Teradata Corporation
Global Privacy Policy

teradata.

Effective Date: 13th October 2021

TERADATA CORPORATION
GLOBAL PRIVACY POLICY

Table of Contents

1 General Information ____ 1

1.1 Effective/Last-Change Date ____ 1

1.2 Scope ____ 1

1.3 Changes and Supplemental Terms ____ 1

1.4 Contact Us ____ 1

1.5 Verifying your Identity when you make Requests under CCPA ____ 2

2 Our Principles: Respecting Your Privacy and Security ____ 3

2.1 "Notice" Principle ____ 4

2.2 "Choice" Principle ____ 5

2.3 "Security" Principle ____ 6

2.4 "Access" Principle ____ 7

2.5 "Accountability for Onward Transfer" Principle ____ 8

2.6 "Data Integrity and Purpose Limitation" Principle ____ 9

2.7 "Recourse, Enforcement and Liability" Principle ____ 12

3 Exercise Your Rights in Line With Our Principles ____ 12

3.1 Your Rights ____ 12

3.2 Breaches ____ 13

3.3 Some Specific Uses of PII ____ 13

3.3.1 Job Applicants/Referrals ____ 13

3.3.2 Employees, Contractors and Workers ____ 15

3.3.3 Marketing/Customer Activities ____ 17

3.3.4 Miscellaneous Other Processing Situations ____ 19

4 Cross-Border Data Processing ____ 19

5 Information Security Guidelines ____ 21

5.1 Related Standards, Laws, Practices and Policies ____ 21

5.2 Operating Procedures ____ 23

5.3 Other Privacy Frameworks and Principles ____ 23

5.4 Internal Policies, Guidance and Practices ____ 24

1 General Information

1.1 Effective/Last-Change Date

13th October 2021

1.2 Scope

This Global Privacy Policy ("Privacy Policy") provides clear, accurate information about the privacy and data protection ("PDP") measures adopted by Teradata Corporation and its subsidiaries worldwide and how we access, collect, use, process, retain, transfer, disclose and handle ("Use") your personally identifiable Information/personal data ("PII"). It applies to all offline and online Use, including Teradata websites, social media sites, education and networking sites, mobile and desktop applications ("apps") and other online portals, contacts and communications between you and Teradata, and to any other scenario to which this Privacy Policy is stated to apply or is incorporated by reference (collectively, our "Sites").

"PII" means any information relating to an identified or identifiable individual, either alone or in reasonable combination with other information available to us. It includes all: personally identifiable information regarding you, to the extent it is subject to privacy law or privacy regulation provisions; and, non-public information identifiable to individuals to the extent it is subject to privacy or confidentiality provisions in written or electronic contracts entered into by or for Teradata.

In this document, "Teradata" includes Teradata Corporation and all of its subsidiaries throughout the world (also referred to as "we" or "us").

As a reflection of the importance we attach to the privacy and security of your PII, Teradata has elected to adopt a globally uniform approach to PDP, as set out in this Privacy Policy. In the unlikely case the standards set by your country's PDP laws exceed the standards in this Policy, then we meet the standards set by your country. Whilst we adopt a globally uniform approach to PDP, your legal rights and remedies are exercisable to the extent provided by applicable law in the relevant country.

Teradata does not and will not sell your or anyone else's PII and requires the same of its service providers. Teradata has not sold your or anyone else's PII to a third party in the 12 months preceding the Effective Date. Teradata offers no financial incentives in exchange for the collection/retention of PII.

1.3 Changes and Supplemental Terms

We will post public notice, through the Effective Date written on the cover page of this document and at the top of this page, at www.teradata.com/privacy for at least 30 days when this Privacy Policy is updated or modified in a material way.

From time to time, we may propose to supplement or amend this Privacy Policy and other PDP terms with site- or interaction-specific information and terms ("Supplemental Privacy Terms"). If so, you will be given notice of any such applicable Supplemental Privacy Terms and the choice to consent or not consent to them.

1.4 Contact Us

Except regarding EEA and California contacts and requests (see below), all countries' contacts and requests regarding your PII, data privacy at Teradata and Teradata compliance with the principles of the EU-U.S. Privacy Shield Framework or the Swiss-U.S. Privacy Shield Framework may be directed to the Teradata Ethics, Compliance & Privacy Office:

by e-mail at: Ethics&ComplianceOffice.TD@teradata.com

or by mail at:

Ethics, Compliance & Privacy Office – Law Department
Attn: Chief Ethics, Compliance and Privacy Officer
Teradata Corporation
17095 Via del Campo
San Diego, California, USA 92127

If you are a resident of California, USA, please contact us at privacy.ca@teradata.com. Please use this email to make requests related to The Californian Consumer Privacy Act ("CCPA"). You may also leave a voice message via our toll-free telephone number **855-729-4835** and we will contact you to action your request. You are kindly encouraged to make use of email rather than the toll-free telephone number to make such requests. We will fulfil your request in accordance with, and to the extent of, our obligations under the CCPA. Please use these contact details if you have a disability and require this Privacy Policy in an alternative format and we will do our best to help. Designated agents should also use these contact details.

Questions from EEA persons related to the processing of their PII and the exercise of their rights under EEA data protection laws should be sent by email to Teradata's EEA Data Protection Officer at: DPO.EEA@teradata.com or by mail to: The Data Protection Officer, Teradata GmbH, Nymphenburger Hoefe NYII, Dachauer Strasse 63, Munich 80335, Germany.

PDP-related issues that are specific to Information Technology ("IT") Security may be directed to our global Information Security Office:

by e-mail at: information.security@teradata.com

or by mail at:
Information Security Office
Attn: Chief Security Officer
Teradata Corporation
17095 Via del Campo
San Diego, California, USA 92127

online at: https://tdhelp.alertline.com/gcs/welcome

or by telephone at: **1-866-455-0993**.

1.5 Verifying your Identity when you make Requests under CCPA

If you are an office-based employee/contractor, we will verify your identity by requiring you to meet in person to confirm you made the request.

If you are not an office-based employee/contractor:

- Request to know categories of PII: Teradata will verify your identity to a reasonable degree of certainty by matching at least two data points provided by you with data points maintained by Teradata that we determine to be reliable for the purpose of verifying your identity.

- Request to know specific pieces of PII: Teradata will verify your identity to a reasonably high degree of certainty by matching at least three pieces of PII provided by you with data points maintained by Teradata that we determine to be reliable for the purpose of verifying your identity, together with, should Teradata deem it necessary, a declaration signed by you under penalty of perjury that it is your PII that is the subject of the request. Teradata shall maintain all signed declarations as part of its record-keeping obligations.

- Request to delete PII: Teradata will verify your identity to a reasonable degree or a reasonably high degree of certainty depending on the sensitivity of the PII and the risk of harm posed to you by unauthorized deletion, using the methods in the previous bullets. You must first submit your request to delete PII, and then separately confirm you want your PII deleted.

- Request to delete from Job Applicants: Teradata will verify your identity by requiring you to log in and make your request via online portal GR8 People (or subsequent provider/portal, if any). This is the also the preferred and most efficient method for you to make your job applicant deletion requests.

Teradata retains the right to vary any of the above verification procedures at its discretion.

2 Our Principles: Respecting Your Privacy and Security

Protecting privacy is part of our culture, values and everyday conduct at Teradata. Integrity, responsibility, being people-focused, and being dedicated to our customers are among the core values we apply to all aspects of our business, including with regard to PDP. Our management sets the tone regarding the importance, requirements, standards and practices applicable to PDP at Teradata.

Our Code of Conduct annual certification and other PDP-related training includes expectations of, and commitments by, all Teradata employees, contractors and business partners to protect data and comply with PDP laws. All individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA shall be informed of all the requirements in the CCPA and how to direct consumers to exercise their rights under the CCPA.

Our Supplier Code of Conduct and our Business Partner Code of Conduct incorporate the principles of the Teradata Code of Conduct, as well as global PDP laws and standards and the principles of the United Nations Global Compact and the Responsible Business Alliance ("RBA", formerly the Electronic Industry Citizenship Coalition ("EICC")) Code of Conduct, as well as this Privacy Policy. For more information, please see https://www.teradata.com/code-of-conduct/ and https://www.teradata.com/corporate-social-responsibility/ (see particularly the "Teradata Corporate Social Responsibility Report" linked to that webpage).

Teradata typically acts as a "data processor" with respect to PII we Use for one of our customers, and our customer typically serves as the "data controller" with respect to that PII.

Teradata typically acts as a "data controller" with respect to PII that we Use for ourselves, such as with regard to our own employees so we may administer their employment, compensation, benefits and human resources management ("HR data") and with regard to customer contacts held in our various marketing databases and related applications and to visitors of our online Sites. Our service providers who Use PII for us typically serve as downstream "data processors" or "sub-processors" for us.

2.1 "Notice" Principle

- Notice of where we operate. We are a global multinational organisation. Our corporate headquarters is located in Rancho Bernardo (San Diego), California. Our Peachtree Corners (Atlanta), Georgia facility is also a primary location (within the U.S.). We are incorporated in the State of Delaware in the U.S. As of December 31, 2019, we operated 97 facilities in 42 countries throughout the world. We own our Rancho Bernardo complex, while all other facilities are leased. We have more than 9,000 employees worldwide, and as such, our information sources, data subjects, data flows and supply-chain spans the globe.

