Schrems II: SCCs valid and effective in practice?

Gonzalo F. Gallego of Hogan Lovells says that Standard Contractual Clauses' applicability is still limited on a practical level.

"All that glitters is not gold…": This is a warning that should be kept in mind by anyone who reads the Opinion of Advocate General Saugmandsgaard Øe of the Court of Justice of the European Union in the case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (*Schrems II*) delivered on 19 December 2019 (the AG's Opinion)[1].

As we all know, *Schrems II* plays an important role in determining the possibility of using the Standard Contractual Clauses[2], probably the most used safeguard for international transfers of personal data under the General Data Protection Regulation (GDPR). This being the case, it is not surprising that the announcement of the publication of the AG's Opinion in this case generated so much expectation.

Perhaps it was that expectation – and the concern that prevailed among the community of data protection professionals after the predictions that appeared on the subject – which motivated the general feeling of relief that ran through the minds of many when on 19 December the Press Release that preceded the publication of the AG's Opinion was published. "The Standard Contractual Clauses are still valid!" was heard and read on the main social media. The title of the Press Release was blunt in this respect: "According to Advocate General Saugmandsgaard Øe, Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries is valid".

However, a more detailed reading of the AG's Opinion takes us away somehow from the wave of optimism that swept through the social networks in the early hours of the publication of the Press Release, to a spot where we still need to "be on guard". Let's have a look at it.

Standard Contractual Clauses are valid... at a formal level...

As it is known, and generally speaking, the imminent risk that threatens the survival of the Standard Contractual Clauses[3] in *Schrems II*, lies in the possibility that the authorities of the country of the data importer may oblige such data importer to disclose the personal data transferred. Such a disclosure could be in execution of powers attributed to such authorities by the legislation of that country and without there being due guarantees according to the European Union. In *Schrems II* these are certain security agencies of the United States, although there is no reason not to extend the same criterion to any other third country. In short, what is intended to be judged is whether Standard Contractual Clauses (that do not in practice prevent the data importer from disclosing data to his country's authorities by applying its legislation), constitute "adequate safeguards" under the European Union's data protection framework.

The answer to this question is given by Advocate General Saugmandsgaard Øe (the Advocate General), who focuses on the formal purpose of the Standard Contractual Clauses. This purpose is to provide safeguards for the processing of data, which make up for the deficiencies that do exist in the legislation of the importer's country. From this point of view, there is no point in questioning the validity of the Standard Contractual Clauses by arguing on the basis of the shortcomings in the legislation of the third country, for example, that such legislation gives its authorities quasi-absolute power to access personal data. The existence of such deficiencies in the laws of the importer's country not only does not invalidate the Standard Contractual Clauses, but is the rationale of the same.

Having said that, in the opinion of the Advocate General, what is relevant at the point of determining the validity (or not) of the Standard Contractual Clauses is to clarify whether they contain measures intended to effectively address the shortcomings of the regulatory framework applicable to the importer in his country as regards the processing of the data transferred? This is somehow a criterion based on the means (and is therefore formal and theoretical) and is not based on the results.

The Advocate General answers this question in the affirmative. In doing so, he relies on the powers and obligations which the Standard Contractual Clauses (for transfers to processors) lay down for both exporting controllers and EU data protection supervisory authorities.

Indeed, firstly, the Advocate General highlights the fact that the Standard Contractual Clauses (clauses 5(a) and 5(b)) establish the power – which the Advocate General actually envisages as an obligation – of the exporter to suspend the international data transfer or to terminate the contract with the importer in the event that the importer is unable to comply with the exporter's instructions and/or with the Standard Contractual Clauses. This is complemented by the powers that the Standard Contractual Clauses (clauses 3, 6(1) and 7(1)) give to the data subjects, who can assert their rights against both the importer and the exporter by going to court and to data protection supervisors.

Secondly, the AG's Opinion refers to the powers – obligations, in fact – that the supervisory authorities have in the field of data protection under Article 58 GDPR and Article 4 of Decision 2010/873, to investigate and ultimately suspend international data transfers which, although formally covered by standard contractual clauses between exporter and importer, are carried out under conditions which do not effectively guarantee the rights of the data subjects in the destination country. Moreover if these powers are not

properly exercised, (i.e. if, for example, a supervisory authority does not prevent a transfer of data to an importer who cannot fulfil his obligations under the Standard Contractual Clauses), it may give rise to a legal claim against the supervisory authority by the data subjects concerned.

