COMCAST BUSINESS

Comcast Business Transfer Impact Assessment
Fact Sheet for Data Exporters

Last updated on: November 16, 2023

Overview

The EU GDPR, the UK GDPR, and the Swiss Federal Act on Data Protection (FADP) (collectively "**European Data Protection Law**") contain rules on the transfer of personal data to recipients located outside the European Economic Area ("**EEA**"), the UK, and Switzerland. Under these rules, you may transfer personal data to a country that is subject to an adequacy decision issued by the competent governmental body in each of these jurisdictions. If the recipient is located in a country that is not subject to an adequacy decision, you must put in place appropriate safeguards such as the European Commission's Standard Contractual Clauses ("**SCCs**") or the UK's International Data Transfer Addendum to the European Commission's Standard Contractual Clauses (the "**UK Addendum**") and carry out a Transfer Risk Assessment before transferring data to that recipient.

The European Commission has adopted an adequacy decision for transfers from the EEA to recipients in the United States that have self-certified under the new EU-US Data Privacy Framework (the "**EU-US Adequacy Decision**"). However, Comcast Business has not certified under this Framework. Instead, customers in the EEA, the UK, and Switzerland (collectively "**Europe**") must implement appropriate safeguards in respect of transfers to Comcast Business. To this end, Comcast Business enters into a Global Data Protection Addendum ("**GDPA**") with each customer which incorporates the SCCs and where applicable, the UK Addendum. This document provides information to help Comcast Business customers (as "**data exporters**") conduct data transfer impact assessments in connection with their use of Comcast Business Solutions. Information about Comcast Business's privacy compliance program is available at the Comcast Business Privacy Center.

Step 1: Map the Transfer

Comcast Business enters into an GDPA with each customer. Pursuant to this GDPA, Comcast Business processes personal data as a data processor, under the control of the Comcast customer who acts as a data controller. The GDPA incorporates the SCCs and the UK Addendum and includes:

- a description of Comcast Business's processing of customer personal data (*e.g.,* purposes, categories / types of data processed, data subjects, and transfers);
- a description of Comcast Business's technical and organizational measures (Comcast Business's template is available at the Comcast Business Privacy Center);
- a list of Comcast Business's subprocessors (Comcast Business's template is available at the Comcast Business Privacy Center).

In order to use our services, you will be required to transfer personal data to Comcast Business located in the United States or directly to our affiliates and third party service providers. If you transfer personal data directly to Comcast Business, we may transfer this data to our third party service providers or sub-processors. The destination of these transfers will depend on the particular Comcast Business Solutions you use, as outlined in the chart below.

Solution	**In what countries does Comcast Business process customer personal data?**
Mid-Market SD-WAN	

	• United States
Managed Enterprise SD-WAN	
Managed Enterprise Router	• Countries in which a customer is using a Comcast Business Solution
Managed Enterprise VPN	
Managed Enterprise Firewall	
Managed Enterprise Wireless / LTE	• Countries in which Comcast Business's subprocessors operate
Managed Enterprise WiFi	
Managed Enterprise Unified Threat Management	

Step 2: Identify Transfer Mechanism

Where personal data is transferred from the EEA to Comcast Business, Comcast Business relies upon the EU SCCs as the lawful transfer mechanism. Where personal data is transferred from Switzerland, Comcast Business relies upon the EU SCCs, amended to reflect the FADP.

Where personal data is transferred from the UK to Comcast Business, Comcast Business relies upon the EU SCCs and the UK Addendum as the lawful transfer mechanism.

Where this personal data is transferred between Comcast Business group companies or transferred by Comcast Business to third-party subprocessors, Comcast Business relies upon separate SCCs entered into with those parties, in conjunction with the UK Addendum where UK transfers are involved.

