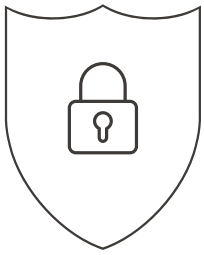
RENAISSANCE numerique

CIVIL LIBERTIES AND ETHICS
JANUARY 2021

SCHREMS II DECISION:

How to break the deadlock?



On July 16th, 2020, with its so-called "Schrems II'' decision, the Court of Justice of the European Union (CJEU) invalidated the deal setting the rules for transatlantic data transfers — the *EU-US Privacy Shield*. In its judgment, the Court estimated that the deal did not guarantee a sufficient protection for the personal data of European citizens[1].

Although the news received a fair amount of media attention when it was released, public interest for the matter has now faded. Still, this decision has put a great number of actors in a long-lasting period of uncertainty and legal insecurity. Among the first to be impacted are European companies: according to a study led by several company federations throughout the European Union, 75% of companies that use Standard Contractual Clauses (SCCs) for international data transfers, regardless of their size, are European[2]. EU citizens are also impacted by this decision, in the sense that they no longer benefit from the data protection mechanism guaranteed by the *Privacy Shield*. Even though the latter was imperfect, it has now been repealed, without anything to replace it.

In this context, Renaissance Numérique organised, on December 16th, 2020, a seminar gathering around thirty actors, including representatives of companies, lawyers, university researchers, MPs and members of the administration. This discussion had two objectives: explore the consequences of this decision by the Court of Justice of the European Union, and consider paths to solve this situation for those concerned by it. This note is fuelled by these exchanges[3].

---

1 "The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield", Court of Justice of the European Union, press release No 91/20, Luxembourg, 16 July 2020 : https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

2 Among the responding companies. "Schrems II. Impact Survey Report", DIGITALEUROPE, BusinessEurope, the European Round Table for Industry (ERT) and ACEA, 26 November 2020: https://www.businesseurope.eu/publications/schrems-ii-impact-survey-report

3 Renaissance Numérique would like to thank all the participants in the seminar of December 16th, 2020 who contributed to this reflection, especially Florence Raynal, Head of the European and International Affairs Department of the *CNIL* (French data protection authority), Théodore Christakis, Professor of International and European Law at Université Grenoble Alpes, Juliette Rouilloux-Sicre, President of the Digital Regulation Committee of the MEDEF (France's largest employer federation) and Etienne Drouard, Partner at Hogan Lovells.

Many concerns relating to the capacity of the actors to implement the "Schrems II decision" have emerged from the discussion. Not only does the decision not provide enough time to the actors for a sensible analysis and an evaluation of the enforceability of the recommendations issued by data protection authorities subsequently, but the decision is also retroactive. Hence, beyond future international data transfers, the conformity of all previous data transfers operated under the *Privacy Shield* since 2016 must be reassessed, hence questioning many current contracts. Some lawsuits have already been filed following the decision, amongst which several are against French companies[4]. However, the results of those procedures and the subsequent legal precedent will most probably not be known before the summer of 2021. Until then, if no political decision is made, many activities will be threatened, at a time when data plays a key role in our economy.

Beyond the legal debate, this decision by the Court of Justice of the European Union weighs strong economic and political aspects that cannot be left to the regulators alone. In an uncertain context, where the position of the next American Administration is not known yet, this situation questions the efficiency of the European model of data protection.

Concerned by this deadlock, Renaissance Numérique, through this reflection, invites the European Commission and Europe's executive power to engage in a dialogue with key stakeholders, in order to establish a shared method for the implementation of the Court's decision.

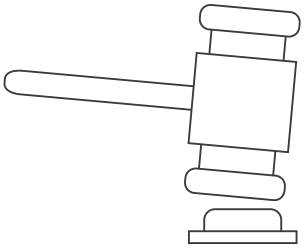
From Schrems I to Schrems II

Although it bears particularly tangible consequences for those concerned, the highly technical nature of the debate seems to be the cause of the lack of political interest. It thus appears crucial to correctly understand the various aspects of the decision.

