# Teradata Guidance on Transfer of European Personal Data in Light of Schrems II

Through this document, Teradata aims to help its customers, who are subject to GDPR, conduct transfer impact assessments in connection with use of its Vantage product in light of the "Schrems II" ruling of the Court of Justice for the European Union and subsequent recommendations from the European Data Protection Board (EDPB). To do this, Teradata provides an overview of the Schrems II decision and the legal backdrop to European personal data transfers, a discussion of the Vantage platform and how customers' personal data may be processed, and considerations for a transfer impact assessment following the EDPB's recommended steps. References to "data" and "customer data" are assumed to include personal data, as defined in GDPR Article 4(1).

## I. Schrems II Decision and the Legal Backdrop to European Data Transfers

The Court of Justice of the European Union ruled in July 2020 (C-311/18 known as "Schrems II") that the EU-US Privacy Shield (the enhanced version of the Safe Harbour program which had been invalidated in the earlier Schrems I judgment) did not meet European requirements regarding the safety of data processed in the US. Additionally, even though the court upheld the validity of the Standard Contractual Clauses (SCC) - a template issued by the EU Commission to safeguard EU data-transfers to countries outside the EU ("Third Countries") in accordance with GDPR Article 46—it raised important considerations for data exporters when using SCCs to ensure that adequate levels of data protection are maintained, namely to ensure that the jurisdiction of the Third Country in which the data is processed provides safeguards "essentially equivalent" to the standards of data protection in the EU. In November 2020, the EDPB, as an independent European data protection body, published recommendations on how to address the Schrems II judgment. Although the EDPB's statements have no legally binding effect, their recommendations are generally considered a quasi-official interpretation of the Schrems II judgment.

## II. The Vantage Platform and Customer Data

Teradata's Vantage platform is provided either on a Cloud as-a-Service basis, including as a managed application (VaaS), or as an on-premises solution. The following discusses potential processing by Teradata of data uploaded by a Teradata customer onto their Vantage platform under various scenarios.

### A. Teradata Cloud Operations

VaaS is supplied using a third-party Cloud Service Provider (CSP), where Teradata provides the software and the CSP provides the storage and compute space for the system and customers' database but does not process personal data (beyond any processing that may occur through the mere storage of data). The CSP does not have access to customer data in the virtual instances that Teradata deploys. Depending on the CSP selected, Teradata's customers may choose from various geographic regions (including the EU) to determine the country or region in which their data is stored, and data will remain stored in that selected country/region.

For the latest version of Vantage in Vantage Enterprise and VantageCloud Lake, Teradata performs all obligations for day-to-day cloud operations without ever accessing or viewing the customer's

data. For previous versions of Vantage Enterprise, to the extent customers grant Teradata database credentials for discrete activities such as upgrades, Teradata never uses those credentials for accessing the customer database, and multiple technical and organizational controls are put in place to prevent the improper use of those credentials (such as strictly limiting who receives the password, how long a password is valid, how the password is shared and by maintaining access logs). For added protection, customers are encouraged to encrypt and/or pseudonymize their data. Such encryption/pseudonymization does not prevent Teradata from carrying out any cloud operation services.

### B. Potential Instances When Teradata May Process Customer Data

In addition, for both on-premises solutions and VaaS, Teradata's customer support and maintenance service personnel generally do not access the customer's data in order to perform their services. To the extent the customer grants Teradata credentials for diagnosing faults and deploying fixes, patches and upgrades, Teradata never uses those credentials for accessing the customer database. Moreover, multiple technical and organizational controls are put in place to prevent the improper use of those credentials (such as strictly limiting who receives the password, how long a password is valid, how the password is shared, and by maintaining access logs). For added protection, customers are encouraged to encrypt and/or pseudonymize their data, which does not prevent Teradata from conducting these customer support and maintenance services.

Only where the customer support team is asked to conduct a query analysis for performance or other error, or where they are asked to conduct a dump analysis could an exception to this general rule of not accessing or viewing personal data exist. In those rare cases, it is possible the queries upon which the customer support and maintenance teams conduct their analysis could contain personal information. There are actions the customer may take to limit or prevent seeing personal data in those situations. For example, the customer may control query analysis by turning the logging off. Alternatively, the customer may present the query or crashdump for analysis (rather than granting Teradata access) after scrubbing it for personal information. Regardless of whether the customer takes those steps, Teradata has strict security and organizational measures to protect customer data, including any personal information in the rare cases that the customer support team may be exposed to it.

