REGOLAMENTO GENERALE PER LA CERTIFICAZIONE PROFESSIONALE SCHEMA PRIVACY: _DATA PROTECTION OFFICER - DPO

STORIA DELLE REVISIONI:				
N°	DATA	MOTIVO	EMETTE	APPROVA
06	2019-05-22	CHIARIMENTI § 6.3. MODIFICHE	RO	AU
07	2020-07-20	ALLINEAMENTO ALLA UNI PDR 66:2019	RO	AU
08	2021-05-21	ELIMINAZIONE RIFERIMENTI ALLA CIRCOLARE N. 03/2018 DEL 13 FEBBRAIO 2018 SOSTITUITA ED INTEGRATA DALLA PDR 66:2019	RO	RL

Art. 1 **Oggetto ed Ambito di Applicazione**

Il presente regolamento stabilisce le condizioni e le procedure per la concessione, il mantenimento, la sospensione, il rinnovo e la revoca della Certificazione del:

- Data Protection Officer - DPO.

Art. 2 **Riferimenti Normativi**

I criteri stabiliti da KHC - Know How Certification, per i processi di Certificazione, recepiscono la normativa nazionale e/o internazionale di riferimento:

- UNI CEI EN ISO/IEC 17024:2012 - Valutazione della conformità - Requisiti generali per gli organismi operanti la certificazione delle persone;
- ISO/IEC 27001:2017 - *Information technology - Security techniques - Information security management systems - Requirements;*
- requisiti cogenti applicabili: Regolamento (UE) 2016/679 del 27 aprile 2016, D.L. 101/2018 e s.m.i.;
- UNI 11697:2017 - Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza;
- UNI 11506 - Attività professionali non regolamentate - Figure professionali operanti nel settore ICT - Requisiti per la valutazione e certificazione delle conoscenze, abilità e competenze per i profili professionali ICT basati sul modello e-CF;
- UNI 11621-1 - Attività professionali non regolamentate - Profili professionali per l'ICT - Metodologia per la costruzione di profili professionali basati sul sistema e-CF;
- UNI 11621-2 - Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 2: Profili professionali di "seconda generazione";
- UNI EN 16234-1 - e-Competence Framework (e-CF) - Framework comune europeo per i professionisti ICT di tutti i settori industriali - Parte 1: Framework (modello di riferimento);
- UNI CEI ISO/IEC 27000 - Tecnologie informatiche - Tecniche per la sicurezza - Visione d'insieme e vocabolario;
- UNI CEI ISO/IEC 29100 - Tecnologie informatiche - Tecniche per la sicurezza -Quadro di riferimento per la Privacy;
- 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"

Art. 3 **Termini e Definizioni**

- *KHC - Know How Certification*: Organismo di certificazione del Personale e della Formazione nei settori Qualità ed Ambiente, di seguito indicato come KHC.
- *Organismo di certificazione del Personale e della Formazione:* Organismo che effettua certificazioni di conformità (relativa ai corsi di formazione) e di competenza (relativa ai professionisti).
- *Certificazione di competenza del Personale*: atto mediante il quale una parte terza indipendente dichiara che, con ragionevole attendibilità, una determinata persona possiede i requisiti necessari e sufficienti per operare con competenza e professionalità nello specifico settore (es. Privacy).
- *Sospensione iscrizione a Registro:* provvedimento di sospensione dell'iscrizione a Registro da parte dell'Organismo di certificazione, per un periodo di tempo determinato, la cui revoca implica la risoluzione delle cause che lo hanno generato.
- *Annullamento iscrizione a Registro:* provvedimento di annullamento dell'iscrizione a registro la cui revoca implica la ripetizione completa dell'iter certificativo.
- *Procedura Valutativa* (PV)/esame certificativo: esame il cui superamento, previo accertamento del possesso dei requisiti previsti dagli Schemi di certificazione applicabili (QI 600101a) e dell'assenza di condizioni ostative giuridiche, consente l'iscrizione al Registro KHC di pertinenza.
- *Consultant*: persona che ha la competenza per effettuare una consulenza in un determinato settore (coma da schema di qualifica).
- *Auditor (Valutatore)*: persona che ha la competenza per effettuare una verifica ispettiva.
- *Data Protection Officer (Responsabile Protezione dati personali)*: E' un profilo corrispondente al profilo professionale disciplinato nel Regolamento UE 2016/679, in particolare all'art. 39. E' 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. Supporta il Titolare o Responsabile nell'applicazione del Regolamento UE 2016/679.
- *Abilità:* capacità di applicare conoscenze e di utilizzare know-how per portare a termine compiti e risolvere problemi.
- *Competenza:* comprovata capacità di utilizzare conoscenze, abilità e capacità personali, sociali e metodologiche in situazioni di lavoro o di studio e nello sviluppo professionale e personale, esercitabile con un determinato grado di autonomia e responsabilità.
- *Conoscenza:* risultato dell'assimilazione di informazioni attraverso l'apprendimento.