The Court's judgment follows the implementation of the General Data Protection Regulation (GDPR) in May 2018, which set the following principle: protection must always remain side by side with the data, wherever it is transferred throughout the world. Subsequently, data can only be transferred to those countries that have data protection standards equivalent to

4 The noyb association, founded by Max Schrems, has filed a complaint against several French companies such as Leroy Merlin, Sephora and Decathlon. "La fin du Privacy Shield : sortons les entreprises de cet imbroglio juridique !", Jean-Sébastien Mariez, *JDN*, 21 December 2020: https://www.journaldunet.com/solutions/dsi/1496487-la-fin-du-privacy-shield-sortons-les-entreprises-de-cet-imbroglio-juridique/

those offered in the European Union (EU), except for specific derogations[5]. Several existing tools can provide a similar level of protection, like the European Commission's adequacy decisions such as the *Privacy Shield*, which recognise that the legal framework of the country receiving the data is in conformity with EU law. This protection can also be insured by contracts, such as Binding Corporate Rules (BCR) and *ad hoc* or Standard Contractual Clauses, through certification, or via codes of conduct. A certain number of these transfer tools are being adapted following the decision of July 16th, 2020. However, until now, this process has not led to the issuance of precisions regarding the methods that should be put in place, and just like the decision itself, it offers no solutions for the actors concerned.



The first decision from the CJEU in this domain, which was issued in late 2015 and is referred to as "Schrems I", was linked to a case opposing Austrian activist Max Schrems to Facebook[6]. Max Schrems considered that the *Safe Harbor* — the predecessor of the *Privacy Shield* — did not provide sufficient protection to the data of European citizens which were transferred to the United States by Facebook at the time. During this first ruling, the Court found that the United States did not provide a level of personal data protection that was essentially equivalent to that of the EU. It invalidated the *Safe Harbor* and called on the European Commission to work on a new framework.

Max Schrems' second appeal, which eventually led to the "Schrems II" decision, focused on the Standard Contractual Clauses (SCCs) used by Facebook to manage its data transfers[7]. Indeed, with the *Safe Harbor* no longer in place, Facebook decided to opt for SCCs. The question was, then: do these clauses bring sufficient protection[8]? The Court of Justice of the European Union considered that the standard contractual clauses are valid because they are essentially nothing more than a tool containing contractual obligations that do not pose any problem. The real problem is the link between the contractual obligations and the legal framework of the country receiving the flows of transferred data. What is at stake is the capacity of the company importing data to respect its contractual obligations in spite of local or national laws. The Court's decision thus raises the issue of possible legal conflicts with foreign legal frameworks, most notably with American surveil-

5 "CHAPTER V — Transfers of personal data to third countries or international organizations" Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Further details on the CNIL's website: https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre5#Article44

6 Judgment "C-362/14 — Schrems", Court of Justice of the European Union, 6 October 2015: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=729154

7 Judgment "C-311/18 — Facebook Ireland and Schrems", Court of Justice of the European Union, 16 July 2020: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=729323

8 "Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 – Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems", Court of Justice of the European Union: http://curia.europa.eu/juris/document/document.jsf?docid=204046&text=&dir=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=687087

lance laws[9] which, indeed, do not enable companies importing data to honour their commitments. Until now, the legal reasoning consisted in ensuring that the importing company respected the guarantees provided for contractually. Following the Court's decision, the reasoning has widened, as it must also be ensured that there is no legal conflict with local legislations that may be higher in the hierarchy of norms. This logic applies to all countries and all data protection tools: if one country's legal system is not compatible with the respect of essential guarantees[10], then there cannot be any protection whatsoever.

A strict interpretation by the regulators that weighs heavily on the actors

Following this decision, on November 10th, 2020, the European Data Protection Board (EDPB), which gathers all national data protection authorities in Europe, published an updated version of the "European Essential Guarantees for surveillance measures"[11]. The first version of these guarantees was designed in 2016, when the *Privacy Shield* was negotiated. They are a sort of guide which contains the conditions to be met in case of governmental interference with fundamental rights. Simultaneously, the European board issued another document, recommending measures aimed at completing the set of tools available for international data transfers, that actually respect the level of personal data protection enforced in the EU[12] [13]. This document offers a methodology for organisations transferring and receiving data, when the country's legal framework does not provide sufficient guarantees. These measures can be contractual, organisational or technical, the latter being privileged by the EDPB.

However, this decision places a disproportionately big responsibility on the organisations that transfer data out of Europe, and the EDPB's recommendations appear hardly applicable. On the one hand, technical measures, like encryption, can be significantly costly and could bar many activities from being

9 The judge ruled on the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, which are part of the US legal regime for surveillance.

10 *See below.*

11 "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures", European Data Protection Board, 10 November 2020: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

12 "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", European Data Protection Board, 10 November 2020: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

13 This document was subject to a public consultation until 21 December 2020.

profitable[14]. On the other hand, concerning essential guarantees, the EDPB considers extremely strict criteria. Companies, very small and big ones alike, do not have the means to analyse the surveillance laws of all of the countries where they operate. A legal analysis of surveillance laws can amount up to 250 000 dollars for the US regime alone. It also appears essential that such analyses be shared between all the actors in order to avoid any interpretation errors, which could be very costly.

