DIGITALEUROPE

31 AUGUST 2020

An early analysis of *Schrems II* – key questions and possible ways forward

Executive summary

The *Schrems II* ruling of 16 July 2020[1] is of great importance for the future of international data flows under the transfer mechanisms established by the General Data Protection Regulation (GDPR).

The Court's finding that standard contractual clauses (SCCs, also known as standard data protection clauses or SDPCs) are in general valid is significant. As SCCs are the most widely used mechanism for international data transfers, they are essential to a globally interconnected European economy – one where European companies, big and small, can benefit from global trade. It is also vital to an open European economy, where EU-based individuals and organisations are able to choose freely between foreign alternatives.

However, the ruling also places substantial obligations on organisations when using SCCs to transfer data, essentially requiring them to assess whether the receiving country provides equivalent data protections to those guaranteed by EU law, in particular with respect to the destination country's surveillance laws. Many of those affected will be small businesses unable to carry out such an analysis, putting these data flows – and Europe's digital recovery – in jeopardy unless supplementary measures are taken.

This raises new questions for both companies and data protection authorities (DPAs) and makes a correct understanding of the ruling's requirements all the more important lest SCCs – and other transfer mechanisms such as binding corporate rules (BCRs) – be evaluated, in practical terms, as unusable.

This document highlights some of the ruling's immediate implications and suggests options for solutions in line with the Court's judgment. In particular, we highlight:

[1] Case C-311/18

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- A set of possible supplementary measures that organisations can adopt in order to complement the third-country 'self-adequacy' assessment mandated by the ruling. Such measures could include: an analysis of the legal circumstances surrounding the transfer; procedural and organisational steps to limit unnecessary and disproportionate third-country data requests; data protection and security certifications to protect against unauthorised access; transparency reporting; and encryption and/or other technological safeguards.
- The need to include such possible supplementary measures in harmonised guidelines from the European Data Protection Board (EDPB), as well as in the European Commission's upcoming revision of the SCCs, in order to prevent conflicting results from both organisations and DPAs.
- The importance of strengthening other transfer mechanisms such as pan-European codes of conduct, certifications and binding corporate rules (BCRs), as well as DPAs' interpretation of derogations, as these can provide stable and reliable tools for organisations to continue their operations and services in line with the EU's data protection framework.
- Finally, our initial assessment of the prospects for a new US adequacy decision to replace the Privacy Shield, for which we look forward to providing more concrete industry input as negotiations evolve. In short, our assessment is that such a renegotiation is technically possible if the political will is there to do so.

Since this ruling requires cautious assessment, complex discussions and constructive and operational guidance, DIGITALEUROPE calls on DPAs to ensure that any review of data transfers or associated enforcement actions are done in a harmonised and proportionate fashion in recognition of the difficulty of the issues involved.

Table of contents

- Executive summary 1
- Table of contents 3
- The value of standard contractual clauses (SCCs) 4
- What the ruling said 5
- The Privacy Shield and SCC 'self-adequacy' assessments 6
- Possible supplementary measures 7

Other contractual clauses 8

Additional safeguards 8

Encryption 9

- Strengthening other transfer mechanisms 9

Codes of conduct and certification 9

Binding corporate rules (BCRs) 10

Derogations 11

- A new US adequacy decision 11

The value of standard contractual clauses (SCCs)

Today, practically no company, irrespective of sector, would be able to do business, let alone take part in international trade, without the ability to transfer data cross-borders. The EU's global trade success is inextricably bound up with the cross-border flow of data with our trading partners, in both the developed and developing world. SCCs are the principal legal instrument relied on by EU-based businesses for transferring personal data to third countries.

There are currently few, if any, scalable alternatives to SCCs. Codes of conduct and certification mechanisms are not yet available at EU level for the purpose of cross-border transfers and BCRs can only be used for intra-group transfers subject to a long and complex approval procedure.

The extensive use of SCCs means that, in the event they cannot be relied upon, severe disruption will be caused to both EU consumers and EU-based businesses across all industrial sectors. This is particularly acute as our economy attempts to recover from the economic repercussions of the COVID-19 pandemic.

The exact level of the resulting economic damage is difficult to assess. However, as the EU is the world's largest exporter of digitally delivered services, accounting for 24% of the world's total trade in services,[2] the economic consequences of not being able to rely on SCCs for an international free flow of data would be profound.

The following are but a few examples of situations where EU-based companies transfer personal data to third countries based on SCCs:

- Where non-EU subsidiaries need to access information stored by the EU headquarters in Europe, e.g. for daily operations concerning customers or business partners.
- Where a company provides 'follow-the-sun' services (that is, 24/7 services across all time zones), which require different groups located across the world (including within the EU) to have access to and receive information from a single database. For example, an EU firm that seeks to provide financial advice to a US business or consumer would need to transfer data to the US as part of business-to-business or business-to-consumer transactions.
- Where EU companies outsource business processes to third-party service providers located outside the European Economic Area (EEA),

[2] https://ec.europa.eu/eurostat/statistics-explained/index.php/World_trade_in_services

which will involve a transfer of personal data from the EU company to the service provider.

