Prot. DC2018SSV023 Milano, 12-02-2018

To all certification bodies accredited in the PRS scheme providing the certification of quality management systems for IT services.
Att.: Scheme managers

To the associations of conformity assessment bodies

Subject: Department of Certification and Inspection – Technical circular N° 03/2018. Requirements for certification and accreditation for conformity to the standard UNI 11697:2017 – Professional profiles regarding the treatment and protection of personal data.

Introduction

This circular provides indications regarding the accreditation of certification bodies for the granting of the certification of professional persons regarding the treatment and protection of personal data in conformity with UNI 11697:2017. This circular was prepared by a working group coordinated by ACCREDIA with the participation of all the main interested parties.

The aim is to set out common rules and criteria for all CBs.

Normative context

Reference should be made to the bibliography of UNI 11697:2017.

1) Rules for certification

Accreditation standard	UNI CEI EN ISO/IEC 17024
Certification standard	UNI 11697:2017
Criteria of competence of the board of examiners	The board of examiners shall possess, collectively, the following competences: 1. knowledge of the rules and criteria defined by the CB for examination of the certificate which shall be in line with the requirements of ISO/IEC 17024; 2. possession of the certificate accredited by ACCREDIA of the profile of the UNI standard which is the object of the exam[1] 3. competence deriving from at least 8 years' experience in matters concerning information security and the protection of personal data; 4. competence deriving from at least 8 years' experience in juridical matters (e.g. lawyer, magistrate,) with proven experience in data protection.

[1] Possession of an accredited certificate must be sufficient to examine:
- An examiner certified as data protection officer may examine DPOs, Managers, Assessors, Specialists
- An examiner certified as Manager may examine Managers, Assessors, Specialists
- An examiner certified as Verifier may examine Assessors, Specialists
- An examiner certified as Specialist may examine a Specialist

Sede operativa e amministrativa: Via Tonale, 26 | 20125 Milano - Italy | Tel. +39 02 2100961 | Fax +39 02 21009637
Sede legale: Via Guglielmo Saliceto, 7/9 | 00161 Roma - Italy | Tel. +39 06 8440991 | Fax +39 06 8841199
milano@accredia.it | www.accredia.it | Partita IVA - Codice Fiscale 10566361001

	The board of examiners shall have at least 2 members. Grandparent For the first three operative years, substituting a member of the board of examiners with accredited certification in the same professional profile which is the object of the assessment (point 2 above) the CB may use a Grandparent possessing at least one of the following requirements: 1. having operated as a manager in an area such as treatment of personal data, information security and the protection of personal data for not less than 8 years; 2. having operated as a manager in an area such as treatment of personal data, information security and the protection of personal data for not less than 3 years and having had other experiences in the same field (also as university teacher for at least 2 years or as technical auditor/expert in management systems for the protection of personal data. It is, nonetheless, necessary to have at least 8 years' experience; 3. having operated as a management systems manager for information security and/or management of ITC services (e.g. persons accredited as Team Leaders to UNI ISO/IEC 27001 or UNI ISO/IEC 20000-1, or CISA auditors) for not less than 8 years; 4. having had important positions in public institutions 6 years or having played an important role in major programs or projects in the area of privacy, or in scientific, normative, technical current affairs activities and similar for not less than 3 years; 5. possession of a professional certificate in compliance with UNI 11506 and with multi-party standards related to ICT security Manager, ICT Security Specialist or web security expert activities, and 2 years' experience as consultant in privacy, i.e. a certification as ISMS Professional on the basis of ISO 27021.
Competece criteria of decision-makers	The CB shall have qualification criteria for decision makers who may be members of the CB's staff, in order to ensure their competence: The criteria shall take into account as follows: • knowledge of the decision-taking processes of the CB; • general knowledge of standard UNI 11697:2017
Duration of the certification	4 years with annual surveillances
Exam modalities for certification (written and oral)	Requirements for access to the certification exam In order to do the exam, candidates must fulfill all the requirements in annex B of UNI 11697:2017, with the clarifications given in point 4.1 of the standard, by means of: • the presentation of suitable documentation, also by means of self-declaration prepared in conformity with article 46 and 47 of Law D.P.R. 445/2000 and also subject to verification upon request of the CB. Uniformity, assessment and contents of the applications - a correction grid must be prepared for the written exam - for the oral exam there must be a list of questions, a representative sample of which will be put to the candidate - for the first written exam the examination board prepares questions which must be at least double in number those in the actual exam. After the first exam, the number of questions is increased until a rotation is achieved where by the same question are not given in the subsequent exams. A similar approach must be adopted for the study activity to be done by the candidates in both

