Icmq S.p.A. (A Socio Unico)
Società Benefit
Via G. De Castillia, 10 – 20124 Milano
Tel. 02 7015081 – Fax 02 70150854
icmq@icmq.org – www.icmq.it
P.I. 13218350158

REGOLAMENTO TECNICO
PER LA CERTIFICAZIONE DEL PERSONALE
NELL'ATTIVITÀ DI

DPO - Responsabile della protezione dei dati

INDICE

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento stabilisce i principi e i criteri per la valutazione delle competenze dei Candidati alla certificazione di “Responsabile della protezione dei dati” (in inglese DPO – Data Protection Officer) e stabilisce le modalità di esecuzione e di valutazione delle prove d’esame.

Il Responsabile della protezione dei dati è un professionista corrispondente al profilo professionale disciplinato nel Regolamento UE 2016/679, all’art. 39. È consentita l’assegnazione a tale profilo di compiti diversi e/o ulteriori inclusi in altri profili di livello manageriale nel rispetto del principio di assenza di conflitto di interessi.

Il Responsabile della protezione dei dati supporta i titolari o i responsabili del trattamento nell'applicazione del Regolamento UE 2016/679 o di altra legislazione applicabile in materia di protezione dei dati. La sua missione è di supportare i titolari o i responsabili del trattamento in merito ai rischi delle attività di trattamento dei dati per garantire l’osservanza del Regolamento UE 2016/679 e delle altre disposizioni locali in materia di protezione dei dati.

Questo profilo è responsabile (accountable) dei seguenti risultati:

- Relazioni periodiche basate sul rischio sull’osservanza delle norme di legge in materia di protezione dei dati personali.

- Documentazione a supporto della richiesta di consultazione preventiva all’Autorità di controllo, a seguito della valutazione d'impatto sulla protezione dei dati.

- Richieste di consultazione all’Autorità di controllo su questioni applicative specifiche.

- Documentazione relativa all’attività di interfacciamento con l’Autorità di controllo (richieste di informazione, procedure di accertamento o verifica, ecc.).

- Documentazione (inclusa modulistica) di interfaccia con gli interessati.

- Indicatori sulla protezione dei dati personali.

- Consulenza in merito a richieste di informazioni sulla legge sulla protezione dei dati e sulla sua applicazione.

Questo profilo è referente (responsible) dei seguenti risultati:

- Pareri sulle valutazioni d'impatto sulla protezione dei dati ai sensi del Regolamento 2016/679.

Questo profilo è collaboratore (contributor) per i seguenti risultati:

- Attribuzione delle responsabilità in ambito trattamento e protezione dei dati personali.

- Budget per la protezione dei dati personali.

- Politica per la protezione dei dati personali.

- Informativa sulla protezione dei dati.

- Requisiti per il trattamento e la protezione dei dati personali.

- Procedure operative per il trattamento e la protezione dei dati personali.

- Sviluppo di una valutazione di impatto sulla protezione dei dati.

- Valutazione del rischio relativo alla sicurezza delle informazioni.

- Piano di trattamento del rischio relativo alla sicurezza delle informazioni.

- Codici di condotta.

- Risposte agli interessati che esercitano i loro diritti.

- Programma di audit per la protezione e il trattamento dei dati personali.

- Programma di formazione, aggiornamento e consapevolezza.

- Notifiche di incidenti che diano luogo a una violazione dei dati personali (alla autorità di protezione dei dati personali).

2. RIFERIMENTI

2.1. Riferimenti di settore

- UNI CEI EN 17740:2024 “Requisiti per i profili professionali relativi al trattamento e protezione dei dati personali”

- UNI/TS 11945:2024 “Valutazione di conformità ai requisiti definiti dalla UNI EN 17740 “Requisiti per i profili professionali relativi al trattamento e protezione dei dati personali"