Given the existence of these "tools" contained therein and in the GDPR, the Advocate General concludes that the Standard Contractual Clauses should be considered valid since from a formal point of view – that is to say, solely on the basis of what they provide for enforcement – they constitute a mechanism which, if complied with, would be capable of creating adequate guarantees in the destination country.

However, the Advocate General's reasoning is on a strictly formal level. He simply responds by using the letter of the Standard Contractual Clauses and the GDPR to the reproaches of the Irish authority and Max Schrems that the signing of Standard Contractual Clauses is not preventing US importers from being forced to disclose data to US security agencies. In short, while the Irish authority and Max Schrems claim that the Standard Contractual Clauses are not being complied with by at least some US importers, the Advocate General considers that, even if this were true, it would be a question beyond to the validity of the Standard Contractual Clauses, since both the Standard Contractual Clauses and the GDPR contain elements which make it possible to prevent such a situation. And it is this gap between what the Standard Contractual Clauses provide for and what happens in practice that challenge the real effectiveness of the Standard Contractual Clauses and makes it necessary for exporters and importers of personal data to operate with caution.

The effectiveness of SCCs is limited on a practical level

The Standard Contractual Clauses are designed to provide safeguards for international transfers that will actually occur. In this sense, what EU exporters (and non-EU importers) expect (and need) from *Schrems II* is a clear statement on whether they can still rely on the Standard Contractual Clauses to legitimise the international transfers of personal data under the GDPR. And, contrary to what people might think, such a statement does not exist in the AG's Opinion (nor will it exist in the final Judgment of the CJEU, if it follows the argument of the first one).

As already noted, the Advocate General considers that the Standard Contractual Clauses are (formally speaking) valid since, if applied on their own terms, they provide adequate safeguards and allow – and indeed oblige – both the exporter and the data protection supervisory authorities to enforce the clauses by the importer or, if that is not possible, to suspend the international transfer.

However, the reasons that justify the validity of the Standard Contractual Clauses also become conditions for such clauses to be effective in practice in providing adequate safeguards for a specific international transfer of data. Failure to meet these conditions means that the Standard Contractual Clauses are insufficient. And this is the crux of the matter.

Indeed, following the reasoning of the Advocate General, for such effectiveness to exist, that is to say, for an international transfer of data to exist legally under Standard Contractual Clauses, it is necessary that the importer processes the transferred personal data only in accordance with the exporter's instructions and the terms of the Contractual Clauses. If for any reason he cannot do so (for example, because the legislation of his country gives the authorities rights of access to the data), the international transfer of data cannot exist (at least not legally) since the exporter or, where appropriate, the relevant data protection authority, must suspend it.

And then, what happens if such an international transfer is not suspended? The Standard Contractual Clauses signed between the exporter and the importer are no longer an adequate safeguard for the specific international transfer envisaged therein. In other words, even if they are valid at a formal level, the Standard Contractual Clauses are no longer effective in practice to legitimise the international transfer, which becomes unlawful.

Thus, the validity of the Standard Contractual Clauses initially declared by the AG's Opinion on a formal level is limited on a practical level: actually the Standard Contractual Clauses only constitute a valid safeguard for an international data transfer in those cases where the importer respects such clauses. And if he does not (or cannot) do so, then the Standard Contractual Clauses are no longer an effective mechanism for that particular case.

But there is still good news: the Standard Contractual Clauses are not invalidated and, therefore, exporters and importers, may still rely on this safeguard in several scenarios, provided that certain measures are implemented, as discussed below.

Consequences and practical recommendations

After weighing up the formal aspects against the practical ones, we do not wish to end this text without listing the main consequences of the AG's Opinion and making some recommendations for those exporters who carry out (and importers who receive) international data transfers of personal data relying on Standard Contractual Clauses:

1. **Stay calm:** The AG's Opinion is only a recommendation to the CJEU. It is not applicable yet.
2. **Hope for the best and prepare for the worst:** The AG's Opinion is not binding on the CJEU. However, in practice, the Court tends to follow the Advocate General's judgement in most cases. Therefore, a prudent approach is to prepare for a judgment in line with the AG's Opinion.
3. **Assume a global application of the criteria of the AG's Opinion:** The *Schrems II* case focuses on international transfers to the US and the Standard Contractual Clauses for transfers to processors. However, the analogous application to other countries and to the Standard Contractual Clauses for transfers to controllers seems clear. Therefore, the effects of *Schrems II* should not be thought to be limited to the case brought before the CJEU. In fact, it affects all international transfers based on any kind of Standard Contract Clauses.
4. **It is not necessary to replace the existing Standard Contractual Clauses for ongoing international**

transfers: For the time being the Standard Contractual Clauses appear to remain valid. Therefore, there is no need to replace them, at least not yet.