Finally, a customer may separately contract with Teradata to perform consulting and/or managed services. Whether in relation to an on-premises system or VaaS, these additional services are usually performed via specific VPN sessions instigated and controlled by the customer and covered by confidentiality provisions. If access is granted beyond a VPN session, the customer determines the appropriate level of additional access for all managed and consulting services. In addition, the customer may choose to encrypt/pseudonymize or otherwise obfuscate all personal data during these sessions, and only in the rarest of situations would Teradata need to see the underlying data to perform managed or consulting services.

## III. Considerations for a Transfer Impact Assessment

In this section, Teradata considers the steps outlined by the EDPB in assessing Third Countries for a transfer impact assessment.

### A. Step 1: Know Your Transfers to Third Countries

As described above, countries outside the European Union, without an approved adequacy decision, are considered Third Countries with regards to the level of data protection required by the GDPR. In almost all cases, Teradata does not access customer data in performing its contractual

obligations. Only in the rarest of cases would Teradata need to access or view the underlying data to perform customer support, maintenance, and consulting or managed services. Because the customer can encrypt/pseudonymize or otherwise obfuscate the data, which Teradata strongly encourages customers to do, transfers of data for Teradata processing may be limited to the narrowest of circumstances by the customer if it chooses. Nonetheless, this section considers all potential transfers of data.

Regardless of whether the customer has encrypted/pseudonymized the data, these transfers are usually to Teradata's Global Development Centers ("GDCs"). Teradata operates all its GDCs under the same data protection principles, applying the same Technical and Organizational Measures (TOMs), as required by GDPR. Teradata's Vantage platform and various GDCs are certified in accordance with ISO 27001. As new products are released, for example Teradata's new Vantage Cloud and Vantage Cloud Lake editions, appropriate certifications will be sought. When accessed by GDC employees, customer data remains stored in the customer-selected location and the relevant team member will access the data under our customers' control, for example via secure connection (e.g. VPN).

The chart below describes Teradata's various processing activities for EU customers and where they occur currently. Teradata may add or remove locations from time -to-time. Teradata will continue to follow these steps to ensure any processing activities are done consistent with the GDPR.

| **Category of Processing Activity** | **Current Location for EU Customers (as may be updated from time to time)** |
|---|---|
| CSP Storage and Compute | Region selected by customer |
| Cloud Operations | No processing for latest version of Vantage Enterprise; transfer to US only for VantageCloud Lake query processing as set out below |
| Customer Support & Maintenance for on-premises and Cloud | Australia, Austria, Belgium, Brazil, Canada, Chile, China, Czech Republic, Egypt, England, France, Germany, India, Ireland, Italy, Japan, South Korea, Malaysia, Mexico, Netherlands, Pakistan, Poland, Singapore, Spain, Taiwan, and the US |
| Consulting Services for on-premises and Cloud (performed under separate SOW) | Depends on customer location. Usually local country, or GDCs in Czech Republic, India, Pakistan, and occasionally the US for remotely performed services |
| Managed Services for on-premises and Cloud | Depends on customer location, with India being the default for remotely performed services |

In general, there are no other transfers of customer data associated with the use of Teradata's Vantage platform because the data is either on-premises or the customer data remains where the customer has elected to have it stored with the CSP. An exception to this rule exists for queries run on Teradata's new VantageCloud Lake edition. Under the new VantageCloud Lake architecture, queries are encrypted and will travel, encrypted, from their country of origin to the US. Results will then be returned, encrypted, from the US to where the query originated. If customers do not also encrypt their data in the system, there will be a point in time when data may be viewable in plain text as the query is unencrypted to be processed in the US prior to the results being returned,

encrypted. However, if the customer data is encrypted in the system, that encryption will remain intact.

## B. Step 2: Verify the Transfer Tool Relied Upon

Teradata relies upon the European Commission's SCCs to appropriately safeguard the transfer, in accordance with GDPR Article 46. Teradata's Data Processing Addendum ("DPA"), incorporating the SCCs, is available here. Annex 1 to Teradata's DPA provides a description of Teradata's processing of personal data. The DPA also links to a description of the technical and organizational security measures for Vantage that are implemented by Teradata in accordance with GDPR Article 32 .