- Notice of what we do. Teradata Corporation is a global leader in analytic data solutions and services. Our analytic data solutions comprise software, hardware, and related business consulting and support services for analytics across an organisation's entire analytical ecosystem, both on-premise and in the cloud. We help customers access and manage data and use analytics to extract business value and insight from their data, to drive business outcomes such as improving a customer's experience through understanding behavioral patterns, driving financial transformation with accurate and timely data and creating more efficient utilization of assets through machine learning of sensor data.

- Our consulting services include a broad range of offerings, such as consulting to help organizations establish an analytics vision, to enable an analytical ecosystem architecture, and to ensure value delivery of their analytical infrastructure.

- Teradata's strategy is based on our core belief that analytics and data unleash the potential of great companies allowing them to make better and faster decisions and attain competitive advantage. We empower companies to achieve high-impact business outcomes through analytics at scale on an agile data foundation. With our focus to lead with business outcomes and a consultative approach, our goal is to serve as a trusted advisor to business and technical leaders in our customers' organizations. Our business analytics solutions are ideally suited for the world's largest companies that have the largest and most complex analytics challenges, where scale and performance of such solutions matter.

- We serve customers around the world in a broad set of industries. Industry segments we serve include communications, ecommerce, financial services, government, gaming, healthcare, insurance, manufacturing, media and entertainment, oil and gas, retail, travel and transportation, and utilities. We focus on business users and technology buyers at the 500 companies with the largest analytics opportunities.

- Teradata has a presence on the web that includes www.teradata.com

- Teradata social media links currently include:

  www.linkedin.com/company/Teradata
  www.twitter.com/Teradata
  www.facebook.com/Teradata
  www.instagram.com/teradata/
  www.youtube.com/Teradata

Notice of when we may Use PII. We acquire, operate, host, outsource, interact with, maintain and service software, applications, hardware, networks, communications systems, websites, information sharing exchanges, social media venues and other sites, blogs, wikis and forums for:

- operating, managing and communicating about our own business, offerings and activities;
- R&D (such as for benchmarking, testing, quality assurance, research, and product/offering strategy, development and integration);
- providing technical, maintenance, support, back-up, recovery, diagnostic, consulting, implementation, and other related services for our customers;
- use by/for our customers, including through solutions we host, such as offerings we provide to or host for our customers in the forms of Software as a Service ("SaaS"), Data Analytics as a Service, or Warehousing as a Service ("DWaaS"), social computing and cloud computing.
- networking sites, such as Peer Advantage, customer or partner education or certification courses, for example via Teradata University Network or our Teradata Certified Professional Program, or via our customer education team.

Notice of Sources of PII we handle. We often Use PII, in either or both electronic/digital form or physical/paper form, regarding a variety of people and entities. These include the following categories:

- "Visitors" - including those who choose to visit the websites, web portals, information exchange sites, blogs, wikis, social media sites, domains, downloadable applications, apps, surveys, questionnaires, webinars, events, conferences, network systems, or facilities we host, own or operate, or have hosted or operated for us, as well as those who communicate with us, including by e-mail or other electronic or digital means, and such as through help-lines, call-centers, telecommunications and the like (with the subset of those who do so through electronic or digital means being referred to as "Online Visitors");
- "Employees" - including applicants, prospective employees, joint, temporary and contract employees, former employees, and retirees, and their qualifying family members, beneficiaries and insureds, such as those who receive or are eligible for benefits from or through us;
- "Customers" - including customer and prospective customers, and their representatives;
- "Partners" - including current and prospective suppliers, vendors, contractors, subcontractors, representatives, distributors, resellers, systems integrators, joint marketers, advertisers, sponsors and services providers;
- "Customer/Partner Constituents" - including people and entities who are the visitors, employees, customers, partners, constituents or other data subjects of our Customers or Partners, such as those about whom data is stored and processed on our solutions by or for our Customers; and
- "Others" - including people who are or may be influencers related to our business or technologies, such as analysts, academia, members of the media, investors, members of subject-area communities, industry communities and geographical or jurisdictional communities in which we operate, and those who do not fit into one or more of the preceding categories.

2.2 "Choice" Principle

Teradata will not release PII to unaffiliated third parties, unless (1) an individual requests it or expressly consents to it, (2) the data is provided to help complete a transaction initiated by the individual, (3) the disclosure is required by law, or (4) the individual has been informed about the possibility of such disclosure and has decided not to opt-out (or has decided to opt-in, double-confirmed opt-in, or meet some other higher standard where that is expressly required by applicable law).

Employees - Teradata will not release PII to unaffiliated third parties, except as specifically provided for under (1) internal corporate policies, (2) as reasonably necessary for employment-related purposes and transactions, (3) the Employee requests it or expressly consents to it, (4) the data is provided to help complete an Employee-initiated communication or transaction, (5) the disclosure is required by law, (6) the Employee has been informed about the possibility of such disclosure and has decided not

to opt-out (or has decided to opt-in, double-confirmed opt-in, or meet some other higher standard where such is expressly required by applicable law) or (7) as provided for elsewhere in this Privacy Policy.

We also will respect your preferences and choices for how we contact you regarding marketing and promotional communications. We may provide you, for example, with opportunities to subscribe to e-mail distributions or newsletters. If you previously signed-up to receive e-mailed information about our products, services, or special offers, but no longer wish to receive those communications you may opt-out from receiving some or all of those types of communications by following the 'unsubscribe' or 'preferences' setting instructions appended to the communication or communicating with us through one of the e-mail addresses or mailing addresses set forth in the "Contact Us" section of this document.

There are other circumstances in which we may share your PII with third parties. For example, we may disclose your PII to a third party: when we, in good faith, believe disclosure is appropriate to comply with the law or a regulatory requirement or to comply with a subpoena or court order; to prevent or investigate a possible crime, such as identity-theft, hacking, cyber-attacks, phishing-attempts or other cyber-crimes; to enforce a contract; to protect the rights, property, intellectual property or safety of Teradata or a third party; to protect other vital interests; and, to satisfy requirements to disclose PII in response to lawful requests by public authorities, including to meet national security or law enforcement requirements; or to a potential buyer or its advisor(s) in connection with any sale or transfer of all or part of our business;

2.3 "Security" Principle

Teradata will take appropriate measures to ensure that PII is protected from access and disclosure not authorized through application of this Privacy Policy, including by limiting access to such information to Employees, service providers and Partners who have a legitimate business need to know it for a purpose permitted by this Privacy Policy, applicable Supplemental Privacy Terms, or with express consent.

We take reasonable physical, administrative, procedural and technical measures to protect PII under our control from loss, misuse and unauthorized access, disclosure, alteration and destruction. In particular, we employ the following security measures, among others:

- *Security policies*. We design, implement and support our IT infrastructure, data center operations, cloud operations, products and services according to documented security policies. At least annually, we assess our policy compliance and make necessary improvements to our policies and practices.

- *Employee training and responsibilities*. We take steps to reduce the risks of human error, theft, fraud, and misuse of our facilities. We train our personnel on our privacy and security policies. We also require Employees to sign confidentiality agreements. We also have assigned to a Chief Security Officer the ultimate responsibility to manage our global information security program.

- *Access control*. We limit access to PII only to those individuals who have an authorized purpose for accessing that information. We terminate those access privileges and credentials following job changes which no longer require such access and upon employment termination. We also have designated local or organizational data protection officers, stewards or managers for various locations and organizations of Teradata, and otherwise as and where required by applicable law.

Data encryption. Our policies and procedures require that wherever practicable we use encrypted connections for any electronic transfers of PII.
Unfortunately, no security measures can be guaranteed to be 100-percent effective. It is important you understand that no site, system or network is completely secure or "hacker proof", "cyber-attack proof" or "cyber-crime proof." It is important for you to guard against unauthorized access to your passwords and the unauthorized use of computers and other electronic/data-access devices you own or control.

We strongly urge you to do your part and take measures to preserve your own data privacy and to protect and secure your own information. Among the practices you should consider are: use differing passwords for differing accounts; use 'strong' passwords; use screen locks; be suspicious of and do not reply to unverified e-mails that include, seek or seek you to confirm your personal, financial or identification information; check web addresses carefully for fake, variant or apparently-misspelled URLs; use e-mail and Internet Service Provider ("ISP") anti-spam functionality, settings and processes; set your browser and device settings to the levels of privacy, cookies and security you desire; and, use, keep-updated, and apply desired settings for security and virus protection software tools on your devices. For information, tips and practices regarding online privacy and data protection, consider visiting an online group or site of your choice (*e.g.,* considering your language, country, location, types of uses, types of data, types of devices and types of communications) that is dedicated to sharing information regarding data privacy and information protection. One you might find helpful and instructive, for example, is http://www.staysafeonline.org/ powered by the National Cyber Security Alliance, and its "***Stop. Think. Connect.***" initiative.

2.4 "Access" Principle

Teradata strives to maintain the accuracy of the PII we hold, including establishing mechanisms allowing consumers and Employees to have the opportunity to review and correct, and in some circumstances obtain deletion of, PII about themselves. You may review and correct, and (to the extent not limited or prohibited by applicable law in your country) have us delete, your PII – please see "Exercise Your Rights" below. In some cases, we may limit or deny your request if the law permits or requires us to do so (for example, we may decline to delete data that we are required by law to retain, such as for tax withholdings and payments). We encourage you to promptly update your PII with us if and as it changes.