Art. 4 **Tutela della Privacy**

Il trattamento dei dati personali, gestiti ed utilizzati da KHC nelle varie fasi previste dal processo di Certificazione, si svolge nel rispetto del diritto alla riservatezza delle persone fisiche e delle Organizzazioni, secondo la normativa attualmente in vigore (D. Lgs 196/2003) e dal 25 maggio 2018, nel rispetto del Regolamento UE 2016/679.

Art. 5 **Requisiti richiesti**

Il soddisfacimento dei requisiti stabiliti da KHC, come riportato nello schema (QI 600101a), parte integrante del presente Regolamento, è condizione necessaria per la concessione della Certificazione.

Art. 6 **Iter di Certificazione del Personale**

6.1 **Certificazione del Data Protection Officer (DPO)**

Il Candidato che desidera aderire allo schema di certificazione KHC, può trovare informazioni e i documenti necessari, nel sito internet KHC (http://www.khc.it/certificazione/privacy/) o richiederli telefonicamente o tramite e-mail a: staffoperativo@khc.it o tramite il sito compilando il form "contattaci".

L'iscrizione al relativo Registro e la relativa certificazione prevede il soddisfacimento delle seguenti fasi:

- presentazione della *Domanda di Certificazione* (QI 600104a) a KHC tramite apposita modulistica, scaricabile da sito http://www.khc.it/certificazione/privacy/, con cui il candidato sottoscrive la presa visione dei documenti ivi richiamati, nello stato di revisione applicabile alla data di sottoscrizione della Domanda di certificazione, consultabili sul sito, comprensiva:
  - del *Curriculum Vitae* aggiornato in FORMATO EUROPEO (sottoscrivendo il consenso al trattamento dati in conformità al riferimento legislativo applicabile al momento della presentazione della Domanda e la dichiarazione ai sensi del DPR 445/2000: dichiarazioni veritiere ai sensi dell'art. 46 e consapevole delle sanzioni previste dall'art. 76);
  - *copia del titolo di studio;*
  - copia del codice fiscale;
  - le evidenze come dichiarate nel CV (es. in riferimento al titolo di studio, all'esperienza lavorativa e alla formazione), atte ad attestare il soddisfacimento dei requisiti, come da schema applicabile;
  - sottoscrizione e relativo rispetto delle Norme Deontologiche (QI 100107), del Regolamento e Manuale d'uso del marchio di certificazione (QI 100108);
  - sottoscrizione per accettazione delle quote applicabili (rif. Fees&Payments. [*Quote*]) QI 600105a rif. http://www.khc.it/certificazione/privacy/*;*
- pagamento della prima quota: alla presentazione della domanda di certificazione. Quota per la valutazione documentale dei requisiti da parte di KHC;
- analisi documentale e dei requisiti dichiarati ed eventuale richiesta di integrazione documentale (attestati, dichiarazione/i da parte di aziende a supporto dell'esperienza richiesta nello schema, ecc.), in conformità a quanto specificato nello Schema KHC applicabile;
- pagamento della seconda quota: prima dello svolgimento della PV. La quota comprende anche il primo anno di iscrizione a registro. Solo ad esito positivo della verifica documentale suddetta, KHC comunica al richiedente il suo status di candidato all'esame e la data della prima sessione disponibile.
- superamento dell'esame certificativo-Procedura Valutativa (PV) **come dettagliato nello schema requisiti QI 60 01 01a**, parte integrante del presente regolamento, con due Commissari KH, il cui obiettivo è quello di valutare la competenza (rif. §5.1 UNI 11697 - e-CF 3.0), abilità e conoscenza (rif. §5.1 UNI 11697) nel settore Privacy (Tabella A). Ove in tale fase dovessero **emergere significative carenze teoriche o di competenza**, l'esame è considerato **non superato**.
- delibera della Certificazione da parte degli Organi KHC preposti, solo a seguito dell'avvenuto saldo delle fatture suddette;
- comunicazione dell'esito dell'iter certificativo, per e-mail;
- inserimento a registro pubblico su http://www.khc.it/registri/registro-figure-professionali/ (attestante l'avvenuta certificazione), ricevimento del certificato (A4 in formato pdf), del marchio professionista certificato (formato jpg) e di un plico contenente il certificato (formato card) ed il Timbro.