For transfers of customer European personal data to third-party sub-processors, Teradata has entered Data Processing Addendums with third-party sub-processors that provide at least the same level of protection, including incorporating the SCCs. A list of Teradata's sub-processors, including all Teradata entities, and a mechanism to subscribe to stay up-to-date on changes is available here.

Because different Teradata entities may process the data depending upon where the processing activity occurs, Teradata uses an intergroup Data Processing Addendum incorporating the SCCs to enable transfers to the appropriate Teradata entity.

Without derogating from Teradata's use and observance of the SCCs as the current primary legal basis for transferring European personal data, Teradata's applicable US entities (currently Teradata Corporation, Teradata Operations Inc., Teradata US Inc., Teradata International, Inc. and Teradata Government Systems LLC) also adhere to the principles of (and have for the time being elected to remain certified to) the Department of Commerce EU-U.S. Privacy Shield Framework. For more information about Privacy Shield, or to access information regarding the status of Teradata's Privacy Shield certification registrations, please go to https://www.privacyshield.gov.

## C. Step 3: Assess the Law and/or Practices of the Third Country

The Court in Schrems II was concerned with the possibility of the US government obtaining access to European personal data. Its decision highlighted two US laws in particular as being potential obstacles to ensuring essentially equivalent protection for personal data in the US—FISA Section 702 ("FISA 702") and Executive Order 12333 ("EO 12333"). As an initial matter, based on a review of the governing legal framework, it is doubtful that Teradata falls under the jurisdiction of FISA 702 or EO12333.

Moreover, in September 2020, the United States government published a White Paper focusing in particular on these two laws and issues that appear to have concerned the Court in Schrems II. A key point in the White Paper included that most US companies do not deal in data that is of any interest to U.S. intelligence agencies, and have no grounds to believe they do. They are not engaged in data transfers that present the type of risks to privacy that appear to have concerned the Court in Schrems II. This seems particularly true with respect to customer data on Teradata Vantage platform.

Teradata does not have any insight into the contents of its customers' data and has no grounds to believe it is the type of data that is of any interest to US intelligence agencies. The fact that, to the best of its knowledge, Teradata has to date not been requested/required by public authorities to provide customer data under relevant laws further confirms this. Any request from public authorities will be addressed on a case-by-case basis and responded to based on the advice of legal counsel, and in accordance with Teradata's applicable company management policy.

Finally, the US government has been trying to address the concerns of the Schrems II decision. In October 2022, President Biden signed an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (E.O.) directing the steps that the United States will take to implement the US commitments under the European Union-US Data Privacy Framework (EU-US DPF), primarily by adding further safeguards in how such activities are conducted, mandating how personal information will be handled, and providing aggrieved data subjects with a forum for review and redress. This is an excellent step, further protecting the rights of data subjects whose personal data is transferred to the US. See EO Whitehouse Factsheet for more information.

In addition to US laws, Teradata has assessed the currently applicable laws of the other Third Countries referenced in Part A above in the light of the concerns raised by the Court in Schrems II, and concludes that, taken together with the measures adhered to under the SCCs and other mitigating controls as described in this document, the laws of these countries do not jeopardize the fundamental rights and freedoms of individuals with respect to the protection of their personal data.

## D. Step 4: Are Additional Supplementary Measures Necessary?

As explained by the EDPB, supplementary measures have a technical, contractual, or organizational nature. Diverse measures that support and build on each other may enhance the level of protection to contribute to reaching EU standards. Teradata's Global Privacy Policy ("Privacy Policy") provides clear, accurate information about the privacy and data protection measures adopted by Teradata Corporation and its subsidiaries worldwide and how Teradata accesses, collects, uses, processes, retains, transfers, discloses and handles personally identifiable information/personal data . In addition, to help Teradata's customers determine whether additional supplementary measures are necessary, some details of Teradata's technical, contractual, and organizational measures are highlighted below.

