PRASSI DI RIFERIMENTO 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”

Recommendations for conformity assessment to UNI 11697:2017 “Unregulated professional activities - Professional profiles related to processing and protection of personal data - Knowledge, skill and competence requirements”

La prassi di riferimento fornisce i requisiti specifici per la valutazione di conformità di parte terza esclusivamente delle figure professionali che operano nell’ambito del trattamento e della protezione dei dati personali, secondo quanto definito nella UNI 11697:2017.

Pubblicata il 19 settembre 2019 ICS 03.120.20, 35.020

ACCREDIA L’ENTE ITALIANO DI ACCREDITAMENTO

UNINFO

UNI ENTE ITALIANO DI NORMAZIONE

Via Sannio 2 – 20137 Milano
Telefono 02 700241
www.uni.com – uni@uni.com

PREMESSA

La presente prassi di riferimento UNI/PdR 66:2019 non è una norma nazionale, ma è un documento pubblicato da UNI, come previsto dal Regolamento UE n.1025/2012, che raccoglie prescrizioni relative a prassi condivise all'interno dei seguenti soggetti firmatari di un accordo di collaborazione con UNI:

UNINFO – TECNOLOGIE INFORMATICHE E LORO APPLICAZIONI
Via Sanfront, 1/C
10138 Torino TO

ACCREDIA – ENTE ITALIANO DI ACCREDITAMENTO
Via Guglielmo Saliceto, 7/9
00161 Roma

La presente prassi di riferimento è stata elaborata dal Tavolo “Valutazione della conformità alla UNI 11697” condotto da UNI, costituito dai seguenti esperti:

Riccardo Bianconi – Project Leader (ACCREDIA)

Nicola Fabiano (UNINFO)

Rosa Anna Favorito (AIOICI)

Franco Fontana (AIOICI)

Paolo Gianoglio (Conforma)

Fabio Guasconi (UNINFO)

Simona Montinari (ALPI)

Attilio Rampazzo (AICQ SICEV)

Emanuele Riva (ACCREDIA)

Si ringraziano Paola Generali, Fabrizio Bulgarelli, Fabio Ferrara, Angelo Freni, Alessandro Frillici, Alessio Pennasilico, Daniele Tumietto e Adalberto Biasiotti di UNINFO per il contributo fornito nell’elaborazione del documento.

La presente prassi di riferimento è stata ratificata dal Presidente dell’UNI il 18 settembre 2019.

Le prassi di riferimento, adottate esclusivamente in ambito nazionale, rientrano fra i “prodotti della normazione europea”, come previsti dal Regolamento UE n.1025/2012, e sono documenti che introducono prescrizioni tecniche, elaborati sulla base di un rapido processo ristretto ai soli autori, sotto la conduzione operativa di UNI.
Le prassi di riferimento sono disponibili per un periodo non superiore a 5 anni, tempo massimo dalla loro pubblicazione entro il quale possono essere trasformate in un documento normativo (UNI, UNI/TS, UNI/TR) oppure devono essere ritirate.

Chiunque ritenesse, a seguito dell’applicazione della presente prassi di riferimento, di poter fornire suggerimenti per un suo miglioramento è pregato di inviare i propri contributi all’UNI, Ente Nazionale Italiano di Unificazione, che li terrà in considerazione.