	the written and oral exams. Taken together, the exams must cover, for all candidates, fundamental skills and knowledge as required by UNI 11697. Continuous updating shall be done to the questions on the basis of normative and technological changes. <u>Criteria for passing the exam</u> To pass the exam the candidate must have obtained a score of at least 65% of the maximum for each individual exam. If the candidate has not passed the exam, the results of the individual tests remain valid for 12 months.
Certification for a number of professional profiles	The candidate who - in possession of the necessary requirements – requests certification for a number of professional profiles at the same exam session, must do the complete exam for the highest profile for which s/he has applied, in accordance with the following classification which goes from highest to lowest: • Data protection management • Privacy management • Privacy assessor • Privacy specialist *Note: the classification does not intend to suggest a hierarchy of importance or complexity of tasks, but it is intended to give an operative indication to the CB.* The following must be added to the full exam: • 10 multiple choice questions for each profile apart from the first one; • One written exam on one case study for each profile apart from the first one; • At least 15 minutes of oral exam for each profile apart from the first one. The candidate who is already certified for more than one profile and applies for certification for others, (apart from data protection managers) must do, at a subsequent session: • 20 multiple choice questions for each profile apart from the first one; • One written exam on one case study for each profile apart from the first one; • An oral exam lasting at least 20 minutes for each further profile. • The candidate who is already certified for at least one profile and applies for certification for data protection manager, at a subsequent session, must do: • 30 multiple choice questions for each profile apart from the first one; • One written exam on 2 case studies; • An oral exam lasting at least 30 minutes.
Annual surveillance (document review)	During the cycle of certification the CB must perform audits to keep and to confirm the validity of the certifications it has issued. The document review may be carried out in the absence of the candidate

	and it concerns the following documents: 1) at least one engagement/activity/contract showing the performance of activities in the area covered by the UNI standard; 2) demonstration by means of an attestation of qualifications/contracts/records/participations and similar/trainings/conventions/teaching activities/reports/normative or technical working groups undertaken during the year and aimed at the maintenance of competences for the certification held, for at least 16 hours per year for the DPO and 8 hours for the other profiles; 3) a "self-declaration" in compliance with articles 46 and 76 of Law D.P.R. 445/2000 containing: a) the activities performed as per point 1 with regard to points 4 & 5 of UNI 11697:2017, specific to the field of data protection, during the year; b) the complete list, as per point 2, of refresher course, conventions attended, seminars, reports, teaching activities related to the sector of privacy as set out in the summary profile charts; c) the existence of complaints related to the certified activity; d) the existence of ongoing legal disputes related to the certified activity; e) regular payment of the annual fees owed to the CB, where necessary. If there are any complaints or legal disputes regarding the CB, their handling must be assessed. A result of surveillance activity may be maintenance, suspension or withdrawal of certification following evaluation of the CB regarding competence, (lack of) consistency of the documents presented or complaints and legal disputes.
Renewal (document review), written and eventual oral exam	At the end of the certification cycle the CB shall perform audits for the renewal of validity of the certifications granted. Apart from gathering the necessary evidence for the surveillance activities, the CB shall ensure maintenance of competences as per point 5 of UNI 11697:2017. During the renewal a written test must be done consisting of multiple choice questions, structured like the certification exam (the criteria for passing the exam are also the same.) If the candidate fails this first test, s/he can repeat it at a coming session (as long as the certificate has not empire), repeating the written test of multiple questions but with the addition of the written exam on the case studies, structured as exams for certification (the criteria for passing the exam are also the same.) In cases of a negative result also in the second test it is necessary to do a complete test for initial certification (multiple choice questions, study cases and oral.)
Transfer of the certificate	The transfer of a certificate issued to a physical person may be completed at any time by presenting a request to the receiving CB, attaching the exiting certificate and undergoing the oral exam with the methods set out in the present certification scheme. The candidate must present to the new CB also the applicable documents for surveillance activities. The candidate must provide evidence of closure of any outstanding matters (economical and technical) opened by the previous CBs towards