5. **Exporters must carry out (and document) processes of analysis and control about the compliance of the importers with their obligations under the Standard Contract Terms:** As we have indicated, the reasoning of the AG's Opinion leads to linking the actual effectiveness of the Standard Contract Terms to the compliance of the same by the importers. It is the exporter's obligation to ensure that such compliance occurs and to suspend the international transfer if it does not. This is not a new obligation. It is in fact a response to the application of the Standard Contractual Clauses. However, the AG's Opinion (and a Judgment of the CJEU in the same vein) may revive the interest of the control authorities on this issue. We therefore recommend that data exporters carry out documented analyses of the compliance status of their data importers with the Standard Contractual Clauses. This should range from the general points (i.e. analysis of the legal framework of the importer's country, with special emphasis on situations where the importer may be forced to disclose data received from the exporter) to the particular ones (i.e. actual compliance situation by the importer with the Standard Contractual Clauses). If after doing such analysis and implementing such controls, it is clear that the importer is in a position to fulfil the Standard Contractual Clauses, then the exporter (and the importer) can rely on that safeguard.
6. **Importers should implement mechanisms in order to "help" the exporters with #6 above:** Some of the measures to be implemented by the EU exporters as per #5 above, may require cooperation from the importer. Actually, if importers have developed their own "solution package" in order to deal with the consequences of *Schrems II*, the exporters (EU clients) may be happy to implement them. For instance, this solution package may include assessment of the disclosure obligations under the laws of the importer; voluntary reporting mechanisms; etc. Importers who anticipate the issues that EU clients (exporters) are facing after *Schrems II*, will be in a better position to retain them. They may even increase their market share!
7. **Consider the implementation of alternative mechanisms to the Standard Contractual Clauses, in some cases:** Finally, in some cases, exporters and importers may want to consider adopting alternative mechanisms to carry out the international transfers which are currently carried out under Standard Contractual Clauses. The "million-dollar question" is obviously what alternative mechanisms to implement? The answer requires a case-by-case analysis. Binding Corporate Rules ("BCRs") (for data controllers or data processors, as the case may be) are almost always the best alternative for international intra-group transfers, while for transfers to third parties outside the group (when no data processor BCRs apply), the use of Standard Contractual Clauses with some contractual supplements may have to be used.

AUTHOR

Gonzalo Gállego is Partner at Hogan Lovells in Madrid, Spain.
Email: gonzalo.gallego@hoganlovells.com

REFERENCES

1 curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=49246
2 It is also in the context of determining the validity of the Privacy Shield, although we do not refer to it in this text which focuses on the Standard Contractual Clauses.
3 In fact, we refer to the Standard Contractual Clauses applicable to transfers to processors, which are the only ones in dispute, although the extension of the Schrems II case to clauses addressed to controllers is clear. Therefore, we will refer here to Standard Contractual Clauses in general, except where it is necessary to be more precise.
4 This Decision approved the Standard Contractual Clauses for data processors. However, there are equivalent articles in the Decisions of the Standard Contractual Clauses for controller to controller transfers.

Italy's DPA issues 11.5 million euro fine on gas and electricity company

Italy's Data Protection Authority, the *Garante*, has fined gas and electric company Eni Gas e Luce for breaching the GDPR in its telemarketing activities and the activation of unsolicited contracts. The Authority carried out an inspection following several dozen complaints. The violations included making marketing phone calls without consent, or not taking into account the opt-out list. Also, data retention times were longer than allowed, and the company had purchased marketing lists from third parties who had not acquired consent to disclose that data. The *Garante*, which issued the fine on 17 January, says that some 7,200 consumers were affected.

• *See bit.ly/37BC79M (in Italian but English click through available)*

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

New GDPR law for Greece

Spyridon Vlachopoulos and **Vassiliki Christou** from the University of Athens explain new aspects and limitations of this law.