SOMMARIO

INTRODUZIONE 3

1 SCOPO E CAMPO DI APPLICAZIONE 4

2 RIFERIMENTI NORMATIVI E LEGISLATIVI 4

3 TERMINI E DEFINIZIONI 4

4 PRINCIPIO 5

5 PROFILI PROFESSIONALI UNI 11697 6

6 PROCESSO DI CERTIFICAZIONE DEL PERSONALE CHE OPERA NELL'AMBITO DEL TRATTAMENTO E PROTEZIONE DEI DATI PERSONALI 6

6.1 PROCESSO DI CERTIFICAZIONE 6

6.2 ORGANIZZAZIONI CHE EFFETTUANO LA VALUTAZIONE DI CONFORMITÀ 6

6.3 COMMISSIONE ESAMINATRICE 6

6.4 DECISION MAKER 7

6.5 REQUISITI DI ACCESSO 8

6.6 PROVE D'ESAME 8

6.7 METODI DI VALUTAZIONE 12

6.8 CRITERI PER IL SUPERAMENTO DELL'ESAME 13

6.9 CERTIFICAZIONE PER PIÙ PROFILI PROFESSIONALI 13

6.10 DURATA DELLA CERTIFICAZIONE 14

6.11 SORVEGLIANZA ANNUALE (ESAME DOCUMENTALE) 14

6.12 RINNOVO DELLA CERTIFICAZIONE 15

7 TRASFERIMENTO DEL CERTIFICATO 15

8 CENTRO D'ESAME (ORGANISMO DI VALUTAZIONE) 15

9 USO DEL MARCHIO DI CERTIFICAZIONE 16

APPENDICE A - ESPERIENZE LAVORATIVE DEL CANDIDATO 17

BIBLIOGRAFIA 19

INTRODUZIONE

ACCREDIA è l'Ente Unico Nazionale di accreditamento istituito in applicazione del Regolamento CE 765/2008, designato dal Governo italiano (Decreto del Ministero dello Sviluppo Economico del 22 dicembre 2009), riconosciuto in Italia ad attestare che gli organismi di certificazione ed ispezione, ed i laboratori di prova di taratura, abbiano le competenze e la dovuta imparzialità per valutare la conformità dei prodotti, dei processi, delle persone e dei sistemi agli standard di riferimento. ACCREDIA opera sotto la vigilanza del Ministero dello Sviluppo Economico e ha un ruolo di pubblica autorità, in quanto l'accreditamento è un servizio svolto nell'interesse pubblico e rappresenta un efficace strumento di qualificazione dei prodotti, persone e servizi che circolano su tutti i mercati. ACCREDIA, membro delle reti internazionali che legano gli Enti di accreditamento attraverso accordi di mutuo riconoscimento (EA e IAF ed ILAC), opera in linea con quanto stabilito dalla norma internazionale UNI CEI EN ISO/IEC 17011 e dalle linee guida applicabili.

La presente prassi di riferimento sostituisce ed integra la Circolare Tecnica 03/2018 di ACCREDIA.

La Circolare Tecnica 03/2018 è stata sviluppata da ACCREDIA per fornire indicazioni per l'accreditamento degli Organismi di Certificazione ai fini del rilascio di certificazioni di profili professionali relativi al trattamento e alla protezione dei dati personali di cui alla UNI 11697:2017. La circolare è stata predisposta da un gruppo di lavoro, coordinato da ACCREDIA, a cui hanno preso parte tutte le principali parti interessate con l'obiettivo di definire regole e criteri comuni per tutti gli enti di certificazione accreditati da ACCREDIA, indirizzando le attività svolte dai soggetti a vario titolo interessati in questo ambito.

Considerata la rilevanza non solo nazionale della UNI 11697:2017, alla luce del Regolamento (UE) 679/2016 del Parlamento europeo e del Consiglio del 27 aprile 2016, ACCREDIA ha ritenuto necessario far recepire la propria Circolare Tecnica 03/2018 dall'Ente Nazionale di Normazione (UNI). Questo ulteriore passaggio permette di completare lo schema di certificazione (requisiti e regole per verificare i requisiti) che, reso disponibile al mercato, è migliore garanzia di uniformità di approccio in quest'ambito a livello internazionale.

La certificazione di persone, rilasciata sotto accreditamento, è un'attività volontaria che costituisce una garanzia e atto di diligenza verso le parti interessate nel rispetto della legislazione vigente (L. 4/2013).

1 SCOPO E CAMPO DI APPLICAZIONE

La presente prassi di riferimento fornisce i requisiti specifici per la valutazione di conformità di parte terza rivolta esclusivamente alle figure professionali previste dalla UNI 11697:2017.

2 RIFERIMENTI NORMATIVI E LEGISLATIVI

La presente prassi di riferimento rimanda, mediante riferimenti datati e non, a disposizioni contenute in altre pubblicazioni. Tali riferimenti normativi e legislativi sono citati nei punti appropriati del testo e sono di seguito elencati. Per quanto riguarda i riferimenti datati, successive modifiche o revisioni apportate a dette pubblicazioni valgono unicamente se introdotte nel presente documento come aggiornamento o revisione. Per i riferimenti non datati vale l'ultima edizione della pubblicazione alla quale si fa riferimento.

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - "Disposizioni legislative in materia di documentazione amministrativa (Testo A)" pubblicato nella Gazzetta Ufficiale n. 42 del 20 febbraio 2001 - Supplemento ordinario n. 30

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 CEI EN ISO/IEC 17024 Valutazione della conformità - Requisiti generali per organismi che eseguono la certificazione di persone

3 TERMINI E DEFINIZIONI

Ai fini del presente documento valgono i termini e le definizioni della UNI 11697 e i seguenti.

3.1 candidato: Richiedente che possiede i prerequisiti specificati ed è stato ammesso al processo di certificazione.

[UNI CEI EN ISO/IEC 17024:2012, punto 3.14]

3.2 certificato: Documento emesso da un organismo secondo le disposizioni della UNI EN ISO/IEC 17024, indicante che la persona nominata ha soddisfatto i requisiti di certificazione.

[UNI CEI EN ISO/IEC 17024:2012, punto 3.5]

3.3 decision maker: Persona interna alla struttura dell'Organismo di Certificazione (OdC), ovvero con un incarico ad personam", che non è stato membro della commissione esaminatrice e che non ha alcun conflitto di interesse né con i candidati alla certificazione professionale, né con le strutture di formazione ove tali candidati sono stati preparati per sostenere l'esame. Il Decision Maker ha la responsabilità di assumere la decisione tecnica sulla certificabilità del candidato, sulla base delle evidenze definite dall'Organismo di Certificazione e dei criteri indicati dalla presente prassi di riferimento. A fronte della valutazione del Decision Maker, la direzione dell'OdC si assume la responsabilità dell'emissione dello specifico certificato di conformità.

