

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htmComputer Law
&
Security Review

Why the certification process defined in the General Data Protection Regulation cannot be successful

Eric Lachaud *

TILT, the Tilburg Institute for Law, Technology, and Society, Tilburg University, The Netherlands

ABSTRACT

Keywords:

Data protection certification
Privacy certification
Data protection seal
Privacy seal
Co-regulation
Self-regulation

This paper analyses the final version of Articles 42 and 43 dedicated to the certification procedures in the General Data Protection Regulation (hereinafter GDPR). It questions the introduction of this procedure in the data protection regulation framework and argues that the purposes assigned to the certification in the GDPR meet the needs of the different contributors to the preliminary discussions to the reform. It also argues that the processes defined in Articles 42 and 43 to issue the certification diverge from the commonly accepted practices in this activity and the processes suggested in the new regulation impede its chance to be successfully implemented.

©2016 Eric Lachaud. Published by Elsevier Ltd. All rights reserved.

1. Introduction

The endorsement of the certification has been enacted with the GDPR¹ and two articles² are now included in the EU regulation framework organizing this procedure. The certification has been recognized in the legal framework of certain

Member States³ and a few schemes (Table 1)⁴ already offer to assess the conformity with the national data protection laws. The oldest one, established fifteen years ago in the German *länder* of Schleswig-Holstein certified the compliance of 200 public bodies with the local data protection law. However, this endorsement represents a noticeable innovation to the extent that this is the first time a complete

* TILT, the Tilburg Institute for Law, Technology, and Society, Tilburg University, P.O. Box 90153, 5000 LE Tilburg, The Netherlands.
E-mail address: eric.lachaud@outlook.com.

¹ See the Joint Statement on the final adoption of the new EU rules for personal data protection of the 14 April 2016. See also European Parliament Press release. Data protection reform – Parliament approves new rules fit for the digital era- Press release – Police cooperation / Citizens' rights / Justice and home affairs – 14-04-2016 - 12:11.

² Article 42 and Article 43.

³ Uzategui Angulo, A. C. (2006). Las marcas de certificacion. Tesis de doctora en derecho – Area des relaciones internacionales – Universidad Federal de Santa Catarina – Brasil.

⁴ See Table 1.

<http://dx.doi.org/10.1016/j.clsr.2016.07.001>

0267-3649/©2016 Eric Lachaud. Published by Elsevier Ltd. All rights reserved.

certification ecosystem⁵ is included into the European law. The scientific literature suggests two approaches to define the certification. Some⁶ envisage it as a conformity assessment process. They argue that the certification is essentially a voluntary assessment process realized by an external and accredited auditor⁷ on the basis of requirements issued by some recognized authority. The assessment, if successful,

⁵ So far, the European regulation used certification processes without ever endorsing them. Only the codes of conduct have been endorsed in Directive 95/46 EC under Recital 26, Recital 61 and Article 27. The CE marking process uses certification procedures to demonstrate the compliance with the harmonized standards. More than 95% of the CE marking are issued following a process of self-assessment called self-declaration of conformity (SDoC). The CE marking promoted an original co-regulation arrangement between the stakeholders involved in this process. The lawmaker, the standardization bodies, the manufacturers and the private certification bodies must collaborate but remain responsible for their part of the process. The lawmaker issues high-level requirements in annexes of the new approach Directives, while the standardization bodies supplement them with technical requirements. Depending on the risk level defined in the Directive, the manufacturer or the third party certification body audits and attests the conformity with the technical standards. Finally the national authorities are entitled to monitor the compliance of the products on their local market. For more details on the CE marking process, see European Commission, "The Blue Guide on the Implementation of EU Product Rules", 2014. See also Barron, M. Creating Consumer Confidence or Confusion? The Role of Product Certification in the Market Today, 2007. Marquette Intellectual Properties Maw review Volume 11 Issue 2, 422. The geographical identifications have been set up in the European countries during the 1930s and 1940s to guarantee the characteristics and the taste of agricultural products according to their geographical origin and a combination of local and natural conditions and production expertise. A European equivalent of this national identification has been created at the initiative of Belgium, France and Luxembourg in 1992 for agricultural except the wine and spirits. The Protected Denomination of Origin (PDO), the Protected Geographical Indication (PGI) and Traditional Speciality Guaranteed (TSG) have been extended to the other countries of the European Union by the European Council Regulation No. 510/2006. Only groups or associations of food producers are allowed to apply for registration to a PDO or a PGI. They are issued without time limitation after an examination by the competent national authorities. See geographical indications and traditional specialties on the website of the European Commission. Accessed 10/04/2016 http://ec.europa.eu/agriculture/quality/schemes/index_en.htm.

