Teradata Guidance on Processing of Customer Data, Including Potential Transfers of Personal Data Under the GDPR

Teradata wants its customers to feel confident about how Teradata processes the data they load into Teradata's Vantage products ("Customer Data"). In addition, Teradata realizes that customers subject to GDPR must conduct transfer impact assessments in connection with use of its Vantage products. This memorandum aims to help Teradata's customers achieve these goals.

Section I describes the limited circumstances in which Teradata may process Customer Data. Section II provides an overview of the Court of Justice for the European Union's (CJEU's) "Schrems II" ruling (C311/18), and the legal backdrop to European personal data transfers—including under the new EU-U.S. Data Privacy Framework. Section III discusses considerations when conducting a transfer impact assessment relevant to Teradata's Vantage products, following the European Data Protection Board's (EDPB's) recommendations.

I. Customer Data and the Vantage Platform

The following section first defines Customer Data as a subset of Customer Confidential Information. Next, it discusses potential processing of Customer Data by Teradata through the Teradata Vantage Platform, which is provided either as an on-premises solution, or on a Cloud as-a-Service basis (including as a managed application, collectively referred to as "VaaS" here).

A. Customer Confidential Information and Customer Data

In general, Teradata treats all information it receives from a customer as confidential, but the agreements between Teradata and its customers set out two different categories of data or information. The first is the very broad category of "Confidential Information," which covers information disclosed by the Customer during the course of doing business. This information is handled pursuant to the confidentiality terms set out in the governing agreement. The second is the narrower subset of Confidential Information, Customer Data. "Customer Data" is generally defined as "all data uploaded by Customer to the Teradata Vantage Platform." Customer Data is handled pursuant to even more stringent terms that are also set out in the governing agreement.

While both Customer Data and Confidential Information are presumed to contain personal data, Teradata's role when it handles Customer Data is different to when it handles Confidential Information. To the extent Teradata may process personal data contained in Confidential Information (which is not Customer Data or derived from Customer Data), it does so as a Controller. For example, in limited circumstances, Teradata may collect and process the names, email addresses, usernames, or usage details of customer's employees while doing business with a customer. This is the case where Teradata collects names and limited other personal data in its ServiceNow database as part of providing customer support.

In processing personal data contained in Confidential Information collected by Teradata for customer support, Teradata notifies individuals of its privacy policy (also available on the Teradata homepage) during support portal registration, access (authentication through PingID), and use. The Teradata privacy policy provides individuals with information regarding when Teradata may use their PII, and how we may process that PII.

As noted in the privacy policy, Teradata commits to comply with all applicable laws, and ensures that the appropriate technical and organizational measures are in place. Any transfers of such data are done in accordance with the requirements of the GDPR and pursuant to Teradata's intragroup processing agreement. In contrast, with respect to the personal data contained in Customer Data, Teradata is a processor for its customers. This memorandum sets out potential processing related to Customer Data.

B. Teradata Cloud Operations

VaaS is supplied using a third-party Cloud Service Provider (CSP), where Teradata provides the software and certain services and the CSP provides the storage and compute space for the system and customers' database. The CSP does not process Customer Data (beyond any processing that may occur through the mere storage of data), and it 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 Customer Data is stored, and Customer Data will remain stored in that selected country/region with two exceptions that both apply to Teradata's VantageCloud Lake product only.

First, is with respect to queries originating outside of the United States. Query service is a global service that sits in the Cloud Control Plane (CCP) layer routed to the United States. When a query is routed to the CCP, the Customer Data is encrypted throughout. As such, this should not constitute a transfer of personal data pursuant to the GDPR even though Customer Data is sent to the United States and back to the EEA as part of this process. Nonetheless, the *encrypted* query is transferred out of its selected storage location to the United States during this process.

Second, is respect with to data stream architecture (DSA) logs, which are logs of customer backup and restore operations. Whereas DSA logs stay exclusively in the customer site for Vantage Enterprise, for VantageCloud Lake, they are scrubbed of Customer Data (including personal data) and sent to the United States. Consequently, this should not constitute a transfer of personal data pursuant to the GDPR.

Otherwise, starting with the VaaS 2.4 version in Vantage Enterprise and for all versions of VantageCloud Lake, Teradata performs all obligations for day-to-day cloud operations without ever transferring, accessing, or viewing the Customer's Data. When earlier versions of Vantage Enterprise are deployed and used, some operations require use of a password that could *theoretically* be used to access or view Customer Data. With those versions, to the extent customers grant such credentials for discrete activities such as upgrades, Teradata never actually 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.

C. Instances When Teradata Personnel *May* Process Customer Data

Teradata employs many types of professionals to support its customers for both their on-premises and VaaS solutions. They include customer support, maintenance service, managed services, and consulting professionals.

Teradata's customer support and maintenance service personnel generally do not access Customer Data to perform their services in connection with either on-premises or VaaS solutions. To the extent a 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 Customer Data, which does not prevent Teradata from conducting these customer support and maintenance services.

