FREQUENTLY ASKED QUESTIONS

Data Transfers - Transfer Impact Assessments

This frequently asked questions (FAQ) document is designed to provide information in relation to VMware's obligation to undertake Transfer Impact Assessments (TIAs) for third country transfers, where VMware is relying upon SCCs or BCRs to transfer personal data outside of the EEA, Switzerland or the UK.

This includes where:

1. VMware as a controller engages a third-party vendor or service provider to process personal data on its behalf.
2. VMware acts as a processor of Customer Content in relation to a specific Service Offering or Support & Subscription Services.
3. VWware as a processor engages a sub-processor to process Customer Content in relation to a specific Service Offering or Support & Subscription Services.

Further information about VMware's existing BCRs for Processors and how VMware responded to the Schrems II decision may be found in the VMware Trust Center FAQs.

Q. What is Schrems II?

A. On July 16, 2020, the Court of Justice of the European Union (ECJ) invalidated the EU-US Privacy Shield in Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (called "*Schrems II*"). The Court confirmed further the European Commission's Standard Contractual Clauses (SCC) provide a legitimate mechanism for transferring personal data to the US and globally, but indicated additional steps would be required to be taken by data exporters established in the EU to ensure adequate protection of EU personal data prior to any international transfers. The EDPB guidelines detail these additional steps.

Q. What are these additional steps?

A. Prior to the transfer of EU personal data outside the EU to a country that does not have an adequacy decision from the European Commission, the data exporter must conduct a Transfer Impact Assessment – evaluate the relevant aspects of the data importer's legal system, in particular any access by public authorities to the data transferred – to determine if there is anything in the law and/or practices of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools being relied upon.

Q. What countries currently have an adequacy decision?

A. Andorra, Argentina, Canada*, Faroe Islands, Guernsey, Israel, Isle of Man, Japan**, Jersey, New Zealand, Republic of Korea, Switzerland, Uruguay, and the United Kingdom. If any of these countries are the recipients of EU personal data, a Transfer Impact Assessment is not required.

*only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA. For more details please see the EU Commission's FAQs on the adequacy finding on the Canadian PIPEDA.

**only covers private sector organisations.

Q. What is a Transfer Impact Assessment?

A. The data exporter of EU personal data is responsible for assessing whether the laws and practice of the recipient (importing/destination) country impact on the effectiveness of the appropriate safeguards provided by the data transfer tools available under Article 46 of the General Data Protection Regulation (GDPR), such as the SCCs. This assessment is known as a Transfer Impact Assessment. The Transfer Impact Assessment focuses on two key aspects of the laws and practices of the recipient country. Firstly, whether the SCCs are enforceable in the recipient country. Secondly, whether the recipient country's regime is such that there is a risk that that EU personal data may be subject to, or accessible under, the country's surveillance regime.

Data Transfers - Transfer Impact Assessments

Q. What if the Transfer Impact Assessment shows a gap in protection?

A. Where the assessment shows that the safeguards are not guaranteed, that is, where there is a gap in protection between what the SCCs provide for and the rule and application of laws in the recipient country, the exporter and importer can adopt supplementary measures to fill the gap. The European Data Protection Board (EDPB) published guidance on supplemental measures. Examples of supplemental measures include organizational, technical and contractual measures. For information regarding the supplemental measures VMware has taken in response to Schrems II, see the FAQs in the VMware Trust Center.

Q. What is VMware's approach to Transfer Impact Assessments?

A. In response to the requirement to perform Transfer Impact Assessments, VMware has developed an internal process which follows EDPB guidance and the UK Information Commissioner's Office's International Transfer Risk Assessment and Tool. This includes undertaking a country level analysis utilising a reputable online regulatory research tool, gathering additional information from our vendors to assess government access, and conducting TIAs as part of the privacy reviews for our products and services, third-party sub-processors and corporate functions. VMware is committed to following the guidance provided by the regulators, albeit the European Data Protection Board (EDPB) and data privacy regulators across Europe have recognised that controllers are not expected to become experts in international surveillance regimes.

Q. Can Customers obtain copies of VMware's Transfer Impact Assessments?

A. VMware does not make any of its internal or third party TIAs available to customers. Customers are responsible for conducting their own TIAs in relation to their use of any VMware Service Offering and the selected hosting location.

To the extent customer requires information to conduct its own TIA, VMware can provide such information to the customer as VMware generally makes available to its customers and as may be reasonably required, subject to obligations of confidentiality.

Q. If the data transfer is reliant on BCRs, is a Transfer Impact Assessment still required?

A. Whilst Schrems II confirmed that Binding Corporate Rules (BCRs) remain a valid transfer mechanism for transfers of personal data outside the EEA, a TIA is still required irrespective of the transfer mechanism used (SSCs or BCRs).

As a result, VMware conducts TIAs on data transfers from the EEA, Switzerland and the UK to third parties which meet the requirements for a TIA.

VMware currently has BCRs in place to legitimise transfers of personal data of its customers from the EEA when it acts as their data processor (EU BCR-Ps) and has made a contractual commitment to extend the protection of the EU BCR-Ps to transfers of personal data outside of the UK to non-adequate jurisdictions until such time that VMware obtains BCR-Ps for the UK (application pending). Under its BCR-Ps, VMware is required to work with the Irish Data Protection Authority to update its BCR-Ps to ensure they comply with applicable law and is required to provide annual updates to the Irish DPA. Further information regarding VMware's BCR-Ps and international data strategy can be found on the VMware Cloud Trust Centre. Also, see the Supplemental Measures Addendum to the DPA.

Q. How likely is it that VMware might receive a request from U.S. authorities under the Foreign Intelligence Surveillance Act (FISA) Section 702 or Executive Order (EO)12333?

A. VMware strongly believes there is a low likelihood that it would be subject to Section 702 or EO 12333 in relation to its provision of the Service Offerings and processing of Customer Content. VMware does not have access to the type of

Data Transfers - Transfer Impact Assessments

customer data that would be of any interest to U.S. intelligence agencies. As stated by the U.S. government in a September 2020 white paper, "[c]ompanies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data." For further information, please see the VMware Statement regarding application of FISA Section 702 and Executive Order 12333 in view of Schrems II and the FAQ on Government Access Request on the VMware Trust Center which outlines VMware's policy regarding handling government access requests.

VMware recently published its VMware Transparency and Law Enforcement Report. To access the Report, please click here.

Q. What is VMware's approach to UK personal data now that the UK is no longer a member the EU?

A. For transfers of personal data outside the UK to jurisdictions that are not deemed adequate, VMware similarly conducts TIAs as required by the Schrems II decision. The UK has deeded any countries deemed adequate by the EU, as of 31 December 2020, to be adequate for the purposes of the transfer of personal data from the UK. VMware will continue to comply with applicable law relating to UK personal data and any requirements for TIAs.

FREQUENTLY ASKED QUESTIONS

Data Transfers - Transfer Impact Assessments

Last revised: 21 March 2022