ICMQ
Certificazioni e controlli
per le costruzioni

CERSA a business unit of ICMQ

ICMQ S.p.A. (a socio unico)
via G. De Castillia, 10 - 20124 Milano
tel. 02.7015.081 - fax 02.7015.0854
icmq@icmq.org - www.icmq.org
Capitale sociale € 750.000 i.v.
REA: MI/1630715
Registro Imprese di Milano
Cod. Fisc. e Part. IVA 13218350158

REGOLAMENTO TECNICO
CERTIFICAZIONE DI PERSONE

PROFILI PROFESSIONALI RELATIVI AL TRATTAMENTO E ALLA PROTEZIONE DEI DATI PERSONALI

UNI 11697

I. **CAMPO DI APPLICAZIONE, DOCUMENTI DI RIFERIMENTO, SCOPO DI CERTIFICAZIONE**	
CAMPO DI APPLICAZIONE	Il presente documento stabilisce i principi e i criteri per la valutazione delle competenze dei Candidati alla certificazione di "Professionista del trattamento e protezione dei dati personali" e stabilisce le modalità di esecuzione e di valutazione delle prove d'esame. NOTA: nel seguito del documento il termine "privacy" è talvolta utilizzato in riferimento ai requisiti dell'insieme di conoscenze, abilità e competenze richieste.
DOCUMENTI DI RIFERIMENTO	– UNI CEI EN ISO/IEC 17024:2012 "Valutazione della conformità - Requisiti generali per organismi che eseguono la certificazione di persone"; – UNI 11697:2017 "Profili professionali relativi al trattamento e alla protezione dei dati personali." – 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" – Regolamento UE 2016/679 – Regolamento generale sulla protezione dei dati (di seguito "Regolamento") – D. Lgs. 101/2018 e s.m.i. Codice in materia di protezione dei dati personali – Raccomandazione 2008/C111/01 (EQF) – Raccomandazione 2009/C 155/02 (ECVET) – PS DOC 01 Condizioni generali contratto PRS
SCOPO DI CERTIFICAZIONE (RIF. PUNTO 4 NORMA UNI 11697)	I Professionisti del trattamento e protezione dei dati personali sono persone le cui conoscenze, abilità e competenze in relazione al profilo posseduto, sono tali da garantire la pertinente gestione del processo di trattamento e protezione dei dati personali, a diversi livelli di complessità e in diversi contesti organizzativi, pubblici e privati. Sono previsti quattro profili professionali in funzione dei compiti di diversa complessità svolti e delle specifiche conoscenze, costituendo un utile supporto per le organizzazioni, che possono meglio orientare le scelte sul professionista con il profilo più adatto alle proprie esigenze, così come per tutte le altre parti interessate: Profilo 1 - **Responsabile della protezione dei dati personali** È il profilo corrispondente a quello disciplinato nel Regolamento UE 2016/679, 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. Profilo 2 – **Manager Privacy** È un profilo pertinente a soggetti con un elevatissimo livello di conoscenze, abilità e competenze in uno specifico contesto organizzativo (sia esso un'area funzionale dell'organizzazione sia il settore di appartenenza della stessa) per garantire l'adozione di idonee misure organizzative nel trattamento di dati personali. Profilo 3 – **Specialista Privacy** È un profilo pertinente a soggetti che supportano il Responsabile per la protezione dei dati personali e/o il Manager privacy nel mettere a punto le idonee misure tecniche e organizzative ai fini del trattamento di dati personali. Profilo 4 – **Valutatore Privacy** È un profilo pertinente a soggetti indipendenti con conoscenze e competenze nel settore informatico/tecnologico e di natura giuridica/ organizzativa che conducono attività del trattamento e della protezione dei dati personali che possono comunque avvalersi di specialisti in entrambi gli ambiti per effettuare attività di audit.

II. **RESPONSABILITÀ E COMPETENZE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI**	
AREE DI RESPONSABILITÀ DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RIF. PUNTO 5.1 NORMA UNI 11697)	**Definizione sintetica** Supporta Titolare o Responsabile nell'applicazione del Regolamento UE 2016/679. **Missione** Fornisce al titolare/responsabile del trattamento il supporto indispensabile ad assicurare l'osservanza del Regolamento UE 2016/679. **Risultati attesi (Deliverables)** • **Responsabile (Accountable)** – Relazioni periodiche sull'osservanza delle norme di legge in materia di protezione dei dati personali. – Documentazione a supporto della richiesta 259 di consultazione preventiva all'Autorità di controllo a seguito di valutazione di impatto ex Regolamento 2016/679. – Richieste di consultazione all'Autorità di controllo su questioni applicative specifiche – Documentazione relativa alle attività di interfacciamento con l'Autorità di controllo (richieste di informazione, procedure di accertamento o verifica, notifica di eventuali violazioni di dati personali) – Documentazione (inclusa modulistica) di interfaccia con gli interessati – Indicatori sulla protezione dei dati personali • **Referente (Responsible**) – Programma di formazione, aggiornamento e consapevolezza. – Pareri su valutazioni di impatto ex Regolamento 2016/679 • **Collaboratore (Contributor)** – 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. – Requisiti per il trattamento e la protezione dei dati personali. – Procedure operative per trattamento e protezione dei dati personali. – Valutazione d'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. – Programma di audit per la protezione e il trattamento dei dati personali.
COMPITI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RIF. PUNTO 5.1 NORMA UNI 11697)	– 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 presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; – sorvegliare l'osservanza del presente 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, compresi 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 connesse al trattamento.

COMPETENZE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RIF. PROSPETTO 1 NORMA UNI 11697)	– Pianificazione di Prodotto o di Servizio – Sviluppo della Strategia per la Sicurezza Informatica – Gestione del Contratto – Sviluppo del Personale – Gestione del Rischio – Gestione delle Relazioni – Gestione della Sicurezza dell'Informazione – Governance dei sistemi informativi
ABILITÀ DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RIF. PUNTO 5.1 NORMA 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 di comunicare – Capacità di analisi – Autogestione e controllo dello stress – Capacità di auto sviluppo – 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 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 gaps – 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 DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RIF. PUNTO 5.1 NORMA 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 – Norme di legge italiane ed europee in materia di trattamento e di protezione dei dati personali – 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 e PIA – 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" – 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 practices 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, i 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 (es. sistemi 375 distribuiti, modelli di virtualizzazione, sistemi di mobilità, data sets)

III. **RESPONSABILITÀ E COMPETENZE DEL RESPONSABILE DEL MANAGER PRIVACY**	
AREE DI RESPONSABILITÀ DEL MANAGER PRIVACY (RIF. PUNTO 5.2 NORMA UNI 11697)	**Definizione sintetica** È responsabile (termine Non utilizzato qui con l'accezione di "data processor" definito dal Regolamento UE 2016/679) per e coordina le attività di trattamento di dati personali. **Missione** Coordina trasversalmente i soggetti coinvolti nel trattamento dei dati personali, al fine di garantire il rispetto delle norme di legge applicabili e il raggiungimento nonché il

