Feedback of CEN-CENELEC JTC13/WG5 Consultation Task Force on EDPB Guidelines 01/2022 on certification as a tool for transfers, Version 1.0

30.09.2022

Introduction

CEN and CENELEC are two of the three European Standardization Organizations (ESOs), whose main common objective is to remove trade barriers for European industry and consumers. The joint mission of CEN and CENELEC is to provide European Standards to foster the European economy in global trading, the welfare of European citizens and the environment, supporting European Union legislation, when needed.

CEN/CLC JTC13 is a joint technical committee the scope of which is to develop standards about Cybersecurity and Data protection to address at best the European needs, including in support of the European regulations. WG5 is the competent Working Group for "Data Protection, Privacy and Identity Management".

Standards are essential tools to help market stakeholders in their practical implementation in the domains of cybersecurity and data protection and for supporting the demonstration of compliance to the EU regulatory obligations, including the ones established by the Regulation 2016/679 (GDPR).

In this framework, the "CEN/CLC/JTC13/WG5 Consultation Task Force" (hereinafter ''the Consultation Task Force'') – is submitting the following document as a contribution to the public consultation on the EDPB "Guidelines 04/2022 on the calculation of administrative fines under the GDPR".

The presence and work of the Consultation Task Force aligns with CEN/CLC JTC 13's strategic business plan and the defined objectives therein, which include JTC 13 being identified as a strategic partner for institutions, agencies and bodies within the EU system being involved in Cybersecurity and Privacy policy and law making, and a strategic partner of EU Member States' national administrations and bodies/entities involved in the Cybersecurity & Privacy policy and law making.

The scope of the Consultation Task Force is to participate in public and private consultations for data protection, privacy and identity management issues initiated, amongst others, by institutions, agencies, and bodies within the EU system, being involved in the Cybersecurity & Privacy policy and law making or initiated by national bodies and entities such as Member States' national supervisory authorities.

For any clarification or questions regarding this feedback, please address this by sending an email to the email addresses:

Maria Raphael - Consultations Group Coordinator: maria@privacyminders.com
Alessandro Guarino - WG5 Convener: a.guarino@stagcyber.eu
Martin Ulherr - JTC13 Secretariat: martin.uhlherr@din.de

Guidelines 07/2022 on Certification as a tool for transfers, Version 1.0		
1. **GENERAL**		
1	1.1	We would suggest identifying better the intended audience of the guidelines, possibly in a short independent paragraph or by reference to section 1.3, where needed. For the avoidance of any doubt, it could be clarified that the primary audience of the Guidelines are the certification scheme owners, the supervisory authorities and the European Data Protection Board and that the secondary audience include the data importers that may be certified under a GDPR Certification mechanism as per art. 46(2)f, the data exporters that may wish to use this mechanism as a tool for transfer, National Accreditation Bodies (NABs) and Certification Bodies, explaining why the guidelines are of their interest.
2.	1.3. Actors involved	The European Standardisation Organisations (ESOs) are separate actors and can be mentioned as such in section 1.3. They can support the development of GDPR Certification Criteria or develop such criteria, as scheme owners. The EU Commission is empowered to promote technical standards, that are considered relevant to GDPR Certification and are delivered by ESOs, as a result of a standardization request or the ESOs' own initiative, as harmonised standards and reference them into an adopted implementing act as per art. 43(9) of the GPDR. The Article 43(9) of the GDPR provides that: *"The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks".* The European Commission with its final report ‘’Data Protection Certification Mechanisms, Study on Articles 42 and 43 of the Regulation (EU) 2016/679’’ had recommended that "*priority will be given to ensuring development of a body of standards that can be an adequate basis for drafting certification criteria under the GDPR. This preferably in the form of European standards, and potentially with the procedure of standardisation requests issued by the European Commission to the ESOs, based on Art. 10 of the Standardisation Regulation"* (par.7.4.1.3, p.167)". The CEN/CLC/JTC13/WG5, in order to provide support to GDPR Certification Schemes under development and/or the development of GDPR Certification Schemes is currently undertaking the following projects: a) JT013037 Privacy Information Management System per EN/ISO/IEC 27701 – refinements in a European context” . b) JT013033 (prEN 17799), a standard on “Personal data Protection requirements for processing operations” focusing on providing a basis for certifying processes and services.