Only where the customer support or maintenance team is asked to conduct a query analysis for performance or other error, or where they are asked to conduct a log or dump analysis could an exception to this general rule of not accessing or viewing personal data contained in Customer Data exist. In those rare cases, it is possible the queries upon which the customer support and maintenance teams conduct their analysis could contain Customer Data, and therefore personal information. A message reminds customers not to load that type of information directly into support tickets. And there are often actions the customer may take to limit or prevent Teradata's professionals seeing Customer Data. For example, the customer may control query analysis in many situations by turning the logging off. Alternatively, the customer may present the query or crashdump for analysis after scrubbing it for personal information rather than granting Teradata access to the raw 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 Customer Data to perform managed or consulting services.

Regardless of whether the customer has encrypted/pseudonymized the Customer Data, these transfers are usually to Teradata's Global Development Centers ("GDCs"). 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). 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 VantageCloud Lake and Vantage Cloud Enterprise editions, appropriate certifications will be sought.

D. Summary of Processing Activity by Location

The chart below describes Teradata's various processing activities for customers and where they occur currently if the customer has not paid for support to be localized. Teradata may add or remove locations from time -to-time. Teradata will continue to follow the transfer impact analysis steps outlined in Section III to ensure processing activities are done consistent with the GDPR.

Category of Processing Activity	**Current Location of Activity (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 U.S. only for VantageCloud Lake as set out in Section I.A.
Customer Support & Maintenance for on-premises and Cloud	Australia, Austria, Belgium, Brazil, Canada, Chile, China, Czech Republic, Egypt, France, Germany, India, Ireland, Italy, Japan, South Korea, Malaysia, Mexico, Netherlands, Pakistan, Poland, Singapore, Spain, Taiwan, U.K. and the U.S.
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

Note: To the extent that a customer elects to use an Application Programming Interface (API) or other means to connect Teradata's VaaS to a third-party software, in that instance the third-party software provider would be the customer's processor acting on the customer's behalf and not a subprocessor acting on Teradata's behalf. As such, any data processing is not captured in the summary of processing activity here.

II. The Legal Backdrop to European Data Transfers

A. Transfers to the US Under EU-U.S. DPF

In July 2023, the European Commission's adequacy decision for the EU-U.S. Data Privacy Framework ("EU-U.S. DPF") came into force. This represents the culmination of work done by policymakers on both sides of the Atlantic to address the CJEU's Schrems II ruling invalidating the EU-U.S. Privacy Shield.[1] Teradata maintained its certification to the Privacy Shield Framework Principles even after it was invalidated, which will ease the transition to the DPF. Teradata has committed to take all necessary steps to complete the self-certification in accordance with the EU-U.S. DPF Principles (with UK Extension) and the Swiss U.S. DPF. Thus, to the extent that Teradata

[1] The Privacy Shield itself was the enhanced version of the Safe Harbour program, which had been invalidated in the earlier Schrems I judgment

transfers (its own or its customers') data from the EEA, U.K., or Switzerland, it may legally do so pursuant to the adequacy decision issued in July.[2]

B. Transfers under SCCs

Although it invalidated the Privacy Shield, in Schrems II, the CJEU upheld the use of the Standard Contractual Clauses (SCCs) generally. In doing so, 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, including the use of a transfer impact assessment. Although the EDPB's statements have no legally binding effect, their recommendations are generally considered a quasi-official interpretation of the Schrems II judgment.

For transfers of Customer Data to the United States, Teradata will continue to honor the SCCs that are contractually in place with the customers. Moreover, Teradata will continue to safeguard EU data-transfers to countries outside the EU that have not been deemed adequate ("Third Countries") through SCCs in accordance with GDPR Article 46 as further elaborated upon in the Schrems II decision and the EDPB's statements.

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

Potential transfers to Third Countries are set out in Section I.C. above.

B. Step 2: Verify the Transfer Tool Relied Upon

Where no adequacy decision is in place, Teradata relies upon the European Commission's SCCs to appropriately safeguard the transfer of customer data, 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 Data uploaded into customer's Vantage system to sub-processors, presumed to contain European personal data by default, 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.

[2] Teradata recognizes that there likely will be challenges to the DPF in European courts, but is optimistic that the DPF may withstand these challenges given the enormous amount of work that went into ensuring the protections to European personal data transferred to the U.S. were "essentially equivalent" to the standards of data protection in the EU.

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. Looking to address the issues raised, the United States government changed how its intelligence community can access European personal data. It also implemented means for non-United States data subjects to seek redress if they believe their data was accessed inappropriately. Thus, with the European Commission's new adequacy decision, the United States should no longer be considered a Third Country requiring a separate transfer impact assessment.

With respect to the Third Countries referenced in Section I.C., Teradata has assessed the currently applicable laws of those Third Countries in the light of the concerns raised by the court in Schrems II. With the support of outside counsel, Teradata 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. Perhaps of 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 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 Section III.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, particularly to Third Countries under the GDPR. 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 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 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 January 8, 2024