Greece's law implementing the GDPR, Law 4624/2019 (the Greek Law), entered into force on 29 August 2019. The new Greek Law is composed of three parts. The first part provides that the Greek Data Protection Authority (DPA), responsible for the enforcement of data protection law, including the GDPR, is the DPA already established under the previous data protection law 2472/1997, and sets out its new competences. The second part contains measures implementing the GDPR. The third part transfers into Greek legal order Directive 2016/680/EU[1]. In this article, we shall focus primarily on the second

Continued on p.3

India's data privacy Bill: Progressive principles, uncertain enforceability

The new Bill includes several notable changes from the previous version and should be followed closely not least due to the government's EU adequacy aspirations, says **Graham Greenleaf**.

India's Modi government has at long last submitted the Personal Data Protection Bill, 2019[1] to India's lower house, the *Lok Sabha*. The government Bill is based on the draft Bill (and Report[2]) prepared by the committee chaired by former Supreme Court Justice Srikrishna,

Continued on p.6

Future PL&B Events

- *Germany's data protection law: Trends, opportunities and conflicts,* 11 March 2020, Covington & Burling, London. **Speakers** include Alexander Filip, Bavarian DPA, and Covington partners from Germany & the UK. **Sessions** include: International transfers; Privacy and labour law; and Enforcement trends. www.privacylaws.com/germany
- *PL&B's 33rd Annual International Conference* St. John's College, Cambridge 29 June to 1 July 2020. www.privacylaws.com/ac (p.31)

privacylaws.com

Issue 163 **FEBRUARY 2020**

INTERNATIONAL report

ISSUE NO 163 **FEBRUARY 2020**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Gonzalo F. Gallego
Hogan Lovells LLP, Spain
Spyridon Vlachopoulos and Vassiliki Christou
University of Athens, Greece
Eleonora Maria Mazzoli
London School of Economics and Political Science, UK
Bertil Cottier
University of Lugano, Switzerland
Kwang Bae Park, Hwan Kyoung Ko and Sunghee Chae
Lee & Ko, South Korea
Letícia Silveira Tavares
HewardMills, UK
Helena Wootton
PL&B Correspondent

Published by
Privacy Laws & Business, 2nd Floor, Monument House, 215 Marsh Road, Pinner, Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Korea amends its privacy laws; Greece adopts GDPR law

On 9 January 2020, South Korea's national assembly adopted amendments to its major data privacy laws. This development is interesting in view of Korea's ambitions to be assessed as EU-adequate (p.21). The same scenario applies to India (p.1) although its Bill is at the start of its legislative stages.

Greece's GDPR implementation has lagged behind other EU Member States but we are pleased to publish now a full report on the specifics of this new law (p.1). Some commentators say, however, that the law was rushed through, and there are some shortcomings in the text.

The EU Commission is already looking at whether certain aspects of the GDPR should be updated (p.10) as the development of new technologies, especially AI, poses new challenges on whether it is possible to apply the regulation in this context (p.14). Our Biometric Identification Roundtable is putting recommendations and questions to the UK regulator on the UK Information Commissioner's position regarding achieving a balance between data minimisation and Artificial Intelligence's need for a vast amount of data. Can minimisation, necessity, accuracy, security and ethics be reconciled with these technological developments? (p.29). More on AI and facial recognition on p.27. As the EU debates the route to take, our correspondent analyses existing regulation. The EU white paper on AI was adopted on 19 February just as we were going to print[1].

Facebook is developing an Oversight Board – how will it work and what will be its relevance? Read a report on this topic on p.18 which raises the question of applying good governance principles to such a large and powerful enterprise.

The much-awaited Court of Justice of the European Union Advocate General's Opinion on Schrems II and Standard Contractual Clauses (SCCs) was issued last December. Despite positive messages, SCCs applicability is still limited on a practical level, our correspondent says (p.11). We await the final decision, expected in the first quarter of 2020.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

1. ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 165+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 165+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

"*PL&B Reports* are an invaluable resource to anyone working in the data privacy, e-commerce or digital marketing fields. Unlike many news feeds or updater services, each Report provides rare depth of commentary and insight into the latest developments."

Rafi Azim-Khan, Partner, IP/IT & Head Data Privacy, Europe, Pillsbury Winthrop Shaw Pittman LLP

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.