If Teradata is engaged to host a solution or manage a cloud solution, we may host/manage Customer/Partner Constituent or "audience-member" information. We respect the privacy of all audience-member information, and (unless otherwise expressly agreed upon in writing) we view and treat it as the Customer's/Partner's confidential information. With respect to data hosted, managed or processed by us, often that data includes only basic contact information, such as name and e-mail address. However, we may obtain any type of data about any individual that our Customer/Partner uploads or otherwise provides access to us in connection with a hosted/managed-solution or sends to us or a hosted/managed solution through online or offline mechanisms. In this regard, we do not control what audience-member information we may receive, host or manage, or what steps the Customer or Partner, as the "data controller", has taken to ensure that the data is reliable for its intended use, accurate, complete, and current. If a Customer or Partner uploads/provides sensitive PII – such as social security or social benefit numbers, bank-account numbers, credit-card or payment-card numbers, passport numbers, driver license numbers, personal health information, access passwords or PINs, or EU sensitive PII, such as racial or ethnic origin, political or religious affiliation, or trade union membership status – (which generally would be contrary to our agreement with a Customer or Partner) we reserve the right, following written notice to the Customer/Partner, to eliminate that information from our servers and/or suspend or terminate the Customer's or Partner's hosted/managing-processing privileges, order or account with us - unless and until the Customer/Partner verifies to our satisfaction that it has valid consent or another valid legal right to do so. We will use audience-member information only as permitted by our contract with the applicable

"data controller" Customer or Partner. We will not share, sell, rent, or trade with third parties for their marketing purposes any audience-member information collected by us for a Customer or Partner, unless that Customer or Partner authorizes us to do so and represents to us that it has, and that it has sole responsibility for obtaining, all appropriate and any legally-required audience-member consents to do so.

For our hosted, managed and cloud solution, our Customer or Partner typically has full control over its audience-member information, whether to correct, update or delete individually identifiable PII it has collected and uploaded/provided. If a Customer or Partner receives a data-access or data-deletion request from an audience-member about whom we host or manage PII and the Customer or Partner would like our assistance in responding to that request, it may contact us and we will strive to respond to such requests without undue delay.

2.5 "Accountability for Onward Transfer" Principle

The EU-U.S. Privacy Shield Framework, Swiss-U.S. Privacy Shield Framework, the EU standard contractual clauses, HIPAA and other countries' laws, as and when valid and in force, and as may be amended from time to time (see more under Section 4 Cross-Border Data Processing), typically allow transfer of PII to a third party who is acting as a service provider, agent or "data processor" if the ultimate "data controller" takes certain steps to assure privacy and security protections. We may disclose PII to others, for example, in the following circumstances:

- to business Partners and subcontractors who need to access it in connection with the performance of requested services or solutions, or as otherwise appropriate in connection with a legitimate business need;
- to service providers who host or facilitate the delivery of online apps, training, seminars and webinars;
- to e-mail-delivery services and other technology providers;
- to third parties who may assist in the delivery of marketing materials, technical support services, or other products, services or other information;
- with authorized reseller/distributor/marketing Partners or our subsidiaries or branches so they may follow up with you regarding products and/or services;
- Applicant Information and Employee data may be shared, on a confidential and use-restricted basis, with our affiliates, subsidiaries, recruiting advisors and service providers, as well as other third parties such as background-screening organizations for the purposes described in this Privacy Policy and for employment-related activities as set forth elsewhere in this document and as reasonably necessary in connection with an Employee transaction or communication, compensation, benefits, tax and social-benefits reporting and withholding, and other legal, compliance and reporting obligations;
- in connection with the sale or transfer of all or part of our business;
- as required or permitted by law, or when we believe in our sole discretion that disclosure is necessary or appropriate to protect our rights, protect your safety or the safety of others, investigate fraud, comply with a judicial proceeding, court order, law-enforcement or government request, or other legal process, or to satisfy requirements to disclose PII in response to lawful requests by public authorities, including to meet national security or law enforcement requirements; and
- to any other third party, with your affirmative consent.

In these situations, we will take reasonable steps to require the recipient to protect your PII in accordance with relevant applicable principles of all applicable laws or framework, and the EU-U.S. Privacy Shield Framework, Swiss-U.S. Privacy Shield Framework, or otherwise take steps to help ensure your PII is appropriately protected.

If consumer or Employee PII is provided to an affiliated third party (*e.g.,* subsidiaries, service providers, contractors or other Partners), or if that affiliated third party is directed to collect PII directly from a consumer or about a consumer on Teradata's behalf, Teradata will require the third party to adhere to similar PDP principles as those that apply to Teradata and that provide for keeping PII confidential and not using it for any other purposes, including not selling PII. Teradata typically achieves this by including any, or a combination of, the following: express contractual provisions in its written agreements with third parties, express provisions in the Teradata Code of Conduct, express provisions in our Supplier Code of Conduct, express provisions in our Business Partner Code of Conduct, express provisions in our written policies, express provisions in our privacy policy/statement (such as this Privacy Policy), express provisions based on EU Model Clauses in written Data Transfer Agreements and other notices and acknowledgements that applicable laws must be complied with and that applicable principles of the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework must be satisfied. See further under "Service Providers" below. When Teradata serves as a data processor for others, such as for our data-controller-customers or as a data processor to another data processor, Teradata typically is required by express contractual provisions to be accountable to the third party and the impacted data subject for breaches by Teradata or Teradata's downstream data processors with respect to that PII. To the extent, if any, that a downstream "data processor" for Teradata breaches its legal or contractual duties with respect to PII that it obtains through or for Teradata and it fails to provide full legally-sufficient remedies directly to you for such breach, Teradata will be accountable for providing you with full legally-sufficient remedies for such breach and will be subject to complaint and remedy jurisdiction as set forth in this document.

Service Providers. In relation to the CCPA, to the limited extent that our service providers collect PII from or about a consumer on our behalf, we direct them that they shall not retain, use, or disclose PII obtained in the course of providing services to us except: i) to process or maintain or collect PII on our behalf and in compliance with the written contract for services and the Supplier or Business Partner Code of Conduct; ii) to retain or employ another service provider as a subcontractor, only where the subcontractor meets the requirements for a service provider under the CCPA; iii) for internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source; iv) to detect data security incidents, or protect against fraudulent or illegal activity; or for the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(4). A service provider is directed not to sell PII provided by, or collected on behalf of, Teradata. A service provider that receives a request to know or a request to delete from a consumer shall immediately inform Teradata using the contact details in the "Contact Us" section above, and the parties will timely decide whether the service provider will act on behalf of Teradata in responding to the request or whether the service provider will inform the consumer that the request cannot be acted upon because the request has been sent to a service provider.

2.6 "Data Integrity and Purpose Limitation" Principle

Teradata will limit the Use of PII to that which is reasonably needed for valid/legitimate business purposes or to comply with applicable laws. Any such data will be obtained by us only through lawful and fair means.

- When you visit us online, we want you to feel secure that we are respecting your privacy. PII we collect about you when you visit us online is the information you choose to provide by Registering or by providing other feedback or consent to us, subject to this Privacy Policy and any applicable Supplemental Privacy Terms. We do not share PII you provide other than for purposes and with other parties as permitted through this Privacy Policy, through applicable Supplemental Privacy Terms, and when you have granted consent (such as when necessary in connection with a

transaction, employment or legal compliance obligations).

- Cookies. We may use cookies on some pages of our Sites to help serve you better each time you return. A cookie is a small element of data that a website may send to your browser and is then stored on your system. The data collected from cookies helps us determine how many people visit our Sites and what pages they view. We use this information to better serve Online Visitors and improve the content and design of our Sites. You may set your web browser to block cookies or warn you before you accept a cookie. Where required by law, we will ask you for your explicit consent to the usage of cookies and will not use them without your consent. If you use your browser settings to block all cookies or choose on first request not to allow cookies, then you may not be able to access all or parts of our Site(s). For more information about cookies, including how to set your internet browser to reject cookies, please go to www.allaboutcookies.org.

Categories of cookies we use include:

- *Strictly necessary (essential) cookies* – These are required for the operation of our Site. They include, for example, cookies that enable you to log into secure areas of our website, use a shopping cart or help us to choose the right language for you.

- *Analytical/performance cookies* – These allow us to recognize and count the number of visitors and to see how visitors move around our Site when they are using it. This helps us to improve the way our Site works, for example, by ensuring that users are finding what they are seeking easily.

- *Functionality cookies* – These are used to recognise you when you return to our Site. This enables us to personalise our content for you and remember your preferences (*e.g.,* language or country/region).

- We also collect information on the domains through which Online Visitors visit us. We use that data to track trends in Site traffic and as the basis for making improvements. Except for essential cookies, cookies will be set to expire after one year – unless you consent otherwise. Our advertisers may also use cookies, over which we have no control; if you do not wish to be exposed to advertiser cookies or other advertiser online tracking, do not select the advertiser's link or content from our Site(s).