- Where EU companies are owned by a non-EU parent company, and reporting lines and performance management require human resources and client information to be available within the group.
- Cloud services rely on the free flow of data across international borders even where the data are primarily stored in the EU, for example to update or replicate data for security purposes or to increase the speed of data transfers.
- Financial and insurance services, including banks and payment platforms as well as other regulated services, could not certify under Privacy Shield and have relied on SCCs to perform necessary transfers of data worldwide. Many of these companies have reporting requirements, anti-money laundering and sanctions statutes, and financial reporting requirements that cannot be localised.

What the ruling said

In *Schrems II*, the Court of Justice of the EU (CJEU) has set out a variety of core requirements that apply to the use of SCCs.

Crucially, the ruling upholds the general validity of SCCs, which the Court has stated are in principle capable of providing the necessary level of protection on their own. However, in other cases, reliance on SCCs will require a complex case-by-case assessment on the part of data controllers and processors, who may either have to supplement SCCs with additional safeguards or otherwise be unable to transfer the data.

The Court has found that in order to rely on SCCs, controllers and processors, in collaboration with the recipient of the data, should conduct what amounts to a ‘self-adequacy’ assessment of the third country’s legal system, based on the full list of adequacy considerations in Art. 45(2) GDPR and taking into account the specific circumstances of the transfer.

In cases where such assessment reveals that effective protection cannot be guaranteed, in particular because of the risk of undue access by public authorities in the third country, the controller or processor will be able to rely on SCCs only if they can adopt ‘supplementary measures’ that can address the inadequacy risk in the third country by implementing reinforced protection to the transferred data.

The Privacy Shield and SCC 'self-adequacy' assessments

The assessment that controllers and processors will have to undertake as to the third country's legal system is exemplified by the Court's analysis of the EU-US Privacy Shield decision. The Court invalidates the decision based on its finding that US law: a) does not provide for the necessary limitations and safeguards for access by public authorities; and b) does not ensure effective judicial protection against such access.

These two requirements are hence paramount to the 'self-adequacy' assessment that controllers and processors must undertake in order to rely on SCCs for a particular transfer. However, in the absence of an adequacy decision, the determination as to whether any surveillance law meets the legal test concerning the necessary limitations, safeguards and judicial protection will be far from straightforward and go well beyond ordinary due diligence.[3]

Given that such assessments are undertaken by the European Commission through the adequacy mechanism, and that only 12 such adequacy determinations are currently in effect, it seems an extraordinary burden to ask controllers and processors – many of which are small businesses with limited resources – to adjudicate on the national security regimes and judicial redress laws of foreign countries. In effect, this would place a prohibitively large hurdle in front of organisations wanting to transfer data across borders and is therefore a threat to the EU's prosperity and digital economy.

In light of this, DPAs should ensure that any review of data transfers or associated enforcement actions are done in a harmonised and proportionate fashion in recognition of the difficulty of the issues involved.

The obligation for a self-adequacy assessment puts an unprecedented burden on organisations for the following reasons:

- While it is possible to evaluate practices of vendors and customers, the assessment of the legal system of a third country is not a typical task expected from private organisations;

[3] Notably, the secrecy around surveillance generally impinges on people's rights to be notified and access information, which are essential for any remedial action. In some EU Member States, such rights are not provided for at all in law, while in others important restrictions apply related to national security, national interests or the reason behind the surveillance. When it comes to effective judicial protection, although courts can be used in all Member States, general access to justice barriers such as costly and lengthy procedures apply as well as the difficulties surrounding providing evidence. See European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union – Volume II*, May 2018

- Different organisations may assess third-country legal systems differently, leading to conflicting assessments and opposite solutions regarding SCCs that could only be resolved by DPAs, hence putting a great strain on DPAs in turn;
- Data protection authorities may also come up with conflicting assessments of third countries, making a harmonised interpretation needed.[4]

DIGITALEUROPE calls for further clarification on the assessment companies are expected to carry out, as the recent FAQ document by the EDPB did not address the points above.[5]

Possible supplementary measures

The very reliance on SCCs is based on the assumption that, given the absence of an adequacy decision, the third country *does not* ensure an adequate level of protection. In light of the ruling, organisations will hence have to consider what 'supplementary measures' they may need to adopt in order to remedy such inadequacy.

