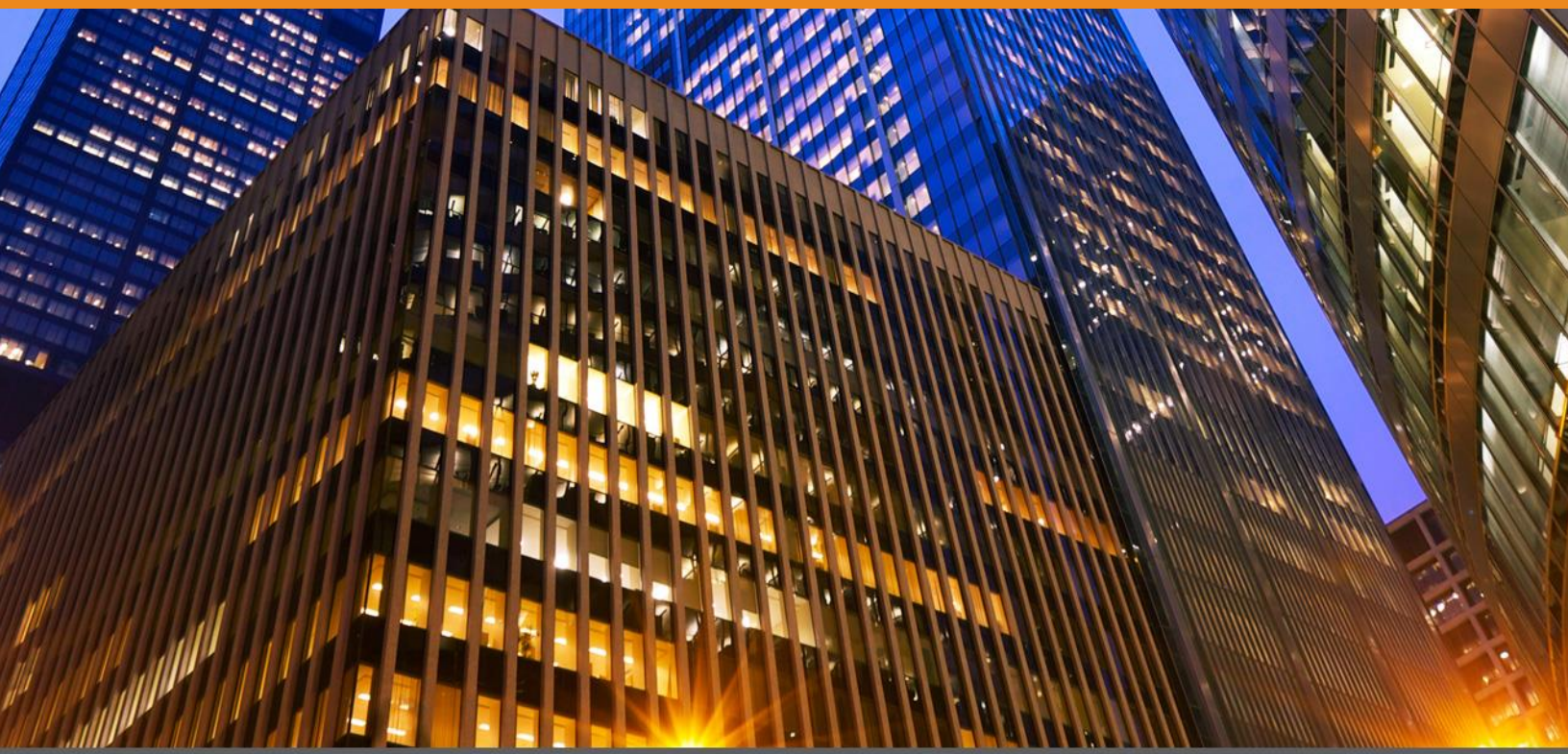
Teradata Corporation
Global Privacy Policy



Effective Date: 04 May 2018

TERADATA.