- *Social Plug-Ins and Share Buttons*. We also may use social plug-ins on or in connection with some of our Sites. When you visit a Site that contains a social plug-in and the social plug-in is selected or enabled, your browser establishes a direct connection to the social plug-in operator's server. The social plug-in operator directly transfers the plug-in content to your browser. The social plug-in provider receives information about your access to sites. We have no influence on the data gathered by the plug-in operator. The Online Visitor is responsible for managing his or her privacy consents, settings and preferences, and addressing with the third-party operator, privacy issues that pertain to his or her use of, or plug-in with, third-party social media sites.

When visiting one of our Sites that contains a social plug-in, your browser will establish a direct connection to the respective social network's servers enabling the respective social network to receive information about you having accessed our Site. We have no influence over the data gathered by the social plug-ins and have no knowledge of or control over the data gathered by the respective social network. To our knowledge, the embedded social plug-ins provide the respective social network with information that you have accessed our Site. If you are logged into the respective social network, your visit can be linked to your account. If you interact with the social plug-ins, the corresponding information will also be shared with the respective social network and linked to your account. Even if you are not logged into the respective network, there is the possibility that the social plug-ins transmit your IP-address to the respective social network.

For the purpose and scope of data collection and the further processing and use of data by the respective social network, as well as your rights and ways to protect your privacy, please see the privacy notices of the respective social networks. While every attempt is made to validate and screen outside links that may be provided through our online Sites, we are not responsible for the content of any outside third-party web sites. Bulletin boards, blogs, wikis, chat rooms, exchanges, share sites, social media venues and similar "forums" (whether operated by or for us, or otherwise) often are open or accessible to others in the forums and may be open to the public or those who otherwise gain access to information posted on or through the forum. Your participation in such forums and what you disclose in such forums is totally your own choice. If you make that choice and include your PII in your posts, it may lead to use of your PII by others, and we will not responsible for any information you decide to make available on or through such forums, nor for any contacts of you by others as a result of your participation in, or your own disclosures on or through, such forums. We reserve the right to monitor such forums operated by, for or about us, and Use information legally posted on or through them. There should be no expectation of privacy by anyone with respect to the content of postings or disclosures he or she voluntarily makes on or through such forums.

- IP addresses and "clickstream" information. Some online clickstream data includes User Information. User Information is information about computers that interact with our systems. This includes:
    - *Web server logs*. In the process of administering our Sites, we maintain and track usage through web server logs. These logs provide information such as what types of browsers are accessing our Sites, what pages receive high traffic, and the times of day our servers experience significant loads. We use Internet Protocol ("IP") addresses to analyze trends, administer Sites, track users' movements, and gather broad demographic information for aggregate use. We use this information to improve the content and navigation features of our Sites. Anonymous or aggregated forms of this data also may be used to identify future features and functions to develop for our Sites and to provide better service or a better user experience. We do not link this information with individually identifiable PII. We also reserve the right to, and may, share aggregated and anonymous information with third parties.
    - *Web beacons*. We and third parties also may employ web beacons on or in connections with our Sites or in connection with e-mails and other electronic/digital communications we send, distribute, or have sent or distributed for us. Web beacons are tiny graphics with unique identifiers, similar in function to cookies, and are used to track the online movements of users. In contrast to cookies, which are stored on a user's computer hard drive, web beacons typically are embedded invisibly on webpages and other online or electronic/digital documents and are about the size of the period at the end of this sentence. Web beacons also may be used, for example, in an e-mail, newsletter or other electronic communication to determine if it has been opened by the user or if web links contained in it have been selected by the user. Where required by law, we will ask you for your explicit consent to the usage of web beacons by us and will not use them without your consent. We are not, however, responsible for any third-party deployment or usage of web beacons.

In connection with our Sites (including e-mails and other electronic/digital communications), we also may use or allow analytics or third-party tracking services that also use cookies, flash-cookies, web beacons or other tracking technologies to track legally-permissible non-individually identifiable PII about Online Visitors to our Sites. When these services and their cookies, flash cookies, web beacons or other tracking technologies are used, it is done in the aggregate to capture usage and volume statistics and to manage content, and, absent your advance affirmative consent, not for any other purpose. Some of our business Partners, Internet advertisers, ad servers and ad networks also may use cookies, flash cookies, web beacons and other tracking technologies to collect information about

users' online behavior and use that information for analytics and to serve advertising aimed to be relevant to particular users (*e.g.,* behavioral advertising) in connection with our Sites or links or advertising connected with our Sites. Some of our Customers, and their business partners, also may use cookies, flash cookies, web beacons and other tracking technologies and analytics in connection with their sites, e-mails, online advertisements or other electronic/digital communications which we host, process or deliver for our Customers. We have no access to or control over these third-party tracking technologies and no responsibility for them or with respect to deployment or use of those kinds of analytic technologies by or for another. This policy applies to and covers the use of such tracking and analytics technologies by and for Teradata only, and it does not cover or apply to the use of tracking or analytic technologies by any third party.

We also may use User Information to help us prevent and detect security threats, fraud or other malicious activity, and to ensure the proper functioning of our solutions, products and services.

2.7 "Recourse, Enforcement and Liability" Principle

Teradata maintains procedures for verifying compliance with the commitments we make in this Privacy Policy and to adhere to the EU-U.S. Privacy Shield Framework principles and the Swiss-U.S. Privacy Shield Framework principles. To do this, we complete a privacy compliance assessment at least annually, make improvements based on the results and use the results to self-certify annually to the EU-U.S. Privacy Shield Principles and Swiss-U.S. Privacy Shield Principles. We also provide the resources identified above in the "Contact Us" section of this Privacy Policy so you may raise privacy-related matters with us, and we provide the "dispute resolution" process noted in the "Cross-Border Data Processing" section of this Privacy Policy so that you have a process and mechanism to enforce compliance with the standards set forth in this Privacy Policy. As also noted above, we are subject to the jurisdiction of, and compliance monitoring and enforcement by, the U.S. Department of Commerce and U.S. Federal Trade Commission and by applicable national Data Protection Authorities with respect to certain PII, such as PII in HR data.

3 Exercise Your Rights in Line With Our Principles

3.1 Your Rights

You have the right to:

- be informed of how we Use your PII, including categories to be collected and the purposes it shall be Used for. This right has been met by providing you with this Privacy Policy;
- request access to/disclosure of any PII we have collected about you, and to request information about the purposes of the processing, the categories of PII concerned, the categories of sources of the PII, the recipients/third parties, if any, to whom the PII has been or will be disclosed and the categories that will be disclosed to such recipients/third parties, and the envisaged period for which the PII will be stored;
- request erasure of PII without undue delay. Teradata may satisfy such requests by anonymisation and/or pseudonymisation where it is not reasonably viable to achieve absolute deletion;
- a copy of your PII undergoing processing, as long as that does not adversely affect the rights and freedoms of others.
- if you are in the EEA, ask to have inaccurate data held about you rectified without undue delay. Please notify us if your personal details change or if you become aware of any inaccuracies in the PII we hold about you;
- if you are in the EEA, restrict data processing where you contest the accuracy of the PII, the processing is unlawful but you oppose the erasure of the data, the controller no longer needs

the PII but you require us to retain it in relation to legal claims in which you are involved, or where you have objected to processing pending verification of whether legitimate grounds of the data controller override yours as the data subject; Where permitted by, and at all times to the standard required by applicable law, Teradata may satisfy such requests by anonymisation/de-identification and/or pseudonymisation;

- if you are in the EEA, not to be subject to any material decision that significantly and adversely affects you being taken by or mandated for us solely by a computer or other automated process. Should you believe that a material decision that significantly and adversely affects you has been taken by or mandated for us solely by a computer or other automated process, please let us know through one of the channels set forth in the "Contact Us" section of this Privacy Policy and we then will review, assess and respond with respect to such through human engagement,
- if you are in the EEA, object to the processing of your PII;
- if you are in the EEA, request data portability;

Requests made under the CCPA are restricted to PII collected in the 12-month period preceding Teradata's receipt of a verifiable request and shall be administered subject to the frequencies and other provisions stated in the CCPA. You shall not receive discriminatory treatment if you exercise your rights as set out in this Privacy Policy. You may designate an authorized agent to make your request on your behalf under the CCPA, and provided you have verified, to Teradata's satisfaction, the authenticity and authority of any such agent, the agent may make requests under the CCPA following the process set out in the "General Information" section above.

All the above global rights are exercisable to the extent as may be limited, excused, prohibited or otherwise provided, by applicable law and associated remedies in the relevant country.

3.2 Breaches

If you consider that Teradata has not handled your PII in accordance with the requirements of this Privacy Policy and applicable laws, then please contact us by the appropriate means identified in the "Contact Us" section above. Any alleged breach will be taken seriously. In the EEA and some other countries, you also have the right to lodge a complaint directly with the supervisory authority for privacy in your country.

3.3 Some Specific Uses of PII

3.3.1 Job Applicants/Referrals

Where Teradata handles recruitment directly with you as a candidate (including also when you are referred to us by others), it may do so via various means, including the use of suppliers who collect your PII and transfer it to Teradata and including the use of third party technology. In such situations, Teradata Corporation or the Teradata subsidiary to which you have provided your PII is the data controller of your PII, and will process PII (which may be held on paper, electronically, or otherwise) about you for the specific and explicit purposes set out below. We recognise the need to treat your PII in an appropriate and lawful manner, in accordance with this Privacy Policy and all applicable laws.

