WHITEPAPER

Q4

# Compliance with EU Data Transfer Requirements

December 2022

**NOTICE**

This white paper is being provided for informational purposes only and (a) does not constitute legal or regulatory advice; (b) does not necessarily represent all Q4 Inc. offerings and practices at any given time as these are subject to change; and (c) does not create any commitments or assurances from Q4 and its affiliates or sub-processors. The responsibilities and liabilities of Q4 to its Customers are controlled by the Q4 Master Subscription Agreement ("MSA") and Data Processing Agreement ("DPA") and this document is not part of, nor does it modify, any agreement between us. Capitalized terms used but not defined in this document will have the meanings provided in the MSA and DPA.

We appreciate international transfers are a complex area to navigate in light of the Schrems II judgment and the new standard contractual clauses ("SCCs") and hope this FAQ helps to answer your key questions from the **European Data Protection Board's recommendations**, as they relate to your use of Q4 products and services. Please also feel free to email any further questions you may have on the topic to **privacy@q4inc.com**.

# Schrems II

### 1) How are international transfers (transfers outside the EEA) handled under the GDPR?

Personal data covered by the GDPR can only be transferred outside of the EEA if an approved mechanism is in place to make sure that a GDPR level of data protection is not undermined.

This means it is important that organizations first know and map all transfers of personal data to non-EEA countries (step one from the EDPB recommendations). Q4 and its sub-processors will process personal data in the following non-EEA countries: Canada, United Kingdom, and the United States.

### 2) What international transfer mechanisms does Q4 use?

Organizations should then identify what transfer mechanism they are relying on for each transfer (step two from the EDPB recommendations). Some countries outside of the EEA (e.g. the UK) benefit from an EU data protection authority decision. We use this mechanism where possible.

We use the SCCs as the mechanism for international transfers of personal data between Q4 Customers and Q4 sub-processors in non-EEA/non-adequate countries. These provide contractual guarantees that the personal data will be protected to a GDPR standard outside of the EEA.

We use the Binding Corporate Rules ("BCRs") - see here and here - for international transfers between different Q4 entities. BCRs are supervisory authority approved policies that govern data protection matters within a group of companies, including regarding international transfer between those entities.

### 3) How does the Schrems II case affect the use of SCCs and BCRs?

Data exporters need to ensure that importing countries provide essentially equivalent protection to the EU for the specific data, especially regarding government surveillance (step three from the EDPB recommendations). If an essentially equivalent level of protection is not provided then, to proceed with the transfer, the data exporter must implement "supplementary measures" in order bring the level of data protection back up to an essentially equivalent standard (step four from the EDPB recommendations).

It is important to note that the Schrems II judgment does not require data localization or EU-only support. Some companies may view this as a preference or as a supplementary technical measure, but it is not an explicit legal requirement.

### 4) What is the relationship between the new SCCs and Schrems II?

The new SCCs came about because the older versions had already become outdated. However, the Schrems II decision provided further impetus for them to be developed. The new SCCs codify the Schrems II requirement to undertake a Transfer Impact Assessment ("TIA"). They also require data importers to take specific data protection steps if they receive a government access request. The new SCCs are already part of the latest Q4 DPA.

### 5) What is a TIA and how do you complete it?

A TIA is a method for assessing if an essentially equivalent level of protection will be provided in the importing country for the specific data being transferred (steps three and four from the EDPB recommendations), including whether local government surveillance laws meet the **EU's Essential Guarantees for surveillance measures**, any relevant practical evidence of government surveillance (e.g. government access requests previously received by the importer) and, if necessary, supplementary measures that may assist in reaching a level of essential equivalency.

### 6) How can you ensure that your data will be adequately protected under the surveillance laws of other countries where Q4 processes it?

As noted above, Q4 has provided summaries of relevant local laws in our TIA. It may be that you assess some of these countries' laws as providing an essentially equivalent level of protection as that in the EU for your data. In that case, no further action would be required for those countries.

If you assess any of these countries' laws as not providing essentially equivalent protection for your data then, depending on the circumstances (e.g. type of data), you may decide there is still no reason to believe the laws will actually be applied to your data. You also may consider the supplementary measures that Q4 has in place (e.g. our enhanced security measures) mean that any essential equivalence issues are adequately addressed.