Google Cloud

Google Cloud's Approach to European Standard Contractual Clauses

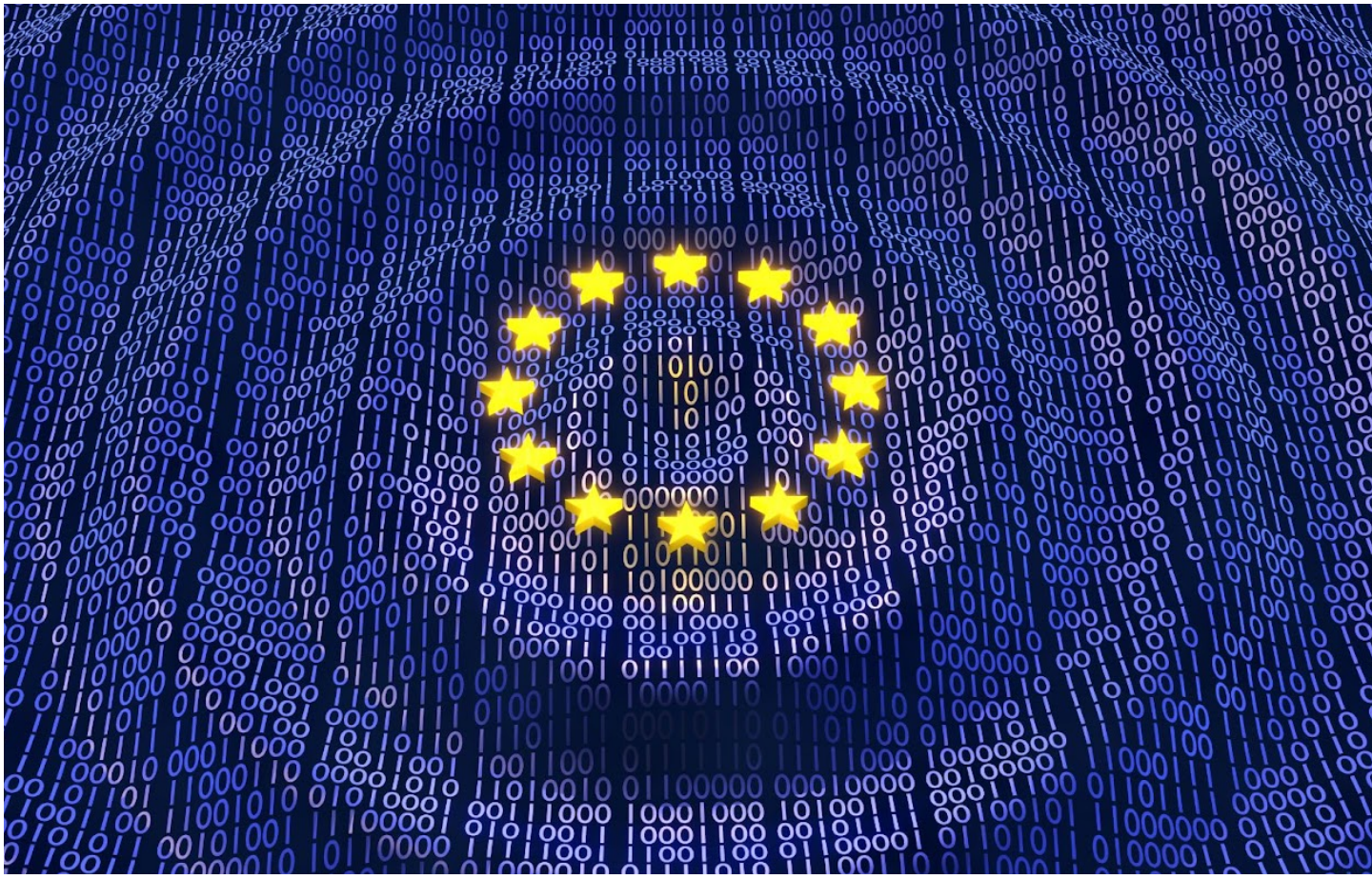

Table of Contents

DISCLAIMER: The content contained in this document is correct as of September 2022. This paper represents the status quo as of the time it was written. Google Cloud's products, security policies, and systems might change going forward as we continually improve protection for our users.

