Att.: To all Certification Bodies accredited to ISO/IEC 17021

Our ref.: DC2017SSV210 *Milan,* 24/07/2017

Subject: **ACCREDIA Department of Certification and Inspection - Circular N° 13/2017**
Informative communication regarding accreditation for the certification scheme ISO/IEC 27001:2013 with integration of the guideline standard ISO/IEC 27018:2014 - Information Technology, Security techniques, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Introduction

With the diffusion of cloud computing there is increasing concern about transparency, confidentiality and control of services delivered: clients are often unaware of how information archived in the cloud is protected, about the location and procedure if they want to change provider or if the provider ceases to operate.

In accordance with the standards in force, responsibility for nonobservance of standards regarding the protection of personal data lies with the owner of the treatment of data: a verifiable standard is therefore necessary for the providers of cloud services to demonstrate their capacity to ensure the continuity of activities and the security and protection of data, including personal data subject to the privacy standards.

With the stimulus provided by the European Commission, the national government authorities and the commissions for the protection of data, ISO and IEC developed a new standard ISO/IEC 27018 (Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors), published in 2014.

Normative context

ISO/IEC 27018 is the first standard aimed at helping to ensure respect for the principles and standards of privacy by the providers of pubic clouds which adopt it. The standard is specifically aimed at service providers of public clouds processing personal data (PII - Personally Identifiable Information) acting as Data (PII) Processors.
It sets out guidelines based on ISO/IEC 27002 taking into consideration the normative requirements for the protection of personal data which can be applied in the general context of risks to IT security of a provider of public cloud services. As they are guidelines, the standard ISO 27018 is therefore not a certifiable standard; nevertheless it is possible to integrate it with an existing ISO/IEC 27001 certificate, issued by a recognized certification body, in order to demonstrate the capacity of the provider to ensure the protection of personal data, based on the integration of the standard with the standard ISO/IEC 27001.

The standard is based on and reinforces the previous standards ISO/IEC 27001 and ISO/IEC 27002 regarding the management of information security and it establishes control objectives, rules and procedures to implement measures for the protection of personal data (PII) in conformity with the privacy principles of ISO/IEC 29100 for providers of cloud services.

Operative office and administration: Via Tonale, 26 | 20125 Milano - Italy | Tel. +39 02 2100961 | Fax +39 02 21009637
Registered office: Via Guglielmo Saliceto, 7/9 | 00161 Roma - Italy | Tel. +39 06 8440991 | Fax +39 06 8841199
milano@accredia.it | www.accredia.it | VAT: IT 10566361001

1) Standards and rules of certification

Accreditation standard	ISO 17021-1:2015, ISO/IEC 27006:2015
Certification standard	ISO/IEC 27018:2014, as addendum to the standard ISO/IEC 27001:2013
Competence criteria of the CB's audit team	The audit team shall possess the following competences, whether it is a single person or, collectively, as a team: • ISO/IEC 27001:2013 auditor, with specific experience in ISO/IEC 27001 audits of at least 5 years, preferably possessing a professional certification. • ISO 20000-1:2012 auditor, with specific experience in ISO/IEC 20000 audits of at least 5 years, preferably possessing a professional certification. Demonstrable knowledge of the standard ISO/IEC 27018:2014 is also required.
Competence criteria of the decision-taker	At least one decision-taking staff member of the CB shall be able to demonstrate: • Qualification as ISO/IEC 27001 auditor, issued in conformity with ISO/IEC 27006 • Knowledge of the standard ISO/IEC 27018:2014
Audit times	Only organizations already holding ISO/IEC 27001 certification may obtain extension to ISO/IEC 27018. To certify an organization against ISO/IEC 27018, a 30% audit time increase is necessary with respect to an audit conducted against ISO/IEC 27001. It is, however, possible to perform an audit against ISO 27001 at different times from the ISO/IEC 27018 audit. Before issuing certification it is necessary to verify all the datacenters where the servers managing the cloud are located. If the ISO/IEC 27001 certificate was issued by a different CB, the duration of the ISO/IEC 27018 audit shall be 50% of the ISO/IEC 27001 audit, and the CB shall have access to the ISO/IEC 27001 reports.
Certificate	It shall always make reference to the standard ISO/IEC 2700, mentioning also use of the guideline ISO/IEC 27018 in its application. It shall also indicate the products / services / applications and processes covered by the certification.
IAF and EA documents	All IAF and EA documents in force for the ISO/IEC 27001 scheme are applicable.

2) ACCREDIA accreditation process

There are various possibilities depending on the ACCREDIA accreditations already obtained by the CB making the application for accreditation or extension.

There is no change to the requirements of ACCREDIA Regulations RG-01 and RG-01-01 for granting accreditation and extension.
For CBs already holding ISO/IEC 27001 accreditation from ACCREDIA, it is not obligatory for them to have issued certificates in this scheme to apply for the extension of accreditation.

The accreditation certificate does not show sectors of accreditation.

If the CB already holds accreditations issued by other accreditation bodies, a case-by-case assessment shall be performed on the basis of the applicable EA / IAF MLA agreements.

A	CBs already accredited for the ISO/IEC 27001 scheme	Document review – duration of 1 day (to be performed preferably at the CB's head office). 1 witness assessment of a duration consistent with the client's organizational size. ACCREDIA reserves the right to assess, on a case-by-case basis, the appropriateness of the organizations chosen for the witnessing for the purpose of the accreditation process and also of the audit groups proposed for accreditation and for the subsequent surveillance activities.
B	CBs not possessing ISO/IEC 27001 accreditation	Accreditation against ISO/IEC 27001 is necessary.

Documentation to be presented to ACCREDIA for the document review:

- Checklist or guideline or instructions prepared and made available by the CB for the assessment team;
- CVs of the auditors and decision-takers;
- Module of the audit report;
- Declaration/certificate issued by the CB;
- List of certificates already issued and the upcoming audit activities (in case it is necessary to perform a witness assessment);
- Contractual procedures/regulations applicable to the audit process as well as internal procedures for the management of the certification files;
- For CBs which DO NOT possess ISO/IEC 17021 accreditation, as well as the above documents, it is necessary to send the documentation required in the application for accreditation.

3) Maintenance of accreditation

For the maintenance of accreditation, throughout the entire period of accreditation except in certain special situations (e.g. management of complaints and remarks, modifications carried out on the scheme of certification, changes to the CB's structure….) the following assessments shall be performed:

- On-site assessments:
  - 0,5 days every year for CBs accredited by ACCREDIA to ISO/IEC 27001
  - 1 day every year for CBs not accredited by ACCREDIA to ISO/IEC 27001

- Witness assessments to be performed during the period of accreditation:
  - If the CB has issued less than 50 certificates in the certification scheme, 1 witness assessment shall be performed every 4 years
  - If the CB has issued between 51 and 200 certificates in the certification scheme, 2 witness assessments shall be performed
  - If the CB has issued more than 201 certificates in the certification scheme, 3 witness assessments shall be performed

We are available for any clarifications.

Kind regards,

Emanuele Riva
Th Department Director