	mantenimento del livello di protezione adeguato in base allo specifico trattamento di dati personali effettuato, coordinando trasversalmente i soggetti in essi coinvolti. **Risultati attesi (Deliverables)** • **Responsabile (Accountable)** – Procedure operative per trattamento e protezione dei dati personali. – Relazioni sullo stato complessivo della protezione dei dati personali (e.g. riesame). – Indicatori sulla protezione dei dati personali. • **Referente (Responsible**) – Budget per la protezione dei dati personali. – Attribuzione delle responsabilità per trattamento e protezione dei dati personali. – Valutazione d'impatto sulla protezione dei dati. – Politica per la protezione dei dati personali. – Requisiti per il trattamento e la protezione dei dati personali. – Misure tecniche ed organizzative per garantire la protezione dei dati per impostazione predefinita. – Consultazioni preventive. – Notificazione di incidenti che comportano una violazione dei dati personali. – Informative. – Risposte conseguenti all'esercizio dei diritti di accesso. – Registri delle attività di trattamento. – Programma di formazione, aggiornamento e consapevolezza. • **Collaboratore (Contributor)** – Valutazione del rischio relativo alla sicurezza delle informazioni. – Piano di trattamento del rischio relativo alla sicurezza delle informazioni. – Codici di condotta. – Programma di audit per la protezione e il trattamento dei dati personali.
COMPITI DEL MANAGER PRIVACY (rif. punto 5.2 Norma UNI 11697)	**Compiti principali** – Assistere il titolare nel dare seguito alle richieste di esercizio dei diritti degli interessati. – Assistere il titolare nel disporre la cancellazione o la restituzione dei dati personali alla conclusione del trattamento. – Informare periodicamente il titolare sullo stato del trattamento e della protezione dei dati personali. – Gestire il budget per la protezione dei dati personali. – Controllare con continuità il livello complessivo di protezione dei dati personali. – Organizzare e attribuire le responsabilità relative al trattamento e alla protezione dei dati personali. – Approvare le politiche e le procedure per il trattamento e la protezione dei dati personali. – Assistere il titolare nell'approvazione delle misure da adottare per gestire i rischi relativi alla protezione dei dati personali. – Partecipare alle attività di valutazione del rischio relativo alla sicurezza delle informazioni. – Adoperarsi per garantire il rispetto dei requisiti in materia di trattamento e protezione dei dati personali anche nelle attività progettuali. – Comunicare, se appropriato, le violazioni di dati personali agli interessati. – Gestire i registri delle attività di trattamento. – Definire e valutare gli SLA e i PLA che devono essere garantiti da terzi eventualmente coinvolti nel trattamento dati personali. – Integrare le attività per la conformità al trattamento dei dati personali con le attività relative ad altri tipi di conformità ove possibile.

COMPETENZE DEL MANAGER PRIVACY (RIF. PROSPETTO 2 NORMA UNI 11697)	– Pianificazione di Prodotto o di Servizio – Assistenza all'Utente – Progettazione di Architetture – Sviluppo della Strategia per la Sicurezza Informatica – Gestione del Contratto – Sviluppo del Personale – Gestione dell'Informazione e della Conoscenza – Gestione del Rischio – Gestione della Sicurezza dell'Informazione – Governance dei Sistemi Informativi
ABILITÀ DEL MANAGER PRIVACY (RIF. PUNTO 5.2 NORMA 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 di comunicare – Capacità di analisi – Autogestione e controllo dello stress – Capacità di auto-sviluppo – Capacità di controllo – Capacità di convincimento – Capacità di coordinamento e gestione dei collaboratori – Capacità decisionali – Flessibilità – Capacità di gestione dei conflitti – Capacità di gestione del gruppo – Iniziativa – Idoneità alla negoziazione – Capacità organizzative – Orientamento ai risultati – 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 ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi – S6 - analizzare gli sviluppi futuri nel processo di business e nell'applicazione della tecnologia – S14 - analizzare la fattibilità in termini di costi e benefici – 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 – S42 - collezionare, formalizzare e validare i requisiti funzionali e non funzionali – S46 - comprendere gli impatti delle nuove tecnologie sul business e come possono fornire valore e vantaggio competitivo (es. open / big data, dematerializzazione opportunità e strategie) – S47 - comprendere gli obiettivi / elementi guida del business che impattano i componenti dell'architettura (dati, applicazioni, sicurezza, sviluppo ecc.) integrarlo nelle esigenze di

	business – S49 - comprendere le architetture di impresa – S51 - comunicare chiaramente con l'utente finale e fornire istruzioni sui progressi nella soluzione dei problemi – S52 - comunicare e pubblicizzare sia i risultati dell'analisi del rischio che i processi di gestione del rischio – S53 - comunicare il valore, i rischi e le opportunità derivanti dalla strategia del sistema informativo – S55 - comunicare le buone e le cattive notizie per evitare sorprese – S60 - contribuire allo sviluppo della strategia di business – S61 - contribuire allo sviluppo della strategia e delle politiche dell'ICT, incluse la qualità e la sicurezza ICT – S66 - costruire un piano di gestione del rischio per fornire e produrre piani di azione preventivi – S71 - definire ed implementare adeguati key performance indicators (KPI's) – S91 - garantire che la proprietà intellettuale (IPR) e le norme della privacy siano rispettate – 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 – S165 - proporre misure efficaci di contingenza – S167 - raccogliere la conoscenza interna ed esterna e i fabbisogni di informazione – S171 - rendere l'informazione disponibile – S176 - seguire e controllare l'uso effettivo degli standard documentativi aziendali – S178 - selezionare soluzioni ICT appropriate basandosi su benefici attesi, rischi ed impatto complessivo – S181 - stabilire un piano di ripristino – S182 - stabilire una comunicazione sistematica e frequente con i clienti, gli utenti e gli stakeholder – S186 - sviluppare modelli e pattern per assistere gli analisti di sistema nella progettazione di applicazioni consistenti – S187 - sviluppare piani di risk management per identificare le necessarie azioni preventive – S198 - valutare l'idoneità di differenti metodi di sviluppo dell'applicazione rispetto allo scenario corrente
CONOSCENZE DEL MANAGER PRIVACY (RIF. PUNTO 5.2 NORMA UNI 11697)	Le conoscenze richieste al Manager Privacy sono elencate al punto 5.2 della Norma UNI 11697. – I principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita – I diritti degli interessati previsti da leggi e regolamenti vigenti – Le reti informatiche – Le reti di telecomunicazione – 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 nell'ambito delle comunicazioni elettroniche – 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 e PIA – Le possibili minacce alla protezione dei dati personali – Strumenti e metodi di pianificazione, programmazione e controllo aziendale

	– Tecniche e strumenti di comunicazione (relazione con Istituzioni, autorità, Forze dell'ordine, enti locali e stampa) – Sistemi e tecniche di monitoraggio e "reporting" – I codici di condotta e le certificazioni applicabili in materia di trattamento e protezione dei dati personali. – K10 - DBMS, Data Warehouse, DSS … ecc. – K11 - framework architetturali – K12 - framework architetturali, metodologie e strumenti per la progettazione di sistemi – K23 - gli standard della sicurezza ICT – K26 - gli strumenti di controllo della versione per la produzione di documentazione – K27 - gli strumenti e gli apparati applicabili per la memorizzazione ed il recupero dei dati – K28 - gli strumenti per la creazione di presentazioni multimediali – K29 - gli strumenti per la produzione, l'editing e la distribuzione di documenti professionali – K35 - i costi, benefici e rischi di un'architettura di sistema – K36 - i differenti documenti tecnici richiesti per la progettazione, lo sviluppo e il deploying dei prodotti, delle applicazioni e dei servizi – K38 - i differenti modelli di servizio (SaaS, PaaS, IaaS), livelli di servizio e contrattualizzazione degli stessi (es. Cloud Computing) – K49 - i metodi di sviluppo delle competenze – K51 - i metodi per lo sviluppo del software e la loro logica (es. prototipazione, metodi agili, reverse engineering, ecc.) – K56 - i principi della progettazione dell'interfaccia utente – 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 practices più rilevanti. – K85 - il ritorno dell'investimento comparato all'annullamento del rischio – K97 - l'impatto dei cambiamenti del business sugli aspetti legali – K98 - l'impatto dei requisiti legali sulla sicurezza dell'informazione – K102 - l'infrastruttura ICT e l'organizzazione del business – 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, i fornitori e i sub-contraenti – K122 - la strategia dell'informazione nell'organizzazione – K127 - le applicazioni esistenti e le relative architetture – K128 - le applicazioni ICT utente rilevanti – 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 (es. 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 (es. big data) – K162 - le problematiche relative ai dati non strutturati (es. data analytics) – K172 - le strategie digitali – K180 - le tecniche di attacco informatico e le contromisure per evitarli – K186 - le tecniche di rilevamento di sicurezza, compreso il mobile e il digitale

