Douwe Korff*
Professor of International Law

WARNING:

THE EU COUNCIL IS TRYING TO UNDERMINE PRIVACY SEALS

(and through this, the General Data Protection Regulation)

I. Introduction

Some people, including myself, believe that good privacy seals, managed by the right bodies, can make a serious contribution to high-level data protection – while bad seals, issued by bodies that are more interested in providing fig-leaves and making money, can seriously harm data protection. The arrangements for data protection certification in the new General Data Protection Regulation (hereafter: "the regulation") are therefore important. The original draft of the regulation, issued by the Commission in January 2012, merely said that certification schemes should be "encouraged" (although it provided for some EU-level harmonisation of the frameworks).

The European Parliament's amended text is much more ambitious in this regard and, if adopted, would make certification schemes both more integrated with the general data protection regime and stronger, also in terms of ensuring that no seals could be issued in one Member State that would undermine data protection in other Member States.

However, the text set out in an EU Council document dated 26 September 2014 and just leaked, shows that the Member States are trying to undermine the good proposals of Parliament.

At II, I first briefly set out the problems with European privacy seal schemes under the current rules. Next, at III, I analyse the relevant provisions in the different versions of the regulation, adopted by the Commission, Parliament and the Council. Finally, at IV, I conclude that if the Council text were to be adopted, the provisions on seals could become a Trojan Horse that could seriously undermine the in principle strong data protection regime in the regulation (*pace* other watering-down attempts by the Council). This note thus seeks to sound a warning to those involved in the upcoming trilateral negotiations on the regulation text, not to allow such a dangerous scheme (or rather, an ill-defined miscellany of schemes) to slip in.

II. Data protection seals and the 1995 Data Protection Directive

There is no explicit provision on data protection- or privacy seals or certification schemes in the main EC data protection directive (Directive 95/46/EC, hereafter "the directive"), although other self-regulatory mechanisms, such as codes of conduct and contractual arrangements are encouraged under it (see Art. 27 *re* codes; Art. 26(2) *re* "appropriate contractual clauses"). Nevertheless, the European Commission has in practice encouraged the establishment of seals, in particular by supporting the establishment of the "European Privacy Seal" (EuroPriSe)

---

* Professor Douwe Korff is an Associate of the Oxford Martin School of the University of Oxford and a Visiting Fellow at Yale University (Information Society Project):
http://www.oxfordmartin.ox.ac.uk/cybersecurity/people/578
http://www.yaleisp.org/people/douwe-korff
He helped to establish the European Privacy Seal (EuroPriSe) scheme discussed in the text.

scheme under an "e-TEN" programme; this was until recently operated by the data protection authority of the German *Land* of Schleswig-Holstein, the Independent Centre for Privacy Protection (or ULD after its German initials), but has recently been passed on to a private German company, 2B.[1] The French data protection authority, CNIL, has also established a certification scheme, under which controllers can certify that they meet certain CNIL-specified criteria (but so far only in relation to privacy training, data protection audit, and one product: cloud computing).[2]

This is not the place to evaluate these, or other, existing data protection- or privacy certification/seal systems.[3] Suffice it to note that these schemes are limited in their potential by three factors in particular:

- because the directive is still implemented in greatly divergent ways in the Member States, a seal that certifies compliance with the standards set out in the directive (such as EuroPriSe) cannot guarantee that the certified product or service also complies with all the idiosyncracies of all the 30-odd national laws (some of which, in some respects, are not in accordance with the directive); while a seal that certifies compliance with one national law (such as the CNIL's *Labels*) does not guarantee compliance with the other laws (or necessarily with the directive);
- the current European rules do not afford seal holders any significant commercial advantage, beyond demonstrating that a company is serious about its data protection compliance;[4] and
- serious seals (like EuroPriSe) are quite expensive in terms of costs of experts in particular, and highly demanding in time and effort on the part of the seal applicant.

