EU Finalises New Model/Standard Contractual Clauses for International Data Transfers

Date : June 7, 2021

Introduction

The European Commission has now finalised and published new Model/Standard Contractual Clauses for international data transfers. **This article looks at this latest development.**

What's this all about?

Under the previous EU data protection regime and the General Data Protection Regulation (GDPR) international data transfers can only be made in certain ways and subject to various conditions. These include country Adequacy Decisions, Binding Corporate Rules, and, probably the most relied on mechanism, Standard/Model Contract Clauses (SCCs).

SCCs consist of a contract entered into between a data exporter and a data importer that impose certain data protection obligations on both parties. SCCs have long been overdue an upgrade which was given even more of an impetus following the European Court's summer 2020 Schrems ruling which invalidated the EU-US Privacy Shield, which we've written about here https://www.corderycompliance.com/ecj-rules-scc-valid-not-ps/. Some GDPR special terms are used in this note which are defined in our glossary at www.bit.ly/gdprwords.

Late last year the European Commission issued draft revised SCCs which were then subject to a public consultation. These SCCs have now been finalised and officially published.

What are the highlights?

Firstly there's now more work involved with SCCs. It is important to stress that the typical approach that existed under the SCCs under the previous data protection regime (prior to the Schrems 2020 ruling) has now gone – no longer is it a question of simply copying and pasting SCCs, completing a few details and signing off. The new approach considers different scenarios to which different modules can be applied and whilst there are general template-style clauses that can be used each time, extra work will still need to be undertaken for each deal especially as regards doing country (and party) due diligence along with putting in place applicable safeguards (whether legal and/or technical). This is the double due diligence test which we've spoken of in our film here http://www.bit.ly/pshielddead.

The new SCCs consist of the following:

- Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council; and,
- Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

Under these decisions:

- The new SCCs are in force from 27 June 2021;
- The existing sets of EU SCCs (i.e. under the previous data protection regime) are repealed as from 27 September 2021;
- Contracts concluded on the basis of what will become the repealed SCCs remain valid until 27 December 2022 "provided the processing operations that are the subject matter of the contract remain unchanged and

that reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards", and "[i]n the event of relevant changes to the contract, the data exporter should be required to rely on a new ground for data transfers under the contract, in particular by replacing the existing [SCCs] with the [new SCCs]."

The key aspects of the SCCs themselves are as follows:

- The new SCCs combine general clauses with a modular approach to cater for various transfer scenarios;
- The basic four types of transfer scenarios under the SCCs are: data controller to data controller; data controller to data processor; data processor to data processor; and, data processor to data controller;
- In addition to using general clauses, data controllers and processors will need to select the module applicable to their situation in order to customise their obligations under the SCCs to their role and responsibilities in relation to the data processing in question;
- It should be possible for more than two parties to adhere to the SCCs. Additional data controllers and processors should be allowed to accede to the SCCs as data exporters or importers throughout the lifecycle of the contract that they are a part of;
- In terms of transparency, data subjects should be provided with a copy of SCCs concerning them and be informed about the categories of personal data processed, the right to obtain a copy of the SCCs in question, and any onward transfers;
- Onward transfers by a data importer to a third party in another third country are only allowed if the third party accedes to the SCCs "if the continuity of protection is ensured otherwise" or in specific situations such as where the data subject gives explicit and informed consent;
- Subject to some exceptions, in particular for some obligations that exclusively concern the relationship between the data exporter and data importer, data subjects should be able to rely on, and where necessary enforce, the SCCs as third-party beneficiaries;
- Whilst the parties are able to choose the law of one of the EU Member States as the governing law for the SCCs, that (governing) law must allow for third-party beneficiary rights;
- In order to facilitate individual redress, the SCCs require the data importer to inform data subjects of a contact point and to deal promptly with any complaints or requests;
- In the event of a dispute between the data importer and a data subject seeking to rely on their rights as a third-party beneficiary, the data subject can lodge a complaint with the relevant Data Protection Authority (DPA) or refer the dispute to the relevant courts in the EU;
- The data importer must agree to respond to enquiries, submit to audits and comply with the measures adopted by a DPA, including remedial and compensatory measures;
- The data importer also has the option of offering data subjects the opportunity to seek redress before an independent dispute resolution body, at no cost;
- Data subjects can be represented by associations or other bodies in disputes against the data importer if they so wish;
- The SCCs set out clauses addressing liability between the parties and with respect to data subjects and about indemnification between the parties;
- Where a data subject suffers material or non-material damage as a consequence of any breach of the third-party beneficiary rights under the SCCs, they are entitled to compensation;
- For data transfers to a data importer acting as a processor or sub-processor, the SCCs require the data importer to make available all information necessary to demonstrate compliance with the obligations set out in the clauses and to allow for and contribute to audits of its processing activities by the data exporter;
- Where a sub-processor is engaged by a data importer, the SCCs set out the procedure for general or specific authorisation from the data exporter and the requirement for a written contract with the sub-processor ensuring the same level of protection as under the clauses;
- Different safeguards will need to be applied in the SCCs according to the specific situations in question where an EU-established data processor transfers data to its data controller, reflecting GDPR obligations for data processors;
- The parties must be able to demonstrate compliance with the SCCs, notably through documentation about data processing activities;
- The SCCs must provide for specific safeguards in light of the summer 2020 European Court Schrems ruling, especially on how to deal with requests from public authorities in that country for disclosure of

transferred personal data;