Il candidato in fase di PV dovrà mostrare un documento di identità in corso di validità, al Commissario d'esame.

Qualora il candidato non abbia concluso con esito positivo l'esame le eventuali singole prove superate rimangono valide per 12 mesi.

6.2 **Trasferimento del certificato (già conforme alla UNI 11697:2017 e UNI PdR 66:2019) rilasciato da altro OdC accreditato**

L'accesso di tali candidati **in conformità a quanto specificato nello Schema** (rif. Schema di riferimento di competenza - QI 600101a), al relativo Registro KHC, è subordinato a:

1. presentazione della *Domanda di Certificazione* (QI 600104a) a KHC tramite apposita modulistica, scaricabile da sito http://www.khc.it/certificazione/privacy/, con cui il candidato sottoscrive la presa visione dei documenti ivi richiamati, compresi *Norme Deontologiche* (QI 10 01 07) e *Regolamento e Manuale d'uso del marchio di certificazione* (QI 10 01 08), consultabili sul sito, nello stato di revisione applicabile alla data di sottoscrizione della Domanda di certificazione, e comprensiva di:
   a) il certificato in corso di validità,
   b) i documenti applicabili per la sorveglianza,
   c) eventuale evidenza della chiusura di eventuali pendenze (economiche e tecniche) aperte con l'OdC precedente nei suoi confronti,
   d) accettazione quote previste e pagamento regolare della quota per il trasferimento, come previsto dalle Quote applicabili (rif. Fees&Payments. [*Quote*]) QI 600105a e consultabili tramite sito rif. http://www.khc.it/certificazione/privacy/,
2. analisi documentale e dei requisiti dichiarati, in conformità a quanto specificato nello Schema di riferimento di competenza) ed eventuale richiesta di integrazione documentale da parte di KHC.;
3. superamento dell'esame orale come dettagliato nello schema requisiti QI 60 01 01a, parte integrante del presente regolamento, con due Commissari KHC, il cui obiettivo è quello di valutare il mantenimento della competenza, abilità e conoscenza nel settore Privacy (Tabella A), come specificato al §6.1.
4. delibera della Certificazione da parte degli Organi KHC preposti solo a seguito dell'avvenuto saldo delle fatture suddette;
5. comunicazione dell'esito dell'iter certificativo, per e-mail,
6. inserimento a registro pubblico su http://www.khc.it/registri/registro-figure-professionali/ (attestante l'avvenuta certificazione e l'eventuale attribuzione di settori specialistici), ricevimento del certificato e del Marchio professionista certificato (formato jpg) e del plico contenente il certificato formato tessera e del Timbro.

Il candidato in fase di PV dovrà mostrare un documento di identità in corso di validità, al Commissario d'esame.