Executive Summary

- Our data processing terms for Google Cloud Platform, Google Workspace (including Workspace for Education) and Cloud Identity enable appropriate modules of the EU Standard Contractual Clauses (SCCs) issued by the European Commission in June 2021 to be applied.
- Our SCC modules may also be applied to UK and Swiss data, in the case of UK data through use of the UK Information Commissioner's International Data Transfer Addendum that became effective in March 2022.
- This paper explains the law underpinning Google's approach to SCCs, and specific details of Google's implementation of those clauses, so that our customers and partners can understand what this approach means for them and their privacy compliance.

Introduction

For years, Google Cloud customers and partners have relied on Standard Contractual Clauses ("SCCs"), previously approved by regulators, to legitimize overseas transfers of their Google Cloud personal data under European data protection laws. Google Cloud offered these clauses alongside the Data Processing and Security Terms ("DPST") for Google Cloud Platform ("GCP") customers and partners and the Data Processing Amendment ("DPA") for Google Workspace (including Workspace for Education) and Cloud Identity customers.

On 4 June 2021, the European Commission issued modernized SCCs for transfers of personal data under the EU's General Data Protection Regulation (the "EU GDPR"). These EU SCCs replaced the SCCs previously approved under Data Protection Directive 95/46 (which were also known as "Model Contract Clauses" or "MCCs"), marking the start of a new era for data transfer compliance. Google introduced the modernized EU SCCs into its compliance offering for new and existing GCP customers and partners, Google Workspace customers and Cloud Identity customers in September 2021.

Then, on 21 March 2022, the UK Information Commissioner's international data transfer addendum (the "UK Addendum") became effective, enabling the use of EU SCCs in amended form for transfers of personal data under the UK version of the EU GDPR (the "UK GDPR"). Google added the UK Addendum to its compliance offering for those customers and partners in September 2022, at the same time as it merged the DPST and DPA into a combined Cloud Data Processing Addendum (the "CDPA").

This paper outlines the rules for data transfers under the EU GDPR, the UK GDPR and the Swiss Federal Data Protection Act ("FDPA") (together, "European Data Protection Law") and explains how Google has implemented the modernized SCCs, including the UK Addendum. It is intended to help customers and partners understand how these SCCs apply to transfers of their Customer Personal Data or Partner Personal Data (as defined in the CDPA).

Note that, for simplicity, all subsequent references to "customers" include GCP partners and to "Customer Personal Data" include "Partner Personal Data".

Also note that the contents of this paper are intended for informational purposes only, and not as legal advice. Anyone who needs legal advice relating to use of Google Cloud services should consult a lawyer.

1. Data Transfers under European Data Protection Law

a. Transfers to third countries generally restricted

The EU GDPR protects the personal data of individuals in the "home territory" of the European Economic Area (the "EEA"). It governs any processing of their data "in the context of the activities of an establishment of a controller or a processor"[1] in that home territory, as well as any processing by a controller or processor located outside the home territory if the processing relates to the offering of goods or services to individuals in the territory or to the monitoring of their behaviour within the territory[2].

Under the EU GDPR, personal data relating to EEA individuals can only be transferred to a foreign country (referred to as a "third country") if an appropriate level of data protection can be ensured there, and only if appropriate protection in that third country is ensured via specifically prescribed transfer solutions[3].

The UK GDPR and Swiss FDPA each impose similar restrictions, with their respective home territories being the UK and Switzerland.

However, if data is shared between two entities (e.g. a controller and a processor), both located within a home territory, no transfer solution is required because the EU GDPR, UK GDPR or Swiss FDPA, as applicable, will bind both entities such that appropriate data protection can be assumed. For example, if Party A located in France (an EEA country) shares personal data with Party B located in Ireland (also an EEA country), no transfer solution is required under the EU GDPR.