### 1. Technical Measures

As noted above, Teradata's DPA also links to a description of the technical and organizational security measures for Vantage that are implemented by Teradata in accordance with Article 32 of the GDPR. Of perhaps most importance, these technical measures include encryption at rest as well as in transit. Encryption is considered one of the most important measures in protecting customer data against unlawful or external disclosure. Customers are also encouraged to apply (and manage the keys for) column level encryption to their data stored on the system. In all cases except in a minority of instances described above, services can be performed on encrypted or pseudonymized data, therefore it is entirely within customers' control to fully protect their data from unauthorized outside view, including Teradata's, if they wish.

### 2. Contractual Measures

Teradata's DPA, incorporating the SCCs, contractually obliges Teradata to adhere to the following requirements:

- **Technical measures**: Teradata is contractually obligated to have in place appropriate technical and organizational measures to safeguard personal data (under both the DPA as well as the SCCs Teradata enters into with customers, service providers, and between entities within the Teradata group).

- **Transparency:** Teradata is obligated under the SCCs to notify its customers in the event it is made subject to a request for government access to customer personal data from a public authority. Teradata will carefully assess any request by a public authority to access customer data

and will only provide access if clearly compelled to do so after a full evaluation. Any public authority must follow applicable legal procedures and Teradata will refuse any request if deemed unlawful. Our customers will be informed about such a request on receipt if this is not explicitly prohibited by law.

### 3. Organizational Measures

Teradata's Privacy Policy highlights many of the organizational measures in place to protect customer data. Teradata takes reasonable physical, administrative, procedural and technical measures to protect PII under its control from loss, misuse and unauthorized access, disclosure, alteration and destruction. In particular, Teradata employs the following organizational security measures, among others:

- **Security policies:** Teradata designs, implements, and supports our IT infrastructure, data center operations, cloud operations, products and services according to documented security policies. At least annually, Teradata assesses its policy compliance and makes necessary improvements to our policies and practices.

- **Employee training and responsibilities:** Teradata takes steps to reduce the risks of human error, theft, fraud, and misuse of our facilities. Teradata trains its personnel on its privacy and security policies. Teradata also requires employees to sign confidentiality agreements.

- **Access control:** Teradata limits access to data only to those individuals who have an authorized purpose for accessing that information. Teradata terminates those access privileges and credentials following job changes which no longer require such access and upon employment termination. Teradata also has a designated EU data protection officer, who can be reached at DPO.EEA@teradata.com, as well as privacy experts in various locations and organizations of Teradata, and otherwise as and where required by applicable law.

- **Onward transfers:** Teradata remains accountable to our customers whenever Teradata shares customer data with service providers. Teradata carefully screens all its service providers and puts contracts in place that provide at least an equivalent level of protection, including incorporating the SCCs where necessary. A list of Teradata's sub-processors, including all Teradata entities, and a mechanism to subscribe to stay up-to-date on changes is available here.

## E. Steps 5 and 6: Determination that No Additional Steps are Necessary at this Time but Continue to Re-evaluate

It is Teradata's practice to comply with all laws that apply to its operations. According to our legal assessment of the currently applicable laws of the Third Countries referenced in Part A above, particularly when assessed in conjunction with Teradata's technical, contractual, and organizational measures, the processing of data described in this guidance does not impinge on the effectiveness of the SCCs or our ability to ensure that individuals' rights remain protected. Therefore, we conclude that the GDPR Personal Data transferred is afforded an adequate level of protection and no additional procedural steps are necessary at this time. Nonetheless, Teradata shall continue to monitor the status on an on-going basis.

# IV. Conclusion

This paper is made available to our customers for information only purposes to help explain the approach Teradata has taken to managing the transfer of personal data to Third Countries. The information in this paper is not intended to constitute legal advice and should not be relied on as

such. There are some issues that each customer must consider based on its own circumstances. For example, Teradata does not have insight into the data, including any personal data, that its customers load onto the Vantage Platform in order to fully evaluate the potential severity of harm that could occur to a data subject due to the loss of privacy of the data. Similarly, Teradata does not have control as to whether its customers apply (and retain the keys to) the recommended column level encryption for their uploaded data in order to fully determine the likelihood of harm arising to the data subject. Teradata recommends customers take their own independent professional advice on the conduct of any transfer impact assessment that may be required to support use of the Teradata service or otherwise as it conducts its own Transfer Impact Assessment. Please contact your Account Manager if you require assistance in assessing the essential equivalence.

**Current as of April 11, 2023**