Google Cloud Whitepaper
November 2025

Google Cloud's Approach to European Data Transfers

Table of Contents

Executive Summary

- The Cloud Data Processing Addendum (CDPA) offers Google Cloud customers[1] the protection of either an "Alternative Transfer Solution" (as defined by the CDPA) or Standard Contractual Clauses (SCCs) for transfers of their Customer Data[2].
- Since September 2023, Google has adopted the EU-U.S. Data Privacy Framework (DPF) as an Alternative Transfer Solution to legitimize certain transfers subject to the EU's General Data Protection Regulation (EU GDPR).
- Since September 2024, Google has adopted the UK Extension to the DPF and the Swiss - U.S. Data Privacy Framework as Alternative Transfer Solutions to legitimize certain transfers subject to the UK version of the GDPR (UK GDPR) and the applicable Swiss Federal Act on Data Protection Act (Swiss FADP) respectively.
- This paper explains the basic requirements for European data transfers and how the solutions adopted by Google enable and simplify lawful transfers.

Introduction

This paper outlines the rules for data transfers under the EU GDPR, the UK GDPR and the Swiss FADP ("European Data Protection Law") and explains how Google complies with them using Alternative Transfer Solutions, while relying on SCCs in limited circumstances.

This paper is intended to help customers using Google Cloud Platform (GCP), Google Workspace including Google Workspace for Education, Looker (original), SecOps Services, Implementation Services and other Google Cloud services understand how their Customer Data is protected when transferred to third countries that have not been approved as providing adequate protection by the European Commission, the UK Secretary of State, or any other relevant authority, as applicable.

---

[1] A partner version of the CDPA applies to partners reselling GCP, Looker (original) and SecOps Services, but this paper uses the term "customers" to refer to both customers and partners.
[2] The EU GDPR, UK GDPR and Swiss FADP, as well as Section 4 (Data Transfers) of the European terms in Appendix 3 (Specific Privacy Laws) of the CDPA, all apply to "Customer Personal Data". However, for the sake of brevity, this paper uses the term "Customer Data" throughout, including to refer to "Partner Data" and "Partner Personal Data" (as those terms are defined in the Partner CDPA).

Note that this paper is intended for informational purposes only, and not as legal advice. Any customer needing legal advice relating to Google Cloud services should consult a lawyer.

Outline of Legal Rules

a. Transfers to third countries

The EU GDPR protects the personal data of identified or identifiable natural persons ("data subjects") in the "home territory" of the European Economic Area (EEA). It governs any processing of their data "in the context of the activities of an establishment of a controller or a processor"[3] in that home territory, and 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[4].

Under the EU GDPR, personal data relating to EEA individuals can only be transferred to a country outside the EEA (a "third country") if an appropriate level of data protection is ensured in that country as specifically contemplated by Chapter V of the EU GDPR[5]. The UK GDPR and Swiss FADP 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 processor), both in the same home territory, no transfer solution is required because applicable European Data Protection Law will bind both entities such that appropriate protection can be assumed.

b. Transfers to adequate countries

One type of transfer solution permitted by European Data Protection Law is a formal decision by the relevant authority[6] that a third country ensures an adequate level of protection.

As of the publication date of this paper:

- those countries approved as adequate under the EU GDPR are listed here, and include the UK, Switzerland, Israel, Japan, South Korea, New Zealand, Argentina, Uruguay and Canada (commercial organisations only);

---

[3] 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.*"

[4] 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.*"