Because of these factors, the uptake on the EuroPriSe and CNIL-seals has been very limited and, indeed, disappointing.[5]

In short: privacy seals/certification schemes have the potential to reduce regulatory and enforcement burdens on supervisory authorities, build consumer- and business-to-business trust and confidence through better information and greater transparency and reliable assurances from competent, respected bodies, and facilitate trade (e.g., by providing the kinds of safeguards and guarantees that the legal rules require in certain respects, but do not always spell out, e.g., as regards processors, data transfers, or cloud computing). However, to date that potential has not been realised.

---

1 See: https://www.european-privacy-seal.eu/EPS-en/Fact-sheet

2 See: http://www.cnil.fr/linstitution/labels-cnil/

3 A report of an EU-commissioned study into privacy seals (Service Contract Number: 258065) is due out shortly. This also discusses the myriad of other, generally more limited schemes in Europe, and the (generally weak) non-European schemes.

4 By contrast, the data protection law of the small German *Land* of Schleswig-Holstein expressly allows public authorities to give preferences to products and services which have been granted the local (Schleswig-Holstein) seal by the local data protection authority (ULD). ULD has issued more than 80 such local seals, including several to Microsoft, see: https://www.datenschutzzentrum.de/guetesiegel/register.htm

5 According to its 2012 annual report, CNIL had received 25 seal applications and had issued 10 seals (as at 15 February 2013; no later data available). EuroPriSe has issued 31 seals (not counting re-certifications) (last checked 01 October 2014).

III. Data protection seals and the draft General Data Protection Regulation

The adoption of a regulation to replace the directive will ameliorate the first of the above-mentioned problems by its very nature: in stead of 30-odd still widely varying national laws transposing the directive in different ways and to different extents, there will now, at least in theory, be one set of directly applicable rules, set out in the regulation. However, the regulation is still replete with quite vague terms ("fair", "adequate", "necessary", etc.), and many terms, including core definitions (such as "personal [=identifiable] data"), still require interpretation and can be applied in different ways in different contexts. It is therefore absolutely crucial, and commendable, that the regulation contains a mechanism to ensure close cooperation and mutual assistance between the national data protection authorities (and between them and the newly-to-be-created European Data Protection Board), and a "consistency mechanism" through which the DPAs and the Commission can object to interpretations and applications of the provisions in the regulation by other DPAs with which they disagree, ultimately resulting in a binding central ruling that must be adhered to by all.[6] In my opinion, the aim of the regulation – ensuring true and full real harmonisation – stands or falls with these mechanisms.

This ought to also apply to seals, if they are to have any real effect – *a fortiori* in relation to seals that might be granted to products or services that are offered (by European or non-European controllers) to European citizens and consumers: it should not be possible for a seal to be issued in one country for such a product, supposedly certifying that the product meets the requirements of the regulation, without the other countries (and the other countries' DPAs) agreeing that that certification is justified. Rather, data protection seals should either be issued at the European level, through a central European body (at least for products and services that are offered in more than one Member State, e.g., online), or seals that may be offered at the national level should be subject to the cooperation- and consistency mechanisms (again at least when they relate to products offered in several EU states or online).

However, the consistency mechanism in particular can only be invoked in relation to "measures" adopted by DPAs that have "legal effects" (Art. 58(2), initial sentence). As we shall see, this has important implications in relation to seals.

I will now discuss to what extent this is reflected in the different versions of the regulation.

Certification in the Commission text

As already noted, the European Commission published the text of the proposed General Data Protection Regulation (GDPR) in January 2012.[7] This text essentially merely requires the Member States and the Commission to "encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors." (Art. 39(1) Commission text), although it also envisages the adoption, by the Commission, of "delegated acts" at some future time, "for the purpose of further specifying the criteria and requirements for [these] data protection certification mechanisms" (Art. 39(2)); and the issuing by the Commission of "technical standards for

---

6 See Chapter VII of the draft regulation.

7 See: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks" (Art. 39(3)).

The Commission text does not mention any specific, concrete, legally binding consequences of the awarding of seals: as under the current schemes, all they do under this text would be to provide some general assurance of compliance. Seals would not amount to a finding of compliance with any "legal effect". The delegated acts and further specifications relating to seals, just mentioned, would, it would appear, not be able to create such effects.