---

[1] Article 3(1) of the EU GDPR states:

> *This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*

[2] Article 3(2) of the EU GDPR states:

> *This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
>
> > *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
> >
> > *(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*

[3] The EU GDPR also provides for a limited number of exceptions, which apply in narrow use cases.

b. Transfers to adequate countries permitted

One type of transfer solution is a formal decision by the relevant regulatory authority that an adequate level of protection is ensured by a third country or specified sectors within that third country (as was the case with the EU-U.S. Privacy Shield, before its invalidation).

As of the publication date of this paper:

- those countries approved as adequate for purposes of the EU GDPR are listed here, and include the UK, Switzerland, Israel, Japan (private sector organizations only), New Zealand, Argentina, Uruguay and Canada (commercial organizations only);
- those countries approved as adequate for purposes of the UK GDPR are listed here and include the EEA, Switzerland and the countries identified above as adequate for EU GDPR purposes; and
- those countries approved as adequate for purposes of the Swiss FDPA are listed here (see those countries in the "List of countries" with an "X" in the "Niveau adéquat pour des personnes physiques" column) and include the EEA and the UK.

If personal data is transferred to a country (or entity) deemed adequate under applicable European Data Protection Law, no additional transfer solution is needed, as the transfer will already comply with applicable transfer rules under European Data Protection Law.

For example, if Party C located in the UK transfers data to Party B located in Ireland, no additional transfer solution is required because Ireland (as part of the EEA) is deemed adequate under the UK GDPR. However, if Party B located in Ireland wants to transfer personal data to Party D in the United States, a transfer solution will be required because the United States has not, as of this paper's publication date, received an adequacy decision under any European Data Protection Law.

c. SCCs as a transfer solution

SCCs are another prescribed means of ensuring appropriate safeguards for EEA/UK/Swiss personal data transferred to third countries that are not already deemed adequate under applicable European Data Protection Law[4].

In order to serve their purpose, any SCCs must be used without modification[5] and entered by:

one party (referred to as the "data exporter") who is located in a home territory or otherwise responsible under applicable European Data Protection Law for the transfer of personal data to a third country considered "non-adequate" under that law; and

another party (referred to as the "data importer") who is located in that third country and receives the transferred data from the data exporter.

[4] Article 46 of the EU GDPR, which permits the use of Standard Contractual Clauses, makes clear that such clauses are intended for use only "in the absence of a decision pursuant to Article 45(3)", i.e. an adequacy decision.

[5] Clause 2 of the SCCs permits the addition of other clauses or further safeguards, provided that they do not contradict, directly or indirectly, the SCCs or prejudice the fundamental rights or freedoms of data subjects.

Different versions or modules of SCCs have always been structured according to whether each of the data exporter and data importer is a controller or processor of the data being transferred.

So, to continue the example above, Party C in the UK would be unable to use SCCs to legitimize the transfer of data to Party B in Ireland, because Ireland has already been approved as providing adequate protection under the UK GDPR (rendering an additional transfer solution redundant). However, if Party B in Ireland transfers data to Party D in the United States, SCCs can be used as the transfer solution, unless the United States or Party D is subsequently approved as adequate, at which point any SCCs in place between Party B and Party D could fall away.

d. Schrems II decision

Note that, following the decision of the Court of Justice of the European Union in the so-called "Schrems II" case, a data exporter intending to rely on SCCs may need to conduct due diligence with respect to the laws applicable in destination third countries and consider the use of certain "supplementary measures" (e.g. encryption), depending on those laws. For more information about the Schrems II decision and its implications for Google Cloud customers, please see the Safeguards for International Data Transfers with Google Cloud whitepaper.

2. Modernized EU SCCs

The modernized EU SCCs issued by the European Commission on 4 June 2021 come in four "modules" and have been specifically designed to cover a wider range of situations than the old MCCs.

Those modules, and the intended roles of the parties to them, are as follows:

Two modules designed for use in the same circumstances as the old MCCs, namely:

- Controller-to-Controller (C2C or Module 1) SCCs, which have never been relevant for Google Cloud customers since Google is a processor, not a controller, of Customer Personal Data; and
- Controller-to-Processor (C2P or Module 2) SCCs, which assume the exporting controller is instructing the importing processor; and

Two completely new modules, namely:

- Processor-to-Processor (P2P or Module 3) SCCs, which assume the exporting processor is instructing the importing processor; and
- Processor-to-Controller (P2C or Module 4) SCCs, which, unusually, assume the importing controller is instructing the exporting processor, and impose lighter obligations than the other modules.