	– K200 - le tecnologie web, cloud e mobile – K201 - le tendenze e le implicazioni dello sviluppo interno o esterno dell'ICT nelle organizzazioni tipiche – K209 - requisiti dell'architettura dei sistemi: prestazioni, manutenibilità, estendibilità, scalabilità, disponibilità, sicurezza e accessibilità

IV. **RESPONSABILITÀ E COMPETENZE DEL RESPONSABILE DELLO SPECIALISTA PRIVACY**	
AREE DI RESPONSABILITÀ DELLO SPECIALISTA PRIVACY (RIF. PUNTO 5.3 NORMA UNI 11697)	**Definizione sintetica** Cura la corretta attuazione del trattamento di dati personali. È l'esperto operativo per la protezione dei dati personali. **Missione** Svolge le attività operative che si rendono progressivamente necessarie durante tutto il ciclo di vita di un trattamento di dati personali collaborando con una figura manageriale (quale, per esempio, il manager privacy competente). **Risultati attesi (Deliverables)** • **Responsabile (Accountable)** – Pareri tecnici sulla protezione e sul trattamento dei dati personali. – Pareri sulla protezione e sul trattamento dei dati personali. • **Referente (Responsible)** – Informative. – Risposte conseguenti all'esercizio dei diritti di accesso. – Procedure operative per il trattamento e la protezione dei dati personali. • **Collaboratore (Contributor)** – Notificazione di incidenti che comportano una violazione dei dati personali. – Valutazione d'impatto sulla protezione dei dati. – Indicatori sulla protezione dei dati personali. – Valutazione del rischio relativo alla sicurezza delle informazioni. – Piano di trattamento del rischio relativo alla sicurezza delle informazioni. – Consultazioni preventive. – Requisiti per il trattamento e la protezione dei dati personali. – Misure tecniche ed organizzative per 610 garantire la protezione dei dati per impostazione predefinita. – Programma di formazione, aggiornamento e consapevolezza.
COMPITI DELLO DELLO SPECIALISTA PRIVACY (RIF. PUNTO 5.3 NORMA UNI 11697)	**Compiti principali** – Condurre le attività di valutazione d'impatto sulla protezione dei dati personali. – Fornire supporto specialistico relativamente a questioni specifiche. – Proporre le misure da adottare per gestire i rischi relativi al trattamento e alla protezione dei dati personali. – Redigere e aggiornare le politiche e le procedure per il trattamento la protezione dei dati personali. – Attuare processi relativi alla protezione dei dati personali. – Attuare soluzioni tecniche per la protezione dei dati personali. – Documentare i processi relativi al trattamento e alla protezione dei dati personali affinché venga riscontrata l'evidenza della conformità del trattamento effettuato. – Documentare la gestione delle soluzioni tecniche per il trattamento e la protezione dei dati personali. – Documentare le violazioni dei dati personali

COMPETENZE DELLO SPECIALISTA PRIVACY (RIF. PROSPETTO 3 NORMA UNI 11697)	– Progettazione di Architetture – Progettazione di Applicazioni – Produzione della documentazione – Assistenza all'Utente – Supporto alle modifiche/evoluzioni del sistema – Sviluppo del personale – Gestione dell'Informazione e della Conoscenza – Gestione del Rischio – Gestione della Sicurezza dell'Informazione
ABILITÀ DELLO SPECIALISTA PRIVACY (RIF. PUNTO 5.3 NORMA UNI 11697)	– Applicare i principi di privacy e protezione dei dati by design e by default ai sistemi informativi – Applicare i principi di privacy e protezione dei dati by design e by default ai trattamenti di dati personali – Gestire le richieste da parte degli interessati che esercitano i loro diritti – Elaborare procedure di trasferimento soggetto a garanzie adeguate e/o norme vincolanti d'impresa verso paesi terzi od organizzazioni internazionali – Capacità di lavoro in gruppo – Capacità di analisi – Flessibilità – Capacità organizzative – Pianificazione e programmazione – Propensione al nuovo – 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 – S13 - analizzare l'impatto sugli utenti dei cambiamenti funzionali / tecnici – S19 - anticipare i cambiamenti richiesti alla strategia aziendale dell'information security e formulare nuovi piani – S20 - anticipare tutte le azioni necessarie a mitigare l'impatto dei cambiamenti (formazione, documentazione, nuovi processi…) – S21 - applicare azioni di contenimento del rischio e dell'emergenza – S28 - applicare metodi di data mining – S37 - capire come le tecnologie web possono essere utilizzate per il marketing – S40 – coaching – S42 - collezionare, formalizzare e validare i requisiti funzionali e non funzionali – S45 - comporre, documentare e classificare i processi fondamentali e le procedure – S47 - comprendere gli obiettivi / elementi guida del business che impattano i componenti dell'architettura (dati, applicazioni, sicurezza, sviluppo ecc.). – S51 - comunicare chiaramente con l'utente finale e fornire istruzioni sui progressi nella soluzione dei problemi – S57 - condividere specifiche funzionali e tecniche con i team ICT che hanno in carico la manutenzione e l'evoluzione delle soluzioni ICT – S89 - garantire che controlli e funzionalità vengano recepiti dalla progettazione – S91 - garantire che la proprietà intellettuale (IPR) e le norme della privacy siano rispettate – S153 - preparare i template per pubblicazioni condivise – S167 - raccogliere la conoscenza interna ed esterna e i fabbisogni di informazione – S168 - raccogliere, immagazzinare, analizzare data sets complessi larghi non strutturati e in formati differenti