3.4 esame: Attività che fanno parte della valutazione, che permettono di misurare la competenza di un candidato, mediante uno o più mezzi quali prove scritte, orali, pratiche od osservazione diretta, come definiti nello schema di certificazione.

[UNI CEI EN ISO/IEC 17024:2012, punto 3.9]

3.5 esaminatore: Persona che ha la competenza per condurre un esame e ove tale esame richieda un giudizio professionale, valutarne i risultati.

[UNI CEI EN ISO/IEC 17024:2012, punto 3.10]

3.6 grandparent: Esaminatore (3.5) qualificato in base ad una procedura interna dell'Organismo di Certificazione che possiede e attesta con evidenze documentali tutti i requisiti previsti dallo schema[1] (3.11).

3.7 imparzialità: Presenza di obiettività.

NOTA 1 Obiettività significa che non esistono conflitti di interesse o che questi sono stati risolti in modo da non influenzare negativamente le attività dell'Organismo di Certificazione.

NOTA 2 Altri termini utili per trasmettere il concetto d'imparzialità sono: obiettività, indipendenza, assenza di conflitto di interessi, assenza di preconcetti, assenza di pregiudizi, neutralità, onestà, apertura mentale, equità, distacco, equilibrio.

[Definizione adattata da UNI CEI EN ISO/IEC 17024:2012, punto 3.15]

3.8 processo di certificazione: Attività mediante le quali un Organismo di Certificazione stabilisce che una persona soddisfa i requisiti di certificazione. Tale processo comprende la valutazione della domanda presentata dal candidato (3.1), la successiva valutazione del candidato e le decisioni relative alla certificazione, il rinnovo della certificazione e all'utilizzo dei certificati e dei loghi/marchi.

[Definizione adattata da UNI CEI EN ISO/IEC 17024:2012, punto 3.1]

3.9 requisiti di certificazione: Insieme di requisiti specificati, comprendenti i requisiti dello schema da soddisfare al fine di rilasciare o mantenere la certificazione.

[UNI CEI EN ISO/IEC 17024:2012, punto 3.3]

3.10 richiedente: Persona che ha presentato una domanda per essere ammesso al processo di certificazione.

[UNI CEI EN ISO/IEC 17024:2012, punto 3.13]

3.11 schema di certificazione: Competenze ed altri requisiti, relativi a specifiche professioni o a categorie di persone specializzate aventi qualifiche o specifiche abilità.

[UNI CEI EN ISO/IEC 17024:2012, punto 3.2]

4 PRINCIPIO

La presente prassi di riferimento è stata elaborata per fornire indicazioni di carattere applicativo in relazione alle modalità di valutazione e certificazione delle persone, in conformità alla norma UNI 11697, che definisce i requisiti di conoscenza, abilità e competenza delle figure professionali operanti nell'ambito del trattamento e protezione dei dati personali.

Il documento fornisce in modo puntuale degli elementi comuni per la trasparenza e l'uniformità dei processi volontari di valutazione di conformità di parte terza finalizzati alla certificazione delle persone, gestiti dagli Organismi di Certificazione, accreditati in conformità alla norma UNI CEI EN ISO/IEC 17024.

[1] L'Organismo deve valutare per tale qualifica il titolo di studio, l'esperienza lavorativa specifica, le competenze e conoscenze acquisite tramite la formazione non formale e informale, ecc.

La prassi si completa con la seguente appendice:

Appendice A - Esperienze lavorative del candidato.

5 PROFILI PROFESSIONALI UNI 11697

La norma UNI 11697 definisce i requisiti di quattro profili professionali:

1. Responsabile della protezione dei dati personali (DPO);
2. Manager Privacy;
3. Valutatore Privacy;
4. Specialista Privacy.

6 PROCESSO DI CERTIFICAZIONE DEL PERSONALE CHE OPERA NELL'AMBITO DEL TRATTAMENTO E PROTEZIONE DEI DATI PERSONALI

6.1 PROCESSO DI CERTIFICAZIONE

Il processo di certificazione come definito dalla UNI CEI EN ISO/IEC 17024 comprende l'insieme delle attività che l'Organismo di Certificazione mette in atto per verificare se il candidato soddisfa i requisiti di competenza, abilità e conoscenza richiesti.