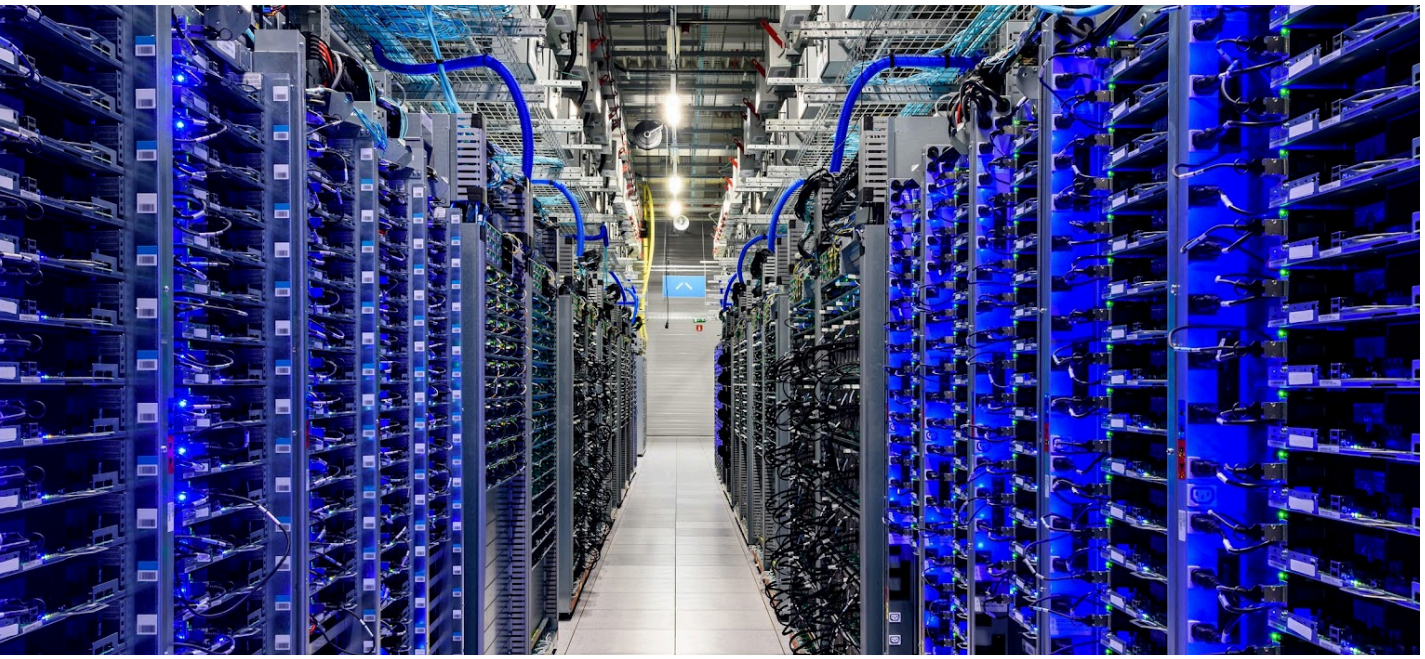
[5] The EU GDPR also provides for a limited number of exceptions, which apply in narrow use cases.

[6] Such decisions are adopted by the European Commission (in the EU), the UK, the Secretary of State (in the UK), and the Swiss Federal Data Protection and Information Commissioner (in Switzerland).

- those countries approved as adequate under 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 under the Swiss FADP 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 third country deemed adequate under the relevant European Data Protection Law, no additional transfer solution is needed, as the transfer will already comply with applicable transfer requirements.

Moreover, where an adequacy assessment has been made by the relevant authority (as reflected in an adequacy decision), there is no requirement under European Data Protection Law for customers (or Google) to complete such assessments themselves.



c. *Other transfers based on adequacy*

Another type of transfer solution permitted by European Data Protection Law is a formal decision by the relevant authority that an adequate level of protection is ensured by an opt-in compliance regime within a third country, as applies in the case of the DPF.

The DPF is an opt-in certification scheme for U.S. organisations, enforced by the U.S. Federal Trade Commission and Department of Transportation, and administered by the Department of Commerce. It includes a set of enforceable principles and requirements that must be certified to, and complied with, in order for U.S. organisations to join the DPF. These principles take the form of commitments to data protection and govern how participating organizations can use, collect and disclose personal data. They include the Accountability

for Onward Transfer Principle which permits onward transfers of personal data by participating organizations subject to compliance with the conditions specified.

The DPF has been operative since July 2023, when the European Commission decided that an adequate level of protection was maintained by the DPF for EEA personal data. The DPF has also been upheld by the General Court of the European Union, which in September 2025 dismissed a challenge to its validity[7].

Similarly:

- the UK Extension to the DPF has been operative since September 2023, when the UK Government decided that an adequate level of protection was maintained by the DPF for UK personal data; and
- the Swiss-U.S. Data Privacy Framework has been operative since August 2024, when the Swiss Federal Council decided that an adequate level of protection was maintained by that Framework for Swiss personal data.

Where an adequacy assessment has been made by the relevant authority (as reflected in an adequacy decision), there is no requirement under European Data Protection Law for customers (or Google) to repeat such assessment.

d. Transfers based on SCCs

SCCs are a means of ensuring appropriate safeguards for EEA/UK/Swiss personal data transferred to third countries, where those countries (or organisations within those countries) are *not* considered adequate under applicable European Data Protection Law[8].

To serve their intended purpose, SCCs must be used without modification[9] and entered by:

- one party (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 the "non-adequate" third country; and
- another party (the "data importer") who is located in the non-adequate third country and receives the transferred data from the data exporter.

Different modules of SCCs may be used, depending on whether each of the data exporter and data importer is a controller or processor of the data being transferred. Those modules are as follows:

- Controller-to-Controller (C2C) SCCs, which have never been relevant for Google Cloud customers since Google is not a controller of Customer Data;

---

[7] See Case T-553/23, Latombe v Commission.
[8] Article 46 of the EU GDPR, which permits the use of SCCs, 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.
[9] 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.