Teradata may also process your PII that we obtain from social media sites and we may use that PII to contact you in relation to specific job opportunities at Teradata and then to progress any job application you may make to us.

Although our recruitment activities are typically managed in-house, Teradata may elect to use external organisations to manage our recruitment activities for us. In such a case, such an external organisation would be the data controller of your PII, and you should check you agree to with its privacy policy/notice

before you submitted any PII to it. If used, such external companies might share PII with Teradata for the purposes specified in this Privacy Policy.

The Type of PII We Hold About You

We will collect, store and use the following categories of PII about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- Any data you include within your resume when applying to a position via the career site
- Email address
- Phone number
- LinkedIn profile
- Public social media profiles (LinkedIn, Facebook profile, Xing, etc.)
- Start date, if an offer is extended
- Location of employment or workplace, if an offer is extended
- Copy of driving licence, if background check conducted (sales only)
- Recruitment information (including copies of education/qualifications, right to work documentation, references and other information included in a CV or cover letter or as part of the application process)
- Employment records (including job titles, work history, working hours, training records and professional memberships)
- Compensation history
- Photograph(s)

We may also collect, store and use the following "special categories" of more sensitive personal information: information about criminal convictions and offences, if a background check is sourced from, and provided by, an authorised background check provider

How We Will Use Information About You

We will process PII about job applicants to help us decide whether to offer you employment or other working position at Teradata, for legal, personnel, administrative and management purposes and to enable us to meet our legal and contractual obligations as a potential employer, for example to conduct background and pre-employment screening checks. We may use PII you voluntarily disclose in connection with compiling government and government-contracting labor statistics.

We will only process your PII where you have given your consent or where the processing is necessary for the performance and efficient administration of your application for employment with Teradata, or where the processing is necessary to comply with our legal obligations. In other cases, we may process your PII where such processing is necessary for the protection of your vital interests, for our other legitimate interests as a potential employer or the legitimate interests of others.

We will only process special categories of PII for example about criminal proceedings or convictions, if you have given your explicit consent, or where the processing is necessary so that we can carry out our obligations, and exercise our rights, in relation to your application for employment or for the protection of your vital interests.

Recipients of your PII

The following categories of recipients/service providers may collect and/or receive your PII: our affiliates, subsidiaries, enterprise hiring management providers, recruiting advisors, outsourced talent acquisition providers, pre-employment screening and background check providers (including, without limitation, government authorities such as the police and taxation office), pension providers, pension trustees and their legal and financial advisors, health insurance providers, life assurance providers, other insurance/benefits providers, payroll processors, governmental authorities associated with the administration of your employment, car providers, and equity program providers. To the extent these recipients are outside of the European Economic Area (EEA), Teradata has contractual arrangements in place with the recipients and/or has relied upon appropriate safeguards. You may obtain a copy of these agreements by contacting the Data Protection Officer. Applicant Information is collected in the country where contact for the position is located, in the U.S. in a central HR information repository and at various applicable app cloud facilities/servers. And service providers, as well as other third parties such as background-screening organizations solely for the purposes described above. Applicant Information is retained according to applicable laws and will be deleted or destroyed as required by applicable law.

Period of Storage

Your PII will be stored at minimum until completion of your job application process. In case your application is unsuccessful, we will store your data for a period which we consider it likely that we may want to contact you again to invite you for an application. Data will be destroyed, erased, or pseudo/anonymised from or in our systems when it is no longer required.

3.3.2 Employees, Contractors and Workers

As your employer, Teradata Corporation is the controller of your PII that is provided, stored, processed or otherwise used by or for Teradata, and this means we are responsible for deciding how we hold and use personal information about you. We will process PII (which may be held on paper, electronically, or otherwise) about you for the specific and explicit purposes set out in this Privacy Policy. We recognise the need to treat your PII in an appropriate and lawful manner, in accordance with this Privacy Policy and all applicable laws.

The Type of PII We Hold About You

We will collect, store and use some or all of the following categories or PII about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- Date of birth
- Gender
- Marital status and dependants
- Next of kin and emergency contact information
- National Insurance number/Social Security number/tax identification number
- Passport details
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Start date
- Location of employment or workplace
- Drivers Licence/Copy of driving licence
- Recruitment information (including copies of CV/resume, education/qualifications, right to work documentation, references and other information included in a CV/resume or cover letter or as part of the application process)

- Employment records (including job titles, work history, working hours, training records and professional memberships)
- Compensation history
- Performance/evaluation information
- Disciplinary and grievance information
- CCTV footage and other video and audio information obtained through electronic means such as swipecard records, and call recordings
- Information about your use of our information and communications systems
- Photograph(s)

We may also collect, store and use some of the following "special categories" of PII:

- Trade union membership
- Information about your health, including any medical condition, health and sickness records
- Information about criminal convictions and offences, if a background check is sourced from, and provided by, an authorised background check provider
- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions

How We Will Use Information About You

We will only process your PII where the processing is necessary for the performance and efficient administration and management of your employment contract/relationship with Teradata and to enable us to meet our legal obligations as an employer, for example to pay you, monitor, evaluate and manage your performance and salary, and to administer and confer benefits in connection with your employment. In other cases, we may process your PII where such processing is necessary for the performance of contracts with our customers, partners and prospects (this may include transfer of information about your education, professional skills, work history and CV/resume), for the protection of your vital interests, for our other legitimate interests as an employer and to comply with our legal obligations as an employer or the legitimate interests of others.

We will process "sensitive PII" relating to employees where you have given your consent or where it is necessary so that we can carry out our obligations, and exercise our rights, in relation your employment or other working agreement or for the protection of your vital interests. This may include for example: information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work; the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation; and in order to comply with legal requirements and obligations to third parties.

Employees should note that, when they choose to participate in on-line chat and internal community collaboration/blogging tools, then what they post will be visible to any employee (or contractor with access rights) of Teradata worldwide. If employees do not accept the public nature of these tools, they must refrain from using them. Employees must never post any type of offensive material.

Recipients of your PII

The following categories of recipients will receive your PII: our third-party enterprise system management and technology provider(s), pension/401K providers, pension trustees and their legal and financial advisors, health insurance providers, life assurance providers, other insurance and benefit providers, payroll processors, governmental authorities associated with the administration of your employment, car providers, equity program providers, customers, prospects and partners. All recipients are required to take appropriate security measures to protect your PII. To the extent these

recipients are outside of the European Economic Area (EEA), Teradata has contractual arrangements in place with the recipients and/or has relied upon appropriate safeguards.

Period of Storage

We will not keep your PII for longer than necessary for the purposes specified above. The criteria used to determine that period are the duration of your employment relationship, the duration of the provision of the benefits associated with your employment and the duration of Teradata's legal, contractual, accounting and reporting obligations that relate to your employment. Data will be destroyed, erased, or pseudo/anonymised from or in our systems when it is no longer required.

3.3.3 Marketing/Customer Activities

Marketing is important to allow Teradata to efficiently address the markets it serves.

The Type of PII We Hold About You

We may collect, store and use some or all of the following categories of PII about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- Date of birth
- Gender
- Location of employment or workplace
- IP Address
- Geolocation of web browsing
- information regarding your current and future objectives or preferences to help us understand how we may be of service to you
- your operating environment to accurately present solutions and capabilities;

PII may be collected and Used by your personal contacts at Teradata, such as account managers or marketing personnel.

PII will also be collected and Used when you submit such PII to Teradata, for example via website form submissions and subscriptions, online forums, such as user groups, bulletin boards, surveys, questionnaires and polls, via live or online events, such as training seminars or conferences, including third-party events sponsored or hosted by Teradata, and through the use of registration, subscription, application download, apps, permission-grant, opt-in and log-on ("Register") procedures, as well as cookies, flash cookies, web beacons and other online technology and marketing tools.

We may further collect log-on/Register information, such as user names of Customer/Partner Constituents who log-on to solutions we host for our Customers or who access online service-related portions of or portals through our Sites.

PII also is collected when you Register or contact us to request or subscribe to newsletters, white papers, events, seminars, user groups, conferences, webcasts, webinars, blogs, wikis, training programs, discounts, coupons or other events or offers, services or forums we might provide, when you provide us with other information in an online or paper form, or when you contact us by e-mail, social media post, paper correspondence, telephone or other means. We also collect PII when you choose to participate in special offers, surveys, questionnaires, polls or contests that we conduct or sponsor.

In these situations, Teradata Corporation is the controller of your PII, and this means we are responsible for deciding how we hold and use personal information about you. We will process PII (which may be held on paper, electronically, or otherwise) about you for the specific and explicit purposes set out in this Privacy Policy. We recognise the need to treat your PII in an appropriate and lawful manner all applicable laws. We may also obtain and process such PII about you from a third party, including social media sites, or if it is otherwise in the public domain.

We will only collect, store and use PII about your private life (such as marital status and dependants, preferred hobbies, and sports teams you support) if you yourself have elected to provide it to us.