6.2 ORGANIZZAZIONI CHE EFFETTUANO LA VALUTAZIONE DI CONFORMITÀ

Per garantire l'efficacia ed efficienza del processo di certificazione e il massimo valore dei risultati della valutazione dei requisiti di cui alla UNI 11697, l'organizzazione che effettua la valutazione di conformità deve essere strutturata in modo da:

- garantire i necessari requisiti di indipendenza, imparzialità, trasparenza, competenza e assenza di conflitti di interesse;
- assicurare l'omogeneità delle valutazioni;
- definire, adottare e rispettare un proprio sistema di gestione per qualità documentato, in grado di garantire l'adozione di processi di certificazione conformi ai requisiti di questo documento e di garantire, altresì, la produzione e conservazione delle relative evidenze oggettive;
- rendere pubblico lo schema di certificazione, garantendo che questo sia coerente con i requisiti previsti dalla UNI 11697 ed alla presente prassi di riferimento.

I requisiti sopra indicati si intendono assolti da Organismi di Certificazione delle persone accreditati in conformità alla norma UNI CEI EN ISO/IEC 17024.

6.3 COMMISSIONE ESAMINATRICE

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

a) la conoscenza delle regole e criteri definiti dall'Organismo di Certificazione per l'esame di certificazione, che devono essere coerenti con quanto richiamato dalla UNI CEI EN ISO/IEC 17024;

b) il possesso della certificazione, sotto accreditamento, del profilo della norma UNI 11697, come riportato nella seguente tabella:

TABELLA DI CORRELAZIONE TRA COMPETENZE COMMISSARI E CANDIDATI	
Certificazione del Commissario	**Candidatura**
DPO	DPO, Manager, Specialista
Manager	Manager, Specialista
Valutatore	Valutatore, Specialista
Specialista	-

c) competenza, maturata a seguito di esperienze lavorative di almeno 8 anni, in ambito giuridico (es. avvocato, magistrato, giurista) con comprovata esperienza nell'ambito del trattamento e protezione dei dati personali e in materie attinenti la sicurezza delle informazioni con comprovata esperienza nell'ambito della protezione dei dati personali.

Per i primi tre anni di operatività, in sostituzione del membro della commissione esaminatrice in possesso di una certificazione sotto accreditamento nello stesso profilo oggetto di valutazione, l'Organismo di Certificazione può servirsi di grandparent (3.6) che posseggono i requisiti di cui ai precedenti punti a) e c).

I membri delle commissioni esaminatrici non possono essere stati docenti nei corsi di formazione specifica dei candidati (nel complesso del corso delle 80 ore, o per singoli moduli) salvo adottare specifiche misure di mitigazione dello specifico rischio per l'imparzialità, come, a titolo di esempio, la presenza in commissione di un ulteriore esaminatore. I Decision Maker non possono essere stati membri della commissione esaminatrice, né docenti nei corsi di formazione specifica dei candidati.

La composizione delle commissioni esaminatrici è una specifica responsabilità dei singoli Organismi di Certificazione (OdC).

6.4 DECISION MAKER

L'Organismo di Certificazione deve dotarsi di criteri di qualifica del Decision Maker, per assicurarsi che possieda adeguate competenze che comprendono i seguenti criteri minimi:

- conoscenza dei processi di delibera dell'OdC;
- conoscenza generale della norma UNI 11697.

A seguito della predisposizione della delibera di certificazione (analisi e parere di certificare o meno), la responsabilità di emettere il certificato di conformità rimane alla Direzione dell'Organismo di Certificazione (OdC), che esprime il parere finale, anche sulla base di ulteriori informazioni, che

possono essere di carattere non solo tecnico, in coerenza con quanto indicato nei regolamenti generale e di schema dell' Organismo di Certificazione (OdC), per le fattispecie applicabili, indicate nei paragrafi relativi alla sospensione e revoca della certificazione.

6.5 REQUISITI DI ACCESSO

Per essere ammessi all'esame i candidati devono soddisfare tutti i requisiti indicati nell'appendice B della UNI 11697, con i chiarimenti forniti dalla Nota riportata al punto 4.1 della norma medesima, attraverso la presentazione di idonea documentazione e dichiarare di non avere in corso altre richieste di certificazione per il medesimo profilo.

Per quanto riguarda la formazione specifica (corso e durata), ci si deve attenere a quanto scritto nell'Appendice B della norma UNI 11697, alla luce del punto 4.1. Il numero di ore complessivo può, quindi, essere raggiunto anche con più corsi di formazione o con l'effettuazione di docenza specifica. Non sono ammesse modalità alternative (come il "training on the job" o l'autoformazione).

Ove dei professionisti abbiano già seguito precedenti percorsi di formazione, non coincidenti con le indicazioni della norma UNI 11697, è cura dell'OdC effettuare una comparazione analitica tra il percorso già seguito dal candidato alla certificazione e il percorso illustrato nella norma medesima, assumendosi le responsabilità relative.

6.6 PROVE D'ESAME

6.6.1 GENERALITÀ

L'esame è strutturato sulla base di tre prove. Le prime due prove sono scritte, la prima basata su domande a risposta multipla per saggiare le conoscenze, la seconda sull'analisi di casi di studio per approfondire aspetti di competenza. Al superamento delle prove scritte, il candidato ha accesso all'esame orale che comprende: una fase di simulazione, delle domande di approfondimento della competenza e l'analisi e valutazione di lavori effettuati. L'esame orale è destinato a valutare in dettaglio le competenze dei candidati e approfondire eventuali criticità emerse nelle prove scritte.