Guidelines 07/2022 on Certification as a tool for transfers, Version 1.0		
	1. **GENERAL**	
3	1.4	Further explanation is required as to the specific reasons that the Certification body must be located in the EEA, considering that art. 58(2) applies to the SAs and not to the certification bodies. .
4	1.5 par.20	**1.** The EDPB requires from the data exporter to make reference to the use of certification as tool for transfers, in the data processing contract pursuant to article 28 of the GDPR or the data sharing contract together with binding and enforceable commitments with the data importer in case of transfers controller to controller. We take the occasion of this paragraph to invite EDPB to clarify whether both Certification and Standard Contractual Clauses (SCCs) can be used as transfer tools for the same international data transfer. In this case, we have the view that reference to the use of Certification as tool for transfers may be sufficient to be included in the Standard Contractual Clauses of art. 46(2)c GDPR and that this should be brought into the attention of the reader. Where both transfer tools are used, the SCCs can also be used in order to satisfy the requirement that the importer shall provide binding and enforceable commitments. Even if the EDPB is of the opinion that the SCCs and Certification cannot be used simultaneously as tools for transfers, it could be clarified, nevertheless, that a data processing agreement between the data exporter and importer can be inspired/guided by the contents of the Commission approved SCCs, for the purpose of binding and enforceable commitments to be provided by the importer. **2.** A requirement is imposed on the exporter to check whether there is a contract or another legally binding instrument between the certified data importer and the certification body, i.e., the certification agreement. We consider that the existence of the certification itself demonstrates the existence a legally binding instrument between the certified data importer and the certification body.

3. SPECIFIC CERTIFICATION CRITERIA		
5	3.1 par. 41	The requirement in a) should clarify to whom the information on the processing activities should be provided.
6	3.2 par. 43(1) b and e	It is recommended that the certification criteria require from the importer that the documentation assessing the legal situation and practices of the third country -par. 43(1)b- and the documentation of the organisation and technical measures implemented -par. 43(1)e are also available to the data exporters, upon request.
7	3.2 par. 43(1)d	For consistency with par. 43(1)c, we would suggest to add the word ''identified'': *"Do the criteria require the importer to have* ***identified*** *and implemented the organisational and technical measures to provide the appropriate safeguards under Article 46 GDPR... ''*
8	3.2. par.43(1) a, c, d	Please check the choice of words ''objective'' and ''scope of certification''.
9	3.2. par.43(2)b	We are of the opinion that the contractual agreements or instruments between importers and exporters must always be a certification criterion.
10	3.2 par.43(4) c	This does not appear to be a criteria: the right to lodge a complaint with the competent supervisory authority is a legal right conferred on the data subjects. There is no involvement from the importer's part.

4. BINDING AND ENFORCEABLE COMMITMENTS TO BE IMPLEMENTED		
11	par. 45-50	Where Standard Contractual Clauses (SCCs) are used as an additional transfer tool (assuming that this is allowed) or where the Certification is used on its own, we are of the opinion that the content of the Standard Contractual Clauses (SCCs) issued by the European Commission should be considered adequate with regards to the commitments that the importer takes for applying the appropriate safeguards provided by the certification mechanism.
12	par.53	**1.**It is stated in the second sub-paragraph that the exporter holding a certification shall accept the decision of the data subject to do so (i.e., to bring a claim against the importer, for the violation of rules under the certification by a data importer, holding a certification outside the EEA, by invoking third-party beneficiary rights before an EEA SA and EEA Court). We consider, the reference to the ‘’exporter’’ to be a clerical error, as it is clear that it is the ‘’importer’’ holding a certification that shall accept this. **2.**The final sub-paragraph requires the contract or other instrument to oblige the importer to notify the exporter and the supervisory authority of the data exporter of any measures taken by the certification body in response to a detected violation of the certification by the same data importer. However, the obligation to inform the supervisory authority lies only with the data controllers. It is suggested to be rephrased as follows: *‘’The existence of an obligation of the data importer, holding a certification, to notify the exporter and, where it acts as a data controller, the supervisory authority of the data exporter, of any measures taken by the certification body in response to a detected violation of the certification by the same data importer’’.*

Yours Sincerely,

Maria Raphael

Co-ordinator of the CEN/CLC/JTC13/WG5 Consultation Task Force

ABOUT CEN AND CENELEC

CEN (European Commitee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization) are recognised by the European Union (EU) and the European Free Trade Association (EFTA) as European Standardization Organizations responsible for developing standards at European level, as per European Regulation 1025/2012. The members are the National Standards Bodies (CEN) and National Electrotechnical Committees (CENELEC) from 34 European countries. European Standards (ENs) and other standardization deliverables are adopted by CEN and CENELEC, are accepted and recognized in all of these countries. These standards contribute to enhancing safety, improving quality, facilitating cross-border trade and strengthening of the European Single Market. They are developed through a process of colaboration among experts nominated by business and industry, research institutions, consumer and environemental organizations, trade unions and other societal stakeholders. CEN and CENELEC work to promote the international alignment of standards in the framework of technical cooperation agreements with ISO (International Organization for Standardization) and the IEC (International Electrotechnical Comission).