The "encouragements" and arrangements envisaged in the Commission text thus fall considerable short of the sort of certification/seal schemes I mentioned earlier, that would be subject to cooperation and consistency mechanisms.

Certification in the EP text

The LIBE Commitee of the European Parliament agreed on an amended text in October 2013,[8] and this text was adopted in March this year by the Parliament as a whole.[9] The EP text significantly amends the proposal in respect of certification schemes, and strengthens the seals.

The amended version of the Regulation adopted by the European Parliament thus, first of all, stipulates that seals must be issued DPAs:[10]

> Any controller or processor may request **any supervisory authority** in the Union, for a reasonable fee taking into account the administrative costs, **to certify** that the processing of personal data is performed in compliance with this Regulation, in particular with the principles set out in Article 5, 23 and 30, the obligations of the controller and the processor, and the data subject's rights.
>
> (Article 39(1a) in the Consolidated LIBE version of the Regulation, emphasis added)

This is not affected by the stipulation that the basic evaluations needed for the seals may be left to third-party accredited experts or "auditors" (Art. 39(1d) of the EP text): under the EP text, the seals will still have to be issued by the DPAs, i.e., the DPAs must at least double-check or certify the evaluation reports of the auditors (similar to the way in which the Schleswig-Holstein DPA, ULD, has until recently certified the European Privacy Seals). This is expressly reaffirmed in the final sentence of Article 39(1d):

> The final certification shall be provided by the supervisory authority.

This is important because, secondly, under the EP text, seals would also have legal effects in some regards:

- a seal will be able to "demonstrate" that a processor offers "sufficient guarantees" in relation to the processing the processor is asked to undertake, to allow the controller to enlist the processor's services in compliance with Article 26(1) (see Art. 26(3a) of the EP text);

---

[8] See: http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf

[9] See: https://www.huntonprivacyblog.com/2014/03/articles/european-parliament-adopts-draft-general-data-protection-regulation-calls-suspension-safe-harbor/

[10] Article 39(2a) adds that "The European Data Protection Board may on its own initiative certify that a data protection-enhancing technical standard is compliant with this Regulation." But this only applies to "technical standards", not to seals for products or services.

- in relation of a data transfer to a country without adequate data protection, a seal that covers the relevant processing by both the controller (the EU-based data exporter) and the recipient (the data importer in the third country) will in itself provide "appropriate safeguards" in respect of the protection of the data; and processing covered by a seal would thus be allowed without further ado.

In other words, under the EP text, a processor who has been issued with a seal could not be held to be lacking in "sufficient guarantees" (at least in respect of the processing for which the seal was issued, if that did not cover the processor's operations generally), as long as the processor complied with the conditions etc. provided for and assessed in the certification process; and transfers of data for which a seal has been issued could not be held to be in breach of the in-principle prohibition on transfers, now contained in Article 42 of the regulation (unless of course the parties failed to meet the conditions etc. provided for and assessed in the certification process). The seals envisaged in the EP text would thus clearly offer concrete legal benefits to seal-holders.

The EP text adds that:

> The supervisory authorities and the European Data Protection Board shall cooperate under the consistency mechanism pursuant to Article 57 to guarantee a harmonised data protection certification mechanism including harmonised fees within the Union."
>
> (Article 39(1c) EP text);
>
> and that
>
> The Commission shall be empowered to adopt, after requesting an opinion of the European Data Protection Board and consulting with stakeholders, in particular industry and non-governmental organisations, delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1-1h, including requirements for accreditation of auditors, conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries. These delegated acts shall confer enforceable rights on data subjects.
>
> (Article 39(3) EP text)

However, as the wording of these provisions make clear, these harmonising measures relate only to the parameters and technical details of the certification scheme (similar to the stipulations in the Commission text, although the EP text rightly allows for better input from the EDPS and other stakeholders).