	– S171 - rendere l'informazione disponibile – S176 - seguire e controllare l'uso effettivo degli standard documentativi aziendali – S182 - stabilire una comunicazione sistematica e frequente con i clienti, gli utenti e gli stakeholder – S186 - sviluppare modelli e pattern per assistere gli analisti di sistema nella progettazione di applicazioni consistenti – S191 - usare e analizzare la web analytics – S198 - valutare l'idoneità di differenti metodi di sviluppo dell'applicazione rispetto allo scenario corrente
CONOSCENZE DELLO SPECIALISTA PRIVACY (RIF. PUNTO 5.3 NORMA UNI 11697)	– I principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita – I diritti degli interessati previsti da leggi e regolamenti vigenti – Le reti informatiche – Le reti di telecomunicazione – Le responsabilità connesse al trattamento dei dati personali – Norme di legge italiane ed europee in materia di trattamento e protezione dei dati personali con particolare riguardo alle disposizioni di rango primario e secondario (regolamenti, provvedimenti, autorizzazioni, linee-guida e standard settoriali, altro) relative agli specifici ambiti di operatività – Norme di legge in materia di trattamento e protezione dei dati personali nell'ambito delle comunicazioni elettroniche – Norme di legge in materia di trattamento e protezione dei dati personali per finalità di Norme di legge in materia di trattamento e protezione dei dati personali per finalità di videosorveglianza – Norme di legge in materia di trattamento e protezione dei dati personali per finalità di marketing e profilazione – Norme di legge in materia di trattamento e protezione dei dati personali per finalità di controllo dei lavoratori – Norme di legge in materia di trasferimento di dati personali all'estero e circolazione dei dati personali extra UE/SEE – Norme di legge per la gestione di dati biometrici – Impiantistica di videosorveglianza – Le metodologie di valutazione d'impatto sulla protezione dei dati e PIA – Le possibili minacce alla protezione dei dati personali con riguardo, in particolare, allo specifico settore di operatività – Le tecniche crittografiche – Le tecniche di anonimizzazione e de-anonimizzazione – Le tecniche di pseudonimizzazione – Le tecnologie IoT (Internet of Things) – Le tecnologie RFID – Le tecnologie di geolocalizzazione – Le tecnologie di identificazione – Le tecnologie di identificazione biometriche – Le tecnologie di tracciamento delle operazioni – I codici di condotta e le certificazioni applicabili in materia di trattamento e protezione dei dati personali – K10 - DBMS, Data Warehouse, DSS … ecc. – K12 - framework architetturali, metodologie e strumenti per la progettazione di sistemi – K26 - gli strumenti di controllo della versione per la produzione di documentazione – K27 - gli strumenti e gli apparati applicabili per la memorizzazione ed il recupero dei dati – K28 - gli strumenti per la creazione di presentazioni multimediali

	– K29 - gli strumenti per la produzione, l'editing e la distribuzione di documenti professionali – K35 - i costi, benefici e rischi di un'architettura di sistema – K36 - i differenti documenti tecnici richiesti per la progettazione, lo sviluppo e il deploying dei prodotti, delle applicazioni e dei servizi – K49 - i metodi di sviluppo delle competenze – K50 - i metodi per analizzare le informazioni non strutturate e i processi di business – K51 - i metodi per lo sviluppo del software e la loro logica (es. prototipazione, metodi agili, reverse engineering, ecc.) – K56 - i principi della progettazione dell'interfaccia utente – K81 - il mobile marketing (es. Pay Per Click) – K87 - il social media marketing – K93 - l'architettura tecnica di un'applicazione ICT esistente – K94 - l'e-mail marketing – K108 - la computer forensics (analisi criminologica di sistemi informativi) – K127 - le applicazioni esistenti e le relative architetture – K132 - le best practice e gli standard nella gestione della sicurezza delle informazioni – K152 - le nuove tecnologie emergenti (es. sistemi distribuiti, modelli di virtualizzazione, sistemi di mobilità, data sets) – K161 - le problematiche legate alla dimensione dei data sets (es. big data) – K162 - le problematiche relative ai dati non strutturati (es. data analytics) – K170 - le specifiche funzionali di un sistema informativo – K173 - le strutture del database e l'organizzazione dei suoi contenuti – K180 - le tecniche di attacco informatico e le contromisure per evitarli – K186 - le tecniche di rilevamento di sicurezza, compreso il mobile e il digitale – K200 - le tecnologie web, cloud e mobile – K209 - requisiti dell'architettura dei sistemi: prestazioni, manutenibilità, estendibilità, scalabilità, disponibilità, sicurezza e accessibilità

V. **RESPONSABILITÀ E COMPETENZE DEL RESPONSABILE DEL VALUTATORE PRIVACY**	
AREE DI RESPONSABILITÀ DEL VALUTATORE PRIVACY (RIF. PUNTO 5.4 NORMA UNI 11697)	**Definizione sintetica** Controlla la conformità del trattamento di dati personali a leggi e regolamenti applicabili. **Missione** Esamina periodicamente il trattamento di dati personali, valutando il rispetto di leggi e regolamenti applicabili e approva le misure necessarie a eliminare eventuali non-conformità rilevate, mantenendo una posizione indipendente da chi svolge attività manageriali e operative. **Risultati attesi (Deliverables)** • **Responsabile (Accountable)** – Report di audit • **Referente (Responsible)** – Programma di audit per la protezione e il trattamento dei dati personali • **Collaboratore (Contributor)** N/A
COMPITI DEL VALUTATORE PRIVACY (RIF. PUNTO 5.4 NORMA UNI 11697)	**Compiti principali** – Programmare, pianificare e svolgere le attività di audit. – Riesaminare la documentazione relativa al trattamento e alla protezione dei dati personali ed effettuare interviste al personale ad ogni livello dell'organizzazione. – Descrivere gli scostamenti rilevati rispetto a leggi e regolamenti applicabili.

COMPETENZE DEL VALUTATORE PRIVACY (RIF. PROSPETTO 4 NORMA UNI 11697)	– Progettazione di Architetture – Progettazione di Applicazioni – Produzione della documentazione – Gestione dell'Informazione e della Conoscenza – Gestione del Rischio – Miglioramento del Processo – Gestione della Sicurezza dell'Informazione
ABILITÀ DEL VALUTATORE PRIVACY (RIF. PROSPETTO 4 NORMA UNI 11697)	– Verificare l'applicazione dei principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita. – Capacità di lavoro in gruppo – Accuratezza – Capacità di analisi – Pianificazione e programmazione – Capacità di sintesi – S5 - analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi – S23 - applicare gli standard, le best practice e i requisiti legali più rilevanti all'information security – S28 - applicare metodi di data mining – S42 - collezionare, formalizzare e validare i requisiti funzionali e non funzionali – S45 - comporre, documentare e classificare i processi fondamentali e le procedure – S47 - comprendere gli obiettivi / elementi guida del business che impattano i componenti dell'architettura (dati, applicazioni, sicurezza, sviluppo ecc.). – S91 - garantire che la proprietà intellettuale (IPR) e le norme della privacy siano rispettate – S171 - rendere l'informazione disponibile – S176 - seguire e controllare l'uso effettivo degli standard documentativi aziendali
CONOSCENZE DEL VALUTATORE PRIVACY (RIF. PUNTO 5.4 NORMA UNI 11697)	– I principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita – I diritti degli interessati previsti da leggi e regolamenti vigenti – 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 nell'ambito delle comunicazioni elettroniche – Norme di legge in materia di trattamento e protezione dei dati personali per finalità di videosorveglianza – Norme di legge in materia di trattamento e protezione dei dati personali per finalità di marketing e profilazione – Norme di legge in materia di trattamento e protezione dei dati personali per finalità di controllo dei lavoratori – Norme di legge in materia di trasferimento di dati personali all'estero e circolazione dei dati personali extra UE/SEE – Norme di legge per la gestione di dati biometrici – Impiantistica di videosorveglianza – Le metodologie di valutazione d'impatto sulla protezione dei dati e PIA – Le possibili minacce alla protezione dei dati personali – Le tecniche crittografiche – Le tecniche di anonimizzazione e de-anonimizzazione – Le tecniche di pseudonimizzazione – Le tecnologie IoT (Internet of Things)