TERADATA

TERADATA CORPORATION
GLOBAL PRIVACY POLICY

Table of Contents

1. Effective/Last-Change Date

04 May 2018.

2. Scope

This Global Privacy Policy ("Privacy Policy") summarizes the privacy and data protection ("PDP") principles, standards, policies, practices and procedures adopted by Teradata regarding "Personal Information" (as defined in this document; also referred to as "PI" or "personal data"). For purposes of this document, "Teradata" includes Teradata Corporation and all of its subsidiaries throughout the world (also referred to as "we" or "us").

We will treat all PI in accordance with this Privacy Policy or as the relevant persons or data subjects ("you") otherwise consent. This Privacy Policy also applies to 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 other documents and communications to which this Privacy Policy applies, is appended to or is incorporated by reference, and where, if required by applicable law, you additionally have agreed or consented to the terms of this Privacy Policy (collectively, our "Sites").

3. Changes and Supplemental Terms

We will post public notice, such as 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. If we wish to propose using PI in a manner different from that stated and applicable at the time of collection, we will give notice of it, and you will be given the choice to consent or not consent to use of that information in such a way. From time to time, we may propose to supplement or amend this Privacy Policy and other PDP terms with site-specific or interaction-specific information and terms, such as with respect to a particular permission-based subscription, membership, forum, transaction, survey, questionnaire, location, country, information-type or particular other web, information exchange or social media site ("Supplemental Privacy Terms"). If so and when applicable to a Teradata Site with which you are interacting, you will be given notice of, and a choice to consent or not consent to, any such applicable Supplemental Privacy Terms.

In addition, Teradata employees and certain contractors with access-credentials to Teradata online networks may access Teradata internal policies, information protection standards and related information that pertain to PDP (including those that pertain to Human Resources ("HR") data) through the internal Teradata online homepage, currently under the "Resources" tab by selecting "Corporate Policies" and/or "Information Security." Supplemental Privacy Terms also may apply to various Teradata-internal employee/contractor-accessible apps and Sites; If so, the employee/contractor will be given notice of, and a choice to consent or not consent to such Supplemental Privacy Terms. Any employee or applicable contractor who does not have online access

to those items will be provided with relevant copies after he or she requests them from his or her Teradata manager, his or her Teradata HR representative or the Teradata Ethics, Compliance & Privacy Office.

4. Contact Us

Questions, concerns, complaints and disputes regarding this Privacy Policy, data privacy at Teradata or Teradata compliance with applicable PDP laws and regulations or 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

Questions from EEA persons related to the processing of their personal data 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 Information Security Officer
Teradata Corporation
17095 Via del Campo
San Diego, California, USA 92127

In addition, questions, concerns, complaints and disputes regarding this Privacy Policy, data privacy at Teradata or Teradata compliance with applicable PDP laws and regulations or with the principles of the EU-U.S. Privacy Shield Framework or the Swiss-U.S. Privacy Shield Framework, as well as regarding other ethics and compliance issues, may be submitted to the Teradata Ethics Helpline. The Teradata Ethics Helpline is a third-party-administered service that is freely accessible online and by telephone around-the-clock (other than during planned maintenance and unplanned outages) and in multiple languages. It also accommodates confidential and anonymous reporting to the extent permissible under applicable laws. The administrator of the Teradata Ethics Helpline refers

matters raised through the Teradata Ethics Helpline to the Teradata Ethics, Compliance and Privacy Office. You may contact the Teradata Ethics Helpline

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

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

5. Introduction

Privacy is a priority at Teradata. Privacy and information security are very important to us. Maintaining trust, securing private information, and respecting the privacy of everyone we encounter are paramount to us.

Protecting privacy is part of our culture, values and everyday conduct at Teradata. Our commitment to privacy and information security goes beyond what is written in this Privacy Policy. That commitment is a part of our foundation and culture. Integrity, responsibility, being people-focused, and being dedicated to our customers are among our core values that we apply to all aspects of our business, including with regard to PDP. Trust and accountability are declared qualities for which we strive and that we recognize amongst our workforce, supply chains and business partners, including with respect to PDP. Our Code of Conduct includes commitments by, and expectations of, us and all Teradata employees, contractors and suppliers to protect data and comply with laws, including with respect to laws that pertain to PDP. We regularly train, reinforce, set the tone and example from management, and communicate with our workforce about the importance, requirements, standards and practices applicable to PDP at Teradata. Our Supplier Code of Conduct and our Business Partner Code of Conduct also incorporate the principles of the Teradata Code, as well as global laws and standards regarding PDP 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 (which includes privacy-related ethics commitments). For more about our culture, values, codes of conduct, ethics and compliance program and related corporate responsibility initiatives, please see http://www.teradata.com/code-of-conduct/ and http://www.teradata.com/corporate-social-responsibility/ (see particularly the "Teradata Corporate Social Responsibility Report" linked to that webpage).