All four modules were updated (as compared to the old MCCs) to reflect the EU GDPR, as well as the Schrems II decision.

3. Use of Modernized EU SCCs for Swiss and UK Purposes

With the introduction of the UK Addendum in March 2022, all four modules of the modernized EU SCCs may now be used, with certain amendments, for transfers subject to the Swiss FDPA or UK GDPR. (Prior to March 2022, the modernized EU SCCs had not been approved for UK GDPR purposes.)

4. Google Cloud's Previous Approach to MCCs

Google is a processor of Customer Personal Data, so historically offered C2P MCCs - rather than the only previous alternative, i.e. C2C MCCs - to protect transfers of that data to third countries in the absence of any applicable adequacy decision.

To ensure that customers in the EEA, UK and Switzerland entered those C2P MCCs with a data importer located in a third country, the counterparty to the Google Cloud C2P MCCs offered globally was Google LLC, located in the United States. This meant that, for example, if a customer based in Germany needed MCCs, it entered those with one entity (i.e. Google LLC, located in the United States) while entering a separate processing agreement (i.e. the DPST/DPA) relating to the same data with another entity, namely, its EEA-based Google service provider (i.e. as identified in the customer's Cloud agreement).

For European and other customers whose Google service provider (as identified in their Cloud agreement) is not Google LLC, the result was a dual contract structure involving overlapping instructions to two different Google entities, aggregated liability and third party beneficiary rights. Due to the lack of any available P2P MCCs, this structure was commonly used across industry, including when customers (i.e. data exporters) were processors.

5. Google Cloud's Updated Approach to SCCs

For Google Cloud customers subject to European Data Protection Law, the modernized EU SCCs removed the need for the complex structure described above, and allowed Google to align its approach to SCCs more closely with potential data flows, instructions from customers and the roles of the parties involved.

However, because various scenarios require specific modules of the modernized EU SCCs to be in place, Google has implemented three modules of those SCCs, plus the UK Addendum (in the form of an additional annex to the EU SCCs), as necessary to support customers' and Google's compliance with European Data Protection Law. Google has also introduced a requirement for customers who are *not* located in Europe, the Middle East or Africa (together "EMEA") to indicate (or "certify") if European Data Protection Law applies to them, so that Google can ensure the appropriate SCCs are entered.

Google's modernized SCCs therefore apply depending on:

1. whether or not the Google service provider (as identified in the customer's Cloud agreement) and customer are each located[6] in a home territory or a third country considered adequate under the relevant European Data Protection Law; and

2. for non-EMEA customers only, whether the customer has certified that European Data Protection Law applies to its use of Google Cloud services, as further described below.

We elaborate on this approach in the context of the various possible scenarios below, using the term "adequate" to encompass both home territories *and* third countries benefiting from adequacy decisions under the applicable European Data Protection Law.

The legal terms that implement this approach are in Sections 10.2 (Restricted European Transfers) and 10.3 (Certification by Non-EMEA Customers) of the CDPA.

Please review the scenario below that applies to you, as well as the certification requirements (for non-EMEA customers) and the relevant legal terms:

- Customers in the EEA, UK or Switzerland
- Customers in Adequate Countries outside the EEA, UK or Switzerland with Google Service Providers in Adequate Countries (e.g. customers in Israel, Japan, Canada and New Zealand)
- Customers in Non-Adequate countries with Google Service Providers in Adequate Countries (e.g. customers in the Middle East (excluding Israel) and Africa)
- Customers in Adequate or Non-Adequate Countries with Google Service Providers in Non-Adequate Countries (e.g. customers in Argentina, Uruguay and the United States)

[6] To determine where a customer is located for purposes related to the modernized SCCs, we use its billing address (as we do to determine the identity of its Google service provider). To determine where a Google service provider is located, we use the registered address of the relevant provider, as listed at https://cloud.google.com/terms/google-entity.