	– Le tecnologie RFID – Le tecnologie di geolocalizzazione – Le tecnologie di identificazione – Le tecnologie di identificazione biometriche – Le tecnologie di tracciamento delle operazioni – Le norme tecniche ISO/IEC per la gestione dei dati personali – Le best practice (metodologie) e gli standard per l'auditing e per l'accreditamento – I codici di condotta e le certificazioni applicabili in materia di trattamento e protezione dei dati personali. – Capacità di lavoro in gruppo – Accuratezza – Capacità di analisi – Pianificazione e programmazione – Capacità di sintesi – K10 - DBMS, Data Warehouse, DSS … ecc. – K12 - framework architetturali, metodologie e strumenti per la progettazione di sistemi – K26 - gli strumenti di controllo della versione per la produzione di documentazione – K27 - gli strumenti e gli apparati applicabili per la memorizzazione ed il recupero dei dati – K28 - gli strumenti per la creazione di presentazioni multimediali – K29 - gli strumenti per la produzione, l'editing e la distribuzione di documenti professionali costi, benefici e rischi di un'architettura di sistema – K36 - i differenti documenti tecnici richiesti per la progettazione, lo sviluppo e il deploying dei prodotti, delle applicazioni e dei servizi – K50 - i metodi per analizzare le informazioni non strutturate e i processi di business – K51 - i metodi per lo sviluppo del software e la loro logica (es. prototipazione, metodi agili, reverse engineering, ecc.) – K56 - i principi della progettazione dell'interfaccia utente – K67 - i rischi critici per la gestione della sicurezza – K83 - il potenziale e le opportunità offerte dagli standard e dalle best practices più rilevanti. – K90 - l'approccio all'auditing interno del sistema informativo – K97 - l'impatto dei cambiamenti del business sugli aspetti legali – K98 - l'impatto dei requisiti legali sulla sicurezza dell'informazione – 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 – K149 - le norme legali applicabili ai contratti – K158 - le possibili minacce alla sicurezza – K161 - le problematiche legate alla dimensione dei data sets (es. big data) – K162 - le problematiche relative ai dati non strutturati (es. data analytics) – K186 - le tecniche di rilevamento di sicurezza, compreso il mobile e il digitale – K200 - le tecnologie web, cloud e mobile – K209 - requisiti dell'architettura dei sistemi: prestazioni, manutenibilità, estendibilità, scalabilità, disponibilità, sicurezza e accessibilità

VI. **PRIMA CERTIFICAZIONE** – **UNI 11697:2017** **CANDIDATI INTERESSATI:** ✓ **Persone in possesso dei requisiti di ammissione per il profilo richiesto**	
PROFILO 1: RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (DPO AI SENSI DEL REGOLAMENTO UE 2016/679)	
RICHIESTA DI CERTIFICAZIONE	La richiesta di certificazione deve essere formulata dal Richiedente utilizzando il modulo allegato "IO 20.8 Richiesta di certificazione ed ammissione all'esame" e dovrà essere integrata dalla documentazione prevista[5)]. Tutti i documenti richiesti possono essere anticipati a ICMQ a mezzo posta elettronica fermo restando che i Candidati, per potere accedere alle prove di esame, dovranno recapitare a ICMQ gli originali dei documenti indicati nel modulo allegato.
REQUISITI DI AMMISSIONE ALL'ESAME	I percorsi di accesso, non alternativi tra loro, prevedono (rif. Appendice B - Norma 11697:2017): a) Titolo di Studio b) Formazione specifica c) Esperienza Lavorativa
TITOLO DI STUDIO	Laurea che includa discipline almeno in parte afferenti alle conoscenze del professionista privacy, legali o tecnico/informatiche[1)]
FORMAZIONE SPECIFICA	Corso di almeno 80 ore[4)] con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[2)].
ESPERIENZA LAVORATIVA	Minimo 6 anni di esperienza di esperienza lavorativa legata alla privacy di cui almeno 4 anni in incarichi di livello manageriale[3)].
EQUIPOLLENZA TRA TITOLO DI STUDIO ED ESPERIENZA LAVORATIVA	Il periodo complessivo di esperienza professionale: si riduce a 4 anni, di cui 3 in incarichi livello manageriale[3)] se in possesso di laurea magistrale; si eleva a 8 anni, di cui 5 in incarichi livello manageriale[3)] se in possesso di Scuola Media Superiore.
PROFILO 2: MANAGER PRIVACY	
RICHIESTA DI CERTIFICAZIONE	La richiesta di certificazione deve essere formulata dal Richiedente utilizzando il modulo allegato "IO 20.8 Richiesta di certificazione ed ammissione all'esame" e dovrà essere integrata dalla documentazione prevista[5)]. Tutti i documenti richiesti possono essere anticipati a ICMQ a mezzo posta elettronica fermo restando che i Candidati, per potere accedere alle prove di esame, dovranno recapitare a ICMQ gli originali dei documenti indicati nel modulo allegato.
REQUISITI DI AMMISSIONE ALL'ESAME	I percorsi di accesso, non alternativi tra loro, prevedono (rif. Appendice B - Norma 11697:2017): a) Titolo di Studio b) Formazione specifica c) Esperienza Lavorativa
TITOLO DI STUDIO	Laurea che includa discipline almeno in parte afferenti alle conoscenze del professionista privacy, legali o tecnico/informatiche[1)]
FORMAZIONE SPECIFICA	Corso di almeno 60 ore[4)] con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[2)].
ESPERIENZA LAVORATIVA	Minimo 6 anni di esperienza di esperienza lavorativa legata alla privacy di cui almeno 3 anni in incarichi di livello manageriale[3)].
EQUIPOLLENZA TRA TITOLO DI STUDIO ED ESPERIENZA LAVORATIVA	Il periodo complessivo di esperienza professionale: si riduce a 4 anni, di cui 2 in incarichi livello manageriale[3] se in possesso di laurea magistrale; si eleva a 8 anni, di cui 4 in incarichi livello manageriale[3] se in possesso di Scuola Media Superiore.

PROFILO 3: SPECIALISTA PRIVACY	
RICHIESTA DI CERTIFICAZIONE	La richiesta di certificazione deve essere formulata dal Richiedente utilizzando il modulo allegato "IO 20.8 Richiesta di certificazione ed ammissione all'esame" e dovrà essere integrata dalla documentazione prevista[5)]. Tutti i documenti richiesti possono essere anticipati a ICMQ a mezzo posta elettronica fermo restando che i Candidati, per potere accedere alle prove di esame, dovranno recapitare a ICMQ gli originali dei documenti indicati nel modulo allegato.
REQUISITI DI AMMISSIONE ALL'ESAME	I percorsi di accesso, non alternativi tra loro, prevedono (rif. Appendice B - Norma 11697:2017): a) Titolo di Studio b) Formazione specifica c) Esperienza Lavorativa
TITOLO DI STUDIO	Diploma di Scuola Media Superiore
FORMAZIONE SPECIFICA	Corso di almeno 24 ore[4)] con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[2)].
ESPERIENZA LAVORATIVA	Minimo 4 anni di esperienza di esperienza lavorativa legata alla privacy.
EQUIPOLLENZA TRA TITOLO DI STUDIO ED ESPERIENZA LAVORATIVA	Il periodo complessivo di esperienza professionale si riduce a 2 anni se in possesso di laurea
PROFILO 4: VALUTATORE PRIVACY	
RICHIESTA DI CERTIFICAZIONE	La richiesta di certificazione deve essere formulata dal Richiedente utilizzando il modulo allegato "IO 20.8 Richiesta di certificazione ed ammissione all'esame" e dovrà essere integrata dalla documentazione prevista[5)]. Tutti i documenti richiesti possono essere anticipati a ICMQ a mezzo posta elettronica fermo restando che i Candidati, per potere accedere alle prove di esame, dovranno recapitare a ICMQ gli originali dei documenti indicati nel modulo allegato.
REQUISITI DI AMMISSIONE ALL'ESAME	I percorsi di accesso, non alternativi tra loro, prevedono (rif. Appendice B - Norma 11697:2017): a) Titolo di Studio b) Formazione specifica c) Esperienza Lavorativa
TITOLO DI STUDIO	Diploma di Scuola Media Superiore
FORMAZIONE SPECIFICA	Corso di almeno 40 ore[4)] con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[2)].
ESPERIENZA LAVORATIVA	Minimo 6 anni di esperienza di esperienza lavorativa legata alla privacy di cui almeno 3 anni in incarichi di audit.
EQUIPOLLENZA TRA TITOLO DI STUDIO ED ESPERIENZA LAVORATIVA	Il periodo complessivo di esperienza professionale si riduce: a 4 anni, di cui 2 in incarichi di audit, se in possesso di laurea; a 3 anni, di cui 2 in incarichi di audit, se in possesso di laurea magistrale.

