

Douwe Korff

*Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford*
douwe@korff.co.uk

6 April 2018

Article 29 Working Party

Via e-mail: JUST-ARTICLE29WP-SEC@ec.europa.eu

To: Ms Jelinek, Chair
Members of the WP29

Cc.: European Data Protection Supervisor, Dr Giovanni Buttarelli

Re: Comments on the Draft Guidelines on the Accreditation of Certification Bodies (WP261)

On 6 February 2018, the Article 29 Working Party (WP29) adopted Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679 (WP261) (“the draft guidelines”). On 16 February, it issued a call asking for comments on these draft guidelines. This letter is a response to that call (with apologies for it being submitted late).

I submit this letter in my own name. I would have liked to consult with, and act with, my fellow data protection advocates in European civil society – but that takes more time than your consultation allows. Still, without claiming to be speaking on anyone else’s behalf, I believe that the views I express in this letter will be widely shared by civil society groups and activists; and I would encourage the WP29 to reach out to them beyond the formal short consultation, on the wider issues relating to certification, noted below.

In particular, I note that the draft guidelines deal only with the legal and technical aspects of accreditation and were issued without the annex that is to actually address the main issues in that regard. In my view, these are major defects and, rather than limiting my comments to this partial document and those limited aspects, this letter therefore focusses on the wider issue of the role of certifications in the new GDPR scheme and the risk of weak certifications, issued not by data protection authorities or even by certification bodies accredited by DPAS, but by certification bodies accredited by accreditation bodies that are not qualified in fundamental rights matters. In this, I draw on earlier articles I wrote on the subject.¹

NOTE:

¹ See:

- Privacy seals in the new EU General Data Protection Regulation: Threat or Facilitator?, in: *Rote Linien zur EU-DSGVO*, in: *Datenschutznachrichten (DANA)*, 3/2015 (August 2015), available here: https://www.datenschutzverein.de/wp-content/uploads/2015/08/DANA_3-2015_RoteLinien_Web.pdf (scroll to p. 128)
- Privacy seals in the new EU General Data Protection Regulation: Threat or facilitator? Part 2: What has it turned out to be?, in: *Datenschutznachrichten (DANA)*, 2/2016 (July 2016), available here: https://www.datenschutzverein.de/wp-content/uploads/2016/07/DANA_2-2016_RoteLinienRevisited_Web.pdf (scroll to p. 77)

Note also the Declaration of interest at the end of this letter.

Douwe Korff

*Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford*

The importance of certification under the GDPR

Much more than under the 1995 Data Protection Directive, the GDPR aims to place the onus of compliance on controllers and processors. Under the accountability principle (Art. 5(2)), reflected in numerous other articles, they will have to **demonstrate** that they comply with the regulation. This “duty to demonstrate compliance” applies both to general matters such as security (Art. 24(1)), privacy by design and -default (Art. 25) and the crucial duty to keep a register of all data processing operations (Art. 30), but also to many specific requirements including:

- Consent (see Art. 7(1));
- Exceptions to obligations in relation to data subjects’ rights (see Arts. 11(2) and 12(5));
- Refusal to comply with objections to processing by data subjects (see Art. 21(1));
- The arrangements between “joint controllers” (see Art. 26);
- The “guarantees” offered by processors (see Art. 28);
- Data security and data breaches (see Arts. 32 and 33);
- Data Protection Impact Assessments (see Art. 35); and
- Transborder data flows (see Art. 46).

The GDPR stipulates that in relation to several requirements, **a data protection certification can be used as “an element by which to demonstrate” relevant matters**, i.e.: general compliance with the obligations imposed on a controller (Art. 24(3)); privacy by design and -default (Art. 25(3)); the existence of “sufficient guarantees” for processors (Art. 28(5)); and compliance with data security requirements (Art. 32(3)). In all these cases, the phrase “an element by which to demonstrate” must presumably be read as the creation of a rebuttable presumption: certifications can be used as part of the evidence to show compliance in these regards – but they do not in and of themselves prove such compliance. In these respects, therefore, data protection certifications are useful, but not conclusive of compliance.

However, in one context this is different: in relation to transfers of personal data to third countries without adequate data protection. Such transfers are in principle prohibited, subject to a limited number of exceptions, including where “appropriate safeguards” are provided by the controller or processor (Art. 46). In this regard, the GDPR stipulates that such appropriate safeguards “may be provided for” *inter alia* by:

an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights (Art. 46(2)(f))

In other words, in relation to transfers of personal data to countries without adequate data protection, certifications are conclusive: they provide, in and by themselves, the required safeguards.

Indeed, the article adds that certifications can achieve this “without requiring any specific authorisation from a supervisory authority” (leading sentence to Article 46(2)).

Who can issue certifications?

In particular in the highly sensitive context of data transfers, it is crucial that certification schemes will ensure that certifications can and will only be issued in cases in which they really provide cast-

Douwe Korff

*Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford*

iron safeguards, “essentially equivalent” to those provided within the EU/EEA by the GDPR. Otherwise, the very same problems and challenges will arise as arose in relation to the discredited “*Safe Harbor*” scheme and the not-much-less contestable (and actually contested) “*Privacy Shield*”.

If certifications are issued by Member States’ DPAs (as is possible under Art. 42(5) GDPR), one may assume that they will indeed be strict and diligent in this respect. In any case, the consistency mechanism can be used, at least in any instance involving cross-border processing, if one DPA were to issue a certification (including one allowing for data transfers to countries without adequate protection) that other DPAs felt was not warranted.