Per lo scritto, devono essere previste griglie di correzione.

Per la prova scritta a risposta multipla, per la prima sessione di esame svolta dall'OdC, la commissione esaminatrice deve preparare domande in numero almeno doppio rispetto al numero di domande previsto per il profilo.

Dopo ogni sessione di esame il numero delle domande deve essere incrementato per creare una base dati/elenco di domande sufficientemente ampi in modo da mitigare il rischio di predisporre testi di esame, per sessioni successive, che contengano serie di domande uguali alle precedenti prove.

Quanto sopra previsto si applica anche ai casi di studio e alle simulazioni.

Le prove d'esame, nel loro insieme, devono ricoprire, per tutti i candidati alla certificazione nel medesimo profilo, le abilità, le conoscenze e le competenze previste dalla norma UNI 11697 per quel profilo.

Le domande devono essere aggiornate tenendo conto dell'evoluzione del contesto normativo e tecnologico.

Per l'orale, è preferibile che le domande sottoposte al candidato siano il più possibile rappresentative delle diverse aree di competenza, compatibilmente con la dinamica di svolgimento dello stesso esame e stante l'approfondimento delle conoscenze garantito dalle domande delle prove scritte.

6.6.2 VERIFICHE PRELIMINARI

L'Organismo di Certificazione, tramite la propria struttura tecnica, con il supporto di almeno un commissario d'esame, dovrà effettuare l'analisi dei curricula dei richiedenti l'accesso all'esame di certificazione per verificare la congruità delle informazioni riportate a fronte dei requisiti indicati nella domanda d'esame (informazioni inerenti il percorso professionale, di formazione, ecc.); inoltre devono essere verificati i documenti comprovanti le attività e i titoli indicati sul curriculum e richiesti, come allegati, dalla domanda di certificazione.

All'esito positivo di questa verifica, l'OdC comunica al richiedente il suo status di candidato all'esame e la data della prima sessione disponibile.

6.6.3 MODALITÀ DI SVOLGIMENTO DELL'ESAME

Il punto 6 della UNI 11697 elenca più metodi di valutazione, riportati di seguito con alcune note di chiarimento.

Si rimanda ai singoli profili professionali riportati nel punto a seguire per comprendere quali di questi metodi siano applicabili e obbligatori.

Prospetto 1 – Fasi esame di certificazione

N°	METODO DI VALUTAZIONE	NOTE DI CHIARIMENTO
1	Esame scritto per la valutazione delle conoscenze	L'esame scritto consiste in una serie di domande chiuse a risposta multipla. La durata complessiva dell'esame è determinata dal prodotto del numero delle domande previste per il profilo per due minuti. Le domande devono coprire gli elementi di conoscenza, previsti dalla norma UNI 11697, per lo specifico profilo. Durante l'esame il candidato può consultare i seguenti documenti forniti dall'OdC o dall'Organismo di Valutazione: – norma UNI 11697:2017; – Regolamento (UE) 679/2016 e s.m.i.; – D.Lgs. 196/2003 per come integrato dal D.Lgs. 101/2018; – raccolta non commentata dei provvedimenti del Garante per la Privacy.

N°	METODO DI VALUTAZIONE	NOTE DI CHIARIMENTO
2	Esame scritto su “casi di studio”	Al candidato vengono sottoposti i casi di studio nel numero previsto per il profilo professionale richiesto. Tali prove sono finalizzate a verificare l'attitudine, le abilità, le competenze e le conoscenze del medesimo su questioni pratiche connesse al profilo professionale oggetto di certificazione. Il caso di studio deve porre al candidato una situazione reale operativa a cui il candidato deve rispondere nel modo più corretto con la trattazione del caso. La durata complessiva dell’esame è determinata dal prodotto del numero dei casi di studio previsti per il profilo per dieci minuti. Per il superamento di ogni prova tipo "caso di studio", composta da più quesiti, il valore del punteggio complessivo attribuito è quello della media dei punteggi dei diversi casi di studio, con il vincolo di aver ottenuto almeno 5/10 per la peggiore delle risposte. Il superamento della prova, si ha con l’ottenimento di un voto medio di 70/100.
3	Risposte errate	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.
4	Esame orale	L’esame orale inizia con l’approfondimento delle risposte errate della prova scritta, ove presenti, e comprende: – simulazioni di situazioni reali operative per valutare, oltre alle abilità e alle 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. NOTA: La “simulazione” sopra richiamata è da intendersi come l’applicazione operativa in sede di esame della fase di “role play” richiesta dalla norma UNI 11697 al punto 6;