NOTE COMUNI A TUTTI I PROFILI:

1) *un laureato con laurea non afferente alle conoscenze del professionista privacy, legali o tecnico / informatiche 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 prestazione d'opera condotta nell'ambito dell'esecuzione di ingaggi professionali. *4) Ove dei professionisti abbiano già eseguito precedenti percorsi di formazione, non coincidenti con le indicazioni della norma UNI 11697 sarà effettuata un'analitica comparazione tra il percorso già seguito dal candidato alla certificazione ed il percorso illustrato dalla norma. Ciò vale a dire che il numero di ore complessivo può essere raggiunto anche con più corsi di formazione e/o con la partecipazione a seminari o con l'effettuazione di docenza specifica.* 5) *Le eventuali "autodichiarazioni", redatte in conformità agli artt. 46 e 76 del D.P.R. 445/2000 possono comunque essere soggette a verifica su richiesta di ICMQ.*	
REQUISITI DI ACCESSO ALL'ESAME DI CERTIFICAZIONE	Per essere ammessi all'esame per la certificazione di un profilo professionale, i Candidati devono soddisfare tutti i requisiti di ammissione sopra indicati per il profilo oggetto di certificazione, tenendo conto dei chiarimenti forniti dalle note comuni a tutti i profili.
REQUISITI DI AMMISSIONE AGLI ESAMI PER LA CERTIFICAZIONE IN PIÙ PROFILI	Per essere ammessi ad un'unica sessione di esami per la certificazione di più profili professionali, i Candidati devono soddisfare tutti i requisiti di ammissione sopra indicati per ciascun profilo oggetto di certificazione, tenendo conto dei chiarimenti forniti dalle note comuni a tutti i profili. I requisiti devono essere soddisfatti attraverso la richiesta di certificazione mod. "IO 20.8 Richiesta di certificazione ed ammissione all'esame" corredata di tutti i documenti necessari, pertanto nel caso di richiesta per più profili, è necessario provvedere alla formulazione della richiesta di certificazione avendo cura di precisare - per ciascuno dei profili professionali oggetto di certificazione - le informazioni necessarie per l'ammissione, ognuna corredata di tutti i documenti. Per la persona già certificata per un profilo che desideri certificarsi per uno o più profili ulteriori, si rimanda alla sezione specifica "**ESTENSIONE DELLA CERTIFICAZIONE".**
VII. **ESAMINATORI E COMMISSIONE DELIBERANTE DI ICMQ**	
ESAMINATORI	La Commissione d'esame possiede, nel suo insieme, i seguenti requisiti: a) la conoscenza delle regole e criteri per l'esame di certificazione definiti da ICMQ in coerenza con quanto richiamato dalla ISO/IEC 17024, b) il possesso della certificazione sotto accreditamento Accredia in uno dei profilo della norma UNI 11697 adeguata al profilo da esaminare secondo i seguenti criteri: i. Un commissario certificato come DPO- Responsabile della protezione dei dati personali può esaminare Candidati alla certificazione di Responsabile, Manager, Specialista. ii. Un commissario certificato come Manager Privacy può esaminare Candidati alla certificazione di Manager, Specialista. iii. Un commissario certificato come Verificatore Privacy può esaminare Candidati alla certificazione di Verificatore, Specialista. iv. Un commissario certificato come Specialista non può esaminare nessun Candidato. 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. La Commissione d'esame è composta da almeno 2 membri. **Grandparent** Per i primi tre anni di operatività, in sostituzione del membro della Commissione d'esame in possesso di una certificazione sotto accreditamento nello stesso profilo oggetto di valutazione (punto b di cui sopra), ICMQ può servirsi di un Grandparent che possieda i

	requisiti indicati nei punti a) e c). Allo scadere dei tre anni, la qualifica di Grandparent decade e il professionista deve certificarsi sostenendo eventualmente un iter di esame semplificato in base a quanto deciso da ICMQ per il caso specifico. In alternativa la certificazione può essere concessa dopo l'osservazione diretta del Grandparent durante la conduzione di almeno tre sessioni di esame e comunque dopo che sia decaduta la qualifica di Grandparent. **Conflitto d'interessi** 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.
DECISION MAKER (COMMISSIONE DELIBERANTE)	Il Decision Maker possiede gli stessi requisiti degli esaminatori ed inoltre soddisfa i seguenti requisiti minimi: a) conoscenza dei processi di delibera di ICMQ b) conoscenza generale della norma UNI 11697 **Conflitto d'interessi** Il Decision Maker, relativamente ai candidati oggetto di delibera di certificazione, non può aver preso parte alla commissione esaminatrice, né può aver erogato docenza nei corsi di formazione specifica frequentati da medesimi candidati
VIII. **ESAMI PER LA CERTIFICAZIONE**	
ESAMI PER LA CERTIFICAZIONE	**Struttura** Gli esami per la certificazione delle competenze dei Candidati, per ogni profilo professionale, sono strutturati in tre prove di cui due scritte e una orale. La complessità delle prove è proporzionata ai requisiti stabiliti per ciascun profilo professionale. – **prove scritte:** 1. **prima prova ("set domande")** per la valutazione delle conoscenze; consiste in un insieme di domande a risposta multipla (per ciascuna domanda sono proposte almeno 4 possibili risposte, di cui una sola corretta). Le domande coprono gli elementi fondamentali di abilità e conoscenza previsti dalla norma UNI 11697 per lo specifico profilo. Durante la prova il Candidato può consultare la norma UNI 11697 e il Regolamento (UE) 2016/679 (ed eventuali successive modifiche) purché privi di commenti e/o appunti. Per ciascuna domanda sono concessi 2 minuti per la rispettiva risposta. 2. **seconda prova ("casi di studio")** volta a verificare le competenze del Candidato su questioni pratiche connesse al profilo professionale oggetto di certificazione. Il caso di studio pone al candidato una situazione reale operativa a cui il candidato deve rispondere, nel modo più corretto, con la trattazione del caso. Per ciascun caso di studio sono concessi 10 minuti. La durata complessiva delle prove scritte è funzione del numero di domande e casi di studio che a loro volta sono dipendenti dal Profilo interessato. – **prova 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 le diverse figure professionali. L'ammissione alla prova orale avviene previo superamento di entrambe prove scritte.