Step 3: Assess Sufficiency of Transfer Mechanism

In line with guidelines from the European Data Protection Board, which are also relevant for the UK and Switzerland, the following aspects of US law should be considered in conducting a Transfer Impact Assessment:

1. Are US laws clear, precise and accessible, specifically this includes:
2. Are there necessary and proportionate grounds for public authorities to exercise powers to access personal data
3. Is there an independent oversight mechanism in place
4. Are there effective remedies for relevant individuals

The EU-US Adequacy Decision provides analysis in relation to aspects of the above:

Processing by US public authorities relating to criminal law enforcement
Recitals 90-118 of the EU-US Adequacy Decision sets out US laws relating to access and use of personal data by US public authorities for criminal law enforcement purposes. Recitals 91-106 provide an overview of US law relating to laws allowing access to personal data and the grounds upon which such access is based. Recitals 107-111 outline the oversight that federal criminal enforcement agencies are subject to, and recitals 112-118 outline the redress available to individuals who are subject to such processing, including the possibility to lodge requests or complaints with criminal law enforcement bodies as well as judicial redress avenues.

Processing by US public authorities relating to national security purposes

Recitals 119-200 of the EU-US Adequacy Decision outline US laws relating to access and use of personal data by US public authorities for national security purposes. Recitals 120-126 outline the US legal framework, including the issuance of Executive Order 14086, which (according to recital 124), strengthens the conditions, limitations and safeguards that apply to all intelligence activities. Recitals 127-154 outline the limitations and safeguards in respect of the collection of personal data for national security purposes, including that such activities must be based on statute or Presidential authorisation and in compliance with US law, including the Constitution. Recital 131 outlines that such activities must only be conducted to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorised. Recitals 154-160 outline the safeguards that processing of personal data collected by US intelligence agencies is subject to. Recitals 160-175 outline the oversight mechanisms which US intelligence agencies are subject to, including the requirements of Executive Order 14086. Recitals 175-200 outline the redress available to data subjects to bring legal action before an independent and impartial tribunal with binding powers.

It is also worth noting that the EDPB Information Note states "[the] EDPB underlines that all the safeguards that have been put in place by the US Government in the area of national security (including the redress mechanism) apply to all data transferred to the US, regardless of the transfer tool used". Although Comcast Business has not certified under the DPF, Comcast Business customers may rely on the above sections of the EU-US Adequacy decision in establishing that an adequate level of protection is afforded to the personal data transferred pursuant to the GDPA and that consequently, no supplementary measures are required.

Step 4: Identify Supplemental Technical, Contractual, and Organizational Measures

- Comcast Business's **Technical Measures** are set out in each customer GDPA (Comcast Business's template is available at the **Comcast Business Privacy Center)**.

- Comcast Business's **Contractual Measures** are set out in each customer GDPA (Comcast Business's template is available at the **Comcast Business Privacy Center)**, and include:

    - **Technical and Organizational Measures:** Comcast Business is obligated both under European data protection law and also contractually, to have in place appropriate technical and organizational measures to safeguard personal data.

    - **Transparency:** Comcast Business is contractually obligated to notify the relevant customer(s) when it has received a government request for customer personal data. If prohibited from providing such notification Comcast Business is contractually obligated to challenge such prohibition and seek a waiver.

    - **Actions to challenge access:** Comcast Business is contractually obligated to evaluate the legality of any government request for customer personal data and challenge it where appropriate.

- Comcast Business's **Organizational Measures** are set out in each customer GDPA (Comcast Business's template is available at the **Comcast Business Privacy Center**).

Step 5: Evaluate Adequacy of Supplemental Measures

In light of the information provided in this document—including Comcast Business's practical experience dealing with government requests, and the technical, contractual, and organizational measures Comcast Business has implemented to protect customer personal data—Comcast Business considers that the risks involved in receiving and processing in the United States personal data from Europe do not impinge on our ability to comply with our obligations as a data importer under the SCCs or to ensure that individuals' rights remain protected. Accordingly, no additional supplementary measures are necessary at this time.

Step 6: Reassess Evaluation at Regular Intervals

Comcast Business will review and, if necessary, reconsider the risks involved and the measures it has implemented to address changing data privacy regulations and risk environments associated with transfers of personal data from Europe.

Legal Notice: Customers are responsible for making their own independent assessment of the information in this document. This document: 1) is for informational purposes only, 2) represents current Comcast Business Solutions and practices, which are subject to change without notice, and 3) does not create any commitments or assurances from Comcast Business and its affiliates, suppliers, or licensors. The responsibilities and liabilities of Comcast Business to its customers are controlled by Comcast Business agreements, and this document is not part of, nor does it modify, any agreement between Comcast Business and its customers.