The Court has given no further indications in its ruling as to what may constitute adequate 'supplementary measures.' The Court has only noted that supplementary measures to remedy a third country's inadequacy may consist of: a) other contractual clauses; or b) additional safeguards.[6]

It is therefore crucial to understand what is expected of organisations in order for SCCs to be applicable to their data transfers. Overall, we suggest that such assessment could include one or more of the following elements:

- Legal circumstances surrounding the transfer: assessing whether the data that is subject to the transfer at hand is likely to be covered by relevant third-country legislation[7] and, if not, considering that SCCs would be sufficient without additional safeguards.
- Procedural and organisational: committing to a principles-based approach to examine government demands for data and appropriately narrow and challenge requests which are not necessary and proportionate.

---

[4] See para. 147 of the ruling

[5] https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf

[6] See Recital 109 GDPR and para. 132 of the ruling

[7] For example, Section 702 of the Foreign Intelligence Surveillance Act (FISA) or Executive Order 12333 (EO 12333) for the US

- Certifications: verification mechanisms such as data protection and data security certifications.[8] These can help demonstrate data minimisation and organisational security measures that protect against unauthorised access.
- Transparency: committing to publish a transparency report detailing numbers of accepted and rejected government demands for data.
- Technical: encryption and/or other technological safeguards.

We call upon the EDPB to issue harmonised guidance, following appropriate consultation with industry stakeholders, as well as to allow sufficient time for EU data exporters to properly shift to approved SCCs that will meet the standards set out by the Court.

The European Commission's upcoming revision of the SCCs in light of the GDPR requirements can also provide clarity as to how controllers and processors can carry out their assessment of third-country laws as well as the necessary supplementary measures.

Other contractual clauses

As explained above, further contractual clauses might, for instance, include policies and practices on the part of the data importer in order to adequately scrutinise or otherwise challenge surveillance requests in the third country. Further contractual clauses may also stipulate transparency and technical security measures.[9]

However, as recognised by the Court, clauses cannot, by their very nature, go beyond contractual obligations that can in no case bind third countries' public authorities.[10] Such additional clauses are therefore likely to create conflict-of-law situations and would likely result in the suspension of data transfers or the violation of the laws in the jurisdiction of the data importer.

In light of this, we believe that the Commission's work on the new set of SCCs will be of great value in order to address these issues in a coherent way.

Additional safeguards

As for possible additional safeguards, these may refer to technical and organisational measures that can be implemented to safeguard the transferred

[8] For example, ISO 27701, providing a globally recognised tool for international data transfers

[9] See next section on additional safeguards

[10] Paras 132-133 of the ruling

data from undue access from third-country authorities. Such measures will need to take into consideration the implementation costs and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood of access and severity for data subjects whose data is transferred.

Encryption

Importantly, although not referenced in the final ruling itself, the *Schrems II* proceedings have hinted at the role that encryption may play, both in transit and at rest. Encryption inhibits surreptitious access by governments (e.g. under EO 12333 during transit) and service providers' ability to hand over data (e.g. end-to-end encryption). It can therefore be expected that encryption will be part of the discussion around ensuring a consistent level of protection for international data transfers.

In this context, and in light of recent debates surrounding encryption, it will be vital to protect companies' ability to develop and implement strong encryption solutions, tailored to achieve the best possible data security and privacy. By contrast, mandates on the design of technology, such as the creation of 'backdoors' or requests for key escrow/disclosure, will have direct repercussions on companies' ability to honour the SCC terms and will hence negatively impact the protection of EU data subjects.[11]

DIGITALEUROPE stands ready to foster potential technical solutions for data encryption, in transfer and at rest, but asks for further guidance to address the CJEU ruling in order to avoid conflicting requirements and access requests by national authorities.

Strengthening other transfer mechanisms

The 'self-adequacy' nature of the SCC requirements set out by *Schrems II* also underscores the need to bolster other transfer mechanisms available under the GDPR, as these may prove more stable and reliable.

Codes of conduct and certification

In particular, due to their comprehensive approval and monitoring procedures, codes of conduct and/or certifications could provide an ideal venue to specify

[11] For more background on encryption, please see our position paper *Encryption: finding the balance between privacy, security and lawful data access*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2020/03/DIGITALEUROPE-Position-on-Encryption-Policy-.pdf

what binding and enforceable commitments organisations must comply with when transferring data to non-EEA destinations.

We regret that transfers have not been included in recent EDPB guidance[12] and now urge the European Commission, Member States, DPAs and the EDPB to foster the creation of pan-European codes and/or certifications addressing data transfers.

To the fullest extent possible, we believe such codes and/or certifications should be available to various industry sectors across the EU, rather than focusing on data transfers pertaining to single sectors. This would maximise benefits for all EU-based companies as well as guarantee an equal level of protection to data subjects across the Union.