	Durante la prova orale sono previsti: 1. **Simulazioni di situazioni reali operative** (Es: role-play), per valutare oltre alle abilità e alle competenze, anche le capacità personali (per esempio, capacità relazionali, comportamenti personali attesi). 2. **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). 3. **L'analisi e la valutazione di uno dei tre elaborati** presentati in fase di domanda di certificazione dal candidato ("IO 20.8.2 Esperienza Lavorativa ex Appendice A PdR 66:2019") e frutto della propria esperienza. Alla commissione esaminatrice deve essere presentato un elaborato redatto secondo un modello (Appendice A - Pdr66:2019) relativo a una situazione lavorativa, considerata significativa dal candidato a fronte della specifica figura professionale richiesta. 4. **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 "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. La durata della prova è variabile per ciascun Profilo interessato. In generale la commissione esaminatrice ha a disposizione mediamente 3 minuti per ciascuna domanda con il vincolo di contenere la durata della prova entro 60 minuti.
IX. **PROVE DI ESAME PER CIASCUN PROFILO PROFESSIONALE**	
RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI	– Prima prova scritta composta da **40 domande** a risposta multipla (durata 80 minuti) – Seconda prova scritta composta da **3 casi di studio** (durata 30 minuti). – Prova orale della 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)
MANAGER PRIVACY	– Prima prova scritta composta da **35 domande** a risposta multipla (durata 70 minuti) – Seconda prova scritta composta da **3 casi di studio** (durata 30 minuti). – Prova orale della 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)
SPECIALISTA PRIVACY	– Prima prova scritta composta da **35 domande** a risposta multipla (durata 70 minuti) – Seconda prova scritta composta da **2 casi di studio** (durata 20 minuti). – Prova orale della 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)
VALUTATORE PRIVACY	– Prima prova scritta composta da **35 domande** a risposta multipla (durata 70 minuti) – Seconda prova scritta composta da **2 casi di studio** (durata 20 minuti). – Prova orale della 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). Nella prova 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
NOTA *nel caso di richiesta di certificazione per più profili, il numero delle prove si modifica come indicato nella specifica sezione di questo documento.*	

X. **VALUTAZIONE DELLE PROVE D'ESAME**	
VALUTAZIONE DELLE PROVE D'ESAME	**Prove scritte:** – **prima prova (set domande)** 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. Il **punteggio massimo** conseguibile per ciascun profilo è: – **quaranta (40)** punti - Responsabile della Protezione dei Dati Personali; – **trentacinque (35)** punti - Manager, Specialista e Valutatore Privacy La **prova è superata** se il punteggio conseguito è almeno il 70% del punteggio massimo: – **ventotto (28)** punti - Responsabile della Protezione dei Dati Personali – **venticinque (25)** punti - Manager, Specialista e Valutatore Privacy. – **seconda prova (casi di studio)** La valutazione di **ciascuno dei casi di studio** costituente la prova di ciascun Candidato è fatta attribuendo un punteggio da zero a 10. La valutazione **dell'intera prova** di ciascun candidato è determinata dal punteggio complessivo costituito dalla media dei punteggi di valutazione attribuiti a ciascuno dei casi di studio costituenti la prova stessa, con il vincolo che il peggior punteggio attribuito non risulti inferiore a 5/10 punti. Il **punteggio complessivo massimo** conseguibile per qualsiasi profilo è: – **10/10 punti.** La **prova è superata** se il punteggio complessivo conseguito è almeno il 70% del punteggio massimo: – **7/10 punti** – qualsiasi profilo professionale. **Prova orale:** La valutazione **dell'intera prova** è determinata dalla somma dei punteggi attribuiti a ciascuna delle quattro sezioni della prova orale (simulazione, approfondimento delle domande eventualmente errate, analisi e valutazione di uno dei tre elaborati, domande specialistiche e argomenti obbligatori). Per la valutazione di ciascuna sezione vengono utilizzate specifiche griglie di valutazione ognuna delle quali considera tre singoli elementi con cui apprezzare le capacità e le competenze del candidato (es. padronanza delle materie, aggiornamento professionale, proprietà di linguaggio, prontezza nelle risposte). A ciascuno di tali elementi viene attribuito un punteggio variabile da 2 (valutazione minima) a 10 (valutazione massima). Il punteggio massimo conseguibile per qualsiasi profilo in ciascuna sezione è 30 punti, e il **punteggio massimo** conseguibile per l'intera prova: – **Centoventi (120) punti.** La **prova è superata** se il punteggio conseguito è di almeno 70% del punteggio massimo: – **Ottantaquattro (84) punti** – qualsiasi profilo professionale.
VALIDITÀ DELLE PROVE SUPERATE	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. L'ammissione al nuovo esame è subordinata ad una nuova formale iscrizione e al pagamento della quota prevista. Trascorsi i 12 mesi, occorre ripetere tutte le prove di esame. Il candidato nei mesi intercorrenti tra l'esame non superato e la sua ripetizione non può

	presentare domanda di certificazione ad altro Organismo di Certificazione, pena l'invalidazione dello stesso processo di certificazione
VALUTAZIONE COMPLESSIVA DELL'ESAME	L'esame è superato se il Candidato raggiunge almeno un punteggio pari al 70% del punteggio massimo in ciascuna delle tre prove.

XI. **RILASCIO, DURATA E ISCRIZIONE AL REGISTRO DELLA CERTIFICAZIONE**	
RILASCIO DELLA CERTIFICAZIONE	Previa valutazione positiva della Commissione Deliberante/Decision Maker che propone la certificazione, previo nulla osta della Direzione, viene rilasciato il certificato "Professionista del trattamento e protezione dei dati personali" nel profilo professionale conseguito e il logo ICMQ, al Candidato che: – ha soddisfatto i requisiti di ammissione all'esame; – ha superato le prove d'esame stabilite nel presente schema; – risulta in regola con tutti gli adempimenti delle Condizioni Generali. Quando necessario viene inviata la notifica dell'ottenimento della certificazione con l'indicazione di tempi e modalità per la consegna del certificato.
ISCRIZIONE AL REGISTRO	Le Persone in possesso di certificazione di Professionista della Privacy sono iscritte ai Registri ICMQ delle Persone certificate.
DURATA DELLA CERTIFICAZIONE	La Certificazione rilasciata ha durata di **4 anni** a partire dalla data della delibera ed è soggetta a conferma annuale.
XII. **MANTENIMENTO DELLA CERTIFICAZIONE**	
MANTENIMENTO E RINNOVO DELLA CERTIFICAZIONE	**<u>Mantenimento</u>** la validità della certificazione di ogni singola Persona certificata è subordinata alla verifica annuale (la prima entro 12 mesi dal rilascio, le altre entro successivi intervalli temporali di 12 mesi) dell'avvenuto pagamento della quota di mantenimento prevista dal Tariffario e della seguente documentazione: – documento comprovante lo svolgimento dell'attività professionale certificata (anche in modo non continuativo) costituito dal modello ICMQ - *IO 20.10 Scheda Di Mantenimento Annuale,* la cui pagina 1 la Persona certificata, a conclusione di ogni prestazione lavorativa, ovvero per ogni anno di attività, è tenuta a rilasciare al proprio cliente/datore di lavoro e sulla quale questo ultimo può esprimere un'opinione sulle attività/servizi svolti e riportare eventuali reclami (nel caso di più prestazioni effettuate, deve essere assicurata la conservazione di tutte le n pagine 1 relative alla scheda IO 20.10); – evidenza di almeno un incarico/attività/contratto attraverso il quale si dimostri di aver operato nell'ambito dei compiti richiamati dalla norma UNI 11697 – dichiarazione resa ai sensi degli artt. 46 e 76 del DPR 445/2000 (presente e da sottoscrivere dalla Persona certificata nel modulo allegato "*IO 20.10 Scheda Di Mantenimento Annuale*") 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; – attestati o altre evidenze di apprendimento per mantenere un elevato livello di conoscenza, e conservare le relative abilità per almeno 16 ore/anno per il DPO, e 8 ore per gli altri 3 profili (vedi NOTA); – copia di eventuali documenti nei quali viene utilizzato il marchio ICMQ. **<u>Rinnovo</u>** La certificazione ha una durata di quattro anni e può essere rinnovata, prima della sua scadenza, 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 un numero di ore (vedi NOTA) complessive nel quadriennio, pari ad almeno:

- 64 per il Responsabile della Protezione dei Dati Personali
- 32 per Manager, Specialista e Valutatore Privacy.