6.3 ***Presenza Ispettori ACCREDIA***

Durante lo svolgimento della PV, oltre alla presenza del Commissario, può essere prevista la partecipazione degli Ispettori ACCREDIA, in fase di accreditamento e successivamente.

6.4 **Date e luoghi di svolgimento Procedura Valutativa (PV)**

Le date e i luoghi in cui è possibile sostenere la PV o i colloqui tecnici previsti dalla PV, sono stabilite da KHC in funzione delle richieste ricevute ed eventualmente concordate con il/i candidato/i. La commissione d'esame sarà composta da due Commissari. In caso di necessità potrà essere svolto l'esame con un solo Commissario in presenza e l'altro in modalità da remoto, con l'uso di tecnologia IT. Eventuali eccezioni/deroghe alla seguente procedura saranno applicate per casi eccezionali dovranno prima essere approvate da ACCREDIA.
La Commissione di valutazione, a fine PV, comunica al candidato l'esito della stessa.

Qualora il candidato non abbia concluso con esito positivo l'esame le eventuali singole prove superate rimangono valide per 12 mesi. il candidato può presentare domanda di ripetizione (non prima di **3** mesi) e ripetere la PV, pagando la quota relativa alla ripetizione (rif. Quote QI 600105a, consultabile sul sito www.khc.it). Nei mesi intercorrenti tra l'esame non superato e la sua ripetizione, il candidato non può presentare domanda di certificazione ad altro organismo di certificazione, pena l'invalidazione dello stesso processo di certificazione.

Tabella A

COMPETENZE (rif. §5.1 UNI 11697 - e-CF 3.0) A.4 Pianificazione di prodotto o di servizio; D.1 Sviluppo della strategia per la Sicurezza Informatica; D.8 Gestione del Contratto; D.9 Sviluppo del Personale; E.3 Gestione del Rischio; E.4 Gestione delle relazioni; E.8 Gestione della Sicurezza dell'Informazione; E.9 Governance dei sistemi informativi
ABILITA' (rif. §5.1 UNI 11697) Contribuire alla strategia per il trattamento e per la protezione dei dati personali, gestire l'applicazione dei codici di condotta e delle certificazioni applicabili in materia di trattamento e protezione dei dati personali, capacità organizzative, capacità di comunicare, capacità di analisi, autogestione e controllo dello stress, capacità di controllo, capacità di autosviluppo, capacità di convincimento, capacità di gestione dei conflitti, iniziativa, idoneità alla negoziazione, pensiero prospettico, tenacia, atteggiamento costruttivo nella soluzione dei problemi, pianificazione e programmazione; *S1*- affrontare le esigenze della formazione continua (CPD) del personale per soddisfare le esigenze dell'organizzazione, *S5*- analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi, *S19*- anticipare i cambiamenti richiesti alla strategia aziendale dell'information security e formulare nuovi piani, *S21*- applicare azioni di contenimento del rischio e dell'emergenza, *S23*- applicare gli standard, le best practice e i requisiti legali più rilevanti all'information security, *S40*- coaching, *S52*- comunicare e pubblicizzare sia i risultati dell'analisi del rischio che i processi di gestione del rischio, *S55*- comunicare le buone e le cattive notizie per evitare sorprese, *S66*- costruire un piano di gestione del rischio per fornire e produrre piani di azione preventivi, *S91*- garantire che la proprietà intellettuale (IPR) e le norme della privacy siano rispettate, *S111*- identificare gap di competenze e skill gap, *S140*- negoziare termini e condizioni del contratto, *S153*- preparare i template per pubblicazioni condivise, *S156*- progettare e documentare i processi dell'analisi e della gestione del rischio, *S167*- raccogliere la conoscenza interna ed esterna e i fabbisogni di informazione, *S171*- rendere l'informazione disponibile, S172- rispondere alle esigenze di sviluppo professionale del personale per soddisfare le esigenze organizzative, *S176*- seguire e controllare l'uso effettivo degli standard documentativi aziendali, *S187*- sviluppare piani di risk management per identificare le necessarie azioni preventive.