Binding corporate rules (BCRs)

BCRs are presently the only data transfer mechanism that carries individual regulatory approval, satisfying DPAs that its contractual safeguards can be complied with.

Although the *Schrems II* ruling does not directly address BCRs, the EDPB has already stated that the BCRs should undergo the same re-assessment by companies as SCCs.[13] Since BCRs are approved by the competent DPAs, the application of the company's own assessment to BCRs on top is misleading and leads to confusion. DIGITALEUROPE urges the EDPB to provide clearer reassurance as to BCRs' continued validity and that no further re-assessment of adequacy is necessary.

The bar for BCRs is very high, with a demanding and time-consuming process that currently has a five-year backlog in some Member States. Besides the lead supervisory authority (SA) and the two co-reviewers, also all other DPAs concerned take part in the review of BCRs, which finally have to be approved by the EDPB.

The current process for the creation and implementation of BCRs should hence be reviewed and streamlined in order to make it more accessible. We urge the

[12] See our responses to the relevant EDPB consultations, available at https://www.digitaleurope.org/wp/wp-content/uploads/2019/01/DIGITALEUROPE%20response%20to%20EDPB%20consultation%20on%20draft%20guidelines%20on%20certification.pdf and https://www.digitaleurope.org/wp/wp-content/uploads/2019/04/DIGITALEUROPE-response-to-draft-EDPB-guidelines-on-codes-of-conduct-and-monitoring-bodies.pdf

[13] See p. E of the EDPB FAQ document on the *Schrems II* ruling, available at https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf

setup of a clear and fast-track process to ensure a broader creation and implementation by industry.

Even if BCRs can be made more efficient, their application remains limited. They remain a tool that can only be used for intra-group transfers and not for data that needs to be transferred outside an individual organisation. Companies using BCRs may also need to establish additional SCCs.

Derogations

We urge the EDPB, in the same way it is reconsidering the use and approval of BCRs and other mechanisms, to revisit the narrow interpretation of the derogations under Art. 49 GDPR. The GDPR does not impose such a narrow view as has been taken by the EDPB in its revised guidance. To the contrary, it is urgent that a holistic, forward-thinking and risk-based approach be applied to the whole of Chapter V and its coherence with Art. 3 GDPR to ensure that European businesses are not isolated from international trade.[14]

A new US adequacy decision

The EU and US remain two jurisdictions that, in addition to having strong economic links, are built on the rule of law, with individual rights and freedoms enshrined in their societal values and legal frameworks.

We believe that options are possible for future negotiations with the US government to remedy the invalidation of the EU-US Privacy Shield decision and provide for a long-term transatlantic transfer mechanism that can satisfy the conditions laid down in the *Schrems II* ruling. For this reason, we welcome the prompt announcement from the US Department of Commerce and the European Commission concerning initial discussions for an enhanced transatlantic data transfer framework.[15]

Necessarily, any such negotiations will need to address the two key aspects for the Shield's annulment, that is: a) the limitations and safeguards for access by US public authorities; and b) effective judicial protection against such access.

We recognise that addressing these two aspects might require changes to US law. However, we urge the European Commission, the Member States, the EDPB and the US government to explore whether the relevant provisions could

[14] See our response to the WP29 public consultation on the draft derogations guidelines, available at https://www.digitaleurope.org/wp/wp-content/uploads/2019/01/DIGITALEUROPE%20response%20to%20public%20consultation%20on%20Guidelines%20on%20Article%2049%20of%20Regulation%202016679%20(wp262)[1].pdf

[15] https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en

instead form the object of a specific agreement between the EU and the US that could complement a new adequacy decision.[16]

We also note that the ruling did not address the balance between the legitimate rights and interests across the areas of data protection, economic well-being and national security. We urge the EU and the US to pursue a broader international conversation on these topics, including defining expectations around government surveillance, as part of a long-term progress towards a sustainable solution to the issue of cross-border data transfers.[17]

We stand ready to support, and provide more concrete input towards, genuine efforts to ensure the long-term viability of transatlantic and global data transfers. Absent a credible new mechanism, strengthening the clarity and uptake of the remaining GDPR data transfer mechanisms and derogations will be all the more essential, as outlined in the previous sections.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Martin Bell

Privacy and Security Policy Officer

martin.bell@digitaleurope.org / +32 492 58 12 80

[16] Pursuant to Art. 46(3)(b) GDPR

[17] An example of such discussions is provided by the recent mandate for negotiations on an EU-US agreement concerning law enforcement access and work to develop a new protocol to the Budapest Convention on Cybercrime. See https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/ and https://rm.coe.int/t-cy-2019-19-protocol-tor-extension-chair-note-v3/16809577ff respectively

DIGITALEUROPE

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20