Privacy and information security also are important customer-relations, employee-relations, contractor-relations, supplier-relations and business-partner-relations and satisfaction issues for us. We have written policies and often agree through contracts and other written undertakings to help assure that we, our suppliers and our service-providers comply with additional PDP requirements, standards and practices, and to help comply with industry, customer, legal, regulatory and individuals' expectations and requirements regarding PDP. More details concerning those laws, requirements, standards, practices and policies are set forth below.

6. Compliance, the EU-U.S. Privacy Shield Framework, Swiss-U.S. Privacy Shield Framework and Data Transfer Agreements

In addition to the compliance-with-laws and other commitments pertaining to PDP as set forth in the preceding section of this Privacy Policy, Teradata, including Teradata Corporation and its U.S.-based controlled subsidiaries, Teradata US, Inc., Teradata Operations, Inc., Teradata International, Inc., and Teradata Government Systems LLC, recognizes, abides by, commits to comply with and self-certifies to compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework, and their underlying principles and sub-principles as set forth by the U.S. Department of Commerce, regarding the collection, use, retention, transfer, disclosure and handling of certain personal, individual and personally-identifiable information collected from or about residents or citizens of the European Economic Area ("EEA"), European Union ("EU") or Switzerland. Those underlying principles include: Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and, Recourse, Enforcement and Liability. More information is set forth below regarding how each of these principles is addressed at Teradata.

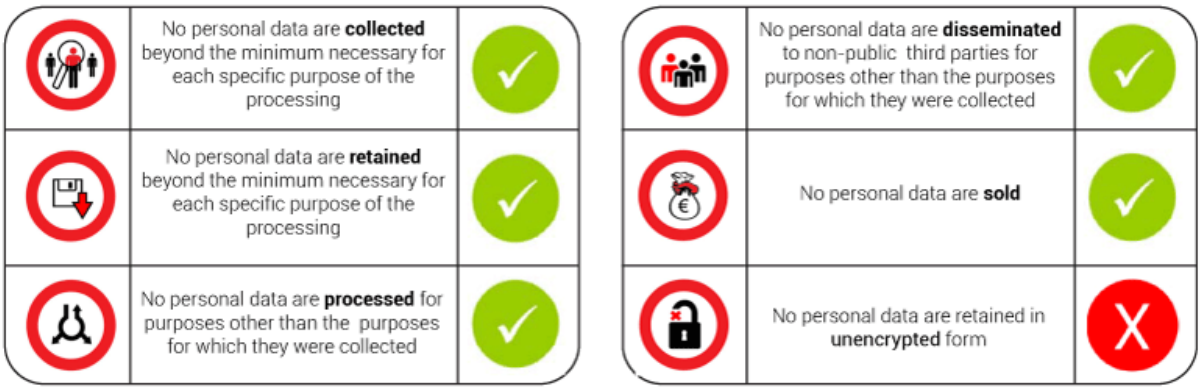
For more information about the EU-U.S. Privacy Shield Framework or Swiss-U.S. Privacy Shield Framework, or to access information regarding the status of Teradata's Privacy Shield certification registrations, please go to https://www.privacyshield.gov.

Teradata also takes measures to comply with EEA/EU/Swiss cross-border data transfer laws that pertain to PI by having in place express consents and written intra-group data transfer agreements among various Teradata subsidiaries and entities in the EEA/EU/Switzerland with various relevant Teradata subsidiaries and entities in United States and other applicable countries ("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 PI with respect to other countries that have been recognized by them as having adequate protections for PI (*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 PI that is transferred to those countries. We have had a number of our intra-group DTAs in place since approximately 2008. We review, change, update and add to the intra-group DTAs as our business, entities, operations, offerings and data flows, and applicable laws, regulations, requirements and frameworks evolve; and, we intend to continue to do so over time. 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 means, even if one of those mechanisms becomes deemed invalid, expired or inapplicable.

