How Does Teradata Process Customer Data?

Teradata wants its customers to feel confident about how Teradata processes the data they load into Teradata's Vantage products ("Customer Data"). To help with that, this document discusses potential processing of Customer Data by Teradata through the 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).

I. 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 (that is not Customer Data or derived from Customer Data), it does so on its own behalf as a "controller" (as the term is used under many privacy laws). 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 collected for customer support, Teradata notifies individuals of its Privacy Statement (also available on the Teradata homepage) during support portal registration, access (authentication through PingID), and use. The Teradata Privacy Statement provides individuals with information regarding when and how Teradata may process that PII.

As noted in the Privacy Statement, 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 applicable privacy laws 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 (as the term is used under many privacy laws). The remainder of this memorandum sets out potential processing related to Customer Data.

II. Teradata Cloud Operations and Customer Data

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 US East, US West, the EU etc.) to determine the country or region in which their Customer Data is stored. Customer Data remains 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. 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. Of course, for customers in the United States, neither of these instances represent a transfer out of region.

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.

III. 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 other 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.

IV. Summary of Customer Data 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. Whenever Teradata adds a processing location, it will continue to follow all applicable data privacy laws. Please see Teradata's Transfer Impact Analysis Memorandum for more information regarding transfers subject to 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 II.
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.

V. Teradata's Response to Data Subject Requests and Government Inquiries

Teradata's obligations related to responding to DSRs and government inquiries are typically set out in its agreements with Customers. In general, because Teradata does not have access to Customer Data as part of its day-to-day operations, it does not get involved in responding to DSRs on a Customer's behalf. Instead, Teradata's on-premises system and VaaS allows Customers to retrieve, correct, delete or restrict personal data, which they can use to respond to DSRs themselves. In the unlikely event, that Customers are unable to independently address a DSR through the Service, upon a Customer's written request, or as required by law, Teradata will provide reasonable assistance to respond to any DSR or requests from data protection authorities relating to the Processing of personal data under the Agreement. If a DSR or other communication regarding the processing of personal data under the Agreement is made directly to Teradata, Teradata will promptly inform Customer and will advise the Data Subject to submit their request to the Customer directly.

Similarly, Teradata is obligated under the standard 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. Customers will be informed about such a request on receipt if this is not explicitly prohibited by law.

VI. Conclusion

This paper is made available to our customers for information only purposes to help explain the approach Teradata has taken to managing the processing and transfer of personal data contained in Customer Data. 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. Please contact your Account Manager if you require assistance in assessing the essential equivalence.

Current as of October 2024