2.2. Riferimenti generali

- UNI CEI EN ISO/IEC 17024 “Requisiti generali per gli organismi che operano nella certificazione del Personale”.
- Legge n. 4 del 14/01/2013 “Disposizioni in materia di professioni non organizzate”
- Raccomandazione del Parlamento Europeo e del Consiglio 2009/C 155/02 del 18 giugno 2009 sull'istituzione di un sistema europeo di crediti per l'istruzione e la formazione professionale (ECVET)
- Raccomandazione del Parlamento europeo e del Consiglio, del 23 aprile 2008, sulla costituzione del quadro europeo delle qualifiche per l'apprendimento permanente (EFQ) (Gazzetta ufficiale C 111 del 6.5.2008).
- EN 16234-1 e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all sectors - Part 1: Framework
- PS DOC 01 Condizioni generali di contratto per la certificazione del personale (vedasi per tutti gli aspetti contrattuali generali)

3. DEFINIZIONI

Si utilizzano termini e definizioni riportati nei documenti di riferimento, in particolare i seguenti:

Candidato: persona che svolge l’attività oggetto di certificazione e che partecipa al processo di certificazione medesimo.

Organismo di Certificazione: Organismo indipendente che attua e gestisce un sistema di certificazione di conformità che consente di dichiarare che determinate persone operano con adeguata competenza e seguono le specifiche di un determinato regolamento tecnico.

Organismo di Valutazione (OdV): Organismo che, indipendente da qualsiasi interesse predominante, è qualificato da ICMQ a preparare e gestire gli esami di certificazione.

Valutazione: azione mediante la quale l’OdV accerta la competenza del candidato e controlla l’operato della persona certificata al fine di giudicare la sua conformità alle norme e regolamenti di riferimento.

Esaminatore: persona incaricata dall’OdV, in possesso di pertinenti qualifiche personali e tecniche, competente a condurre gli esami e ad assegnare i relativi punteggi.

Certificato: documento rilasciato da ICMQ in conformità alle regole dello schema di certificazione e definito nelle Condizioni Generali di Contratto.

Centro di esame: luogo qualificato da ICMQ nel quale vengono svolti gli esami.

Prova scritta: test scritto con domande a risposta multipla, ossia formulazione di una domanda che dà origine a tre potenziali risposte, una delle quali è corretta, mentre le restanti due sono errate o incomplete.

Prova pratica: prova composta da un caso di studio relativo ad una problematica specifica all'attività professionale e di complessità coerente al livello professionale.

Prova orale: colloquio tra candidato ed esaminatore che valuta le conoscenze specifiche e le nozioni teoriche del candidato definite dal presente regolamento.

Si utilizzano inoltre i seguenti acronimi:
RSC = Responsabile Schema di Certificazione
OdC = Organismo di Certificazione
OdV = Organismo di Valutazione
CdC = Comitato di Certificazione

4. ESAME DI CERTIFICAZIONE

4.1. Requisiti di accesso all'esame

Per essere ammesso all'esame di certificazione il candidato deve documentare i requisiti minimi riportati sotto forma di tabelle per ciascuno profilo:

SCHEMA RIASSUNTIVO REQUISITI DI ACCESSO AL PROCESSO DI CERTIFICAZIONE (Rif. APPENDICE B requisiti per l'accesso ai profili professionali)			
PROFILO	**APPRENDIMENTO FORMALE**	**APPRENDIMENTO NON FORMALE**	**APPRENDIMENTO INFORMALE**
DPO Responsabile della protezione dei dati	diploma di scuola secondaria di secondo grado	Corso di almeno 80 ore con attestazione finale avente per argomento la gestione della protezione dei dati e della sicurezza delle informazioni [b)]	8 anni di esperienza lavorativa legata alla protezione dei dati, di cui almeno 5 anni in posizioni manageriali [c)]
	Laurea che includa discipline almeno in parte afferenti alle conoscenze del professionista della protezione dei dati, legali o tecnico / informatiche [a)]		6 anni di esperienza lavorativa legata alla protezione dei dati, di cui almeno 4 anni in posizioni manageriali [c)]
	Laurea magistrale che includa discipline almeno in parte afferenti alle conoscenze del professionista della protezione dei dati, legali o tecnico / informatiche [a)]		4 anni di esperienza lavorativa legata alla protezione dei dati, di cui almeno 3 anni in posizioni manageriali [c)]

a) Un laureato con laurea non afferente alle conoscenze del professionista della protezione dei dati, legali o tecnico / informatiche è da considerarsi equiparato a un diploma di scuola media superiore.

b) È ammissibile la riduzione delle ore di formazione richieste fino a un massimo del 10% in caso di possesso di certificazioni professionali riconosciute come attinenti alle conoscenze richiesta al professionista in questione. Il numero di ore complessivo può 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).

c) Le posizioni di livello manageriale possono includere anche attività rilevante svolta nell'ambito di attività di consulenza o di prestazione d'opera condotta nell'ambito dell'esecuzione di ingaggi professionali.