	him or her. The certificate issued retains the expiry date of the previous one.
Exam centre	To use an exam centre which is external to the CB, perhaps situated at an association or professional association, could constitute a threat to the principle of impartiality (see also Accredia regulation RG-01-02) which the CB must manage adequately (risk analysis). The dates of the exams must be communicated to sufficiently in advance to the CB so that it can plan audits, also unannounced or mystery audits). Audits (including unannounced or mystery audits) at the exam centre must be accounted for in the contract agreement between the exam centre and the CB. it is the CB's task to specify, on the basis of the identified risk, the frequency and the modalities. The CB shall also have available (and shall make available to the accreditation body if requested) the statistics detailing the results of previous exams at the various centres in order to be able to evaluate any inaccuracies. The qualification of the examiner shall be managed by the CB. For remote or online exams see Accredia regulation RG-01-02.
Migration	CBs which have issued certifications (out of ACCREDIA accreditation either before or after the publication of UNI 11697), according to owner schemes, must perform a comparative analysis for each profile certified with respect to the corresponding UNI standard which states any discrepancies between the access requirements, the knowledge, competences and skills required, the modalities of performance used and the contents of the exams. This analysis must be submitted to ACCREDIA for evaluation together with the documents for accreditation to define any different and simplified certification process in conformity with the UNI standard for persons in possession of previous certifications.
Evaluation of the results of learning activities	Point 6 of UNI 11697 specifies many methods of evaluation with notes of clarification. Reference may be made to the individual profiles given in the following paragraph to understand which of these methods are applicable and mandatory.

N°	Methods of evaluation	Notes of clarification.
1	Evaluation of the CV	This must include the documents proving the activities and training stated by the candidate.
2	Written exam for the evaluation of knowledge	The written exam consists of a series of closed answer questions, each of which has at least 4 possible answers of which only one is right (multiple choice questions). The questions must cover basic aspects of skills and knowledge as defined in UNI 11697 for the specific profile. A maximum of 2 minutes can be given for each question. During the exam the candidate can consult UNI 11697 and the Regulation (EU) 2016/679 (and subsequent modifications).
3	Case studies written	The candidate undergoes a case study aimed at verifying the

	exam	attitude, skill, competences and knowledge of practical matters related to the professional profile concerning the certification. There are four possible answers to the case study of which only one is right (multiple choice questions). There is a time limit of 10 minutes for each case study.
4	Oral exam	Ths is necessary for an in-depth understanding of any uncertainties encountered in the written exams and/or a better understanding of the candidate's knowledge of all the areas of the standard UNI 11697, for the various professionals. During the oral exam there shall also be: • simulations of real operative situations (e.g.: case studies, practice activities, role-plays etc.), to evaluate, as well as the skills and competences, personal abilities: ability in interpersonal relations, expected behaviour); • analysis and evaluation of completed tasks. This method also includes a comparison, in the presence of the candidate, to better understand the skills evaluation, knowledge and ability in interpersonal relations.

Modalities for the exams

Below there is information regarding the the methods of evaluation, stating which methods are applicable and obligatory for the various profiles.