a. Customers in Adequate Countries with Google Service Providers in Adequate Countries

i. Customers in the EEA, UK or Switzerland with Google Service Providers in Adequate Countries

Customers located in the EEA, UK or Switzerland are inevitably subject to European Data Protection Law when they use Google Cloud services[7] but, because their Google service provider is in an adequate country (e.g. Ireland, which is considered adequate under the UK GDPR and Swiss FDPA), these customers can transfer Customer Personal Data to their Google service provider, and receive data from it, without needing to enter SCCs or certify. Instead, the P2P SCCs - which Google service providers in adequate countries enter with subprocessors, and publish for transparency - allow Google to assume responsibility for subsequent transfers of Customer Personal Data to subprocessors in non-adequate countries.

For all Google Cloud customers in the EEA, UK or Switzerland, this approach means streamlined contracts and simplified (and transparent) data transfer compliance that is aligned with potential data flows, with Google assuming all the obligations imposed by the P2P SCCs, including the data exporter's due diligence obligations with respect to third country laws. Google will also continue to offer the supplementary measures and maintain the Schrems II resources described in the Safeguards for International Data Transfers with Google Cloud whitepaper.

ii. Customers in Adequate Countries outside the EEA, UK or Switzerland with Google Service Providers in Adequate Countries

1. Customers Subject to European Data Protection Law

Customers who are located in adequate countries outside the EEA, UK or Switzerland, and whose use of Google Cloud services is subject to European Data Protection Law, do not need to enter SCCs to transfer or receive Customer Personal Data if their Google service provider is also in an adequate country. Instead, these customers can rely on their Google service provider to legitimize subsequent transfers via the published P2P SCCs entered with subprocessors (provided that, in the case of non-EMEA customers, they have certified as described below). This applies for Google Cloud customers in Israel, Japan (for private sector customers), Canada (for commercial customers) and New Zealand, for example. Again, for these customers, Google's approach means streamlined contracts and simplified data transfer compliance.

2. Customers Not Subject to European Data Protection Law

Google's implementation of SCCs does not directly impact customers who are located in adequate countries outside the EEA, UK or Switzerland, whose Google service provider is in an adequate country, and whose use of Google Cloud services is *not* subject to European Data Protection Law. However,

[7] Limited exceptions may apply, for example in the case of NGOs who have immunity under treaty.

non-EMEA customers in this category should bear in mind that if at any point their use of Google Cloud services becomes subject to European Data Protection Law, they will need to certify immediately, as described below.

b. Customers in Non-Adequate Countries with Google Service Providers in Adequate Countries

If a customer is located in a non-adequate country and has a Google service provider located in an adequate country, that customer does not need SCCs when transferring Customer Personal Data to its Google service provider, even if the customer is using Google Cloud services subject to European Data Protection Law.

However, when a Google service provider is located in an adequate country (e.g. Ireland), European Data Protection Law obliges that service provider to use the P2C SCCs when transferring Customer Personal Data to its customers in non-adequate countries, regardless of whether the data relates to European individuals.

The CDPA therefore automatically applies the P2C SCCs to any Google Cloud customer who is located in a non-adequate country and whose Google service provider is in an adequate country. For example, the P2C SCCs apply automatically to Google Cloud customers in the Middle East (excluding Israel) and Africa, without these customers needing to certify.

Note that even if a customer in this category is processing Customer Personal Data on behalf of others (rather than on its own behalf)[8] or is a true processor under European Data Protection Law, the P2C SCCs are more suitable for use in these circumstances than the P2P SCCs, because the latter assume that the data exporter issues instructions to the importer, while the reverse is true here (i.e. the customer as data importer issues instructions to its Google service provider as exporter).

While the P2C SCCs impose lighter obligations than other modernized SCC modules, customers entering them are responsible for the importer's obligations under these clauses (with their Google service provider assuming the exporter's obligations).