Il rinnovo avviene a fronte della richiesta del professionista prima della fine della validità della certificazione posseduta, utilizzando il modulo "IO 20.8 Richiesta di certificazione ed ammissione all'esame" che dovrà essere integrato dalla documentazione prevista.

NOTA:

L'impegno di ogni Persona certificata per il suo aggiornamento professionale è richiesto per le discipline, tematiche ed argomenti riconducibili esclusivamente alla security e alla sua evoluzione di contesto; tale impegno viene valutato in crediti formativi con i seguenti criteri:

– partecipazione a convegni/seminari e/o corsi di formazione afferenti a temi di Privacy privi di verifica finale	0,5 crediti all'ora
– partecipazione a corsi di formazione/aggiornamento afferenti a temi di Privacy con superamento della verifica finale	1 credito ogni ora
– pubblicazione di testi in tema di Privacy con case editrici di livello nazionale	1 testo = 8 crediti
– pubblicazione di articoli in tema di Privacy su riviste specializzate	1 articolo = 1 credito
– attività di docenza in materie di Privacy	1 ora di docenza = 1 credito

Si specifica che il raggiungimento dei 64 o dei 32 crediti formativi prima della scadenza quadriennale non esenta dal dover proseguire nella formazione continua, ovvero dall'acquisizione dei 16 o degli 8 crediti formativi per ogni anno rimanente al rinnovo.

Esame per il rinnovo

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

L'impegno di ogni Persona certificata per il suo aggiornamento professionale è richiesto per le discipline, tematiche ed argomenti riconducibili esclusivamente alla privacy e alla sua evoluzione di contesto; per la verifica documentale vengono considerati validi:

1. almeno un incarico/attività/contratto attraverso il quale si dimostri di aver operato nell'ambito dei compiti richiamati dalla Norma UNI;
2. la dimostrazione tramite titoli (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. un'"autodichiarazione" ai sensi degli artt. 46 e 76 del D.P.R. 445/2000 contenente:
   a. le attività svolte, di cui al punto 1 rispetto ai punti 4 e 5 della norma UNI 11697:2017, specifiche nel campo della protezione dati, durante l'anno;
   b. l'elenco completo, di cui al 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 reclami relativi all'attività certificata;
   d. la presenza di contenziosi legali in corso relativi all'attività certificata.

XIII. **PROVE DI ESAME AGGIUNTIVE PER CERTIFICAZIONE IN PIÙ' PROFILI**	
CANDIDATI INTERESSATI: ✓ **Persone in possesso dei requisiti di ammissione per più profili** ✓ **Persone in possesso di una Certificazione UNI 111697:2017 accreditata in corso di validità**	
PROVE D'ESAME AGGIUNTIVE	**Richiesta di certificazione relativa a più profili nella medesima sessione di esami** Il Candidato, in possesso dei necessari prerequisiti per ciascun profilo richiesto, deve sostenere l'esame completo per il più alto dei profili, secondo la seguente classificazione (dal più alto al più basso): – Responsabile della protezione dei dati – Manager Privacy – Valutatore Privacy – Specialista Privacy All'esame completo vanno aggiunte: – 10 domande a risposta multipla per ogni profilo aggiuntivo; – 1 "caso di studio" per ogni profilo aggiuntivo; – 15 minuti di esame orale per ogni profilo aggiuntivo; Le prove integrative riguardano le conoscenze e le abilità specifiche di ogni profilo richiesto. La valutazione delle prove aggiuntive per ciascun profilo aggiuntivo avviene con gli stessi criteri previsti per le prove del più alto dei profili richiesti.

XIV. **TRASFERIMENTO**	
– **di una certificazione UNI 11697:2017 in corso di validità da altro ODC (Organismo Di Certificazione) ACCREDITATO** **CANDIDATI INTERESSATI:** ✓ **persone in possesso di una certificazione accreditata in corso di validità**	
TRASFERIMENTO DELLA CERTIFICAZIONE	Il Professionista certificato da altro Organismo di Certificazione accreditato in qualità di Professionista della Privacy può richiedere il trasferimento della sua certificazione valida – **solo per lo stesso Profilo** – compilando al riguardo il modulo "IO 20.8 Richiesta di certificazione ed ammissione all'esame" ICMQ accoglie la domanda di trasferimento solo se accompagnata da: – la copia del certificato in essere in corso di validità; – una sintesi degli esiti relativi al precedente esame; – l'evidenza di chiusura di eventuali pendenze (economiche e tecniche) nei confronti dell'OdC cedente, compresa la gestione di eventuali reclami; – il pagamento della quota prevista nel tariffario in vigore. ICMQ provvede a: – esaminare la documentazione prodotta dal professionista certificato; – (eventualmente) richiedere informazioni/documenti supplementari. Qualora venissero riscontrate carenze per il trasferimento richiesto, l'iter di valutazione viene interrotto e il Professionista informato della necessità di rimuovere le carenze riscontrate. Nel caso di riscontro positivo, **tenendo conto dello stesso profilo certificato oggetto della richiesta di trasferimento**, ICMQ provvede a: – invitare il Professionista (previa accettazione dei relativi oneri di spesa) a sostenere l'esame orale con le stesse modalità della prima certificazione.

	In caso di superamento dell'esame, ICMQ provvede a: – sottoporre l'esito delle suindicate attività alla Commissione Deliberante di ICMQ cui compete la decisione di trasferimento; – rilasciare in seguito la nuova certificazione; aggiornare il registro dei Professionisti della Privacy certificati
NOTA BENE: – ***Non sono accettabili le richieste di estensione ad altri profili professionali contestuali al trasferimento sopra descritto della certificazione.*** *Tali richieste possono essere valutate ed eventualmente effettuate solo una volta deciso il trasferimento, rilasciata la nuova certificazione ed aggiornato il registro.*	

XV. **ESTENSIONE alla certificazione UNI 10459/DM269 (Ambito Vigilanza Privata) – CASO (A)**	
CANDIDATI INTERESSATI: ✓ **Persone in possesso di una Certificazione UNI 11697:2017 rilasciata in prima emissione da ICMQ accreditata in corso di validità**	
ESTENSIONE DELLA CERTIFICAZIONE AL PROFILO DI RESPONSABILE DELLA PROTEZIONE DEI DATI	Il candidato già certificato in un profilo professionale può richiedere la certificazione per il Responsabile della protezione dei dati dimostrando di possedere i requisiti richiesti per l'accesso alla certificazione in tale profilo. In tal caso dovrà sostenere le seguenti prove – 30 domande a risposta multipla; – 2 "casi di studio"; – Colloquio della durata minima di 30 minuti.
ESTENSIONE DELLA CERTIFICAZIONE AD ALTRI PROFILI PROFESSIONALI	Il candidato già certificato in un profilo professionale può richiedere la certificazione per altri profili (escluso il Responsabile della protezione dei dati), dimostrando di essere in possesso dei requisiti richiesti per l'accesso alla certificazione in tali profili. In tal caso dovrà sostenere le seguenti prove – 20 domande a risposta multipla per ogni profilo oltre al primo; – 1 "caso di studio" per ogni profilo oltre al primo; – Esame orale della durata minima di 20 minuti per ogni ulteriore profilo. La valutazione delle prove per ciascun profilo oggetto di estensione avviene con gli stessi criteri previsti per le prove di prima certificazione.