4.2. Conoscenze, abilità e competenze

Il professionista operante nell'ambito del trattamento e della protezione dei dati personali svolge un'ampia gamma di attività aventi frequentemente natura trasversale rispetto agli altri processi aziendali, sia rispetto al ciclo di vita del trattamento - dalla progettazione fino alla cessazione - sia rispetto ai temi trattati, tecnologici, legali e di altro tipo.

Il professionista operante nell'ambito del trattamento e della protezione dei dati personali contribuisce quindi alla gestione o alla verifica di un insieme più o meno ampio di processi e sistemi informativi

coinvolti nel trattamento di dati personali per conto di persone fisiche o giuridiche quali per esempio enti, istituzioni, associazioni, soggetti pubblici o privati.

Ai fini del processo di certificazione del Responsabile della protezione dei dati è richiesta l'evidenza del possesso delle competenze necessarie allo svolgimento dei propri compiti.

Tale evidenza è data dalla dimostrazione di essere in grado di applicare, in relazione ai compiti del profilo, requisiti di conoscenza, abilità e capacità personali (aspetti comportamentali).

4.2.1. Compiti

I principali compiti associati a questo profilo sono:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri in materia di protezione dei dati;
- sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresa l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni relative al trattamento.

Il seguente prospetto 1 mostra le competenze assegnate e i livelli richiesti secondo l'e-CF

previsto dalla EN 16234-1.

Competenza e-CF	Descrizione e-CF	Livello	Descrizione livello di competenza
D.8 Gestione del Contratto	Fornisce e negozia il contratto in conformità con i processi organizzativi. Garantisce che il contratto e i risultati finali siano forniti in tempo e soddisfino la qualità standard e siano in linea ai requisiti di conformità. Indirizza le non conformità, segnala problemi significativi, guida piani di ripristino e, se necessario, modifica i contratti. Mantiene l'integrità del budget. Valuta e indirizza il fornitore al rispetto degli standard legali, sanitari e di sicurezza. Stabilisce e mantiene rapporti con i fornitori.	3	Valuta le prestazioni di contratto e monitora gli indicatori di prestazione. Assicura le prestazioni dell'intera supply chain. Influenza i termini del contratto di rinnovo.
D.9 Sviluppo del Personale	Esegue la diagnosi delle competenze individuali e di gruppo, identificando i fabbisogni di competenze e le lacune di competenze. Esamina le opzioni di formazione e sviluppo e seleziona la metodologia appropriata tenendo conto delle esigenze individuali, progettuali e aziendali. Forma e guida individui e team verso il soddisfacimento delle esigenze di apprendimento.	3	Monitora e affronta lo sviluppo e le esigenze di individui e squadre.

E.3 Gestione del Rischio	Implementa la gestione del rischio nei sistemi informativi attraverso l'applicazione della politica e della procedura di gestione del rischio definita dall'impresa. Valuta i rischi per l'attività dell'organizzazione, inclusi web, cloud e dispositivi mobili e risorse. Documenta i potenziali rischi e i piani di contenimento.	4	Fornisce la leadership necessaria a definire e rendere fattibile una policy di risk management considerando tutti i possibili vincoli, compresi quelli tecnici, economici e politici. Delega incarichi.
E.4 Gestione delle Relazioni	Sviluppa relazioni commerciali positive con l'ambiente dei diversi stakeholder ambiente facilitando la collaborazione multidisciplinare del team. Mantiene comunicazione regolare con colleghi, clienti, partner e fornitori, mostra empatia con i loro diversi contesti e prospettive. Garantisce che le diverse esigenze, preoccupazioni o reclami delle parti interessate siano compresi e affrontati in conformità con la politica organizzativa.	4	Fornisce leadership in complesse relazioni multi-stakeholder autorizzando investimenti quando necessari. Diffonde consapevolezza aziendale dei benefici legati ad un approccio multidisciplinare.
E.8 Gestione della Sicurezza delle Informazioni	Gestisce le politiche di sicurezza delle informazioni e dei sistemi tenendo conto degli aspetti tecnici, umani, delle minacce organizzative e altre minacce rilevanti, in linea con la strategia IT e aziendale e riflette la cultura del rischio dell'organizzazione. Distribuisce e gestisce gli operativi e gli specialisti (ad esempio forensic, threat intelligence e controlli intrusione), risorse necessarie per garantire la capacità di gestire gli incidenti di sicurezza, e formula raccomandazioni per il miglioramento continuo della politica di sicurezza e strategia.	3	Valuta misure e indicatori di gestione della sicurezza e la conformità alla policy di sicurezza delle informazioni. Investiga e propone le misure di rimedio per eventuali violazioni della sicurezza.