Finally — and this is probably the greatest limit to the EDPB's interpretation — very few countries actually meet the level of protection that the essential guarantees require, even within the European Union, including France. If one analyses all of the surveillance laws of the members of the Council of Europe that have been brought before the European Court of Human Rights (ECHR), only Sweden passes the test[15]. Moreover, this case is still pending and awaiting a new decision by the Grand Chamber of the Court[16]. In addition, in its decisions of October 6th, 2020 relating to the conservation and transfer of data[17], the CJUE considered that several European member states, including France, did not meet European legal standards when it came to surveillance laws.

At the moment, at least fourteen inquiries against French surveillance laws are being examined[18]. In a twenty-year span, the European Commission has been able to grant an adequacy decision to only eleven countries[19]. Within the latter, whose adequacy status is currently being reviewed, one can ponder if all respect the essential guarantees, such as Israel for example.

In May 2015, during the deliberations around the draft "Surveillance law" in France — which led to the creation of the French CNCTR[20] —, Renaissance Numérique had pointed out the fact that the envisioned legal framework did not provide any independent control nor a judicial one[21], not even effective appeal mechanisms for those concerned. In this regard, the procedural criteria chosen by the European Court of Human Rights in order to meet purpose and proportionality requirements, also put forward by the CJEU in

14 Beyond the cost and depending on the purpose, the risk of encryption or pseudonymisation is also that the data becomes unusable by the recipient.
15 Judgment "Case of Centrum för Rättvisa v. Sweden", European Court of Human Rights, 19 June 2018: http://hudoc.echr.coe.int/eng?i=001-184290
16 Théodore Christakis, ""Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1)", *European Law Blog*, November 2020: https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/
17 Judgments "Case C-623/17" and "C-511/18, C-512/18, C-520-18", Court of Justice of the European Union, 6 October 2020: http://curia.europa.eu/juris/document/document.jsf?docid=232083&text=&doclang=EN&pageIndex=0&cid=698054; http://curia.europa.eu/juris/document/document.jsf?mode=req&doclang=EN&docid=232084
18 "Mass Surveillance", thematic factsheet, European Court of Human Rights, October 2020.
19 "Adequacy decisions", European Commission, 14 January 2019: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
20 *Commission nationale de contrôle des techniques de renseignement*, the French national commission in charge of controlling surveillance techniques.
21 According to law 2015-912 of 24 July 2015.

its Schrems II decision, did not seem satisfactory in the legal framework in place[22].

Even the European institutions, with their high level of legal expertise — which companies cannot access — have proven to be wrong four times in the past: regarding the *Safe Harbor*, the *Privacy Shield*, and the Passenger Name Records (PNR) agreements with the United States[23] and Canada[24]. How could companies possibly be better equipped to meet such requirements? There are two major risks: companies may be tempted to bleed themselves dry with huge legal fees, or to choose not to comply, which would cause great harm to the GDPR and to European citizens.

A decision that goes beyond the sphere of personal data rights

In addition to being strict, these recommendations seem to omit the essential principle of the hierarchy of norms that is at the foundation of law. Behind this decision hides a conflict of sovereignty between states, since it is considered that some countries' laws are unfit to justify a transfer of data to them. What is at stake is the capacity of governments to access data that is protected by foreign rights. Still, no actor can formally promise that they will disobey their country's sovereign legal system. Considering this hierarchy of norms, it appears complicated for Standard Contractual Clauses alone to solve a sovereignty conflict, especially as it would mean overlapping with laws that are superior to them. Analysing this decision therefore requires going beyond considerations around data protection, and to look into other legal disciplines such as international and constitutional law.

On this matter, the Court's decision also raises a fundamental conflict when it comes to human rights, which is the one between surveillance laws and privacy protection. This tension has always existed. These are combinatory rights. What company could possibly refuse to abide by its national laws if

22 The powers given to the CNCTR are mainly to exercise prior documentary control of the formal regularity of the control measures. However, the CNCTR does not have effective powers to control the relevance or proportionality of the intended (*a priori* control) or implemented (*a posteriori* control) supervisory measures. Moreover, the remedies available under the condition of a personal interest to act are rendered meaningless by the confidentiality of the surveillance measures which, by nature, do not allow a person to know whether — or to demonstrate that — they are subject to surveillance measures.

