ARTICLE

Accreditation and certification in the light of the new Privacy Regulation. Certainties and expectations

Filippo Trifiletti – Accredia General Director

Modern society revolves around and evolves according to the collective value of data, a strategic resource not only for economic but also for cultural development, and for raising awareness. Today's IT and telecommunications play a fundamental role in human activities, and their pervasive reach creates priorities and criticalities which include the protection of personal information, processed and registered by many people using different instruments and multiple support systems. Often the user does not know how much personal data are archived, where they are archived and, especially, how to be protected from misuse of data. This has increased the need - particularly in the context of the global economy - for common standards for verifying the capacity of the suppliers of services for data management also to protect data, whilst maintaining the information flows which lie at the heart of the free market.

On the European level, on May 25, 2016, the EU Regulation for data protection and on the free movement of personal data N° 679/2016 (GDPR), came into force in all EU countries. The Regulation introduces clearer rules concerning privacy and consent and restrictions to the automatic processing of personal data. It encourages the creation of mechanisms for certifying data protection, seals and marks, with the aim of attesting the conformity of processing by controllers and processors (article 42). It specifies both the bodies which can legitimately and independently issue data protection certifications and the difference between them, with any autonomous, distinct and resulting possibility of granting certifications against the standard.

Certifications can be granted (article 43) by:

- Certification bodies which must be accredited by the competent supervisory body or by the national accreditation body, nominated in accordance with Regulation EU 765/2008 (in Italy Accredia), or by both. The reference standard for accreditation is ISO/IEC 17065:2012 which regulates the granting of product certifications.
- The supervisory body of the Member State – in Italy the guarantor for personal data protection.

The criteria for certification generically referred to in the GDPR are approved by the supervisory body or by the EU Committee for personal data protection as established by the Regulation.

The Member States shall ensure that the accreditation of certification bodies is entrusted to one or to both of the bodies referred to in the Regulation. The supervisory body has the exclusive task of accrediting, on the basis of the evaluation of the requirements of the Regulation, the bodies which verify the conformity of the controllers and data processors who adhere to the codes of conduct provided by associations or other bodies of their categories. Compliance with the codes of conduct or with a system of certification may be used as a factor for demonstrating fulfilment of the obligations of the data controller.

Under the Regulation the European Commission may perform actions for establishing technical standards regarding the mechanism of certification and the seals and marks for data protection as well as the modalities for promoting and recognizing them. It also states the EU policies with regard to the special needs of small and medium enterprises but it does not state which criteria should be adopted (price, simplification, diversification of certification schemes). It is therefore necessary to formulate unambiguous policies to ensure the uniformity of processing of data subjects seeking certification.

The provisions of the GDPR concerning accreditation and certification, however, leave some questions open. Issues related to the attribution of competences and responsibilities between the supervisory bodies and the accreditation bodies such as the actions which the supervisory body may undertake in terms of standardization, accreditation, certification and monitoring of the application of the controls which, if applied contemporarily, may result in incompatibilities which require attention. It is also unclear as to whether ISO/IEC 17065 should also be applied by the supervisory body in cases where the supervisory body grants certifications.

It also needs to be clarified as to whether conformity assessment schemes will be able to have different weight and fields of application. In accordance with Regulation 679/2016 the accreditation schemes drawn up on the basis of criteria approved by the EU Committee become valid at EU level. If EA (European co-operation for accreditation – the European accreditation infrastructure) does not evaluate regulated schemes, it becomes the task of the EU guarantor for data protection to harmonize such schemes amongst Member States. Moreover, the additional requirements of accreditation regarding ISO/IEC 17065 which, on the basis of the GDPR, the member state supervisory bodies may introduce, would not be covered by the EA MLA and IAF MRA agreements of mutual recognition, creating potential criticalities, especially for multinational companies.

It is also necessary to evaluate how it will be possible to reconcile the activities of the standardization bodies in these matters with those of the European Commission, and the various possibilities of validity of schemes based on owner schemes, technical standards or documents issued by the Commission. Clarification is also needed regarding the application of codes of conduct concerning the granting of a certification and its exemptions with regard to corporate responsibilities.

With respect to these matters, the personal data protection guarantor is collaborating at EU level with the competent authorities of other Member States to define a common framework of criteria for the accreditation of bodies and the granting of certifications on the market.

On March 30, 2018, the period of public consultation on the guidelines relating to article 43 of Regulation 679 was concluded, and the results are still being waited for. *The Article 29 Working Party* which worked on the guidelines, was set up on the basis of article 29 of the Directive 95/46, also operating as an independent consultation body consisting of one representative of the national authorities for personal data protection, the European guarantor for data protection and also a representative of the European Commission.

In Italy, Accredia, as the sole national accreditation body, supports the guarantor by offering all its experience in the accreditation of certification bodies so as to ensure the correct implementation of Regulation 679/2016 in Italy. The legislator has not yet established who shall have the responsibilities and competences for the accreditation of certification bodies in accordance with the Regulation. Regarding this, Accredia and the guarantor have clarified[1] that, until a decision is taken by the legislator, the certification of persons and certifications issued regarding privacy or data protection, can without doubt constitute a guarantee and an act of diligence towards the parties interested in implementing a voluntary system of analysis and control of the principles and reference standards, but they cannot be defined as being in conformity with articles 43 and 44 of Regulation 679/2016. This is due to the fact that the "additional requirements" for the accreditation of certification bodies and the specific criteria for certification have yet to be determined.