How We Will Use Information About You

We will usually only process your PII where you have given your consent or where we have a legitimate interest to process your PII - in the context of marketing activities, this is the performance and efficient administration of the relationship we have with you or your employer or the party with whom you have a worker contract, who is our customer or customer prospect, to help us sell and keep you informed about our products and services or events, and otherwise perform marketing activities, including direct marketing and behavioral marketing and advertising and personalized web experiences, to serve you better, and to maintain open communications with you.

Other referral-related information we collect: Certain communications and forums we operate in connection with our Sites and business, or we host or process for our Customers or Partners, may include the ability for you to "refer a friend" or "forward to a friend", or provide a testimonial (collectively, a "Referral"). You must not make a Referral that discloses PII or confidential information you do not have the legal right to share with us; where consent from the referred-person is required by law or through a contractual obligation you have, then you are responsible for obtaining that consent before you provide the Referral. If you make such a Referral, we may track that you made the Referral and share the information that you made the Referral with the referred-person or referred-party.

In other cases, we may process your PII to comply with our legal obligations or the legitimate interests of others. Please note that if you elect to provide us with information relating to your personal life, we may process that data, store it in our databases and use it to market our products and services to you. We will never disclose such personal information to third parties without your consent.

Recipients of your PII

The following categories of recipients may receive your PII: our enterprise customer relationship management and marketing automation tools providers from time to time, including but not limited to our Salesforce and Transcend databases and systems, and our employees and contractors who are associated with the administration of your employer's account with Teradata. To the extent these recipients are outside of the European Economic Area (EEA), Teradata has contractual arrangements in place with the recipients and/or has relied upon appropriate safeguards.

Please note that the use of chatbot technology on our website(s) to optimize user experience/deliver personalized content will result in your IP address and any other PII you supply being collected directly by our 3rd party supplier and its subprocessors, but only for the purpose of providing its service to Teradata. We can supply names of supplier/subprocessors on request.

Period of Storage

We will not keep your PII for longer than necessary for the purposes specified above. The criteria used to determine that period are the duration of your tenure with our customer or customer prospect

and the duration of Teradata's legal and contractual obligations and potential business relationship with our customers and customer prospects. Data will be destroyed, erased, or pseudo/anonymised from or in our systems when it is no longer required.

3.3.4 Miscellaneous Other Processing Situations

We, or third parties who administer on our behalf, may also collect PII of persons (usually limited to name, job title, contact details and, where applicable, university affiliation) when:

- we respond to your requests for example: to process orders and processing downloads for product demonstration or evaluation;
- you log on to our networking sites, such as Peer Advantage, enrol in our customer or partner education or certification courses, for example via Teradata University Network or our Teradata Certified Professional Program, or via our customer education team; We will only use your PII for the purposes of administering such activities and recommending other education/certification courses or events and networking opportunities we believe you may be interested in, or as otherwise stated on any form/log-in credentials you may at the time complete and submit;
- we maintain or upgrade a system - our technical staff may require periodic access to services data to monitor system performance, test systems, run support diagnostics, verify configurations and usage levels, and develop and implement updates, upgrades and patches to systems; when you submit incidents via our customer services incident reporting portal, currently called Teradata@YourService;
- providing technical support including, to address performance and fix issues; on occasion, we may develop new versions, patches, updates, and other fixes to our programs and services, such as security patches addressing newly discovered vulnerabilities, in which cases, in accordance with the terms of a Customer contract or order for such, we may remotely access a user's computer, as permitted under the terms of an applicable contract, to troubleshoot a performance issue, and we also may use such information to provide product updates and notices;
- you log on (for example as an authorised representative/administrator of our customers or partners) to any environments we may host for our customers, such as Cloud/data centre-hosted environments;
- we meet legal requirements. We may be required to provide certain PII to comply with legally-mandated reporting, disclosure, or other legal process requirements, such as to satisfy requirements to disclose PII in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Period of Storage

Your PII will only be stored for the period necessary for you to carry out the activities specified above. Data will be destroyed, erased, or pseudo/anonymised from or in our systems when it is no longer required for the purpose(s) it was collected.

4 Cross-Border Data Processing

Our privacy practices are designed to help to protect your PII all over the world. We take a multidimensional approach to PDP compliance by at least one of several different legally-recognized mechanisms, even if one of those mechanisms becomes invalid, expired or inapplicable. As a multi-national group of companies, Teradata's applicable US entities (namely Teradata Corporation, Teradata Operations Inc., Teradata US Inc., Teradata International, Inc. and Teradata Government Systems LLC) have certified to the Department of Commerce that they adhere to the principles of the

EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework with regard to PII collected from or about residents or citizens of the European Economic Area ("EEA"), European Union ("EU") or Switzerland and, following the withdrawal of the United Kingdom ("UK") from the EU, will do so with regard to residents or citizens of the UK (or as may otherwise be required by UK law). Privacy Shield principles include: Notice; Choice; Security; Access; Accountability for Onward Transfer; Data Integrity and Purpose Limitation; and, Recourse, Enforcement and Liability. You can read how we address those principles above in "Our Principles: Respecting your Privacy and Security".

If there is any conflict between the terms of this Privacy Policy, Supplemental Privacy Terms or an applicable contract and the applicable EU-U.S. Privacy Shield Principles or Swiss-U.S. Privacy Shield Principles, including as they may relate to the UK after the UK leaves the EU, the applicable EU-U.S. Privacy Shield Principles or Swiss-U.S. Privacy Shield Principles, shall prevail and govern.

Privacy Shield-Related Dispute Resolution. Teradata has committed to refer all unresolved Privacy Shield-related PDP complaints/disputes from EU, EEA or Swiss citizens or residents regarding their PII transferred to or for Teradata in the U.S. to an independent dispute resolution services provider and dispute resolution mechanism, and will do the same regarding UK citizens/residents after the UK leaves the EU (or as may otherwise be required by UK law). The provider for such PII-related complaints/disputes is the International Center for Dispute Resolution ("ICDR"), international division of the American Arbitration Association ("AAA"), and the dispute resolution mechanism is the ICDR/AAA International Arbitration Rules, based on documents only and as modified by applicable ICDR/AAA EU-U.S. Privacy Shield Procedures or applicable Swiss-U.S. Privacy Shield Administrative Procedures, and as such may be applied to the UK after it leaves the EU.

Consistent with the principles of the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework, if you are subject to such a framework you may initiate and proceed with this dispute resolution mechanism without any filing fees or dispute-resolution-provider administrative costs being borne by you (*i.e.,* Teradata will be responsible for all filing fees and dispute-resolution-provider administrative fees for such dispute resolution mechanism), and there is the possibility, under certain conditions, for you to invoke binding arbitration. If Teradata does not timely acknowledge or satisfactorily address your PII-related privacy complaint/dispute/problem within 45 days after our receipt of your notice, you may contact the ICDR/AAA and initiate that independent dispute resolution process.

For online access to information about the ICDR/AAA EU-U.S. Privacy Shield or U.S.-Swiss Privacy Shield programs or to initiate a complaint under the ICDR/AAA EU-U.S. Privacy Shield or U.S.-Swiss Privacy Shield Programs, please visit https://go.adr.org/privacyshield.html. For citizens and residents with unresolved privacy complaints/disputes in countries that are not subject to the EU-U.S. Privacy Shield Framework or U.S.-Swiss Privacy Shield Framework, or to the extent your home country does not recognize the above-described dispute resolution provider or dispute resolution process as valid, complaints/disputes may be referred to the AAA and resolved in accordance with the AAA's Commercial Arbitration Rules (see http://www.adr.org), the U.S. Federal Trade Commission, U.S. Department of Commerce, or a data protection authority ("DPA"), court or other forum of competent jurisdiction over the applicable Teradata entity and the data subject. Irrespective of the foregoing, all complaints and disputes regarding HR data that includes employee PII is subject to jurisdiction of the applicable DPA for the country/location of the relevant Teradata employee (including applicants and former employees and their families and beneficiaries regarding whom PII is disclosed to or obtained by Teradata).

For more information about the EU-U.S. Privacy Shield Framework or Swiss-U.S. Privacy Shield Framework, or to access information regarding the status of Teradata's Privacy Shield certification registrations, please go to https://www.privacyshield.gov.

Teradata also takes measures to comply with EEA/EU/Swiss and other countries' cross-border data transfer laws that pertain to PII by having in place express consents and written intra-group data transfer agreements among various Teradata subsidiaries and entities around the world ("Data Transfer Agreements" or "DTAs"). The intra-group DTAs incorporate EEA/EU/Swiss-approved "Standard Contractual Clauses" (also referred to as "Model Clauses"). We also comply with EEA/EU/Swiss data transfer laws regarding PII with respect to other countries that have been recognized by them as having adequate protections for PII (*e.g.,* Israel, Argentina, Canada and New Zealand) by complying with and/or being subject to the jurisdiction of the applicable laws and regulations of those countries for PII that is transferred to those countries. We review and update the intra-group DTAs as our business evolves. Teradata's multidimensional approach to PDP compliance with respect to EEA/EU/Swiss data transfer laws and regulations enables us to comply with EEA/EU/Swiss data transfer laws and regulations by at least one of several different legally-recognized mechanisms, even if one of those mechanisms becomes invalid, expired or inapplicable. After the United Kingdom leaves the European Union, PII transferred from the UK to the EEA and from the EEA to the UK will be processed in accordance with the DTAs or as may otherwise be required by UK law).