4.2.2. Conoscenze

Le conoscenze associate a questo profilo sono:

- I principi di protezione dei dati, inclusa la protezione dei dati fin dalla progettazione (by design) e per impostazione predefinita (by default)
- I diritti degli interessati previsti da leggi e regolamenti vigenti
- Le responsabilità connesse al trattamento dei dati personali
- Norme di legge locali ed europee in materia di trattamento e di protezione dei dati personali
- Sviluppi legali legati a decisioni giudiziarie locali ed europee
- Norme di legge in materia di trasferimento di dati personali all'estero e circolazione dei dati personali extra UE/SEE
- Le metodologie di valutazione d'impatto sulla protezione dei dati
- Le possibili minacce alla protezione dei dati personali
- 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
- Tecniche e strumenti di comunicazione (relazione con Istituzioni, autorità, Forze dell'ordine, enti locali e stampa)
- Le tecniche crittografiche
- Le tecniche di anonimizzazione
- Le tecniche di pseudonimizzazione
- Sistemi e tecniche di monitoraggio e "reporting"
- Strumenti per la produzione, l'editing e la distribuzione di documenti professionali
- K49 - 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 delle informazioni
- K71 - tipici KPI (key performance indicator - Applicazione del Regolamento UE 2016/679)
- K83 - il potenziale e le opportunità degli standard e delle best practices più rilevanti
- K85 - il ritorno dell'investimento comparato all'evitamento del rischio
- K98 - l'impatto dei requisiti legali sulla sicurezza dell'informazione
- K108 - computer forensics
- K115 - la politica di gestione della sicurezza delle aziende e le sue implicazioni per l'impegno con i clienti, i fornitori e i sub-fornitori
- K122 - la strategia dell'informazione nell'organizzazione
- K130 - best practice (metodologie) e standard nell'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 - norme legali applicabili ai contratti ICT
- K152 - nuove tecnologie emergenti (per esempio sistemi distribuiti, modelli di virtualizzazione, data set, sistemi mobile)
- K158 - possibili minacce alla sicurezza
- K161 - sfide relative alla dimensione dei data set (per esempio big data)
- K162 - sfide relative ai dati non strutturati (per esempio data analytic)
- K180 - tecniche di attacco informatico e contromisure per evitarli

4.2.3. Abilità

Le abilità associate a questo profilo sono:

- Analizzare il trattamento dei dati personali e valutarne la conformità ai requisiti legali applicabili
- Verificare l'applicazione della protezione dei dati fin dalla progettazione (by design) e della protezione per impostazione predefinita (by default)
- Verificare l'applicazione appropriata dei principi di protezione dei dati
- Identificare i ruoli, le responsabilità e le basi legali per il trattamento dei dati personali
- Contribuire alla strategia per il trattamento e la protezione dei dati personali
- Contribuire alla fornitura di informazioni corrette agli interessati