N°	METODO DI VALUTAZIONE	NOTE DI CHIARIMENTO
		– analisi e valutazione di uno dei tre elaborati presentati in fase di domanda di certificazione dal candidato e frutto della propria esperienza lavorativa (alla commissione esaminatrice deve essere presentato un elaborato redatto secondo un modello - vedere Appendice A - relativo a una situazione lavorativa, considerata significativa dal candidato a fronte della specifica figura professionale richiesta). La discussione di questo elaborato è parte integrante dell'esame orale; – domande su tematiche complementari a quelle del 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. Per l'approfondimento di ciascuna domanda la commissione esaminatrice deve avere a disposizione mediamente 3 minuti con il vincolo di non superare i 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). Ove, in tale fase, dovessero emergere significative carenze teoriche o di competenza, l'esame deve essere considerato non superato. Durante l'esame orale si deve prevedere l'approfondimento, di per tutti i candidati, 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.

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 d'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 dei candidati 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 e/o tecnico facilitatore nella compilazione dei verbali di esame, senza avere alcun diritto di esprimere pareri sulle valutazioni dei membri della commissione.

Il verbale di esame deve prevedere la registrazione (nel corpo del testo o come allegato) delle domande di esame somministrate con le diverse prove in generale e, per singolo candidato, delle

prove scritte sostenute, con la relativa correzione, e delle domande orali, con la relativa valutazione dei due commissari di esame. Tali 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.

6.7 METODI DI VALUTAZIONE

Prospetto 2 – Metodi di valutazione dei profili professionali

N°	PROFILI PROFESSIONALI	METODO DI VALUTAZIONE
1	Responsabile della protezione dei dati personali	• Una prova scritta composta da almeno 40 domande a risposta multipla • Esame scritto su almeno 3 casi di studio • Esame orale dalla durata minima di 40 minuti (compresa la simulazione di situazioni reali operative, della durata di circa 10 minuti, e l'analisi e la valutazione di lavori effettuati)
2	Manager Privacy	• Una prova scritta composta da almeno 35 domande a risposta multipla • Esame scritto su almeno 3 casi di studio • Esame orale dalla durata minima di 40 minuti (compresa la simulazione di situazioni reali operative, della durata di circa 10 minuti, e l'analisi e la valutazione di lavori effettuati)
3	Specialista privacy	• Una prova scritta composta da almeno 35 domande a risposta multipla • Esame scritto su almeno 2 casi di studio • Esame orale dalla durata minima di 30 minuti (compresa la simulazione di situazioni reali operative, della durata di circa 10 minuti, e l'analisi e la valutazione di lavori effettuati)
4	Valutatore Privacy	• Una prova scritta composta da almeno 35 domande a risposta multipla • Esame scritto su almeno 2 casi di studio • Esame orale dalla durata minima di 30 minuti (compresa la simulazione di situazioni reali operative, della durata di circa 10 minuti, e l'analisi e la valutazione di lavori effettuati) • Nell'esame orale, il candidato deve dimostrare di avere competenza specifica per la predisposizione di piani di audit specifici per la fattispecie oggetto di valutazione, quindi di avere conoscenza e competenza anche nell'ambito del campionamento necessario a garantire la conformità ai requisiti del GDPR

6.8 CRITERI PER IL SUPERAMENTO DELL'ESAME

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 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 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.

6.9 CERTIFICAZIONE PER PIÙ PROFILI PROFESSIONALI

È possibile sostenere l'esame di certificazione per più profili in una medesima sessione o in più sessioni.

Il candidato che - in possesso dei requisiti di accesso previsti dalla UNI 11697:2017 - richieda la certificazione nella medesima sessione per più profili, sostiene l'esame completo per il profilo classificato come più complesso e sostiene prove di esame ridotte, per ciascuno dei profili aggiuntivi, come di seguito descritto:

- 10 domande a risposta multipla per ogni profilo aggiuntivo;
- un esame scritto su 1 "caso di studio" per ogni profilo aggiuntivo;
- minimo 15 minuti di esame orale per ogni profilo aggiuntivo.

Il candidato, già certificato per almeno un profilo, che richieda, in una sessione di esame successiva, la certificazione di profili aggiuntivi, diversi dal Responsabile della protezione dei dati personali (DPO), sostiene prove di esame ridotte, per ciascuno dei profili aggiuntivi, come di seguito descritto:

- 20 domande a risposta multipla per ogni profilo aggiuntivo;
- un esame scritto su 1 "caso di studio" per ogni profilo aggiuntivo;
- esame orale della durata minima di 20 minuti per ogni profilo aggiuntivo.

Il candidato, già certificato per almeno un profilo, che richieda, in una sessione di esame successiva, la certificazione per il profilo di Responsabile della protezione dei dati personali (DPO), sostiene le seguenti prove di esame:

- 30 domande a risposta multipla;
- un esame scritto su 2 "casi di studio";
- esame orale della durata minima di 30 minuti.