Teradata typically acts as a "data processor" with respect to PI we access, collect, use, process, retain, transfer, disclose or handle for one of our customers, and our customer typically serves as the "data controller" with respect to PI processed by or for that customer.

With respect to PI that we access, collect, use, process, retain, transfer, disclose or handle for ourselves, such as with regard to our own employees so we may manage, account for and provide their employment, compensation, benefits and human resources management ("HR data") and with regard to visitors of our online Sites, Teradata typically serves as the "data controller." Our service providers who access, collect, use, process, retain, transfer, disclose or handle PI for us typically serve as downstream "data processors" or "sub-processors" for us.

Overview regarding how we handle Personal Information when we are the "data controller":



Teradata has accountability for PI that it receives under applicable EU-U.S. Privacy Shield Principles or Swiss-U.S. Privacy Shield Principles and subsequently transfers to a third party, as described in the EU-U.S. Privacy Shield Principles and Swiss-U.S. Privacy Shield Principles that are accessible through the corresponding links above. Teradata remains responsible and liable under those Principles if third-party agents who Teradata engages to process applicable PI on Teradata's behalf do so in a manner inconsistent with those Principles, unless Teradata proves that it is not responsible for the event giving rise to the damage at issue. With respect to PI transferred from the EEA/EU/Switzerland to Teradata in the U.S. or Teradata data processors or sub-processors, 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, the applicable EU-U.S. Privacy Shield Principles or Swiss-U.S. Privacy Shield Principles shall prevail and govern.

Questions, Issues, Complaints and Disputes. Teradata commits to try to address all questions, concerns, complaints and disputes you may have with us regarding your privacy and our collection or use of your PI. You may submit questions, concerns, complaints and disputes directly to Teradata at the e-mail or mailing addresses set forth under the "Contact Us" heading of this document, or through the Teradata Ethics Helpline, also as set forth under the "Contact Us" heading of this document. With respect to PDP-related complaints and disputes, we commit to respond within a reasonable timeframe, not to exceed 45 days, or any shorter time period required by law, and include a description of our assessment of the merits of the complaint/dispute/problem and of how we will rectify the complaint/dispute/problem.

Dispute Resolution. Teradata also has committed to referral of all unresolved PDP complaints/disputes from EU, EEA or Swiss citizens or residents regarding their PI transferred to or for Teradata in the U.S. to an independent dispute resolution services provider and dispute resolution mechanism. The provider for such PI-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. 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 PI-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 http://info.adr.org/safeharbor/. For citizens and residents of 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, but who have unresolved privacy-related complaints about or disputes with Teradata, 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 PI 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 PI is disclosed to or obtained by Teradata).

Teradata compliance with this Privacy Policy is subject to monitoring and enforcement by the U.S. Department of Commerce and the U.S Federal Trade Commission, and Teradata will cooperate with applicable national DPAs with respect to such compliance and any complaints/disputes arising from residents or citizens of that country. We also commit to maintain records regarding implementation of our PDP policies and make them available upon request by U.S. authorities or the above-designated independent dispute resolution provider. And, we commit to appoint a designated Data Protection Officer ("DPO") within Europe and each applicable country as, where and when required by applicable law, such as the European General Data Protection Regulation ("GDPR").

7. Other Privacy Frameworks and Principles

In developing and validating our privacy and privacy-related information security policies and standards, we respect, have adopted and/or have taken into account many additional major frameworks and principles developed and applied around the world (many of which also have been incorporated into the laws of various countries, provinces, states and other jurisdictions), 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 Personal Data
- 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 Personal Data Files
- International Standards on Privacy and Personal Data Protection (the "Madrid Resolution" on International Privacy Standards)
- Asia Pacific Economic Cooperation ("APEC") Privacy Framework
- European Data Protection Directive (EU Directive 95/46/EC)
- European Privacy and Electronic Communications Directive (EU Directive 2002/58/EC)
- European General Data Protection Regulation ("GDPR")
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 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.