- Gestire l'applicazione dei codici di condotta e delle certificazioni applicabili in materia di trattamento e protezione dei dati personali
- Capacità di comunicare
- Capacità di analisi
- Autogestione e controllo dello stress
- Capacità di autosviluppo
- Capacità di controllo
- Capacità di convincimento
- Capacità di gestione dei conflitti
- Iniziativa
- Idoneità alla negoziazione
- Capacità organizzative Pensiero prospettico
- Pianificazione e programmazione
- Atteggiamento costruttivo nella soluzione dei problemi
- Tenacia
- S1 - affrontare le esigenze della formazione continua (CPD) del personale per soddisfare le esigenze dell'organizzazione
- S5 - analizzare gli asset critici dell'azienda e identificare debolezze e vulnerabilità riguardo a intrusioni o attacchi
- S19 - anticipare i cambiamenti richiesti alla strategia aziendale dell'information security e formulare nuovi piani
- S21 applicare azioni di contenimento
- S23 - applicare gli standard, le best practice e i requisiti legali più rilevanti all'information security
- S40 - coaching
- S45 - comporre, documentare e catalogare i processi e le procedure essenziali
- S52 - comunicare e pubblicizzare sia i risultati dell'analisi del rischio sia 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 d'azione preventivi
- S91 - garantire che la proprietà intellettuale (IPR) e le norme della protezione dei dati siano rispettate
- S111 - identificare lacune (gap) di competenze e di abilità
- 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 - monitorare e adottare l'uso effettivo degli standard aziendali per le pubblicazioni
- S187 - sviluppare piani di gestione del rischio per identificare le azioni preventive richieste

4.3. Richiesta di certificazione

Il candidato che intende sostenere l'esame per ottenere la certificazione deve presentare all'OdV la Richiesta di certificazione (PS MOD01_DPO), debitamente firmata, allegando tutti i documenti richiesti:

- documento d'identità e codice fiscale
- curriculum vitae
- copia del titolo di studio
- attestato di frequenza e superamento di uno o più corsi per un totale di almeno 80 ore con attestazioni finali aventi per argomento la gestione della protezione dei dati e della sicurezza delle informazioni preferibilmente qualificato da organismo di certificazione che operi in conformità alla norma UNI CEI EN ISO/IEC 17024 per la certificazione delle persone (sulla base dei contenuti della presente norma), ed erogato da Università riconosciute dal MIUR oppure da enti/organismi di formazione.
- In alternativa o a complemento della formazione, copia degli incarichi come docente.
- Evidenze dell'esperienza professionale (sono accettate le seguenti evidenze: dichiarazioni rilasciate dal datore di lavoro, buste paga, contratti, incarichi professionali, fatture)
- Tre elaborati frutto della propria esperienza redatti secondo un modello conforme all'Appendice A della UNI/TS 11945:2024 (PS MOD01_DPO_Allegato A).

Al ricevimento della richiesta, ICMQ ne verifica e registra i dati ed effettua, con il supporto di almeno un commissario d'esame, la verifica documentale dei requisiti sopra indicati.

Ove dei professionisti abbiano già seguito precedenti percorsi di formazione, non coincidenti con le indicazioni della norma UNI EN 17740, ICMQ può effettuare una comparazione analitica tra il percorso già seguito dal candidato alla certificazione e il percorso illustrato nella norma medesima.

Per essere ammessi all'esame il candidato deve dichiarare:

- di non avere in corso altre richieste di certificazione per il medesimo profilo presso altri OdC;
- di non aver sostenuto con esito negativo presso altro OdC un esame per il medesimo profilo, negli ultimi tre (3) mesi

Nel caso di valutazione documentale negativa viene richiesta al candidato l'integrazione della documentazione fornita per dare evidenza della soddisfazione dei requisiti e/o colmare le lacune indicate da ICMQ. A seguito dell'invio della documentazione integrativa, ICMQ procederà a nuova valutazione e comunicherà al candidato l'ammissione o meno all'esame di certificazione.

4.4. Svolgimento degli esami

L'esame ha lo scopo di verificare le conoscenze, le competenze e le capacità del candidato.

Gli esami si svolgono presso un Centro d'Esame o in modalità on-line (da remoto). Al candidato verrà comunicato all'atto dell'accettazione della richiesta di certificazione l'indirizzo del Centro d'Esame, nel caso di esame in presenza, o verranno fornite le credenziali di accesso alla piattaforma utilizzata nel caso di esame da remoto.

