eco Association and i2Coalition – Transatlantic Dialogue on Data Transfer: Standard Contractual Clauses

Since 2019, the transatlantic dialogue constitutes a joint format for discussion on digitalization topics of high relevance to both the U.S. and the EU, introduced by the European-based **eco – Association of the Internet Industry** (**eco Association**) and the U.S.-based **Internet Infrastructure Coalition** (**i2Coalition**). On 24 September 2021, the latest transatlantic dialogue was held to offer an update on the transfer of personal data and data protection on both sides of the Atlantic, with a particular focus applied to the implementation and impacts of the new set of **Standard Contractual Clauses** (**SCCs**), as approved by the European Commission in June 2021. Especially since the EU/U.S. Privacy Shield was invalidated in 2020, any company or individual wishing to transfer personal data from the EU to the U.S. or other third countries must currently rely on SCCs in order not to risk a violation of data protection law.

The transatlantic dialogue was hosted by **Lars Steffen**, Director International at the eco Association, and brought together representatives of the Internet industry from both sides of the Atlantic.[1] The four guest speakers were: **Thomas Rickert**, Director Names & Numbers at eco and the founder of rickert.law; **Oliver Süme**, Chair of the Board at eco and partner at Fieldfisher; **David Snead**, Co-Founder and Policy Working Group Chair of i2Coalition and General Counsel at cPanel; and **Ann Morton**, Senior Policy Adviser at i2Coalition and Member & Counsel at AP Morton & Company LLC.

GDPR as the framework for transatlantic data transfer

Thomas Rickert provided an initial overview on the global reach of the EU's General Data Protection Regulation (GDPR). Prior to the GDPR's introduction, European lawmakers were troubled by the fact that companies from third countries (i.e., companies not based within the EU) were collecting and processing the data of European data subjects without the option for these data subjects to track where that data was going, to object to its transfer, or to exercise their pre-GDPR privacy rights. This was the rationale for extending the territorial scope of data protection under the GDPR. The consequent primary concept is that controllers and processors within the EU now need to comply with the GDPR, regardless of where the processing takes place. This means that, if they hire somebody or use services from outside of the EU, the processing still needs to occur within the framework of the GDPR. Furthermore, if controllers or processors outside the EU target customer groups or audiences in European Member States and offer goods and services or monitor their behavior, they also need to comply with the GDPR.

As Rickert noted, if a company is undertaking regular business with European partners or is targeting European individuals or businesses, there are few exceptions with regard to the need to comply with the GDPR. There is also an additional clause with which many businesses are unfamiliar: namely, the representative clause. This means that if a business based outside of the EU falls under the GDPR, it needs to appoint a GDPR representative base inside the EU. The logic here is to allow not just European authorities, but also agreed data subjects, to have somebody within the EU with whom they can communicate. This clause is now beginning to be enforced, with one decision already having been made to fine a business without an appointed representative by over 500,000 Euro.

[1] The eco Association/i2Coalition transatlantic dialogue took place as one of a series of roundtable discussions hosted by both associations. Due to Covid-19, on this occasion the dialogue was held virtually as a webinar.

In order to comply with the GDPR, a helpful tool is SCCs. But before examining the SCCs in more detail, **Oliver Süme** proceeded to refer to the general requirements for international data transfer, given that the GDPR basically sets out two very important rules. Firstly, a legal ground is required for any processing of personal data as defined in the GDPR. Secondly, when it comes to international data transfers, an additional legal ground is called for. The most important legal grounds to be found in practice are as follows:

1) **Adequacy Decisions:** A so-called "adequacy decision" applies to certain jurisdictions for which the European Commission has officially confirmed a level of data protection that is similar to that supplied by the GDPR. In such jurisdictions, the adequacy decision is a company's legal ground and no additional measures or other safeguards are required.

2) **Standard Contractual Clauses:** In countries such as the U.S. where the level of data protection has not been confirmed as akin to that set out by the GDPR, there have been two important additional legal grounds that most companies have used in the past. The first of these was the Privacy Shield, which was suspended last year by the European Court of Justice (ECJ). As such, the most important legal ground for international data transfers is now the SCCs, an instrument which has been in place for many years. In viewing this instrument, the European Commission decided some time ago that these SCCs would need an update: firstly, because the GDPR came into effect in May 2018, meaning that the legal environment and the regulatory framework for data protection in the EU experienced a fundamental change and the SCCs needed an associated update in that regard; and secondly, the ECJ's decision to annul the Privacy Shield led to a further required update. The updated set of SCCs is now in place since the implementation decision was made by the European Commission on 4 June 2021.