8. Related Standards, Laws, Practices and Policies

Teradata Corporation is a publicly-traded company listed on the New York Stock Exchange ("NYSE"). It 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 also is subject to the standards, controls and obligations of the Sarbanes-Oxley Act of 2002, Section 404 ("SOX"). Collectively, the requirements of

these bodies and laws include controls, validation of compliance and disclosure of material non-compliance with respect to certain procedures, policies and controls. Accordingly, when we come to possess, control, process, transfer or transmit PI 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. PI categories and PDP laws, including related litigation and regulatory rulings, we monitor and take acts to comply with, where, and as applicable, include:

- 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 Personal Data 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 PI 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 PI to third parties for the their direct marketing

purposes; to request such information from us, please send us an e-mail at one of the e-mail addresses 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 PI 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 PI 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 PI 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 http://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 and protect PI 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).

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. These include:

- 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 17799 certification has been achieved for our remote security processes and procedures
- ISO 27001:2005 or 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 fulfill 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.

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. Features, functions and offerings in this area 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. Because these aspects of our business, products, services, business alliance partner offerings, and InfoSec COE resources and offerings are extensive and being changed, updated and expanded continuously, please visit and browse our Sites for current information related to our PDP products, services, offerings, partners and resources.

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 the following global policies (a Teradata "Corporate Management Policy" is designated below as a "CMP"; a Teradata "Corporate Finance and Accounting Policy" is designated below as a "CFAP"):

- 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 their understanding of and compliance with – shortly after they are hired by us and annually thereafter and 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 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 practices, procedures and 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 PI is not used or disclosed for any illegal or impermissible purpose. Newly-hired employees are also required to sign agreements and acknowledgements to agree and verify they will protect, not make unauthorized use of, and not make unauthorized disclosure of private and confidential information to which they may have access through Teradata, and all employees confirm such each time they log-on to our network and systems, as well as 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.

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 PI 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.

With respect to consulting, professional services and managed services activities we perform for our customers, we generally control and segregate access to PI 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 PI 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' PI 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 do not involve access to or possession of customer data that includes PI, particularly with respect to PI that is individually-identifiable or individually-sensitive. In the exceptional circumstances where we do, controls, practices and procedures are applied to secure and limit access to the PI. 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 PI. If PI 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 PI 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 managing according to their requirements. Teradata also, upon occasion and as set forth in the applicable engagement contract, functions 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. 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 collection, use, and retention of PDP about you in connection with such third-party websites is governed by the privacy policies, if any, of such third-party websites.

Written contracts typically are entered into and apply to each circumstance applicable to us that involve PI. For example, written contracts are entered where: our solutions are located and services are performed onsite for a customer; we provide services offsite through a GDC; we are running tests, benchmarks or providing technical support services; or, we are hosting a solution for a customer. Also, contracts may be entered into between various Teradata subsidiaries to help assure and document that adequate PDP measures are implemented, information is secured, and applicable laws are complied with, including those that pertain to trans-border data export, transfers and flows (*e.g.*, adopting and applying EU-U.S. Privacy Shield Framework principles, Swiss-U.S. Privacy Shield Framework principles or EU Standard Contractual Clauses (Model Clauses) in Data Transfer Agreements). We also enter into written contracts with our applicable service

providers, contractors and subcontractors; these contracts typically include or incorporate confirming and supplemental PDP and compliance-with-laws obligations.

9. Principles – EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Alignment

The following further identifies the key principles aligned with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework that we apply to data privacy and privacy-related information security at Teradata, particularly with respect to PI from or about individuals, employees and online visitors. We apply these principles even where and to the extent the EU-U.S. Privacy Shield Framework or the Swiss-U.S. Privacy Shield Framework may be deemed inapplicable or invalid, and we also apply them through Data Transfer Agreements and practices intended to comply with applicable local/country PI and PDP laws and regulations. For each of the identified principles, the following aligns with and provides additional information about how those principles are incorporated into, and applied by us through, our polices, practices and procedures. Relevant statements and portions of the preceding sections of this Privacy Policy also apply to and are incorporated into this section by reference.