- There should be a warranty to say that there is no reason to believe that the laws in the importer country prevent the importer from fulfilling its obligations under the SCCs;
- Parties should take account of the specific circumstances of the transfer, such as the content and duration of the contract, the nature of the data to be transferred, the type of recipient, the purpose of the processing, along with the relevant laws and practices of the third country of destination and any safeguards put in place to supplement those under the SCCs. Effectively this will be a Transfer Impact Assessment (TIA) – a bit like a Data Protection Impact Assessment but looking at the transfer and destination of the data.;
- As regards the impact of the relevant laws and practices of the third country on compliance with the SCCs, different elements may be considered as part of an overall assessment, including reliable information on the application of the law in practice such as case-law and reports by independent oversight bodies, along with the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer;
- The data importer must notify the data exporter if, after agreeing to SCCs, it has reason to believe that it is not able to comply with the SCCs. If the data exporter receives this notification or otherwise becomes aware that the data importer is no longer able to comply with the SCCs, it must identify appropriate measures to address the situation. The data exporter is also required to suspend the transfer if it considers that no appropriate safeguards can be ensured;
- Where possible, the data importer is to notify the data exporter and the data subject if it receives a request from a public (including judicial) authority under the law of the country of destination for disclosure of personal data transferred pursuant to the SCCs – the data importer is to also notify them if it becomes aware of any direct access by public authorities to such personal data; and,
- If, following a review of the legality of a request from a public authority, the data importer concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the third country of destination it should challenge it.

What about Brexit?

Following Brexit the UK is no longer part of the EU so the new EU SCCs will not apply to data transfers from the UK to elsewhere; we've written and made films about Brexit and data protection here https://www.corderycompliance.com/brexit-uk-vs-eu-gdpr-faqs/ and here https://www.corderycompliance.com/dt-after-brexit/ and here https://www.corderycompliance.com/dp-after-brexit/. The UK will however be adopting its own set of SCCs in due course and is expected to publish draft SCCs this summer which will then be subject to a public consultation. It won't be surprising if the UK SCCs closely resemble the EU ones.

What about enforcement?

Enforcement of the data transfer rules is a hot topic at the moment particularly with the recent announcement that German DPAs had agreed on a questionnaire based approach as a prelude to enforcement (see https://bit.ly/gerenforce). We have also had activity in other countries including a suspension of data transfers to Cloudflare despite SCCs being in place (see https://bit.ly/schremsport). Data transfer is one of our 5 key themes of the first 5 years of GDPR enforcement. You can find out more about this and watch our film here https://bit.ly/GDPR5film.

What are the takeaways?

Plenty of work will need to be done to ensure compliance. The following will need to be considered:

1. Consider reviewing all of your existing SCCs to be able to replace them and prepare a methodology to do this – the new modular approach will require time and resources to adapt to. You might also want to cross-reference your data map or GDPR Art. 30 records of processing to make sure there are no transfers left out;
2. Whilst the transition period until the end of 2022 might seem a long time many organisations will either have many existing SCCs to eventually replace or plenty of new ones to introduce so make time to make the

changes and prioritise the order of the ones to change. Bear in mind also that if a contract between parties is renegotiated or otherwise changed during that transition period the new SCCs are the ones that will have to be (immediately) applied and the work required to then change to the new SCCs will have to be turned around quickly;

3. When putting together your new SCCs take care because the SCCs cannot be modified "*except to add or update information in the Annexes [concerning details about the data exporter and importer, the description of the data transfer, the technical and organisational measure (TOMs) in place, and, the list of sub-processors]. This does not prevent the Parties from including the [SCCs] laid down in [the SCCs] in a wider contract, and to add other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the [SCCs] or prejudice the fundamental rights or freedoms of data subjects*" – it may be best to use outside counsel to help with this task;
4. Data importers and exporters should review their processes and systems (TOMs) to ensure that personal data is kept secure;
5. Data exporters should review their contracts to ensure that data importers will inform them about data breaches without undue delay and in sufficient detail;
6. Data importers should ensure that they have adequate procedures to retain (for a limited time only), delete and/or return personal data;
7. Procedures to document compliance will need to be set up including a TIA process. Data exporters should consider creating or adapting questionnaires to send to data importers to do due diligence on the data importers about the laws and practices of the country where personal data is to be sent to and to do due diligence on the data importers themselves;
8. Data importers should consider developing or revising procedures to handle data requests made by public authorities – having a process in place to make sure any requests from law enforcements etc. are dealt with at the appropriate level may make a data exporter's TIA easier;
9. Even if you are able to rely on your existing SCCs you must still have done your summer 2020 European Court Schrems ruling due diligence with respect to them;
10. Remember your transparency obligations. Some privacy policies for example specifically refer to the old set of SCCs. You may need to review internal and external privacy policies too. Data importers and exporters should create procedures to inform data subjects about SCCs and to be able to supply them with SCCs either redacted or in summary form.

More information

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. It includes a monthly call to keep up-to-date with GDPR changes across the EU. GDPR Navigator also includes films, template and written guides on topics including:

- Accountability and Audit
- Geographical reach
- Data Controller or Data Processor – what do these terms mean and which are you?
- Fine determination – work out what the consequences of a breach might be
- Appointing processors – how to reduce your risk
- One-stop-shop – determine who your regulator will be
- Binding Corporate Rules
- The security provisions of GDPR

For information about our Cordery GDPR Navigator tool please see http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/

We report about data protection issues here: https://www.corderycompliance.com/category/data-protection-privacy/.

The new EU model/standard clause can be found here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2021:199:TOC

For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/ and our Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary.

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd
Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com