Old vs. New Standard Contractual Clauses

The graphic below highlights the difference in the structure between the old and new set of SCCs, with the clear merit of the newer set being that of enhanced flexibility and openness.

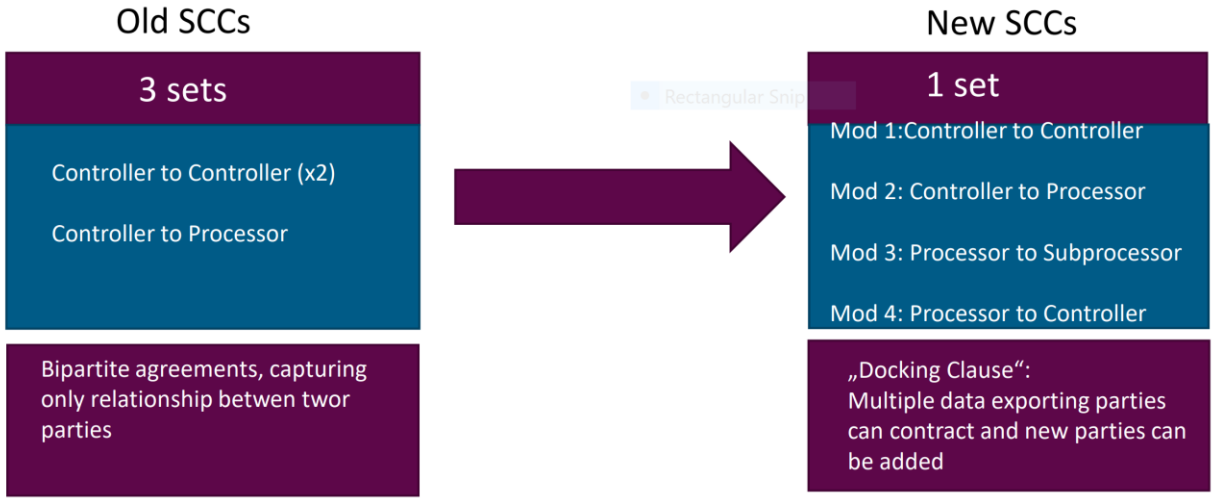

Figure 1: Difference in structure between the old and new SSCs (Source: Süme/Fieldfisher)

As Süme's graphic shows, there were three sets of SCCs in the past. The old SCCs had only a bipartite agreement that captured the relationship between two parties and which did not provide a solution for incorporating additional parties into the SCCs. The new SCC structure comprises just one set, but this provides for much more flexibility because it comprises four different modules

dealing with four different relations between two parties that act as an importer and exporter for data. This effectively makes the new SCCs much more flexible. In addition, one of the aspects of the new SCCs is a so-called "docking clause". This is another instrument that provides for more flexibility, as it enables multiple data exporting parties to contract with each other, and allows new parties to be added to an agreement once it has been signed by the initial signatories. This is of particular value for any group of companies that has to deal with intercompany data flows between a number of entities.

As Süme emphasized, the SCCs are essentially all about "standards". Data flows and the role of parties as controllers or processors have to be considered before putting together the adequate SCC modules. These standards can be put together automatically, with a number of tools existing in the market that can be used in order to create the set of modules relevant for a business's individual combination of importers and data exporters. One tool in this regard, MySCCcreator, was developed by Süme's law firm Fieldfisher. This offers assistance in composing the different modules under the new SCCs. Nonetheless, the need for a business to fulfill an individual part itself is very important, meaning that each business needs to collate a range of information and understand that not everything can be automated within new SCCs. In particular, a core element of the SCCs is a description of the technical and organizational measures that are implemented by the data importer in order to safeguard and protect the transfer of this personal information and personal data. All in all, there is quite an important part of the SCCs that needs to be individualized.