- Controller-to-Processor (C2P) SCCs, which assume the exporting controller is instructing the importing processor;
- Processor-to-Processor (P2P) SCCs, which assume the exporting processor is instructing the importing processor; and
- Processor-to-Controller (P2C) SCCs, which, unusually, assume the importing controller is instructing the exporting processor, and impose lighter obligations than other modules.

SCCs impose contractual obligations on both the data exporter and data importer. For example, depending on the module used, SCCs may require both parties to complete transfer impact assessments. They may also require the data exporter to implement "supplementary measures" (a term derived from the decision of the Court of Justice of the European Union in the so-called "Schrems II" case[10], and used to refer to certain contractual, technical or organisational safeguards), depending on the outcome of the data exporter's transfer impact assessment.

Google Cloud's Approach

Google retains various modules of the EU SCCs in the CDPA, as well as UK and Swiss versions of those SCCs, but Google Cloud's SCCs only apply to transfers of EEA/UK/Swiss Customer Data that are *not* covered by Alternative Transfer Solutions. For details, see Section 4 (Data Transfers) of the European terms in Appendix 3 (Specific Privacy Laws) of the CDPA. These European terms include a commitment from Google to inform customers if Google adopts (or ceases to adopt) an Alternative Transfer Solution.

a. DPF coverage

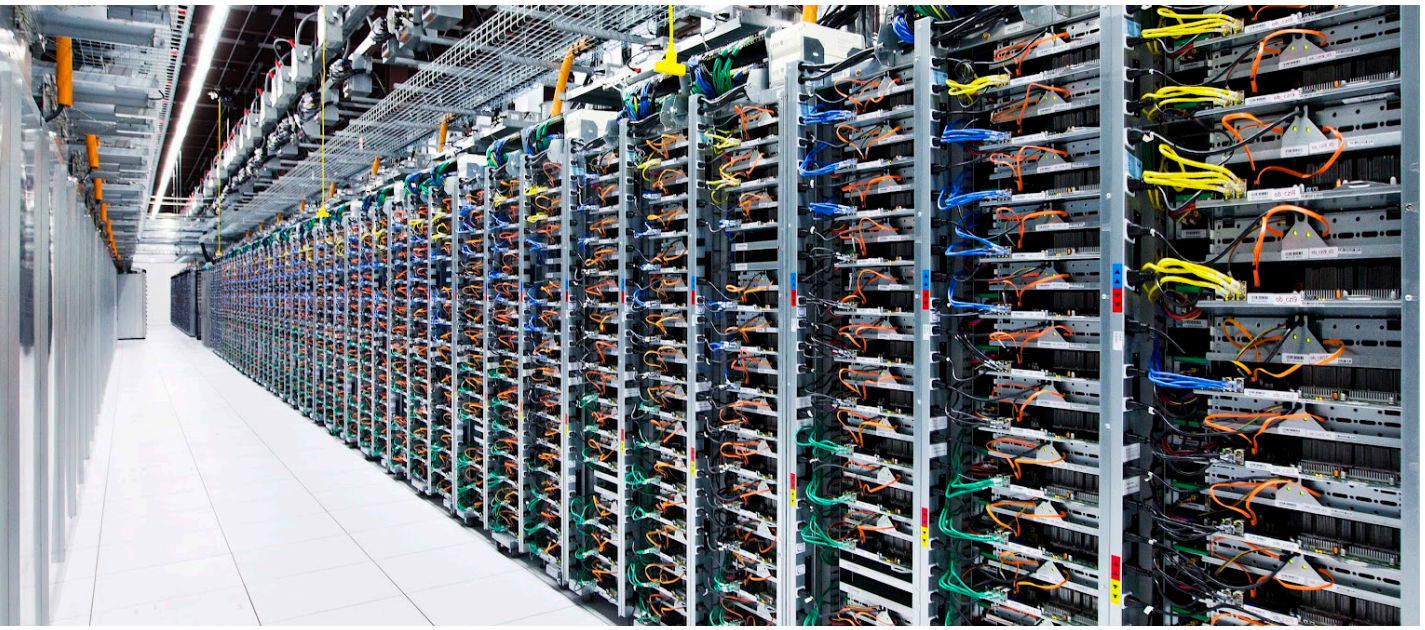
In September 2023, Google informed customers (via this page) that it had adopted the DPF as an Alternative Transfer Solution for EEA Customer Data transferred to or onwards from the United States. Google was able to adopt the DPF in this way because Google LLC (located in the U.S.) has certified its compliance with the Principles and requirements of the DPF. Given the European Commission's adequacy decision for the DPF including all its Principles, EEA Customer Data transferred to or onwards from Google LLC is considered adequately protected.