It is therefore important to note that under the EP text the actual issuing of a seal by a DPA would constitute an administrative act of such an authority: the issuing of seals is part of each DPA's brief to implement and apply the Regulation within their jurisdiction (cf. Art. 53(1)(ia) of the EP text).

This in turn will mean that the cooperation- and consistency mechanisms set out in Chapter VII of the regulation will apply to the issuing of individual seals. The EP text indeed amends the provisions on these mechanisms and distinguishes between cooperation in individual cases (Arts. 54a, 55 and 56 EP text), consistency in matters of general application (Art. 58 EP text), and consistency in individual cases (Art. 58a EP text). This results in the following scheme:

- In deciding on whether to issue a seal in relation to processing by a controller who is established in more than one Member State, or who processes personal data on residents of more than one Member State – i.e., in relation to any cross-border operating company, including especially companies offering products and services throughout the EU (and beyond) over the Internet – there will be a need to first establish who is the "lead authority"; and next, that lead authority will be required to consult "all other competent supervisory authorities" on whether or not a seal should be issued (cf. Art. 54a(1) and (2) of the EP text). Those other authorities must then provide "mutual assistance" as required (Art. 55); and the DPAs may decide to deal with the matter through a "joint operation" (Art. 56);
- At the request of any DPA, the EDPB can issue an opinion on which DPA should be regarded as the lead authority; and in the end, the EDPB can decide the matter (Art. 54(3) and (3a) EP text);
- Moreover, since (as just shown) under the EP text seals will carry certain legal effects, in particular in relation to processors and data transfers, the issuing of a seal will constitute a "measure intended to produce legal effects within the meaning of Article 54a". Consequently, in such cases – i.e., in casu, in relation to seals applied for by cross-border-operating companies and Internet-based companies – the "consistency mechanism" provided for in Article 58a of the EP text comes into play. Under this mechanism, the relevant lead authority must inform the other DPAs of the intended measure – i.e., of his intention to issue a seal for such a company – and the other DPAs can then refer the matter to the newly-to-be-created European Data Protection Board, if they have "serious objections" to the measure, i.e., to the seal being awarded to the company, service or product in question.

Clearly, the seals envisaged in the EP text are much more serious and carry much more weight than the largely unspecified ones that the Commission text "encourages", in particular in relation to cross-border-operating and/or online companies (including non-EU companies): a seal issued under the EP text to such companies, either without objection from any other DPAs than the seal-issuing "lead authority", or after having gone through the consistency mechanism and having been found to be in accordance with the regulation, clearly has strong legitimacy throughout the EU/EEA: it will truly demonstrate full compliance with the regulation, throught the EU/EEA, and it will have the stipulated legal effects throughout the EU/EEA.

The seals envisaged in the EP text thus address all the issues mentioned earlier that have to data hampered certification schemes:

- They would convincingly certify compliance with the fully harmonised rules in the regulation; and this would be accepted, or would have to be accepted, by all DPAs (either because they did not object to the seal being issued after having been notified of the intended awarding of the seal, or because the issuing of the seal was ruled to be in accordance with the regulation under the consistency mechanism);
- The seal would bestow clear and valuable legal and commercial benefits on the seal-holder; and
- This would warrant the costs and effort involved in obtaining the seal.

Moreover, I believe that such "heavy" seals, thus seriously embedded in the harmonised EU rules, would offer true assurances to citizens and business, and seriously positively contribute to ensuring data protection at a high level.

In my opinion, the EP text in this regard thus promises important benefits to business and consumers alike.

Certification in the Council text

On 26 September 2014, a Council document was produced by the Council data protection committee, DAPIX, that dealt with the chapter in the regulation dealing (*inter alia*) with certification schemes (Chapter IV).[11] This internal, restricted ("*Limité*) but quickly leaked document contains specific texts for the relevant provisions on seals in the regulation.