23 "The Court annuls the Council decision concerning the conclusion of an agreement between the European Community and the United States of America on the processing and transfer of personal data and the Commission decision on the adequate protection of those data", Court of Justice of European Communities, 30 May 2006: https://curia.europa.eu/en/actu/communiques/cp06/aff/cp060046en.pdf

24 "The Court declares that the agreement envisaged between the European Union and Canada on the transfer of Passenger Name Record data may not be concluded in its current form", Court of Justice of the European Union, 26 July 2017: https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf

authorities ask it to give away data for security purposes? The European Union hails the GDPR, while other states have their economy and national security at stake. The security-liberty equilibrium is not dealt with by the GDPR, which is a text about freedom. Hence, the interpretation of this decision requires an expertise which goes far beyond that of data protection authorities, which are not constitutionalists nor antiterrorism specialists. The real issue here is one of balancing fundamental rights and of complying with the European Convention on Human Rights. On this matter, the CJEU's decision offers a certain degree of latitude to guarantee such a balance and its enforceability.

This equilibrium becomes even more contentious at a time when more and more legislative initiatives are set up throughout the European Union to organise public authorities' access to encrypted data. An illustration of this tendency can be seen in the resolution on encryption adopted by the Council of the European Union on December 14th, 2020, which aim is notably to allow investigative and judicial powers to access these data[25].

The agenda is now unclear

These issues all relate to the traditional sovereign missions of states, and therefore should be handled by the European Commission and European executive power, as well as by member states. In the meantime, regulators and companies keep rejecting the responsibility to take action on one another, and actors risk being continuously jeopardised by this lasting uncertainty. The question no longer is how to break the deadlock, but who will free the European Union from it. For now, it seems that this issue is being viewed as secondary to the big digital files that are currently being dealt with by the European Commission, such as the *Digital Services Act* and the *Digital Markets Act* published last December. However, it has become urgent to take action.

The Schrems II decision does not offer a grace period giving time for companies to adjust. Renaissance Numérique calls on the European Commission and Europe's executive power to open a dialogue with all stakeholders, in order to deliver a coordinated enforcement of the decision issued by the Court of Justice of the European Union. This dialogue should allow European authorities to gather all relevant expertise, beyond the sole data protection sphere, for instance experts of international and constitutional law or secu-

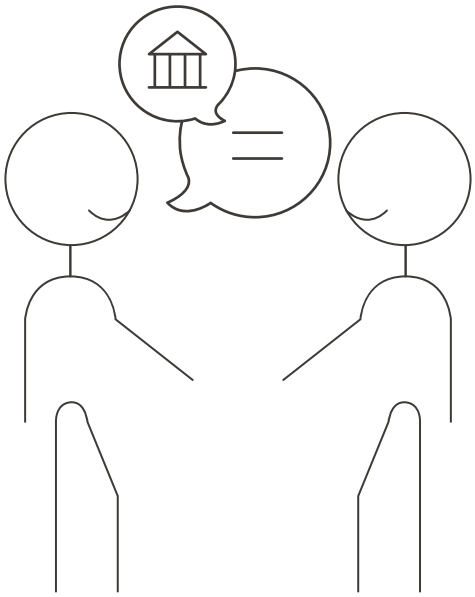
25 "Encryption: Council adopts resolution on security through encryption and security despite encryption", Council of the European Union, 14 December 2020: https://www.consilium.europa.eu/en/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Encryption:+Council+adopts+resolution+on+security+through+encryption+and+security+despite+encryption

rity issues. This would offer the possibility to build a comprehensive set of guidelines in order to identify existing solutions and explore paths to solve the current situation.

This would also allow a deeper assessment of the enforceability of the solutions proposed by the EDPB, and to translate them subsequently into clearer criteria or more tangible solutions for companies.

Within this framework, Renaissance Numérique calls for the development of a proportionate risk approach, taking into account in particular the degree of sensibility of the transferred data. Concerning highly sensible data, reinforced measures could be envisioned, as opposed to less sensible data. This mid-level step could make it possible to break the deadlock, while waiting for a more robust international agreement to be set up.

At a time when digital sovereignty becomes a source of conflict in the digital sphere, a genuine solution can indeed only come from a new international deal with the United States.



Further resources

"The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield", Court of Justice of the European Union, press release n°91/20, 16 July 2020: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

"Recommendations 02/2020 on the European Essential Guarantees for surveillance measures", European Data Protection Board, 10 November 2020: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

"Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", European Data Protection Board, 10 November 2020: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

Théodore Christakis, ""Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers", *European Law Blog*, November 2020, Part 1: https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/; Part 2: https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2; Part 3: https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/

—

Author

Jennyfer Chrétien, Executive Director, Renaissance Numérique

Contributors

Loane Bedouet, Project Assistant, Renaissance Numérique

Etienne Drouard, Partner at Hogan Lovells

Translation

Pol-Euan Lacombe, Project Assistant, Renaissance Numérique

Proofreading

Jessica Galissaire, Studies Manager, Renaissance Numérique

We also thank **Théodore Christakis**, Professor of International and European Law at Université Grenoble Alpes, for sharing his expertise with us.