However, as the WP29 document notes, under the GDPR, Member States may opt for alternative arrangements: they can allow their DPA to accredit other bodies to issue certifications (Art. 43(1)(a)), or they can allow national accreditation bodies (as named under Regulation (EC) No 765/2008) to accredit certification schemes (Art. 43(1)(b)). Under these alternatives, **certifications can therefore be issued by entities that are one-, or even two arms-lengths removed from DPAs.**

One serious problem with the last option – accreditation by general national accreditation bodies – is that those bodies are not equipped to deal with fundamental rights issues. They typically accredit certification bodies assessing and certifying purely technical matters, such as the safety of medical implant devices, or children’s toys, or food. The protection of fundamental rights is a totally different matter. **In my opinion, the Member States’ general accreditation bodies are fundamentally unsuited to accredit schemes aimed at upholding and reinforcing fundamental rights strongly enshrined in the EU Charter of Fundamental Rights and the case-law of the CJEU.**

This is recognised to some extent in the GDPR, in that it requires the DPAs or the EDPB to issue the criteria for accreditation, and more specifically in that it stipulates that in relation to accreditation by general accreditation bodies, those criteria/requirements “shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies” (Art. 42(3)). In the Draft Guidelines, it is also explicitly recognised that industry standards such as EN-ISO/IEC 17065/2012 are not sufficient in relation to GDPR compliance certification and must be “complemented” by additional standards.

But as noted, **the WP29 Draft Guidelines fail to include precisely those “complementary requirements” (beyond saying that they should include “special expertise in the field of data protection”: p.12). The annex that is supposed to spell this out further is simply not there. Without the further detail, the Draft Guidelines provide no assurance at all that the one- or two-arms-lengths schemes will adequately protect the right to data protection, or that the certifications issued under them will really “demonstrate compliance” with the GDPR.**

What is more, it is unclear whether certifications issued by bodies other than DPAs (and the issuing of which therefore does not constitute a “decision” of or a “measure” taken by a DPA) can be challenged under the consistency mechanism (although we would argue that they could, by other DPAs challenging the non-use by the challenged DPA of its power to demand that a certificate not be issued, or if issued, be withdrawn: Art. 58(2)(h)).

Douwe Korff

*Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford*

Pan-EU/EEA certification schemes

Although the GDPR requires the Member States, the DPAs, the EDPB and the Commission to “encourage” the establishment of data protection certification mechanisms, “**in particular at Union level**” (Art. 42), the regulation is unclear about the conditions and processes for the establishment of pan-EU/EEA schemes. The regulation does not appear to allow the EDPB itself to issue certifications (cf. Art. 42(5), which only mentions national DPAs and bodies accredited by DPAs or national accreditation bodies). However, it would not seem to be impossible for the EDPB to accredit bodies willing and capable of issuing pan-EU/EEA certifications. Alternatively, such schemes could be endorsed jointly by all the DPAs, acting within the EDPB.

I believe that pan-EU/EEA certification schemes, formally endorsed by the EDPB or all the EU DPAs acting together in the EDPB, are far to be preferred over national schemes. In particular, a proliferation of national schemes could lead to a race to the bottom, with controllers and processors – including non-EU/EEA controllers and processors – looking for the “easiest”, least-demanding certification schemes as a way to reduce their obligations under the GDPR (possibly even avoiding full compliance), and in particular to by-pass the stringent conditions imposed by the GDPR on transfers of personal data to third countries without adequate protection.

Conclusions

The WP29 Draft Guidelines fail to address the most important issues concerning certification, and even say that the as-yet-unpublished guidelines in the not-yet-available annex will “not constitute a procedural manual for the accreditation process performed by the national accreditation body or the supervisory authority”, but rather will only “provide[] guidance on structure and methodology and thus a toolbox to the supervisory authorities to identify the additional requirements for accreditation” (p. 12).

In my opinion, certification schemes are much too important – especially in relation to transborder data flows – to be addressed only in this superficial, technical and largely unspecified way.

We call on the WP29 to **urgently** provide an opinion on the ways in which it can be assured that certification schemes will really only lead to certifications at the highest level, and in particular to ensure that certifications will not be used to undermine the strict regime for transfers of personal data from the EU/EEA to third countries that do not provide “adequate” (that is: “essentially equivalent”) data protection to that provided by the GDPR.

In my view, this should mean that the WP should express an explicit preference for certifications issued by DPAs themselves, subject to the consistency mechanism, or at least for the accreditation of such schemes to be done by DPAs rather than by general accreditation bodies (which are completely unsuited for such a task).

The WP29 should also expressly clarify that the consistency mechanism will be applied also to certifications issued by bodies other than DPAs.

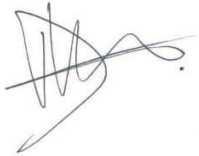
And the EDPB, once established, should urgently move towards the accreditation of (a) pan-EU/EEA certification scheme(s) at the highest level, and adopt a policy that would require controllers and processors involved in cross-border processing operations within the EU/EEA and/or data transfers to third countries without adequate data protection to seek such pan-

Douwe Korff

*Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford*

EU/EEA certifications for such cross-border operations, rather than certifications issued by national schemes.

Yours sincerely,



Douwe Korff (Prof.)

Disclosure of interest:

I was involved as a leading legal expert in the establishment of the European Privacy Seal (*EuroPriSe*) scheme, originally set up with EU support at the offices of the data protection authority of the German *Land* of Schleswig-Holstein, *ULD*. I continue to be an accredited legal expert with the *EuroPriSe* scheme, which is now run as a separate private entity – but which still applies the strict, high-level assessment criteria I helped to draft when it was first established. However, this letter is not aimed at supporting any particular existing or future GDPR certification scheme.