N°	Professional profiles	Method of evaluation
1	Personal data protection manager	• exam of the CV and requirements of the standard; • written exam consisting of at least 40 multiple choice questions; • written exam regarding at least 3 case studies; • oral exam lasing at least 40 minutes (including simulations of real operative situations lasting about 10 minutes and evaluation of completed tasks);
2	Privacy manager	• exam of the CV and requirements of the standard; • written exam consisting of at least 35 multiple choice questions; • written exam regarding at least 3 case studies; • oral exam lasing at least 40 minutes (including simulations of real operative situations lasting about 10 minutes and evaluation of completed tasks).
3	Privacy specialist	• exam of the CV and requirements of the standard; • written exam consisting of at least 35 multiple choice questions; • written exam regarding at least 2 case studies; • oral exam lasing at least 30 minutes (including simulations of real operative situations lasting about 10 minutes and evaluation of completed tasks).
4	Privacy evaluator	• exam of the CV and requirements of the standard; • written exam consisting of at least 35 multiple choice questions; • written exam regarding at least 2 case studies; • oral exam lasing at least 30 minutes (including simulations of real operative situations lasting about 10 minutes and evaluation of completed tasks).

2) Accreditation process

Various cases may occur on the basis of ACCREDIA accreditations already held by the CB making the application for accreditation or extension.

The requirements of ACCREDIA regulations RG-01 and RG-01-02 for the granting of accreditation or extension remain unchanged.

If the CB is already accredited by another accreditation body, it must perform a case-by-case evaluation on the basis of the applicable EA / IAF MLA agreements and in accordance with the requirements made by the competent authority (if necessary).

A	CB already accredited for the scheme ISO/IEC 17024	Document review of 1 day (to be performed, if possible, at the CB's premises). Observation of 1 exam session (the session chosen may also regard a number of the profiles covered by the UNI standard). Accreditation of each individual professional person according to the UNI standard is granted only following a direct observation of the person in question (it is not possible to obtain accreditation of a professional person who has not been observed at an exam. Flexible accreditation is not possible.
B	CB not yet accredited to ISO/IEC 17024, but accredited for other accreditation schemes	Apart from as stated in point A, an assessment of 2 days is carried out the the CB's head office.
C	CB not yet accredited in any scheme	Apart from as stated in point A, an assessment of 4 days is carried out the the CB's head office.

Documentation to present to ACCREDIA for the document review in cases of CBs applying for extension:

a) Procedures or internal instructions made available by the CB for the management of the object scheme of the present circular;
b) Applicable contractual procedures / regulations regarding this scheme;
c) Criteria of qualification for examiners and decision-makers;
d) CVs of the examiners and decision-makers and criteria where by the CB gave them these positions;
e) Fax of the certificate issued by the CB;
f) List of the certificates already issued for the various profiles and list of coming exams (necessary data for planning the observation of the exam);
g) For CBs WITHOUT ISO/IEC 17024 accreditation, apart from the above documents, it is necessary to send the documents requested in the application for accreditation.

If the CB is applying for initial accreditation, the documents to send are those stated in the applications DA-00 e DA-01.

3) Maintenance of accreditation

For the maintenance of accreditation throughout the period of accreditation, except in certain special situations such as the handling of complaints and remarks, modifications to the certification scheme, changes to the CB's staff structure, legal cases etc., the following assessments shall be performed:

- if the CB has issued up to 20 certificates in this certification scheme, all the profiles for which it is accredited, 1 exam of at least 1 profile must be observed and 1 on-site scheme-specific assessment must be conducted;

- if the CB has issued between 21 and 200 certificates in this certification scheme, taking into consideration all the profiles for which it is accredited. 2 exams of at least 2 profiles must be observed and 1 on-site scheme-specific assessment must be conducted;
- if the CB has issued over 200 certificates in this certification scheme, taking into consideration all the profiles for which it is accredited. 2 exams of at least 2 profiles must be observed and 2 on-site scheme-specific assessments must be conducted;

it is confirmed that every year ACCREDIA shall conduct an assessment at the CB's head office to assess conformity to with ISO/IEC 17024.

We are available for any clarifications.

Kind regards,

Emanuele Riva
Director of the Dept. of Certification and Inspection