Süme also referred to the so-called transfer impact assessment, which means that a business also needs to carry out an impact assessment that is balancing the risks of a data transfer in the light of the data protection regime of a particular third-party country.

In summing up his input, Süme concluded that while automation is possible and things are becoming more flexible with the availability of far more individual SCCs, the key challenge requiring the most attention is the individual aspects of the SCCs.

Individual facets of the SCCs

In delving into the specific aspects of the SCCs, **Thomas Rickert** commented that the "real fun begins" with annexes and with the data transfer impact assessment. Companies need to describe the parties, the description of the transfer, the nature of the processing, purposes of processing, and retention periods. They also need to identify the supervisory authority that would be competent for the case, which would typically be where the GDPR representative is located. An additional requirement is to address Technical and Organizational Measures (TOMs), which must be described in very specific terms, covering points ranging from pseudonymization, encryption, I.T. security, and data quality to data retention, accountability, data portability, etc.

In particular, Rickert homed in on Clause 14 of the new SCCs, which refers to local laws and practices affecting compliance, and which is the clause where the data transfer impact assessments are visible. Clause 14(a) highlights the Commission's requirement in this regard:

> *"The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data on measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses."*

Rickert acknowledges that this is quite complicated to take on board, particularly given that the Commission proceeds in a footnote to explain that companies should take a look at case law, the previous behavior of governments, and what information has and has not been requested.

A helping hand for supplementary measures

Nonetheless, as Ricket emphasized, there is help in sight for all of the supplementary measures, with this made available by the European Data Protection Board (EDPB), the latter which was established by the GDPR and which is composed of representatives of the EU national data protection authorities. The EDPB's Article 29 Working Party came up with a document that was recently updated in June 2021 and which focuses precisely on the safeguards that need to be worked on when it comes to data transfers. The 50-page document covers, in detail, items such as encryption, as well as technical and organizational measures. In addition, the document contemplates different scenarios with the U.S.'s Foreign Intelligence Surveillance Act (FISA), works through use cases for cloud companies in areas such as data storage, and proposes a suggested methodology on how this can be approached. The core content is:

1. Know your transfers.
2. Verify the transfer tool that your transfer relies on (either SCCs, binding corporate rules or adequacy decisions).
3. Assess third-country legislation relevant to Article 46 GDPR.
4. Identify and adopt the supplementary measures.
5. Take any formal procedural steps that might be required in order to implement those additional steps.
6. Reassess everything after a certain period of time.

Rickert concluded by noting that the new SCCs entered into force on 27 June 2021 and that, on 27 September (three days after the transatlantic dialogue), the old SCCs were to be repealed, meaning that companies could only enter into third party arrangements using the new SCCs. Nevertheless, existing contracts can still be valid until the end of 2022. These include the old SSCs, but it needs to be borne in mind that the ECJ has required companies to add supplemented safeguards to these SCCs.

The business perspective on the Standard Contractual Clauses in the U.S.

In turning specifically to the U.S., **David Snead** provided an overview on how SCCs are being viewed there. While initial relief was evident when the SCCs came out, this has been tempered somewhat by the amount of detail that is required in addressing the SCCs. This is seen to create a great deal of work for businesses that are seeking to be efficient with their contracting processes. For those companies who have clickwrap agreements, the SCCs are regarded as particularly onerous.

From a positive perspective, Snead commented that the GDPR provides a framework for analyzing privacy throughout an organization for businesses throughout the world, and particularly businesses in the U.S. In turn, the SCCs have created a framework that makes customers comfortable and allows them to comply with local laws and, in particular, has created an element of transparency. Snead indicated a positive stance towards the way that the SCCs allow various aspects of business to work together. For example, the transparency policy provides a way for people to look at how responses to U.S. government requests for data are handled, how often that happens, and how businesses respond. These tools can be used to help customers become more comfortable in their compliance with GDPR obligations. It provides information related to business practices, which might address some of the statutory compliance issues related to the U.S. Snead's company is using

disclosures to supplement this, as he believes many U.S. companies are. If Snead were to advise regulators, this supplementary approach is the path he would recommend.