9.1 "Notice" Principle

Through this Privacy Policy Teradata provides notice to online visitors, consumers, employees, customers, partners and others ("you") with clear and accurate information about our policies, practices and procedures that pertain to the collection, use, retention, transfer, disclosure and handling ("Use") of Personal Information ("PI"), and our compliance with privacy and data protection ("PDP") standards and laws.

Teradata believes and recognizes that you have the right to be informed about PI being collected regarding you individually and about the intended-use of that PI. We believe and recognize that you have the right to determine whether you will allow collection or other Use of your PI, to know the purpose of that collection and Use, and to unsubscribe or otherwise opt-out if you do not wish, or no longer wish, to have some or all of your PI collected, Used at all, or Used for a particular purpose (other than as expressly set forth herein, such as when necessary in connection with a transaction, employment or legal-compliance obligations). We also believe and recognize that you have the right to review individually-identifiable PI about you that we collect, retain or otherwise Use, and you have the right to have a way to update, correct and/or obtain deletion of such PI (except to the extent we are required by law to maintain it).

Teradata will apply these principles through practices that have the equivalent effect of this policy regardless of the specific technologies utilized for the collection or other Use of your PI. We also will apply these principles to your PI, whether it is in electronic or paper form.

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 a company's entire analytical ecosystem. We help customers access and manage data and use analytics

to extract business value and insight from their data. We work with our customers enabling them to leverage data and analytics to drive business outcomes such as, but not limited to:

- Improving a customer's experience through understanding behavioral patterns.
- Driving financial transformation with accurate and timely data.
- 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. We do this through flexible deployment options, including the Teradata Cloud and public clouds, as well as on-premises on Teradata hardware or commodity hardware.

The Teradata 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 both the business and technical leaders in our customers' organizations. Our business analytics solutions and technology 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 with offerings for the world's largest analytic data opportunities. 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 where we operate. We are a global multinational company. Our corporate headquarters is located in Dayton, Ohio, although our Rancho Bernardo (San Diego), California and Johns Creek (Atlanta), Georgia facilities are also primary locations (within the U.S.). We are incorporated in the State of Delaware in the U.S. As of December 31, 2017, we operated 112 facilities in 44 countries throughout the world. We own our Rancho Bernardo complex, while all other facilities are leased. We have more than 10,000

employees worldwide, and as such, our information sources, data subjects, data objects, and data flows often span the globe. Our supply-chain reaches across the globe.

Notice of the types of information we handle. We acquire, administer, operate, host, outsource, interact with, maintain, support 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; and,
- use by or 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 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 whose information we handle. In connection with these activities and other interactions incidental to our business, we often access, collect, store, process, disseminate and otherwise Use information, in either or both electronic/digital form or physical/paper form, regarding a variety of people and entities. These include those in the following categories:

- "Visitors" - including those who choose to visit, respond to or use 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 other categories.

Notice about Personal Information. For purposes of this Privacy Policy, "Personal Information" or "PI" 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; personal information regarding and identifiable to you to the extent it is subject to privacy law or privacy regulation provisions, protections or restrictions; and, non-public information regarding and identifiable to individuals to the extent subject to privacy or confidentiality provisions, protections or restrictions in, or incorporated into, written or electronic contracts entered into by or for Teradata.

Notice about collection and use of Personal Information regarding Online Visitors. As set forth in more detail below, we collect information about Online Visitors to our online Sites, including 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. If you choose to Register, such as to receive more information about us, our products or services, or about our Customers or Partners or their products or services, we may ask for certain information in order to keep you informed about available information, products, services and offerings, to serve you more effectively and efficiently, and to maintain open communications with you. In addition to contact information, our request may include, but not be limited to: name, title, company, postal address, telephone numbers, and e-mail address; information regarding your current and future objectives or preferences to help us understand how and when we may be of service to you; your operating environment to accurately present solutions and capabilities; and, other information from time-to-time to aid us in improving our communications, online Sites and marketing efforts. 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. PI 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 PI when you choose to participate in special offers, surveys, questionnaires, polls or contests that we conduct or sponsor.