Essentially, they show that the Council wants to reject the EP proposals for a strong system of harmonised, consistent data protection seals with real effects, and to revert back to the vague promisses of "encouragement" in the Commission text – if anything watering the system down even further.

Thus, first of all, the Council text, like the Commission text, merely calls upon the Member States and the Commission to "encourage" the establishment of data protection certification schemes (while adding the EDPB to the addressees for this call) (Art. 39(1) Council text). The only difference is that Council text calls for this to be done "in particular at Union level", where the Commission text referred to "in particular at European level" (*idem*). Thus, the Council wants to remove the EP stipulation that DPAs must ("shall") implement certification (cf. Art. 52(1)(ja) EP text).

Secondly, under the Council text seals may be issued *either* by a DPA *or* by another "certification body" approved by an official national accreditation body (such as the UK Accreditation Service, UKAS).[12] In other words, under the Council text, certification schemes could be essentially almost completely "out-sourced" to a body other than the national DPA, as long as the body was accredited (i.e., meeting appropriate organisational and management and financial requirements) and met any specific requirements laid down by the DPA (but the assessment of which would also be left to the accreditation body). Specifically, although the relevant DPA would be "provide[d] ... with the reasons for granting or withdrawing [a] requested certification" (Art. 39(5) Council text), in countries that opted for such an out-sourced scheme, the seal would be issued by the accredited certification body, and not by the DPA.

---

[11] Presidency Note to COREPER, Brussels, 26 September 2014 (original: English), institutional file number 2012/0011(COD), document number 12312/3/14REV3 (hereafter referred to as the "Council text"), leaked on the Statewatch website at:
[ADD LINK]
The document also deals with important other issues addressed in Chapter Iv of the regulation, including data protection by design and default, joint controllers, data security, data breach notification, data protection impact assessments and prior consultation, in-house data protection officers, but these are not discussed here.

[12] See: http://www.ukas.com/ The Council text refers more specifically to "*the National Accreditation Body named in accordance with Regulation (EC) 765/2008 of the European parliament and the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products in compliance with EN-ISO/IEC 17065/2012 and with the additional requirements established by [the DPA of the Member State in question].*" (Art. 39a(1)(b) Council text).

Not suprisingly, under such a scheme, the DPA would not in any way be bound by the assessment of the certification body that the assessed product or service meets the requirements of the regulation: see Article 39(2) Council text, which expressly stipulates that:

> A certification ... is without prejudice to the tasks and powers of the [competent] supervisory authority.

There is a suggestion to the contrary in Article 39(1) of the Council text, where this says that

> seals or marks may also be established for the purpose of **demonstrating the existence of appropriate safeguards** provided by controllers or processors that are not subject to this Regulation (emphasis added)

As we have seen, under the EP text, seals can indeed "demonstrate", in a legally binding way, that certain requirements of the regulation are met.

However, under the Council text, seals would not have any such real effects. Rather, seals could just be taken into account in assessing compliance. As the Council text puts it explicity in relation to a variety of issues, in identical terms, "*An approved certification mechanism pursuant to Article 39 may be used as* ***an element to demonstrate compliance***" with relevant requirements such as: compliance with a code of conduct (Art. 22(2b) Council text); compliance with privacy-by-design and –default requirements (Art. 23(2a)); with the requirement of processors to offer "sufficient guarantees" (Art. 26(2aa)); with data security requirements (Art. 30(2a)); and presumably with requirements relating to data transfers to countries without adequate protection (but the relevant provisions are not covered by the Council document).

The point to be made here is that allowing seals to be taken into account in this way, as an "element" in a wider assessment, means that the seals by themselves alone are not seen as "demonstrating" the matter in question. In other words, although they may have some legal weight, they do not in themselves have any "legal effects".