[8] Strictly speaking, if a customer in a non-adequate country is not itself subject to European Data Protection Law, it can be neither a processor nor a controller, since those concepts derive from European Data Protection Law.

c. Customers in Adequate or Non-Adequate Countries with Google Service Providers in Non-Adequate Countries

i. Customers Subject to European Data Protection Law

Where a Google Cloud customer has a Google service provider in a non-adequate country (e.g. the United States) and is using Google Cloud services subject to European Data Protection Law, then regardless of whether the customer is located in an adequate or non-adequate country, the customer will need to enter the appropriate module(s) of the modernized SCCs with its service provider to legitimize transfers of its Customer Personal Data. The CDPA therefore automatically applies those SCCs (including the UK Addendum) to these customers once they certify as described below.

For example, if a customer in the United States is a controller of Customer Personal Data under the EU GDPR (e.g. because it offers goods to EEA residents), it will need to use the EU C2P SCCs when transfering Customer Personal Data to its Google service provider in the United States. Or if a US customer is a controller of Customer Personal Data under the UK GDPR (e.g. because if offers goods to UK residents), it will need to use the EU C2P SCCs, as amended via the UK Addendum, when making those transfers. In either case, the customer will need to certify.

Similarly, if a US customer is a processor of Customer Personal Data under the EU GDPR (e.g. because its processing activities relate to the offering of goods to EEA residents), it will need to use the EU P2P SCCs for these transfers (*in addition to* the EU C2P SCCs if it is both a processor *and* controller under the EU GDPR). And if that customer is also a processor under the UK GDPR, it will also need to use the UK Addendum. In any of these scenarios, the customer will need to certify.

The same will apply for customers who are controllers and/or processors in adequate countries such as Argentina or Uruguay, because their Google service provider is in the United States. Those customers too will need to certify if their use of Google Cloud Services is subject to European Data Protection Law.

Once any customer with a service provider in a non-adequate country does certify that it is subject to European Data Protection Law, the customer automatically enters all appropriate SCCs (including the UK Addendum) with its Google service provider. Particularly for customers whose service provider is not Google LLC, the result is a simpler contract structure than applied previously, since customers always enter SCCs with the same Google entity as they instruct under the CDPA (i.e. their Google service provider), allowing their Google Cloud agreements to incorporate all applicable SCCs.

Certifying customers who enter the modernized SCCs are responsible for the exporter's obligations under the applicable clauses (with their Google service provider assuming the importer's obligations), and may need to conduct due diligence and consider supplementary measures in light of the Schrems II decision. Google will continue to offer the supplementary measures and maintain Schrems II resources described in the Safeguards for International Data Transfers with Google Cloud whitepaper.

ii. Customers Not Subject to European Data Protection Law

Google's implementation of SCCs does not directly impact Google Cloud customers whose Google service providers are in non-adequate countries (regardless of whether the customers are in adequate or non-adequate countries) and whose use of Google Cloud services is *not* subject to European Data Protection Law. However, customers in this category should bear in mind that if at any point they become subject to European Data Protection Law, they will need to certify immediately, as described below.

6. Certification

To ensure that appropriate SCCs are entered as and when required, all customers outside EMEA whose use of Google Cloud services is subject to any European Data Protection Law (e.g. because they offer goods or services to EEA, UK or Swiss residents, or monitor their behaviour, or because their processing activities relate to such offers or monitoring), need to certify, via the admin console, that they are subject to European Data Protection Law. They also need to identify their competent European data protection authority/ies, via the admin console. Instructions for both steps are here for Google Cloud Platform and here for Google Workspace (including Google Workspace for Education) and Cloud Identity.

Conclusion

The modernized SCCs have significantly evolved, as compared to the MCCs issued under Directive 95/46. Google welcomes this progress, particularly the fact that suitable SCCs now exist for a wider range of use cases. We recognize, however, that the multiple SCC modules, and their implications for customers - depending on their and their Google service provider's locations, and the interplay between those locations and adequacy decisions - has introduced new complexity.

We trust that this paper clarifies our new approach to data transfers, and believe that Google Cloud's closer alignment of the modernized SCCs with the potential data flows involved in our services - and with the roles of the parties involved - will ultimately help to simplify and reinforce compliance for our customers, while maintaining the high level of protection of Customer Personal Data they have come to expect.

Additional information about Google Cloud and privacy compliance is available at the Google Cloud Privacy Resource Center.