9.2 "Choice" Principle

Teradata commits to provide consumers and employees with information on the intended use of PI pertaining to them, and with mechanisms permitting the exercise of choice by them regarding disclosure of that information. More specifically:

Consumers - Teradata will not release PI to unaffiliated third parties, unless (1) the consumer requests it or expressly consents to it, (2) the data is provided to help complete a consumer-initiated transaction, (3) the disclosure is required by law, or (4) the consumer 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 PI to unaffiliated third parties, except and only 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, or (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).

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 PI with third parties. For example, we may disclose your PI 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 PI in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In addition, your PI may be transferred and/or assigned to another company that acquires the stock, or all or part of the assets or operations of Teradata (or of an applicable Teradata business operation or Teradata organization), for example, as the result of a sale, merger, reorganization, dissolution, bankruptcy, receivership or liquidation. If such a transfer or assignment occurs, the acquiring/assignee company's

Use of your PI also will be subject to this policy and the privacy preferences and choices you have expressed to us. While we are committed to maintaining the privacy and security of your PI in compliance with this policy and to the extent reasonably possible, we cannot and do not promise or guarantee that your PI always will remain totally private.

9.3 "Accountability for Onward Transfer" Principle

The EU-U.S. Privacy Shield Framework, Swiss-U.S. Privacy Shield Framework, HIPAA and other laws typically allow transfer of PI 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 PI 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 PI in response to lawful requests by public authorities, including to meet national security or law enforcement requirements; and

- to any other third party with, and to the extent of, your affirmative consent.

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

Trans-border data transfers/flows. Teradata is a global company with technical systems and processes that cross various national and other jurisdictional borders. PI collected by us may be transferred across country, state, provincial and other jurisdictional borders, and stored, transported or processed in the U.S. or any other country in which we operate or maintain facilities for the purposes of data consolidation, storage, transportation, information management and other Use. Trans-border data transfers of PI are performed only if and as permissible by applicable law and, where required by applicable law, with the consent of the data subject. We will handle your PI collected by our systems in a consistent manner, as described in this Privacy Policy, any applicable Supplemental Privacy Terms and your affirmative consent, even if the laws in some relevant countries or jurisdictions may provide less protection for your PI. Our privacy practices are designed and intended to help to protect your PI all over the world.

If Consumer or Employee PI is provided to an affiliated third party (*e.g.,* subsidiaries, service providers, contractors or other Partners), Teradata will require the third party to adhere to similar PDP principles as those that apply to Teradata and that provide for keeping such data confidential and not Using it for any other purposes. Teradata typically achieves this by including 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 document), 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. 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 PI. To the extent, if any, that a downstream "data processor" for Teradata breaches its legal or contractual duties with respect to PI 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.

9.4 "Security" Principle

Teradata will take appropriate measures to ensure that PI 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 PI 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 Information Security Officer the ultimate responsibility to manage our global information security program.

Access control. We limit access to PI 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 the company, 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 PI.

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 and implement 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.

9.5 "Data Integrity and Purpose Limitation" Principle

Teradata will limit the collection and other Use of sensitive individually identifiable PI 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. Individually identifiable PI 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. When we do receive that kind of PI from you, we do not share it 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 voluntary choice. If you make that choice and include your PI in your posts, it may lead to use of your PI 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 PI. 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 PI 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.

How we use personal information. We also may use PI for the following purposes:

To respond to your requests. These requests may include processing orders and processing downloads for product demonstration or evaluation.

To 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. This may include providing technical support including through a customer support portal. Any temporary copies of services data created as a necessary part of this process are maintained only for time periods relevant to and necessary for those purposes.

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 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. We also may use such information to provide product updates and notices.

To provide informational services. We may use PI while providing online forums, such as user groups, bulletin boards, surveys, questionnaires and polls. We may do so while delivering live or online events, such as training seminars or conferences, including third-party events sponsored or hosted by Teradata.

To meet legal requirements. We may be required to provide certain PI to comply with legally-mandated reporting, disclosure, or other legal process requirements, such as to satisfy requirements to disclose PI in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

To market products and services. We may use such information to inform you about products, services or events, and otherwise perform marketing activities, including for and to enable direct marketing and behavioral marketing and advertising and personalized web experiences.

