della protezione dati, durante l'anno, per almeno un **incarico/attività/contratto** nel quale si dimostri di aver operato nell'ambito dei compiti richiamati ai punti 4 e 5 della Norma UNI 11697; 2) **aggiornamento professionale per almeno 16 ore/anno** - ovvero l'elenco completo dei corsi di aggiornamento, partecipazione a convegni, seminari, relazioni, docenze, durante l'anno, inerenti gli argomenti relativi al settore della privacy come declinato nelle tabelle riepilogative per profilo, dimostrabile tramite titoli (attestati/contratti/registri partecipazione e similari) di partecipazione ad attività di formazione/convegni/docenze/relazioni/gruppo di lavoro normativo o tecnico; 3) la presenza di **reclami** relativi all'attività certificata; 4) la presenza di contenziosi legali in corso relativi all'attività certificata; 5) evidenze documentali della corretta gestione di eventuali reclami e contenziosi. In quest'ultimo caso sarà responsabilità di KHCvalutare l'adeguatezza della relativa gestione, sulla base della tempestività e congruenza delle azioni intraprese dal professionista. Dopo la risposta iniziale, da fornire entro 10 gg lavorativi al reclamante, il professionista provvede ad adottare le misure necessarie 8compreso il mancato seguito a reclami ritenuti non applicabili) entro 6 settimane calendariali, dando la necessaria risposta al reclamante. Di tale processo (ricezione del rclamo, prima risposta, analisi e azione discendente) il professionista deve tenere adeguata tracciabilità documentale. 6) pagamento regolare delle quote annuali dovute a KHC, come previsto dalle Quote applicabili e consultabili tramite sito rif. http://www.khc.it/certificazione/privacy/ **Note:** L'attività di sorveglianza può avere come esito il mantenimento, la sospensione o la revoca della certificazione a fronte della valutazione effettuata da parte di KHC in merito a completezza, congruità della documentazione presentata nonchè gestione di eventuali reclami e/o contenziosi legali.
Rinnovo (quadriennale, dalla data di certificazione)	Per rinnovare la validità della certificazione oltre a raccogliere le evidenze già previste per l'attività di sorveglianza (continuità dell'esperienza ed aggiornamento professionale/anno, documentato), si verifica che siano mantenute le competenze previste al punto 5 della UNI 11697:2017. Il DPO certificato deve superare, una prova scritta composta da domande a risposta multipla, strutturato come l'esame di certificazione.

	Nel caso in cui 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). La procedura prevista dal rinnovo della certificazione deve essere completata entro il periodo di validità del certificato, per evitare che il certificato scada e venga revocato. P**er cui il professionista dovrà, improrogabilmente, inviare tutta la documentazione e concordare una sessione d'esame almeno 60 giorni prima della scadenza.**
TRASFERIMENTO DEL CERTIFICATO	
Trasferimento del certificato rilasciato da altro OdC accreditato	Il trasferimento del certificato può essere perfezionato in qualsiasi momento, presentando la Domanda di certificazione a cui deve allegare: a) il certificato in corso di validità, b) i documenti applicabili per la sorveglianza, c) il pagamento regolare della quota per il trasferimento, come previsto dalle Quote applicabili e consultabili tramite sito rif. http://www.khc.it/certificazione/privacy/, d) eventuale evidenza della chiusura di eventuali pendenze (economiche e tecniche) aperte con l'OdC precedente nei suoi confronti. A seguito del **superamento dell'esame orale**, come indicato al punto "PV", l'evidenza della delibera positiva da parte del Comitato di Delibera (CdA), si completerà l'iter di trasferimento del certificato, con l'emissione del certificato e l'inserimento sul registro on-line KHC. Il certificato emesso manterrà la scadenza di quello precedente. L'avvio dell'iter certificativo tramite la Domanda di certificazione, comporta da parte del candidato, la sottoscrizione ed il rispetto delle *Norme Deontologiche* e del *Regolamento e Manuale d'uso del marchio di Certificazione (consultabili sul sito www.khc.it)***.**

Note: il presenta Schema Requisiti ed il Regolamento Generale QI 60 01 00a, di cui il presente schema è parte integrante, sono sottoscritti dal candidato nella "Domanda di certificazione" QI 60 01 04a ed annualmente con la sottoscrizione dell'Autodichiarazione prevista dalla sorveglianza/rinnovo della certificazione, nello stato di revisione applicabile. Tutti i documenti richiamati in questo schema, sono consultabili all'indirizzo http://www.khc.it/certificazione/privacy/.