NOTA La classificazione dei profili per complessità, è la seguente:

- Responsabile della protezione dei dati personali (DPO);
- Manager Privacy;
- Valutatore Privacy;
- Specialista Privacy.

Tale classificazione, che non intende creare una gerarchia degli stessi, è basata sui compiti, attività nonché abilità e conoscenze previste dalla UNI 11697:2017, ed è funzionale a dare un'indicazione operativa all'OdC in merito al livello di completezza delle competenze in ambito GDPR.

6.10 DURATA DELLA CERTIFICAZIONE

La certificazione ha validità di 4 anni e il suo mantenimento è subordinato all'esito positivo della sorveglianza effettuata dall'OdC con cadenza annuale.

6.11 SORVEGLIANZA ANNUALE (ESAME DOCUMENTALE)

Durante il ciclo di certificazione, l'Organismo di Certificazione, anno per anno, deve effettuare delle verifiche, per mantenere e confermare la validità delle certificazioni emesse, per ogni singolo professionista certificato.

La verifica documentale può essere effettuata in assenza del candidato e riguarda i seguenti documenti:

1) almeno un incarico/attività/contratto attraverso il quale si dimostri di aver operato con continuità nell'ambito dei compiti richiamati dalla norma UNI 11697;

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 16 ore/anno per il DPO, e 8 ore per gli altri 3 profili;

3) una "autodichiarazione" ai sensi degli artt. 46 e 76 del D.P.R. 445/2000 contenente:

   a) le attività svolte di cui al precedente punto 1), rispetto ai punti 4 e 5 della norma UNI 11697, specifiche nel campo della protezione dati, durante l'anno;

   b) l'elenco di cui al precedente punto 2), dei corsi di aggiornamento, partecipazione a convegni, seminari, relazioni, docenze, inerenti gli argomenti relativi nel settore della privacy come declinato nelle tabelle riepilogative per profilo;

   c) la presenza di eventuali reclami e/o contenziosi relativi all'attività certificata;

   d) il pagamento regolare delle quote annuali dovute all'Organismo di Certificazione, se previste.

Nel caso in cui siano presenti reclami o contenziosi legali spetta all'OdC valutare l'adeguatezza della relativa gestione, sulla base della tempestività e congruenza delle azioni intraprese dal professionista. Dopo la risposta iniziale, da fornire entro 10 giorni lavorativi al reclamante, il professionista provvede ad adottare le misure necessarie (compreso il mancato seguito a reclami ritenuti non applicabili) entro 6 settimane calendariali, dando la necessaria risposta al reclamante. Di tale processo (ricezione del reclamo, prima risposta, analisi e azione discendente) il professionista deve tenere adeguata tracciabilità documentale.

L'attività di sorveglianza può avere come esito il mantenimento, la sospensione o la revoca della certificazione a fronte della valutazione dell'OdC in merito alla completezza, congruità della documentazione presentata nonché gestione di eventuali reclami e/o contenziosi legali

6.12 RINNOVO DELLA CERTIFICAZIONE

Il rinnovo della certificazione è condotto dall'Organismo di Certificazione, a fronte della richiesta del professionista prima della fine della validità della certificazione posseduta.

Oltre a raccogliere, verificare e valutare le evidenze già previste per l'attività di sorveglianza, l'OdC deve assicurarsi che siano mantenute le competenze previste dal punto 5 della norma UNI 11697.

In sede di rinnovo, il professionista sostiene una prova scritta con domande a risposta multipla strutturata come la prima prova scritta di certificazione (sola conoscenza).

Nel caso in cui il candidato non superi tale prova, questi può ripeterla in una sessione successiva, durante il periodo di validità della certificazione. In questo caso il professionista ripete la prova scritta con domande a risposta multipla e sostiene, in aggiunta, l'esame scritto sui casi di studio.

In caso di esito negativo del secondo tentativo, il professionista, sostiene nuovamente l'esame di certificazione (domande a risposta multipla, casi di studio ed esame orale). Nel frattempo, se scade il periodo di validità del certificato, lo stesso viene revocato.

NOTA Tutte le prove previste per il rinnovo sono strutturate e hanno i medesimi i criteri di superamento di quelle dell'esame di certificazione.

7 TRASFERIMENTO DEL CERTIFICATO

Il trasferimento tra OdC accreditati di un certificato rilasciato ad un professionista, può essere perfezionato in qualsiasi momento, presentando richiesta all'OdC subentrante, con allegato il certificato in corso di validità, e sostenendo l'esame orale con le stesse modalità previste per la certificazione.

Anche i documenti applicabili per la sorveglianza devono essere presentati dal candidato al nuovo Organismo.

Il candidato deve anche fornire l'evidenza di chiusura di eventuali pendenze (economiche e tecniche) aperte dall'Organismo precedente nei suoi confronti.

Al completamento con esito positivo di questa istruttoria, l'OdC subentrante deve deliberare l'emissione del proprio Certificato di Conformità, che manterrà la scadenza di quello precedente.