CONOSCENZE (rif. §5.1 UNI 11697)
I principi di privacy e protezione dei dati by design e by default, i diritti degli interessati previsti da leggi e regolamenti vigenti, le responsabilità connesse al trattamento dei dati personali, le responsabilità connesse al trattamento dei dati personali, norme di legge italiane ed europee in materia di trattamento e di protezione dei dati personali, norme di legge in materia di trattamento e protezione dei dati personali per all'estero e circolazione dei dati personali extra UE/SEE, le metodologie di valutazione d'impatto sulla protezione dei dati e PIA, le possibili minacce alla protezione dei dati personali, tecniche e strumenti di comunicazione (relazione con Istituzioni, autorità, Forze dell'Ordine, enti locali e stampa), sistemi e tecniche di monitoraggio e "reporting", le tecniche crittografiche, le tecniche di anonimizzazione e de-anonimizzazione, le tecniche di pseudonimizzazione, le norme tecniche ISO/IEC per la gestione dei dati personali, i codici di condotta e le certificazioni applicabili in materia di trattamento e protezione dei dati personali;
K26-gli strumenti di controllo della versione per la produzione di documentazione, *K49*- i metodi di sviluppo delle competenze, *K60*- i processi dell'organizzazione ivi inclusi le strutture decisionali, di budget e di gestione, *K67*- i rischi critici per la gestione della sicurezza, *K71*- i tipici KPI (key performance indicators), *K83*- il potenziale e le opportunità offerte dagli standard e dalle best practice più rilevanti, *K85*- il ritorno dell'investimento comparato all'annullamento del rischio, *K98*- l'impatto dei requisiti legali sulla sicurezza dell'informazione, *K108*- la computer forensics (analisi criminologica di sistemi informativi), *K115*- la politica di gestione della sicurezza nelle aziende e delle sue implicazioni con gli impegni verso i clienti, fornitori e i sub-contraenti, *K122*- la strategia dell'informazione nell'organizzazione, *K130*- le best practice (metodologie) e gli standard nella analisi del rischio, *K132*- le best practice e gli standard nella gestione della sicurezza delle informazioni, *K139*- le metodologie di analisi dei fabbisogni di competenze e skill, *K149*- le norme legali applicabili ai contratti, *K152*- le nuove tecnologie emergenti (per esempio sistemi distribuiti, modelli di virtualizzazione, sistemi di mobilità, data sets), *K158*- le possibili minacce alla sicurezza, *K161*- le problematiche legate alla dimensione dei data sets (per esempio big data), *K162*-le problematiche relative ai dati non strutturali (per esempio data analytics), *K180*- le tecniche di attacco informatico e le contromisure per evitarli.