However, Snead also contends that the SCCs create a kind of "Catch 22" for U.S. businesses and talked about a scenario where a business might implement these clauses, create contractual requirements binding it to its customers, and then suddenly get a FISA subpoena. As he put it, he believes that no U.S. court is going to enforce a commercial contract in lieu of requiring compliance with a government order. The fundamental issue that the U.S. and the EU are struggling with has still not been addressed. In looking at surveillance both in the U.S. and the EU, he finds that its interpretations are cultural in nature. He regards this "Catch 22" as something that needs to get resolved at the political, and not at the commercial level.

When it comes to the GDPR, Snead posed a question concerning how many European companies are complying with Brazilian privacy laws, and concluded that associated discrepancies are impacting on companies' willingness to continually reinvent their business practices or their contractual practices in order to accommodate the GDPR. He gave the example of how, at cPanel, where he is General Counsel, his company not only complies with GDPR, but also the California Consumer Privacy Act (CCPA) and other U.S. state obligations. In contrast, he posited that not many EU businesses are complying with California's privacy regulations. He believes that the GDPR and SCCs have created an illusion of transparency, and that only the largest and most zealous organizations are really going to dive into an organization's policies and disclosures. He worries that privacy is very quickly shifting from something that is of fundamental importance to businesses and customers, to just becoming a checkbox exercise.

Snead summarized by reasserting his belief that the GDPR and SCCs are fundamentally beneficial for businesses who are sharing data across the Atlantic. Nonetheless, he is concerned that increasingly complex methods are being used to remedy a problem, and that this needs to get solved at a political level.

The policy perspective on the Standard Contractual Clauses in the U.S.

Ann Morton described the policy approach to privacy in the U.S. as still evolving and not fully formed. While a few states – California, Virginia, and Colorado – have enacted their own privacy laws, a comprehensive and uniform federal policy is not yet in place – a fact that has been repeatedly emphasized by the i2Coalition. In this regard, the i2Coalition is in a process of once again elevating privacy discussions with the U.S. government and their EU counterparts in order to try to solve the issue of the inadequacy finding regarding the Privacy Shield. While no solution yet exists, Morton acknowledged that lessons can be drawn from assessing ongoing implementation of the GDPR in Europe and from the California CCPA. She noted that other states in the U.S. which are considering passage of their own privacy bills are learning from the CCPA, which in turn has drawn on lessons learned from the EU's implementation of the GDPR. Virginia and Colorado are due to come into effect in 2023.

From Morton's perspective, aside from having to comply with European law, one of the challenges in the U.S. is the difficulty presented by the national patchwork of privacy laws. At present, this means that, as a practical matter, companies doing businesses in all of the states frequently must comply with the strictest law. Even if a uniform federal law does come to pass, there will nevertheless be a significant level of cost and uncertainty involved. While in the past several months, federal privacy legislation discussions have accelerated in Congress, especially in light of negotiations being held between the Biden administration and the EU on a replacement for the Privacy Shield, bipartisan consensus on a uniform comprehensive law has not yet emerged.

Morton highlighted the fact that the new Chair of the Federal Trade Commission (FTC), Lina Khan, is extremely active on and knowledgeable about big tech issues in the U.S., especially regarding the intersection of antitrust and privacy. Khan recently received a letter from senior Democrat Senators, led by Senator Blumenthal of Connecticut, which proposed that the FTC should initiate a rulemaking on consumer data privacy which could be conducted in parallel to Congress activity. Such a move by the FTC could also offer a safety valve if Congress does not succeed in reaching consensus and passing the law.

Morton went on to say that a policy-making dynamic very often seen in the U.S. concerns the states tackling issues independently and resembling test environments. For example, California adopted its preferences from the GDPR, while Virginia is following suit with more of a pro-business law. Morton regards Colorado's approach as being somewhat "in the middle", in so far as it is also simulating the elements that it likes from the GDPR, is favoring a risk-based approach, and is limiting its scope to certain businesses that process a specific number of consumers' data and meet a specified revenue threshold.

One way or another, as Morton sees it, these state-based laws provide little assistance and add operational complexity to companies doing business in 50 states or on a global level. This leads to businesses having to question whether they should comply with the strictest law, or whether they should simply abandon markets where compliance with local legislation is too burdensome. Morton drew attention to the massive debate about antitrust and big tech power occurring at present in the U.S., which is having a significant impact on the overall regulatory environment. For companies other than the likes of Google, Facebook, or Amazon, the question concerns what they really have to do to be safe and to avoid risks.