5 Information Security Guidelines

5.1 Related Standards, Laws, Practices and Policies

As a publicly-traded company listed on the New York Stock Exchange ("NYSE"), Teradata Corporation is subject to the regulations of, disclosure duties of, and oversight by the U.S. Securities and Exchange Commission ("SEC"), as well as the listing standards and requirements of the NYSE. It is also subject to the Sarbanes-Oxley Act of 2002, Section 404 ("SOX"). Collectively, these requirements include controls, validation of compliance and disclosure of material non-compliance with respect to certain procedures, policies and controls. Accordingly, when we process PII that is subject to PDP laws, we implement policies, practices and procedures intended to comply with those requirements, and we implement controls, testing and validation procedures, such as reviews and audits, to help assure they are complied with. PII categories and PDP laws, including related litigation and regulatory rulings, that we monitor and strive to comply with, include, as applicable:

- Health/Medical (*e.g.,* the Health Insurance Portability and Accountability Act of 1996, Security Rule ("HIPAA"), the Health Information Technology for Economic and Clinical Health ("HITECH") Act in the U.S., and related Omnibus Rules);

- Financial Accounts/Transactions (*e.g.,* the Graham-Leach-Bliley Act ("GLBA"), Privacy and Safeguards Rules in the U.S.);

- Consumer Credit and Credit Cards (*e.g.,* the Fair and Accurate Credit Transactions Act ("FACTA"), Disposal Rule and Safeguard provisions);

- Electronic records and electronic signatures (*e.g.,* FDA Title 21 CFR Part 11 of the U.S. Code of Federal Regulations regarding Food and Drug Administration ("FDA") guidelines);

- Deceptive acts/practices with respect to information (*e.g.,* U.S. Federal Trade Commission ("FTC") regulations, guidelines and rulings);

- Commercial e-mail spam (*e.g.,* Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act of 2003 in the U.S.; the Canadian Anti-Spam Law ("CASL"));

- Personal information and electronic documents (*e.g.,* the Federal Trade Commission ("FTC") Act in the United States; the Personal Information Protection & Electronic Documents Act

("PIPEDA") in Canada; the Federal Data Protection Act in Germany; the PII Act in Sweden; the Data Protection Act in the United Kingdom ("UK"); the Privacy Act in Australia; the Personal Information Protection Act in Japan; CNIL regulations in France; and other privacy protection laws and regulations in China, India and many other countries, provinces and states throughout the world, including the California Online Privacy Protection Act and the Massachusetts Data Security Regulation);

- Personal information possessed and/or processed by government bodies (*e.g.,* the U.S. Privacy Act and, in Canada, the Freedom of Information and Protection of Privacy Act ("FIPPA"));

- Government-issued identification numbers and related information (*e.g.,* various laws pertaining individually identifiable data and identification numbers pertaining to social benefits, public service, social security, driver licenses, etc.);

- Safeguards and notices/remedies for breached data (*e.g.,* various laws requiring proper storage, handling and protection of PII when shared with vendors and service providers, and providing for notices and remedies for certain data breaches);

- California's 'Shine the Light' Law (*e.g.,* Under California Civil Code Section 1798.83, if you are a California resident and your business relationship with us is primarily for personal, family or household purposes, you may request certain data regarding our disclosure, if any, of certain PII to third parties for the their direct marketing purposes; to request such information from us, please send us an e-mail at the California-specific e-mail address under the "Contact Us" heading of this document, specifying in that request if you are a California resident and that you are making a "Request for California Privacy Information"; you may make such a request up to once per calendar year (or more frequently to the extent provided for by applicable law); if applicable, we will provide you by e-mail with a list of the categories of PII disclosed to third parties for their direct marketing purposes during the immediately preceding calendar year, along with the third parties' names and addresses; not all PII sharing is covered by this law);

- Children and students (*e.g.,* the Children's On-line Privacy Protection Act of the United States ("COPPA") and California Student Online Personal Information Protection Act ("SOPIPA"). (No one who has not reached the age of majority in his or her country may use our Sites unless supervised by an adult. Whether or not the preceding sentence applies to you, if you are under 13 years of age, do not register on any of our Sites, do not make any purchases through any of our Sites, and do not send any information about yourself to us, including your name, address, telephone number or e-mail address. In the event we learn we have collected PII from a child without verification of parental consent, we will delete that information. We do not knowingly collect information from children under the age of 13 (or the age of majority in applicable countries) and do not knowingly target our websites, social media, offerings, business activities or other Sites to children. We encourage parents and guardians to take an active role in their children's online, mobile and social media activities and interests. Our goal is to comply with all applicable laws and regulations relating to collection and use of information from children, including COPPA. If you believe we have received information from a child or other person protected under such laws, please notify us immediately by e-mail. We will take reasonable steps not to use or share that information further, and to remove that information from our databases);

- Disabled users (*e.g.,* As a matter of practice, we strive to comply with the sixteen standards for Web Accessibility, written by the Access Board for Section 508 of the U.S. Workforce Reinvestment Act of 1998 (select the following link for more information: http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-

standards), as may be updated from time to time or comparable accessibility standards. We also strive to comply with other accessibility laws, requirements and standards that may apply to our Sites, depending on location and local laws (for example, see the "Teradata Accessibility" link posted at https://www.teradata.com/corporate-social-responsibility/ regarding our accessibility Privacy Policy for Ontario, Canada, which is intended to align with requirements of Ontario, Canada, laws)).

We also have in place physical, technical, procedural and administrative safeguards designed to implement reasonable and appropriate security measures to protect PII from unauthorized access, disclosure and use. Teradata uses security protocols and mechanisms to exchange and transmit sensitive data, such as sensitive financial account data. When sensitive data, such as a credit-card or payment-card account number or security code is entered on our Sites, we encrypt it using secure socket layer ("SSL") technology (or like replacement technology that is at least as secure as SSL).

5.2 Operating Procedures

Teradata also has developed and complies with standard operating procedures designed to meet or exceed various internationally-recognized standards related to PDP to the extent relevant to us and our activities:

- National Institute of Standards and Technology ("NIST") Cybersecurity Framework with regard to our cyber crisis response planning and procedures, and our cybersecurity incident management process
- ISO 15408 for Common Criteria security certification has been achieved for various versions of our flagship Teradata Relational Database Management System ("RDBMS") software
- ISO 27001:2013 certification and compliance has been achieved regarding information security management practices for a Global Consulting Center ("GDC") location of our professional services organization
- Service Capability and Performance ("SCP") Support Standard certification has been achieved by us for best practices in the services industry, including with respect to PDP
- ISO 9001:2008 certification for Teradata Research & Development ("R&D", also referred to as "Teradata Labs") has been achieved with respect to a quality management system to provide products which fulfil customer and regulatory requirements and aim to enhance customer satisfaction – including with respect to features and functions in our products and product development pertaining to PDP
- Capability Maturity Model Integration ("CMMI") Level 3 including Integrated Product and Process Development ("IPPD") has been achieved by us for development of products and services from conception through delivery and maintenance, including with respect to PDP features and functions
- IT Infrastructure Library Framework for high-quality, effective, compliant and proactive managed services
- Payment Card Industry - Data Security Standards ("PCI-DSS") have been satisfied and verified for credit/payment-card transactions where we are the merchant or are hosting such a solution for a customer who is the merchant
- Other indicators – our commitments to and achievements regarding excellence in corporate governance, responsibility and controls has been validated and recognized by us repeatedly having been included in the World's Most Ethical Companies listing and Dow-Jones Sustainability Indices.

5.3 Other Privacy Frameworks and Principles

Our privacy and information security-related policies reflect many additional major frameworks and principles applied around the world, including:

- ISO 29100:2011 (Privacy Framework)
- ISO 27002:2013 (Information Technology – Security Techniques – Code of Practice for Information Security Controls)
- ISO 27018:2014 (Protection of customer PII/data privacy in public cloud environments)
- Online Privacy Alliance Guidelines
- Organisation for Economic Co-operation and Development ("OECD") Guidelines on the Protection of Privacy and Trans-border Flows of PII
- OECD Guidelines for Multinational Enterprises (Article VIII regarding Privacy)
- OECD Guidelines for the Security of Information Systems and Networks
- United Nations ("UN") Guidelines for the Regulation of Computerized PII Files
- International Standards on Privacy and PII Protection (the "Madrid Resolution" on International Privacy Standards)
- European Privacy and Electronic Communications Directive (EU Directive 2002/58/EC)
- Asia Pacific Economic Cooperation ("APEC") Privacy Framework
- European General Data Protection Regulation ("GDPR")
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of PII, and its Additional Protocol regarding Supervisory Authorities and Trans-border Data Flows
- *Cybersecurity in the Golden State*, a 2014 guide by the California Attorney General for businesses regarding PDP
- Australian Privacy Guide by the Office of the Australian Information Commissioner, Mar. 2015
- Article 29 Working Party opinions ("WP29") regarding PDP
- Self-Regulatory Principles for Online Behavioral Advertising ("OBA Principles")
- Council of Better Business Bureaus ("BBB") and Direct Marketing Association ("DMA") PDP principles
- Mobile Marketing Associations Code of Conduct for Mobile Marketing.

