ARTICLE

CERTIFICATION WITHIN THE MEANING OF THE GDPR – EASILY ACCESSIBLE DOES NOT MEAN FREE OF CHARGE!

| 16/12/20 | Florence Chafiol Alice Hourquebie

This analysis was commissioned by Microsoft.

Article 43 (6) of the General Data Protection Regulation (hereinafter the "GDPR") provides that the accreditation requirements and the certification criteria must be "*made public by the supervisory authority in an easily accessible form*".

But what does the notion of "easily accessible" mean: does it imply that the certification criteria approved by the competent supervisory authority or by the European Data Protection Board ("EDPB") must be made public free of charge?

European players, and the EDPB in particular, are in favor of and encourage the publication of certification and accreditation criteria, while at the same time acknowledging and respecting the copyright protecting such standards. In a study commissioned by the European Commission, the authors of the report encourage the publication in full of the certification criteria in view of the transparency requirements, while recalling the existence of a proprietary right.

For its part, the French approach consists in recognizing the existence of copyright protection over standards presenting an original nature on the basis of which the copyright holder has the right to make these standards available to the public in return for financial consideration, i.e. payment of a fee. However, an "exception"·to the copyright monopoly applies when a standard is of mandatory application, based on the constitutional principle that laws must be accessible.

In the opinion of the authors of this article, insofar a certification, pursuant to Articles 42 and 43 of the GDPR, is not mandatory, there is no requirement to make standards (or certification criteria), which are the result of the efforts made by private players and copyright-protected works, available in their entirety free of charge.

1. French law relating to the publication of standards

1.1. The protection of standards under copyright and the "exception" to this rule

As recently recalled by the courts: a standard, provided it meets the originality requirement, is eligible for copyright protection. It is effectively possible to recognize a copyright protecting a technical standard if it meets the originality requirement which is the corollary for protection of a work. As held by the Court of Appeal of Orléans in a case involving a set of forms:[1] *"it is not necessary for a work to have a particular level of originality in order for it to be protected by copyright".*

This principle is reiterated in the Senate information report on standardization:

> ● "*Standard-setting bodies – whether at the national, European or international level, effectively benefit from an intellectual property right, which can be equated with copyright, in respect of the standards they develop and which entitle them to control their dissemination.*"[2]

1.2. Impact of the voluntary nature of the standard on access thereto and the copyright "exception"

Based on administrative case law, there is however an exception to the monopoly held by the copyright holder stemming from the mandatory nature of compliance with a standard. Accordingly, Article 17 of the decree dated June 16th, 2009 provides that:

> ● "*Standards are of voluntary application. However, standards may be made mandatory by order signed by the Minister in charge of industry and by the interested minister or ministers.* ***Standards that are made mandatory can be viewed free of charge on the website of the French national standards body [AFNOR]***."

In a first landmark ruling, the French Council of State[3] considered that the provisions of Article 17 requiring mandatory standards to be viewable free of charge implemented a superior principle, in this case the objective, which has constitutional value, of accessibility to the law.

In that case, based on its finding that the standards at issue had not been the subject of any publicity measure and that the only way to access them was to purchase them from AFNOR, the Council of State held that the order imposing compliance with these standards could not make a standard mandatory when free and open access to it was not guaranteed.[4]

A year later, in a second ruling,[5] the Council of State confirmed the existence of an exception to the monopoly by affirming that the fact that a standard is copyright-protected should not prevent it being made freely available at no charge since it is of compulsory application.

French case law is therefore cut and dry: a mandatory standard must be made available freely and without charge. Conversely, a voluntary standard effectively benefits from copyright protection and is not intended to be made available without charge.

Legal theory is also clear about the fact that standards are provided for financial consideration:

> ● "*Also, access to the private national technical standard is only possible in consideration of payment of a fee. This barrier can only be removed by ministerial approval, in the name of respecting the constitutional objective of that the law must be accessible.*"[6]

It should be borne in mind here that certification und the GDPR is voluntary. Article 42 (3) of the GDPR effectively provides that:

- *"The certification shall be voluntary and available via a process that is transparent."*

2. The interpretation of the notion of "easily accessible" by european player

As regards certification, Article 43(6) of the GDPR provides that *"The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means."*

The GDPR also makes several references to the notion of "easily accessible", such as when it clarifies the notion of transparent processing, which requires that "*any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used*"[7]

The EDPB has made known its position many times regarding the establishment of a certification mechanism under the GDPR, encouraging the greatest possible transparency, but without challenging the copyright protection of standards.

2.1. The position of the European Data Protection Board

The European Data Protection Board has published many guidelines on certification and in particular guidelines on the accreditation of certification bodies under Article 43 of the GDPR[8] tackling the publication issue under Article 43(6).