Art. 7 **Validità, sorveglianza, mantenimento e rinnovo**

	Figure professionali: DPO
Validità /Durata della certificazione (dalla data della delibera della certificazione/prima emissione del certificato) con sorveglianze annuali.	4 anni
Sorveglianza annuale per il mantenimento della certificazione Nota: l'aggiornamento del certificato con il riferimento anche alla UNI PdR 66:2019, sarà effettuato in occasione della prima sorveglianza del professionista certificato, successiva all'aggiornamento dell'accreditamento di KHC da parte di ACCREDIA, in riferimento alla prassi.	Nel periodo di validità della certificazione, per confermare la validità della certificazione, annualmente il professionista certificato prima della scadenza annuale (il riferimento è la data di inserimento a registro), deve inviare a KHC il modulo **"Autodichiarazione" QI 60 01 10** (ai sensi degli artt. 46 e 76 del D.P.R. 445/2000) scaricabile dal sito rif. http://www.khc.it/certificazione/privacy/, dove elencare: 1) **continuità dell'esperienza lavorativa** - ovvero evidenze documentali delle attività svolte, specifiche nel campo della protezione dati, durante l'anno, per almeno un **incarico/attività/contratto** nel quale si dimostri di aver operato nell'ambito dei compiti richiamati ai punti 4 e 5 della Norma UNI 11697; 2) **aggiornamento professionale per almeno 16 ore/anno** - ovvero l'elenco completo dei corsi di aggiornamento, partecipazione a convegni, seminari, relazioni, docenze, durante l'anno, inerenti gli argomenti relativi al settore della privacy come declinato nelle tabelle riepilogative per profilo, dimostrabile tramite titoli (attestati/contratti/registri partecipazione e similari) di partecipazione ad attività di formazione/convegni/docenze/relazioni/gruppo di lavoro normativo o tecnico; 3) la presenza di **reclami** relativi all'attività certificata; 4) la presenza di contenziosi legali in corso relativi all'attività certificata; 5) evidenze documentali della corretta gestione di eventuali reclami e contenziosi. In quest'ultimo caso sarà responsabilità di KHC valutare l'adeguatezza della relativa gestione, sulla base della tempestività e congruenza delle azioni intraprese dal professionista. Dopo la risposta iniziale, da fornire entro 10 gg lavorativi al reclamante, il professionista provvede ad adottare le misure necessarie 8compreso il mancato seguito a reclami ritenuti non applicabili) entro 6 settimane calendariali, dando la necessaria risposta al reclamante. Di tale processo (ricezione del reclamo, prima risposta, analisi e azione discendente) il professionista deve tenere adeguata tracciabilità documentale. 6) pagamento regolare delle quote annuali dovute a KHC, come previsto dalle Quote applicabili e consultabili tramite sito rif. http://www.khc.it/certificazione/privacy/ **Note:** L'attività di sorveglianza può avere come esito il mantenimento, la sospensione o la revoca della certificazione a fronte della valutazione effettuata da parte di KHC in merito a completezza, congruità della documentazione presentata nonchè gestione di eventuali reclami e/o contenziosi legali.

Sospensione e annullamento/revoca della certificazione Il provvedimento di sospensione ha una durata massima di 6 mesi, superati i quali il provvedimento si trasforma in annullamento della certificazione. KHC si riserva il diritto di sospendere e/o annullare la relativa certificazione, (tramite comunicazione scritta: raccomandata A/R – o PEC), nel caso in cui si presentino le seguenti condizioni a) – b):	a) - Mancato pagamento delle quote previste; - Mancata completezza, mancata congruità della documentazione presentata nonchè gestione di eventuali reclami e/o contenziosi legali.; - Mancato rispetto delle Norme Deontologiche e del Regolamento e Manuale d'uso del marchio di Certificazione; - Comportamenti screditanti l'immagine di KHC. b) Richiesta di disdetta da parte dell'interessato (3 mesi prima della scadenza quadriennale, tramite comunicazione scritta: raccomandata A/R o PEC). **In caso di annullamento** o sospensione della certificazione, il professionista si impegna a cessare immediatamente ogni riferimento alla certificazione sospesa o annullata e restituire qualsiasi certificato (in corso di validità) o timbro rilasciato dall'Organismo di certificazione.
Iscrizione in caso di annullamento	In caso di annullamento il soggetto può iscriversi nuovamente ai registri KHC ripercorrendo l'intero processo o parte di esso, previa autorizzazione KHC (es. verifica della continuità dell'esperienza lavorativa e aggiornamento professionale, come previsto per il rinnovo della certificazione nello Schema applicabile, se presenta la domanda entro 1 anno dall'annullamento).
Rinnovo Tacito Rinnovo in assenza di richiesta di disdetta da parte dell'interessato, 3 mesi prima della scadenza quadriennale della certificazione, in seguito a:	Per rinnovare la validità della certificazione oltre a raccogliere le evidenze già previste per l'attività di sorveglianza (continuità dell'esperienza ed aggiornamento professionale/anno, documentato), si verifica che siano mantenute le competenze previste al punto 5 della UNI 11697:2017. Il DPO certificato deve superare, una prova scritta composta da domande a risposta multipla, strutturato come l'esame di certificazione. Nel caso in cui non superasse questa prima prova, può ripeterla in una sessione d'esami successiva (se la certificazione non è già scaduta), ripetendo la prova scritta composta da domande a risposta multipla ma con l'aggiunta dell'esame scritto sui casi di studio, strutturato come l'esame di certificazione (rimangono invariati anche in questo caso i criteri per il superamento dell'esame). In caso di esito negativo anche di questa seconda prova, è necessario effettuare un esame completo di prima certificazione (domande a risposta multipla, casi di studio e orale). La procedura prevista dal rinnovo della certificazione deve essere completata entro il periodo di validità del certificato, per evitare che il certificato scada e venga revocato. P**er cui il professionista dovrà, improrogabilmente, inviare tutta la documentazione e concordare una sessione d'esame almeno 60 giorni prima della scadenza.**