⁶ "Certification is a method of (conformity) assessment" Eijlander, P., Evers, G., De Moor, A. J. and Peters, H. (2003). De inkadering van certificatie en accreditatie in beleid en wetgeving [The framing of certification and accreditation policies and legislation]. A study commissioned by the Ministry of Economic Affairs. Instituut, Centrum voor Wetgevingsvraagstukken, Universiteit van Tilburg, 2003 - 194 pp, 12.

⁷ "Certification is the (voluntary) assessment and approval by an (accredited) party on an (accredited) standard" Meuwissen, M. (2003) Technical and economic considerations about traceability and certification in livestock production chains, In Jahn, G. et al. (2005) The reliability of certification: quality labels as a consumer policy tool, *Journal of Consumer Policy*, 28, 57.

Table 1 – Data protection certification schemes active in Europe in 2016.

#	Scheme name	Origin	Number of certification issued (in 2013)
2	Data privacy and security certification	The Netherlands	1
3	Data protection audit certificate	Hungary	7
4	E-privacy seal	Germany	12
5	EuroCloud Star Audit Software as a Service	Germany	20
6	European Privacy Seal – EuroPriSe	Germany	25
7	Fair Data	UK	17
8	Good Priv@cy	Switzerland	50
9	Gütesiegel Datenschutz Mecklenburg-Vorpommern	Germany	0
10	Label CNIL Coffre-fort numérique, formations informatique et libertés, gouvernance informatique et libertés, Procédures d'audit	France	44
14	OBA certification	Germany	0
15	OCPD – Federal ordinance on privacy certification (SR 235.13)	Switzerland	20
16	Privacy Seal – Gütesiegel	Germany	200
17	SCHUFA PrivacySeal	Germany	7
18	SQS – OCPD (based on Swiss Regulation 235.13)	Switzerland	15
19	Trusted Ads	UK	0
20	Trusted Site Privacy	Germany	20
21	E-privacy App	Germany	0

leads to the issuance of a formal attestation of conformity⁸. A second approach⁹ mainly defines the certification as an attestation of conformity. Its issuance is conditioned by the achievement and maintenance of the conformity with the requirement that it is periodically challenged. From a legal

⁸ 'Certification schemes . . . provide assurance (through a certification mechanism) that certain characteristics or attributes of the product or its production method or system, laid down in specifications, have been observed' EU best practice guidelines for voluntary certification schemes for agricultural products and food-stuff (2010/C 341/04).

⁹ "Third party attestation related to products, processes, systems or persons" in ISO/IEC 17000:2004 - Conformity assessment – Vocabulary and general principles– subclause 5.5 "A process by which a third party give a written assurance that a product, a process or a service is conform to the specified requirements" in ISO/EN 45020:2007 – Standardization and Related Activities – General Vocabulary "Certification includes all activities under which an independent, expert and reliable institution adopts and writing that there is a justified confidence that a clearly defined object (product, process, system or the competence of a person) meets predetermined requirements" Dutch Ministry of Industry (2003) Kabinetsstandpunt over het gebruik van certificatie en accreditatie in het kader van overheidsbeleid'.

Download English Version:

<https://daneshyari.com/en/article/4957922>

Download Persian Version:

<https://daneshyari.com/article/4957922>

[Daneshyari.com](https://daneshyari.com)