8 CENTRO D'ESAME (ORGANISMO DI VALUTAZIONE)

Ove l'OdC intenda affidare all'esterno, in tutto o in parte, le attività operative relative al processo di certificazione, deve rispettare le prescrizioni di cui al punto 6.3 della norma UNI CEI EN ISO/IEC 17024 nella versione vigente. A questo proposito può essere contrattualizzato un "Centro di Esame" (Organismo di Valutazione). Un "Centro di Esame" (Organismo di Valutazione) è una organizzazione (un'Associazione Professionale, un Ordine Professionale), qualificata dall'OdC, che organizza e conduce le sessioni di esame. Tale organizzazione deve operare sotto il controllo e secondo le specifiche/procedure emesse dall'OdC e assicurare la propria imparzialità nei confronti di ogni candidato che richiede la certificazione, portando all'attenzione dell'OdC tutte le minacce effettive o potenziali alla propria imparzialità.

Poiché tale modalità costituisce una possibile minaccia al principio dell'imparzialità (si veda anche quanto previsto dall'Organismo di Certificazione) deve gestire tale situazione adeguatamente nell'analisi dei rischi.

In particolare, le date d'esame devono essere preventivamente comunicate, secondo la tempistica stabilita dall'OdC nel contratto con l'OdV o Centro di Esame, all'Organismo di Certificazione, perché questo possa pianificare delle verifiche, non annunciate o in incognito (c.d. mistery).

L'OdC determina, in base al rischio identificato, la frequenza e la modalità delle verifiche.

Le verifiche dal personale dell'Organismo di Certificazione presso il Centro d'Esame devono essere previste contrattualmente fra le parti.

L'OdC deve rendere disponibili all'Ente di Accreditamento, sia su richiesta, sia in occasione delle verifiche sullo specifico schema, le statistiche degli esiti degli esami erogati nei vari centri d'esame.

NOTA 1 La qualifica iniziale e il monitoraggio periodico dei commissari d'esame che operano nell'ambito della struttura del "Centro di Esame" deve essere gestita dall'Organismo di Certificazione.

NOTA 2 Per alcuni schemi il centro di esame è definito Organismo di Valutazione.

9 USO DEL MARCHIO DI CERTIFICAZIONE

Le organizzazioni che effettuano la valutazione di conformità devono prevedere regole per la concessione della licenza d'uso del proprio Marchio di certificazione che includa anche l'utilizzo del marchio UNI.

NOTA Il Marchio di conformità UNI ha lo scopo di attestare che i requisiti dei prodotti/servizi, sistemi o persone certificati siano stabiliti dall'UNI tramite la pubblicazione di norme o prassi di riferimento.

APPENDICE A - ESPERIENZE LAVORATIVE DEL CANDIDATO

A.1 GENERALITÀ

La presente Appendice propone un fac-simile in cui il candidato, in fase di presentazione della domanda di certificazione per uno dei quattro profili considerati nella presente prassi di riferimento, deve inserire l'esperienza lavorativa che ritiene più significativa a fronte della specifica figura professionale (vedere punto 6.6).

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.

A.2 MODELLO DI PRESENTAZIONE ESPERIENZA LAVORATIVA DEL CANDIDATO

La compilazione del modello che segue deve far riferimento ai contenuti previsti nella UNI/PdR 66:2019:

ESPERIENZA LAVORATIVA DA DISCUTERE IN SEDE DURANTE L'ESAME ORALE

Profilo richiesto:

□ Responsabile della protezione dei dati personali (DPO)

□ Manager Privacy

□ Specialista Privacy

□ Valutatore Privacy

Periodo di riferimento:

data di avvio (__/__/____)

data di termine (__/__/____)

Settore di attività: ……

Oggetto della consulenza/attività gestita dal candidato:
……
……
……
……
……

Denominazione/breve descrizione/obiettivo/i del progetto:
……
……
……
……
……
……
……

Modalità adottate dal candidato per la gestione dell'attività sopra descritta:
……
……
……
……
……
……
……
……
……

Descrizione di maggior dettaglio che comprenda le attività, metodi e/o strumenti utilizzati dal candidato, i principali documenti e risultati del progetto, le criticità riscontrate, le soluzioni:
……
……
……
……
……
……
……
……
……

BIBLIOGRAFIA

[1] 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

[2] ISO/IEC 27021 Information technology - Security techniques - Competence requirements for information security management systems professionals

ENTE ITALIANO
DI NORMAZIONE

Membro italiano ISO e CEN
www.uni.com
www.youtube.com/normeuni
www.twitter.com/normeuni
www.twitter.com/formazioneuni
www.linkedin.com/company/normeuni

Sede di Milano
Via Sannio, 2 - 20137 Milano
tel +39 02700241, Fax +39 0270024375, uni@uni.com

Sede di Roma
Via del Collegio Capranica, 4 - 00186 Roma
tel +39 0669923074, Fax +39 066991604, uni.roma@uni.com