We also have an Information Security, Privacy and Regulatory Compliance ("InfoSec") Center of Expertise ("COE") through which we have experienced and certified experts and consultants who provide information, training, tools, resources, best practices and consultation to our business and our customers and business alliance partners regarding privacy protection, privacy compliance and information security. These include encryption, intrusion detection and prevention, vulnerability management, risk assessments, operating system hardening, authentication, identity management, control of access rights, virus protection, disk scrubbing, auditing and monitoring, network security, physical security, database security, security policies and procedures, certification and accreditation.

5.4 Internal Policies, Guidance and Practices

Teradata has numerous internal written global policies (plus local policies in many jurisdictions and supplemental business, organizational, departmental and function/role-specific policies) that pertain to PDP, including:

- Protecting Information within Teradata (CMP 1402)
- Confidential Information Disclosure (CMP 1407)
- Protection of Personal (Employee/Workforce) Data (CMP 204)
- Privacy of Protected (Employee) Health Information (HIPAA) (CMP 205)
- Information Technology Infrastructure Requirements (CMP 1404)
- Data Management (CMP 1406)

- Record Retention (CFAP 111)
- Sharing of (Teradata) Financial Information (CMP 820)
- Publication of Proprietary Technical Information (CMP 911)
- Responding to Governmental Requests for Information (CMP 916)
- Electronic Data Interchange ("EDI") for Trading Data (CMP 1405)
- Corporate Security (CMP 1700)
- Internal Accounting Controls – Information Systems (CFAP 1809)

We publish an "Information Security" ethics guide for our employees that all relevant employees are required to read, receive training on, and certify to – shortly after they are hired by us and annually thereafter in connection with our Code of Conduct training and certification processes. We also publish a "Social Media Guide" for our employees, reinforcing that our PDP policies and practices also apply to their uses of social media.

We publish a "Rules of the Road" IT Security reference document for all Teradata employees and contractors, as well as "Data Protection Awareness – Frequently Asked Questions (FAQ)". In addition to PDP being addressed in our Code of Conduct, our employee Code of Conduct training, our Supplier Code of Conduct and our Business Partner Code of Conduct, we also provide our employees with standalone periodic training regarding PDP.

We have internal IT practices and procedures that pertain to PDP. Our internal written IT Information Protection Standards ("IPS"s) include:

- IPS Administration (IPS 101)
- Information Protection Data Center and Operations Requirements (IPS 102)
- Application Development/Deployment Standards (IPS 103)
- Secure Firewall Implementation (IPS 107)
- User ID and Password Management (IPS 109)
- Platform Compliance Monitoring, Administration & Oversight (IPS 115)
- Server Operating System Security Requirements (IPS 119)
- IT Service Production System Access Authorization Requirements (IPS 125)
- Wireless Network Security Requirements (IPS 127)
- Teradata Information at Non-Teradata Sites (IPS 128)
- Information Security for Connecting Outsourced Development & Support (IPS 129)
- Information Security for Teradata Global Consulting Centers (IPS 130)
- Encryption Standard for Teradata (IPS 131)
- Uses of Non-Teradata-Owned Apple Laptops on the Teradata Network (IPS 132)

Other IT practices we employ to help protect privacy and information include: penetration, vulnerability and firewall tests; anti-virus tools on all workstations; deployment of anti-spam and anti-phishing tools; URL and e-mail filtering; deployment of patch management tools; deployment of host-based intrusion detection system ("IDS") and firewall protection tools; deployment of data loss prevention ("DLP") tools; deployment of network access control tools; scans and blocks for advance persistent threats ("APT"); tests, scans, spot-checks, validations and reviews by internal auditing, as well as third-party subject-matter-expert service providers; deploying full disk encryption on all Teradata laptop computers; encryption on all Teradata servers and selected desktops; deploying Mobile Device Management ("MDM") security tools and requirements for certain mobile devices used to access the Teradata network; and, deploying Multi-Factor-Authentication ("MFA") tools and requirements such as for remote/mobile access to PII through our internal-use apps and Sites. We maintain and regularly update an IT Security internal online site for our employees where information relevant to information security is aggregated and made accessible to our employees.

Our main IT infrastructure production systems are operated from highly secure data centers that are designed and implemented to help assure PDP is achieved. Those systems are routinely backed-up, the back-up data is secured, and redundancy, disaster recovery and business continuity planning are built-in to our practices and procedures with respect to that data.

We conduct background checks and screening (subject to applicable laws) regarding proposed new-hire employees; these are conducted with the prospective employee's express permission or otherwise in compliance with applicable laws, and we have arrangements in place with third-party service providers who assist us with background checks and screening to help assure that the rights of individuals are honored and that their PII is not used or disclosed for any illegal or impermissible purpose. Newly-hired employees are also required to sign agreements providing that they will protect, and not make unauthorized use or disclosure of, private and confidential information that they may have access to through Teradata. All employees confirm such each time they log-on to our network and systems, at which time they also acknowledge and confirm that they are granting us permission to monitor their use of our network, systems, internal-use apps, internal-use Sites and other IT resources, with no expectation of personal privacy by them, to the maximum extent permitted by law.

With respect to consulting, professional services and managed services activities we perform for our customers, we generally control and segregate access to PII that our customers possess or process, and comply with other industry-driven and customer-driven privacy and information security practices. For example, for most of our services engagements for deployments of our solutions at our customer sites or at our customer-selected data centers, we either do not have access to the PII in our customers' data, or, where we do, we often do so solely through secure workstations and network connections provided and managed by or for, the customer, used only for that purpose, and accessible by log-on credentials and other security measures only by our authorized personnel who are in need-to-know positions with respect to that data. Typically, for our customer onsite solutions, we do not access or take possession of our customers' PII or other sensitive data, nor remove it from our customers' sites.

The same applies with respect to our Global Development Centers ("GDC"s), such as those in the Czech Republic, Philippines, India, and Pakistan. The services performed at those centers typically employ stricter controls, practices and procedures are applied to secure and limit access to the PII. Where applicable laws or contract provisions prohibit or restrict access to solutions or information from locations, from countries, or by citizens or residents of other than where the solution or data is located, we implement procedures to help assure we comply with those requirements.

When we run research, development or technical support tests and benchmarks against data for our customers, we rarely have access to or take possession of actual unmodified individually-identifiable PII. If PII is involved, sensitive individually-identifiable data elements typically are encrypted, obfuscated, truncated or otherwise made anonymous. In the exceptional circumstances where we access or take possession of sensitive individually-identifiable PII for critical testing, support or benchmarking, controls, practices and procedures are applied to secure and limit physical and electronic access to the data and data rooms, data centers and facilities involved.

When we host solutions for our customers, we require that it be done on systems that are separate from the IT infrastructure we use and access to manage and operate our own business. The data of various hosted customers is segregated from the data of other customers. Hosted solutions are operated from secure third-party-owned or third-party-operated data centers designed and implemented to help assure that PDP is achieved. The solutions we host, as set forth in the applicable hosting contracts or in standards incorporated into the contracts with our respective customers, are routinely backed-up, the back-up data is secured, and redundancy, disaster recovery and business continuity planning are built-in to our practices and procedures with respect to the hosted-data. Typically, with respect to environments where we serve as a data processor for our data-controller-

customers, the hosted-environment and cloud-environment contracts make it the primary responsibility of our data-controller-customers to specify their policy, government and industry regulatory compliance requirements. We work with our hosted customers and cloud customers to help assure their data is stored, processed and managed according to their requirements. Teradata may also, if contracted to do so, function in the role of consultant to our customers and will help identify and bring to the attention of our customers PDP risks or non-compliance issues we notice in the normal course of business while providing services, hosted offerings or cloud offerings.

When we provide education/certification courses, such as via Teradata University Network and Teradata Certified Professional Programs, Teradata will Use information collected about you to confirm your eligibility for such courses and to use associated websites. Teradata will Use your registration information to send you messages from time to time. You may opt out of receiving such messages, except such messages as Teradata believes are necessary for the administration of associated websites (for example, changes of policy, violations of the terms of use, or compromises to the registration data). If you opt in to receive specific subscriptions to Teradata publications, Teradata will use your registration information to electronically deliver those specific publications to you. Teradata does not disclose your registration information to unaffiliated third parties or use your registration information for any other purposes. Teradata may collect the Internet Protocol address of your computer for data about use of associated websites. Teradata uses cookies to remember your "sign in" information as a convenience to you, maintain a certain user interface state for associated websites, and track your usage associated websites. Please read our Cookie notice on our public websites, and submit your preferences accordingly. Teradata may collect data about pages visited and services used by you. Teradata may match such data to information about you (for example, your user registration). Teradata may provide such data to the executive directors and advisory board members of Teradata University Network. In the case of students, Teradata may provide such information to the student's professors and teaching assistants. Such data may be used in efforts to make associated websites more useful to the Teradata University Network community and to enforce the terms of use for associated websites. Teradata may publish aggregates of such data in descriptions promoting associated websites. The content you submit may be viewed by other members of the Teradata University Network community accessing associated websites. Associated websites may contain links to third-party websites. The Use of PDP about you in connection with such third-party websites is governed by the privacy policies, if any, of such third-party websites.

END OF DOCUMENT