For both reasons – the seals not being issued by a DPA, and the seals not having legal effects – the issuing of seals under the Council text would not constitute an administrative act with legal effects on the part of the DPA in countries that choose this option (as the UK in particular appears to want to do).

Consequently, the issuing of seals in such countries would not be subject to either the cooperation or the consistency mechanisms in the regulation. The DPAs would not have to inform other DPAs of the fact that they were asked to issue a seal in relation to a controller offering products or services also in other Member States (or online), or processing personal data on data subjects in other Member States; they would not have to consider whether they would be the appropriate (lead) authority to deal with such a request; they would not have to ask for, let alone heed, the views of other DPAs on the issuing of the seal; and they could not be made to deal with the proposed issuing of a seal to such a company under the consistency mechanism; the decision could not be overruled from Brussels.

Yet at the same time, in spite of such seals not having any formal standing, in practice the DPA in the country in question (who was after all informed of the reasons for granting the seal, by a body appointed by that DPA itself) would be unlikely to take enforcement action against a company with the seal, as long as the company adhered to the conditions etc. set out in the seal.

IV. Conclusions

The above analyses of the different versions of the regulation shows two clearly opposed views of certification schemes. On the one hand, the European Parliament wants to introduce a strong certification scheme, operated by the DPAs within a harmonised EU framework. Seals would be given real, important legal effects, of real benefit to companies – but (in particular in respect of cross-border-operating or online companies, including non-EU ones) only if they were subject to close scrutiny by all the EU DPAs, and the EDPB, and if it were agreed between them, or decided under the consistency mechanism at the highest [Brussels] level that it was appropriate to issue the seal in the particular instance. Such seals would therefore also offer real assurances to consumers nd citizens.

By contrast, the Council would allow Member States to either opt for relatively strong seals issued by DPAs (such as the French *Labels*), or for an almost completely out-sourced certification scheme under which seals would be issued by an accredited certification body separate from the DPA (and not subject to directions from the DPA, other than in terms of general guidance). The out-sourced seals would have no formal legal effect – but would also by-pass all European cooperation and consistency mechanisms. Yet they would still in practice largely exempt the companies that were awarded such seals from enforcement action by the DPA in question (as long as they complied with the conditions etc. set out in the seals).

In my opinion, a certification scheme allowing the latter kinds of seals would introduce a Trojan Horse into the new EU data protection regime. International companies, including the so-called "Internet giants" (Microsoft, Google, Yahoo, Facebook, Twitter, etc.) could – and almost certainly would, just as now – pick and choose to apply for seals in EU states in which they would hope to be given relatively lax treatment; where they feel they can relatively easily obtain a seal – from an out-sourced body. The DPAs in other countries would not be asked to give their views; they could not challenge the issuing of the seal (indeed, even the DPA in the country in question would only be informed of the issuing of the seal and the reasons for it). Yet they would then of course rely on the seal, or seals, they obtained to argue that their operations are fully compliant with the regulation. DPAs in other Member States, and the EU bodies concerned (including the Commission) would probably be less inclined to pursue such companies in such circumstances for non-compliance.

I would urge those who are going to be involved in the upcoming trilateral negotiations over the final text of the regulation and who take data protection to heart, to reject the Council text and support the EP one in respect of certification schemes.

That is not to say that some compromises are impossible. For instance, a Member State could still largely outsource a certification system to an accredited certification body (so as to avoid imposing further burdens on its DPA), yet retain the advantages of the EP scheme, if it left the final decision on each seal to its DPA, acting on the "recommendation" of the certification body. That way, it would still be the DPA that took the decision. If at the same time, such a seal would be given the effect of demonstrating compliance in certain contexts (rather than just being allowed to be an "element" in evidence), that would mean that the cooperation and consistency mechanisms would still come into play – which will ensure that appropriately high-level pan-EU scrutiny would be applied, in particular to cross-border and online companies. I hope this note will stimulate that debate.

- o – O –o -