Art. 8 **Ricorsi**

Qualsiasi persona o Organizzazione può presentare ricorso contro decisioni prese da KHC nei suoi confronti, riguardo a:
- certificazione;
- sospensione, annullamento o rinnovo della certificazione.

Tale ricorso deve essere inoltrato in forma scritta, a mezzo raccomandata A/R, al Responsabile dell'Organismo, entro 30gg dalla data di ricevimento della comunicazione.
Il ricorso dovrà contenere:
- le generalità del soggetto presentante il ricorso;
- descrizione dettagliata di eventi, fatti, motivazioni oggetto del ricorso.

L'Amministrazione valuta il contenuto del ricorso e comunica al Responsabile dell'Organismo la decisione presa, in modo che questi possa comunicare, in forma scritta, al soggetto interessato la decisione presa entro tre mesi dal ricevimento dello stesso.

Il soggetto interessato ha 30 gg per ricorrere in appello. Dalla data di ricezione della richiesta di appello, KHC ha 3 mesi di tempo per risolvere la controversia. In caso di mancata risoluzione dopo i 3 mesi, la stessa è affidata ad una terna arbitrale costituita da:
- un rappresentante del Comitato di Delibera;
- un rappresentante del soggetto che presenta ricorso;
- il Presidente del Consiglio d'Appello (terza parte indipendente, scelto da entrambi o in mancanza di accordo dal Presidente del Foro di Catania).

L'esito dell'appello sarà comunicato, in forma scritta, dal Responsabile dell'Organismo al soggetto interessato.
In tutti i casi le spese sono da considerarsi a carico del soggetto che presenta ricorso ad eccezione dei casi di riconosciuta fondatezza.

Art. 9 **Reclami / suggerimenti**

Qualsiasi persona o Organizzazione può inoltrare reclami /suggerimenti a KHC, in riferimento a sue attività o attività svolte da persone o Organismi posti sotto certificazione/qualifica da parte di KHC.

Il reclamo/suggerimento, che può essere inviato attraverso lettera - via posta ordinaria, fax o e-mail, dovrà contenere:
- le generalità del soggetto presentante il reclamo/suggerimento;
- descrizione dettagliata di eventi, fatti, motivazioni oggetto del reclamo/suggerimento.

Il reclamo/suggerimento sarà gestito dal RO (Responsabile dell'Organismo) e l'esito della gestione sarà comunicato dal RO al soggetto interessato, entro 15 gg lavorativi.

Art. 10 **Proprietà del certificato KHC**

Il certificato KHC rilasciato ai professionisti, è di proprietà esclusiva di KHC.
Il professionista, si impegnano con la sottoscrizione della Domanda prevista dall'iter certificativo, a non utilizzare il certificato in maniera fuorviante e ad astenersi da ulteriore promozione della certificazione durante un periodo di sospensione della certificazione o di fare riferimento alla stessa in caso di annullamento della certificazione.

Art. 11 **Imparzialità**

KHC gestisce i propri processi, le proprie attività di certificazione in maniera imparziale (rif. *Dichiarazione di imparzialità* sul sito www.khc.it : *corporate*). KHC non preclude l'accesso alla certificazione a persona in alcun caso.