With regard to risks, Morton noted the current enforcement focus on large fines for big tech companies who are either being investigated in relation to antitrust issues, or who in some cases already are being sued under antitrust and competition law by the Department of Justice, the FTC, or the State Attorneys General. Morton stressed that i2Coalition is carefully tracking all of this activity and any ensuing legal court decisions or settlements, given that these outcomes could impact the businesses of i2Coalition members. She highlighted the value of working on these matters with the eco Association to educate policymakers about regulatory impacts and costs for companies that are not the "huge players".

Morton is of the opinion that, while this is not always recognized by the press, there is sentiment within the U.S. government to try to come up with practical, implementable solutions to consumer data privacy. In addition to the letter that some Senate Democrat leaders sent to the FTC in support of a privacy rulemaking, Morton reported that the Senate Commerce Committee will start some hearings at the end of September on general privacy and data security issues at which the Privacy Shield negotiations could be discussed. A planned second hearing will focus on online safety and privacy for children, with the latter fueled by the recent front-page Wall Street Journal reports on Facebook, Instagram, and the mental health impact of social media on children and teens. Nonetheless, as Morton concludes, there is still a difficult road ahead to pass a comprehensive federal privacy bill. This is what makes the SCCs so important in the interim.

The future of data protection legislation in the U.S. and the EU

Following on from the speakers' inputs, **Lars Steffen** proceeded to ask what they thought might be the next steps for evolving data protection legislation in the U.S. and the EU.

Rickert recalled that, while the GDPR was initially derided by many, numerous companies learned to see its value in terms of understanding what and how data was being processed in their systems. This led to a lot of companies upping their game in dealing with data, a development that has been

appreciated by not only lawmakers, but also companies from outside Europe. A range of new privacy laws have emerged in recent years, with more currently in the making; interestingly, many of these are actually copies of the GDPR or resemble certain aspects of the ideas that were enshrined in this regulation. While Rickert acknowledges many issues with the GDPR – for example, the fact that it doesn't make a distinction between small companies and those big companies that can afford to implement all of the requirements – he believes that the GDPR has made a significant contribution to the understanding of data privacy and user rights.

In terms of the perspective between the EU and the U.S., Rickert stressed that the historical context needs to be taken into consideration, given that the data protection regimes in Europe and the U.S. are so different. He believes that European individuals have greater trust in their governments than in companies when it comes to their data. In the U.S., on the other hand, people have greater trust in companies, meaning that an all-encompassing privacy law was previously not required. Nonetheless, the arrival of Safe Harbor was regarded as a big benefit. As Rickert reported, after Safe Harbor was invalidated on the basis of Schrems I, the lawmakers from both sides of the Atlantic came up with privacy issues in record time. However, the Privacy Shield didn't really address the root cause of Safe Harbor's invalidation, meaning that Rickert wasn't surprised that the Privacy Shield was subsequently also invalidated. Ultimately, he is of the view that, until the understanding of privacy converges in the U.S. and the EU, we will repeatedly face the same issue. But what we do know is that, economically, the most important data transfers can take place, and Rickert hopes that new tools will be developed.

David Snead also shared the opinion that the GDPR is worthwhile in the sense that it provides a tool for companies in the U.S. to analyze their privacy practices and where data is. He also agreed that many of the differences between the U.S. and Europe are cultural issues that are not going to just get sorted out diplomatically. He expressed the opinion that the U.S. and the EU have a great deal of shared cultural values which should be borne in mind when talking about how to solve these problems. While the political systems in both areas are not completely aligned, he believes that they have a sufficient level of similarity to allow a way to be found to share data.

In closing, **Ann Morton** added that, in the U.S., there is a current focus on protecting civil rights, and protecting marginal, vulnerable communities and children, even if a comprehensive approach can't be agreed upon. She sees a dynamic in the Congress which acknowledges that a bipartisan agreement in some fashion and with some hard work eventually can be arrived at. Regarding the Privacy Shield negotiations, she believes that the U.S. and EU will work diligently to reach a practical solution, given that they are in line with each other on human rights and other key cultural values and that resolving this issue is important for sustaining robust transatlantic trade.