Similarly, in September 2024, Google informed customers (via this page) that it had adopted:

- the UK Extension to the DPF as an Alternative Transfer Solution for UK Customer Data transferred to or onwards from the U.S., in reliance on Google LLC's certification to the DPF; and

[10] See Case C-311/18, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems.

- the Swiss - U.S. Data Privacy Framework as an Alternative Transfer Solution for Swiss Customer Data transferred to or onwards from the U.S., in reliance on Google LLC's certification to that framework.



b. SCC coverage

Given the Alternative Transfer Solutions adopted as described above, and Google LLC's central role in engaging Google Cloud subprocessors, as of the publication date of this paper Google Cloud's SCCs apply *only* in the following two scenarios:

- where the customer is located[11] in the Middle East (including Turkey, excluding Israel) or Africa and contracts with Google Cloud EMEA Limited (GCEMEA) as its service provider:
    - in this scenario, European Data Protection Law obliges GCEMEA to use the EU P2C SCCs when transferring Customer Data to the customer, regardless of whether the data relates to European data subjects, and the CDPA automatically applies those SCCs; and
- where the customer contracts with a service provider (other than Google LLC) located in a non-adequate country *and* the customer's processing of Customer Data via Google Cloud services is subject to European Data Protection Law (as certified by the customer, if required by the CDPA, as further described below):
    - in this scenario, since the customer's use of Google Cloud services is subject to European Data Protection Law, the customer needs to enter the appropriate

[11] To determine where a customer is located, we use its billing address (as we do to determine its Google Cloud service provider). To determine where a Google Cloud service provider is located, we use the address of the relevant provider given at https://cloud.google.com/terms/google-entity.

SCC module(s) with its service provider to legitimize the transfers of Customer Data that are *not* covered by Alternative Transfer Solutions, and the CDPA automatically applies the appropriate SCCs once the customer certifies if required;
- for example, if a GCP or Google Workspace customer located in Australia is a controller of Customer Data under the EU GDPR, the customer needs to use the EU C2P SCCs when transferring Customer Data to Google Australia Pty Ltd (its service provider) and needs to certify because the CDPA requires certification for GCP and Google Workspace.

In all other scenarios - including for all customers located in the EEA, the UK, Switzerland and the U.S. - a combination of adequacy decisions for third countries and Google's adoption of Alternative Transfer Solutions will mean that Google Cloud's SCCs do *not* apply.

c. *Certification*

To ensure that appropriate SCCs are applied when required, Google requires all GCP, Google Workspace and Cloud Identity customers who are located outside Europe, the Middle East and Africa (EMEA) and whose use of the relevant services is subject to European Data Protection Law to certify as such via the admin console. They also need to identify their competent European data protection authorities, via the admin console, as described here for GCP and here for Google Workspace and Cloud Identity. For details, see Section 4.2 (Certification by Non-EMEA Customers) of the European terms in Appendix 3 (Specific Privacy Laws) of the CDPA. Customers using other Google Cloud products are not required to certify, nor are GCP, Google Workspace or Cloud Identity customers located in EMEA.

Conclusion

Google's adoption of Alternative Transfer Solutions - namely the DPF, the UK Extension to the DPF and the Swiss-U.S. Data Privacy Framework - for transfers of Customer Data to and from the U.S. simplifies compliance with European transfer rules for many Google Cloud customers (while retaining SCCs for others[12]). It means that customers located in the EEA, the UK and Switzerland - as well as U.S. and other customers whose Google Cloud service provider is Google LLC - no longer rely on SCCs to legitimise transfers of their Customer Data under European Data Protection Law. It also means that U.S. and other customers whose Google Cloud service provider is Google LLC are no longer bound by SCC obligations related

[12] For customers in the Middle East (including Turkey, excluding Israel) and Africa, EU Processor-to-Controller SCCs will automatically apply, even if the customers are not processing European personal data. For customers in other non-adequate third countries whose service provider is *not* Google LLC *and* who use Google Cloud services to process EEA/UK/Swiss personal data, SCCs will apply to a limited extent (alongside one or more of Google's Alternative Transfer Solutions, which will apply to certain onward transfers of customers' data), only if the customers certify that they are subject to EEA/UK/Swiss data protection law as required by the CDPA.

to transfer impact assessments or supplementary measures[13].

We trust that this paper clarifies Google's approach to data transfers, and reinforces Google's continued commitment to privacy compliance and protection of customers' data. Additional information about Google Cloud and privacy compliance is available at the Google Cloud Privacy Resource Center.

Google Cloud
November 2025

[13] Customers may still decide to complete transfer impact assessments and/or implement supplementary measures for other compliance purposes.