L'esame è costituito dalle seguenti prove, somministrate separatamente:

Prova scritta: la prova ha la finalità di accertare le conoscenze.

La prova consiste in 40 domande chiuse a risposta multipla (una sola risposta fra quelle proposte è corretta).

Tempo assegnato: 80 minuti.

Durante l'esame il candidato può consultare i seguenti documenti forniti da ICMQ o dall'OdV:

- norma UNI EN 17740;

- 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.

Casi studio: Tali prove sono finalizzate a verificare l'attitudine, le abilità, le competenze e le conoscenze del candidato su questioni pratiche connesse al profilo professionale del DPO - Responsabile della protezione dei dati. Il Candidato dovrà sviluppare 3 casi studio, che lo pongono in situazioni reali operative, nel modo più corretto in base alla trattazione del caso.

Tempo assegnato: 30 minuti (10 minuti per ciascun caso studio).

Prova orale: colloquio individuale con la commissione d'esame.

L'ammissione al colloquio individuale avviene previo superamento di entrambe le prove scritte.

Il colloquio individuale ha la finalità di integrare e approfondire la valutazione delle capacità espresse da ogni Candidato durante le prove scritte e di approfondire le informazioni presentate dal Candidato.

Il colloquio riguarderà:

1. **L'approfondimento tassativo delle risposte errate** fornite dai candidati alle domande delle prove scritte, con un tempo di almeno 3 minuti per ogni domanda da approfondire (il tempo necessario utilizzato per questo approfondimento si aggiunge a quello complessivo previsto per la prova orale).

2. **Domande su tematiche complementari** a quelle della prova set domande 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 la prova è previsto l'approfondimento, per tutti i candidati, della conoscenza dei concetti di (ove non siano già stati trattati in sede di esame scritto):
   - "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.

3. **Simulazioni di situazioni reali operative** (Es: role-play), per valutare oltre alle abilità e alle competenze, anche le capacità personali (per esempio, capacità relazionali o comportamentali).

4. **L'analisi e la valutazione di uno dei tre elaborati** presentati in fase di domanda di certificazione dal candidato (PS MOD 01DPO _Allegato A) e frutto della propria esperienza. Alla commissione esaminatrice deve essere presentata una situazione lavorativa, considerata significativa dal candidato.

Tempo assegnato: minimo 40 minuti (compresa la simulazione di situazioni reali operative, della durata di circa 10 minuti, e l'analisi e la valutazione di lavori effettuati), massimo 60 minuti.

4.5. Valutazione dell'esame

La valutazione dell'esame viene effettuata assegnando un punteggio, come descritto in dettaglio nella tabella successiva e nel rispetto dei seguenti criteri:

Prova scritta - set domande
viene assegnato un punteggio da zero (0) a quaranta (40).
La valutazione della prova di ciascun Candidato è fatta attribuendo 1 punto per ogni risposta corretta e zero punti per le risposte errate e per quelle non compilate.
Il punteggio conseguito per la prova risulterà dal numero delle risposte corrette.
La prova è superata se il punteggio acquisito è di almeno 28 punti (70% del punteggio massimo)

Caso di Studio:
ad ogni caso viene assegnato un punteggio da zero (0) a cento (100).
A ciascuno degli elementi significativi e qualificanti della trattazione del caso studio viene attribuito una parte del punteggio stabilito per la prova, in modo che il complessivo risulti quello massimo di 100 punti.

Il punteggio conseguito per il singolo caso risulterà dalla somma delle valutazioni eseguite per i singoli elementi.
La prova è superata se la media delle tre (3) valutazioni è di almeno 70/100 (70% del punteggio massimo), con il vincolo che il caso (1) con la peggiore valutazione non sia inferiore a 50/100.

L'accesso al colloquio individuale è vincolato al superamento di entrambe le prove scritte.

Colloquio individuale

Viene assegnato un punteggio da zero (0) a quaranta (40).