The EDPB rephrases the language used by GDPR, specifying in particular that:

- *"Therefore, to ensure transparency, all criteria and requirements approved by a supervisory authority shall be published. In terms of quality and trust in the certification bodies, **it would be desirable, if all the requirements for accreditation were readily available to the public**."*

Without further clarification of the concept of "publication", the EDPB simply uses the term again when specifying the general requirements for accreditation and states, in particular, that:

- "*The accreditation body shall in addition to the requirement in 4.6 ISO/IEC 17065/2012 require from the certification body that at minimum:*
  ***1. all versions (current and previous) of the approved criteria used within the meaning of Article 42(5) are published and easily publicly available**, as well as all certification procedures, generally stating the respective period of validity; […]*";

While the EDPB did not take this opportunity to provide a practical definition of "easily available", it did at least specify that the certification criteria must made published. As the notion of publication is itself not specified, this could pertain as much to a free publication as to a paid publication.

However, in EDPB Opinion 4/2020 on the draft decision of the competent supervisory authority of the United Kingdom, regarding the approval of the requirements for accreditation of a certification body, the EDPB notes that ISO 17065 will be used as "certification criteria", together with the additional requirements set up by the UK supervisory authority.

In this respect, the EDPB noted that **ISO standards are subject to intellectual property rights**, and that this was the reason why it would not make reference to the text of the related standard in its opinion.[9]

2.2. The interpretation of articles 42 and 43 of the GDPR in a study commissioned by the european commission

The European Commission commissioned a study on Articles 42 and 43 of the GDPR; the final report having been published in February 2019.[10]

While the notion of "easily accessible" is not explicitly defined, references to the transparency criteria recur throughout the report. In point of fact, the report's authors, while refraining from saying that the publication of the certification criteria is mandatory, insist on the fact that it is necessary and encourage the European Commission in this direction.

They also propose a certain number of options to encourage the development of certification at all of the successive stages, from the drafting of certification criteria to the certification of the certification body itself.

They do, however, point out in their report - following an analysis of existing certifications - that most of these certification criteria are not always available. While the report advocates for the certification criteria to be published in their entirety to ensure transparency and maintain trust in the certification mechanisms, they acknowledge that there are proprietary rights over the assessment methodologies[11] and consider that one solution could be the publication and unhindered access to the "main rationale" of the relevant assessment methodology.[12] The authors also give the example of a summary as an alternative option.[13]

It would seem here that the recommendation made by the authors of the report to the European Commission is for the certification mechanism to be published only in part: understood here as meaning the main rationale of the assessment method, but without any further clarification regarding its nature or its content.

This being the case, it is reasonable to surmise that publication of the certification criteria as such, on a free-of-charge basis, is in no way mandatory at present.

In this respect, the report cites the example of an existing certification called "Ryerson Privacy by Design", which publishes an extensive list of control points,[14] which auditors use to assess the certification requirements.

In conclusion, and by way of possible recommendations, the report explains that one of the options to be considered would be for the Commission to publish a policy or guidance for the EDPB, providing a template for publication of the criteria and assessment methodology or else a summary thereof.

It is interesting to note that the authors of the report develop their line of reasoning by clearly excluding the certification criteria from the publication of the certification mechanisms by the EDPB in the register provided by Article 42(8).[15]

The report establishes the state of play of European legislation as it pertains to the issue of the publication of certification criteria: in a nutshell, there is no requirement to publish these criteria, and a proprietary right exists with respect to such criteria. The recommendation made by the report to require the free publication of such criteria is just that, a simple recommendation.

Written by Florence Chafiol, Alice Hourquebie and Ariane Seyed-Movaghar

[1] Commercial Court of Orléans, commercial division, ruling of June 15th, 2006, No. 05/02452.

[2] Information report by Mrs. Élisabeth Lamure, Senator for the Rhône – Report No. 627 (2016-2017) *Où va la normalisation ? - En quête d'une stratégie de compétitivité respectueuse de l'intérêt general* (Where is standardization headed? - In search of a competitiveness strategy that respects the general interest).

[3] The *Conseil d'Etat* serves as legal advisor to the executive branch and as the supreme court for administrative justice.

[4] Council of State, February 10th, 2016, No. 383756, Fédération nationale des mines et de l'énergie.

[5] Council of State, 6th division, July 28th, 2017, No. 402752.

[6] *Du standard international à la norme technique nationale : l'exemple du Codex Alimentarius* (From an international standard to a national technical standard: example of the Food Code)– RFDA 2019 p. 985.

[7] GDPR, recital 39.

[8] "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" – Last updated on June 4th, 2019.

[9] Opinion 4/2020 on the draft decision of the competent supervisory authority of the United Kingdom regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43(3) GDPR.

[10] "Data Protection Certification Mechanisms Study on Articles 42 and 43 of the Regulation (EU) 2016/679 Final report" – February 2019

[11] "*While we hold that the certification criteria should in their entirety be published to ensure transparency and safeguard the reliability of the certification, seal, and mark, it is true that there are proprietary rights over assessment methodologies which feed concerns over sharing publicly the methodologies.*"

[12] "*Another solution would be publication and unhindered access to the main rationale of the assessment methodology.*"

[13] *"Other certifications use other methodologies such as Protection Goals or Control Goals, which they summarise on their websites.*"

[14] See, in particular: https://www.ryerson.ca/content/dam/pbdce/certification/PbD-Brochure.pdf.

[15] "*In addition, if a data protection certification mechanism is interpreted to include the assessment methodology, apart from the certification criteria and other organisational or procedural issues, then such methodology should be included in the register of the EDPB (Art. 42(8) GDPR).*"