To date, Accredia has accredited the owner scheme against ISO/IEC 17065, managed by a body which issues ISDP©10003:2015 certifications of processes for the protection of natural persons regarding the processing of personal data – Regulation EU 679/2016. This scheme may be revised if any additional criteria to articles 42 and 43 of the regulation are introduced by the competent national authority.

A personal data protection certification which is already active also conforms with ISO/IEC 27001 regarding management systems for information security, integrated with the guideline ISO/IEC 27018[2]. It is aimed at public cloud service providers processing personal data (PII - Personally Identifiable Information) which operate as data processors. The implementation of the guidelines contributes towards ensuring respect for the principles and standards of privacy by the public cloud service providers who use it. It is a management system certification which is accredited in compliance with ISO/IEC 17021-1, and not in compliance with ISO/IEC 17065, indicated as a reference by the GDPR.

Publication is currently underway of the new UNI publicly available specification (PdR) "Guidelines for the management of ICT personal data in accordance with Regulation EU 679/2016 (GDPR)", drawn up by the working table "Digital privacy management process requirements" led by UNI with the participation of Accredia and other stakeholders. It consists of two parts: one support part to the definition and implementation of the processing of personal data, and the other part containing the conformity requirements. The document is intended for organizations which process data using IT instruments, with particular attention to the small and medium enterprises which may use a standardized guidance, in line with the GDPR.

[1] see ACCREDIA DC Circular N° 30/2017 "Informative circular regarding product accreditation (ISO/IEC 17065) of certifications issued in conformity with the ISDP scheme 10003:2015 - Reg. EU 679/2016" in www.accredia.it/documenti.

[2] see ACCREDIA DC Circular N° 13/2017 "Informative circular regarding accreditation for the certification scheme ISO/IEC 27001:2013 with integration of the guideline ISO/IEC 27018:2014" in www.accredia.it/documenti.

The correct implementation of effective data processing with IT modalities can become a competitive tool for organizations intending to demonstrate their conformity (as well as being a yardstick for judgment by the competent authorities) with the added value of certification by independent third parties, according to the requirements of ISO/IEC 17065.

Concerning the definition of staff competences the Regulation 679/2016 finds an effective complementary element in the standard UNI 11697:2017 (published in November, 2017) "Unregulated professional activities – professional profiles relating to personal data processing and protection - requirements of knowledge, ability and competence". The Regulation provides for the presence of a data protection officer (DPO) in all public enterprises in which data processing presents risks and in enterprises which process sensitive data. The competence of the DPO can be certified under accreditation voluntarily, on the basis of the requirements of the standard UNI 11697, in accordance with the specifications set by Accredia in the relative circular[3].

Accredia has involved the interested parties (including UNINFO and the guarantor) in the definition of common rules and criteria for all certification bodies and it is hoped that the standard will be promoted at EU level (CEN) for professional data protection officers, privacy managers, privacy verifiers and privacy specialists.

Italy is one of the EU's leading countries in the protection of privacy and Accredia continues to give all possible technical support to the guarantor and to the standardization body, offering its know-how in accreditation. Accreditation means guaranteeing reliability for institutions, enterprises and consumers, and accredited certifications ensure the conformity of systems, processes, products, services and persons with the requirements of the national and international standards. Accredia is signatory to the European EA MLA and worldwide IAF MRA agreements of mutual recognition for the global recognition of certifications. There are, therefore, all the necessary provisions in place for protecting citizens and their fundamental rights to security and the protection of personal information.

[3] See ACCREDIA DC Circular N° 3/2018 "Requirements for certification and accreditation in conformity with the standard UNI 11697:2017 – Professional profiles relating to the processing and protection of personal data" in the website www.accredia.it/documenti.

Accredia *is the sole national accreditation body nominated by the Italian government. Its task is to attest the competence, impartiality and independence of laboratories and bodies which verify the conformity of products, services and professional persons with the reference standards, facilitating free movement of goods and ensuring the protection of public interests concerning health, safety and the environment.*

Accredia is a private non=profit association operating in the public interest and under the aegis of the Ministry of Economic Development, for guaranteeing institutions, business and consumer protection.

Accredia has 67 members and it represents all the parties involved in accreditation and certification activities, including 9 ministries (Economic Development, Environment, Health, Defence, Infrastructures and Transport, Internal affairs, Labour and Agriculture), 7 major public entities and 2 national standardization bodies – UNI and CEI, and also: 13 business and trade organizations, associations of accredited certification and inspection bodies, testing and calibration laboratories, associations of consultants and consumers and public utility suppliers such as the national rail network and the national power network.

Accredia is a member of the EU and international accreditation networks and signatory to the international agreements of mutual recognition under which the tests and certifications of bodies and laboratories accredited by Accredia are recognized in Europe and worldwide.