Durante il colloquio vengono affrontati i seguenti argomenti con un punteggio variabile da 4 (valutazione minima - carente) a 10 (valutazione massima - ottima) risultante dalla valutazione congiunta dei due esaminatori:

1. risultati della prima prova scritta - approfondimento delle risposte errate. Gli esaminatori approfondiscono ciascuna domanda errata della prima prova, per un massimo di 12 domande e con un tempo a disposizione di almeno 3 minuti ciascuna.
   La valutazione complessiva è data dalla media delle valutazioni di ciascuna domanda, in quanto rapporto tra la somma dei punteggi e il numero di domande. Il superamento di questa sezione è ostativo a quello dell'intera prova orale, pertanto il colloquio orale non può proseguire. Punteggio minimo > 4/10 (carente);

2. Domande a discrezione degli esaminatori. Gli esaminatori pongono delle domande su tematiche di loro scelta e devono prevedere 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, a meno che questi non siano già stati trattati in sede di esame scritto. La valutazione complessiva è data dalla media delle valutazioni di ciascuna domanda, in quanto rapporto tra la somma dei punteggi e il numero di domande.

3. Simulazioni di situazioni reali operative (Es: role-play). La valutazione complessiva è data dalla media delle valutazioni di ciascun esaminatore;

4. Analisi e la valutazione di uno dei tre elaborati. La valutazione complessiva è data dalla media delle valutazioni di ciascun esaminatore.

Il colloquio orale è superato se il punteggio acquisito è di almeno 28 punti (70% del punteggio massimo), fatta salva la condizione ostativa del punto 1 in cui il candidato non deve risultare carente.

Nella tabella seguente è riportato un riepilogo dell'esame:

Tipo di esame	durata	punteggio minimo per il superamento di ogni singola prova
Prova scritta set domande	80 minuti	28/40 (≥ 70%)
Casi di studio	30 minuti (10 minuti per caso)	Media dei tre casi 70/100 (≥ 70%) (valutazione minima 50/100 per 1 solo caso)
Colloquio Individuale	minimo 40 minuti massimo 60 minuti	28/40 (≥ 70%) (valutazione >4/10 per approfondimento risposte errate)

L'esame si considera superato se tutte e tre(3) le prove raggiungono un punteggio minimo del 70%, nel rispetto dei singoli vincoli di valutazione.

Con il superamento dell'esame e con la successiva delibera del CdC, ICMQ rilascia un certificato di competenza professionale.

4.6. Ripetizione dell'esame

Il Candidato che non ha superato l'esame può, entro i 12 mesi successivi ma non prima di 3 mesi dalla data del primo esame, sostenere nuovamente l'esame.

La ripetizione d'esame sarà limitata alla/e prova/e non superata/e.

L'ammissione al nuovo esame è subordinata ad una nuova formale iscrizione, mediante compilazione del ps mod01_DPO_ripetizione esame e al pagamento della quota prevista.

Trascorsi i 12 mesi, occorre ripetere tutte le prove di esame, ripresentando la Richiesta di certificazione (PS MOD01_DPO), debitamente firmata, allegando tutti i documenti richiesti e pagando la quota intera d'esame.

Nei mesi intercorrenti tra l'esame non superato e la sua ripetizione, il candidato non può presentare domanda di certificazione ad altro OdC, pena l'invalidazione dello stesso processo di certificazione.

5. REGISTRO DELLE PERSONE CERTIFICATE

Ogni persona certificata viene iscritta nel "Registro delle persone certificate", pubblicato sul sito www.icmq.org e sul Database Accredia (www.accredia.it). Ciò consente di verificare lo stato della certificazione (validità, sospensione, revoca) nonché i dati della persona certificata.

6. MANTENIMENTO DELLA CERTIFICAZIONE

La validità della certificazione di ogni singola Persona certificata è subordinata alla verifica annuale dell'avvenuto pagamento della quota di mantenimento prevista dal Tariffario e della seguente documentazione:

1. modello ICMQ – ps mod02 DPO_Scheda di Mantenimento Annuale-Rinnovo contenente:
   - anagrafica del professionista certificato da aggiornare
   - dichiarazione di svolgimento dell'attività professionale certificata
   - dichiarazione resa ai sensi degli artt. 46 e 76 del DPR 445/2000 di non avere contenziosi legali in corso e/o ricevuto reclami dai propri clienti oppure, in caso di reclamo, copia della documentazione relativa alla gestione del reclamo stesso;
   - dichiarazione resa ai sensi degli artt. 46 e 76 del DPR 445/2000 di assenza di condanne penali per reati non colposi anche se solo in primo grado e di provvedimenti relativi all'applicazione di misure di prevenzione, di decisioni civili e di provvedimenti amministrativi inerenti all'attività di Responsabile della protezione dei dati - DPO.
2. attestati o altre evidenze di apprendimento e/o aggiornamento professionale per mantenere un elevato livello di conoscenza, e conservare le relative abilità comprovanti l'acquisizione di almeno 16 crediti formativi (vedi NOTA);
3. copia di eventuali documenti nei quali viene utilizzato il marchio ICMQ.
4. copia della disposizione di bonifico della quota annuale per il mantenimento della certificazione.

NOTA: Per l'ottenimento dei 16 crediti formativi dovrà essere dimostrato:

- il superamento (verifica di apprendimento) di uno o più corsi riguardanti il trattamento e/o la protezione dei dati;

  e/o

- l'erogazione di docenze in riguardanti il trattamento e/o la protezione dei dati;

per una durata complessiva minima di 16h all'interno dell'anno di validità del certificato (le 16 ore possono essere cumulate con una delle due opzioni sopra esposte o con una combinazione delle stesse).
Non saranno accettate altre tipologie di formazione (formazione erogata, formazione senza verifica di apprendimento, convegni, ecc..).

Al termine degli accertamenti ICMQ rilascia una dichiarazione di sussistenza della competenza che costituisce parte integrante del certificato.

Il mancato invio della documentazione richiesta può comportare l'attivazione, da parte di ICMQ, delle procedure di sospensione e revoca come previsto dalle condizioni generali di contratto.

7. RINNOVO DEL CERTIFICATO

La certificazione ha una durata di **quattro anni** e può essere rinnovata, prima della sua scadenza, per il primo periodo quadriennale, previa esecuzione della verifica dell'avvenuto pagamento degli importi previsti dal Tariffario per il rinnovo e della stessa documentazione delle verifiche di mantenimento, con la precisazione che deve essere documentata l'acquisizione di almeno 16 crediti/anno (vedi NOTA).

Nell'anno del rinnovo, in caso di mancato raggiungimento dei crediti formativi previsti, il rinnovo stesso della certificazione è subordinato ad un colloquio orale del tipo di prima certificazione (privo della sezione relativa agli approfondimenti degli eventuali errori della prima prova scritta), aggiuntivo alla verifica documentale.

NOTA: Per l'ottenimento dei 16 crediti formativi dovrà essere dimostrato:

- il superamento (verifica di apprendimento) di uno o più corsi riguardanti il trattamento e/o la protezione dei dati;

  e/o

- l'erogazione di docenze in riguardanti il trattamento e/o la protezione dei dati;

per una durata complessiva minima di 16h all'interno dell'anno di validità del certificato (le 16 ore possono essere cumulate con una delle due opzioni sopra esposte o con una combinazione delle stesse).
Non saranno accettate altre tipologie di formazione (formazione erogata, formazione senza verifica di apprendimento, convegni, ecc..).

8. TRASFERIMENTO

Il trasferimento da altro Organismo di certificazione accreditato di un certificato rilasciato ad un professionista può essere perfezionato in qualsiasi momento, presentando richiesta a ICMQ e allegando quanto segue:

- il certificato in corso di validità e, ove applicabile, ultima dichiarazione di mantenimento;
- una dichiarazione dell'OdC cedente in merito all'assenza di pendenze tecniche ed economiche oppure in assenza di quest'ultima o decorsi 5 giorni lavorativi dalla richiesta, il professionista certificato può presentare una dichiarazione redatta ai sensi dell'ex DPR 445/2000 dando comunque evidenza di avere fatto richiesta del documento all'OdC cedente;
- sintesi delle risultanze dell'ultimo esame sostenuto rilasciate dall'Ente cedente.

Al completamento con esito positivo di tale istruttoria, ICMQ delibera l'emissione del proprio Certificato di Conformità, con la medesima scadenza di quello precedente e con la specifica che il certificato è stato emesso in precedenza da altro OdC.

ICMQ informerà l'OdC cedente del completamento del trasferimento.