Applicant/Employee information we collect. We also collect "Applicant Information" – individually identifiable PI such as name, home address, personal telephone number, resume and other information you voluntarily provide when you submit a job application to us (directly or through and an app or third-party recruiter), including sensitive information such as racial or ethnic origin, membership in a political association or trade union, or health information if you choose to provide it as part of the job application or other information form, either online or on paper (including voluntary disclosures you may make in connection with compiling government and government-contracting labor statistics). We also collect names and contact information for referrals and alternative-contact people if provided as part of the job application process. PI from references and alternative-contact people may only be provided to us by the applicant or employee; if you are the applicant/employee please provide PI regarding a reference or contact-person only after you have received consent from the reference or alternative-contact person. 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. Applicant Information is used solely to assess the applicant's qualification and skills, to communicate with the applicant, to verify the submitted-information, including reference and background checks to the extent permitted by applicable law, and for legal-defense-purposes as necessary. Applicant Information 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 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. Applicant Information (including any changes or updates thereto) will be added to your employment record and may be Used for employment-related purposes if, when or after you have become a Teradata Employee. We also collect and otherwise Use Employee data and PI as set forth elsewhere in this document, and otherwise as reasonably necessary and in connection with the employment relationship, Employee transactions, Employee contracts, and Employee compensation, benefits, social-benefits-reporting and withholding, tax withholding and reporting, and the like.

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 PI 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.

9.6 "Access" Principle

Teradata strives to maintain the accuracy of the PI we hold, including establishing, as appropriate, mechanisms allowing Consumers and Employees to have the opportunity to review and correct, and in some circumstances obtain deletion of, PI about themselves.

You may review and correct, and (to the extent not limited or prohibited by applicable law) have us delete, your PI that we hold by requesting such by e-mail or correspondence addressed to one of the applicable sources identified in the "Contact Us" section of this policy. When you do so, please provide your name, mailing address, and a clear description of the information you wish to review, correct or have deleted. We will respond promptly within the time limits established by applicable law, but at least within 30 days after your request. For your protection, we may ask you for additional information to verify your identity. In most cases, we will provide the access you request and will correct or delete any inaccurate information you discover. In some cases, however, 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 PI 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 PI – 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 PI, 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 PI 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 PI 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 no later than 30 days after our receipt of the request.

9.7 "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 questions, issues, concerns, complaints and disputes with us, and we provide the "dispute resolution" process noted above in the "Compliance, Privacy Shield Framework and Data Transfer Agreements" section of this Privacy Policy to help assure 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 PI, such as PI in HR data.

10. General Data Protection Regulation (Compliance and Generally Applicable Provisions regarding EEA Personal Data)

Many, if not all, of the principles and provisions of the General Data Protection Regulation ("GDPR") as applied to EU/EEA personal data are complied with through application of the foregoing provisions of this Privacy Policy. This section further describes how the GDPR applies to the foregoing provisions of this Privacy Policy as applied to EU/EEA personal data, and also what they mean with respect to application of the GDPR to the particular categories of EU/EEA personal data detailed below. To the extent, if any, that the following supplements the foregoing, such additional provisions shall apply and become effective as of 25 May 2018 and they take precedence over the foregoing if there is any conflict between them.

Teradata is a global company with personnel, technical systems and processes that cross various national and other jurisdictional borders. Personal data collected by us may be transferred across country, state, provincial and other jurisdictional borders, and stored, transmitted or processed in the U.S. or any other country in which we maintain facilities

for the purposes of data consolidation, storage, information management and other Uses.

10.1 Data Security

We will take reasonably appropriate measures to help prevent or mitigate unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. We will have and apply reasonably appropriate procedures and technologies intended to maintain the security, integrity and availability of all personal data from the point of collection to the point of destruction. We will transfer personal data to a third party only if it agrees to comply with those procedures and policies, or if it puts in place reasonably adequate measures itself.

10.2 Processing in Line with Your Rights

You have the right to:

- Be informed of how we process your personal data (this right has been met by providing you with this Privacy Policy);
- Request access to any personal data we hold about you, and to request information about the purposes of the processing, the categories of personal data concerned, the recipients to whom the personal data has been or will be disclosed, and the envisaged period for which the personal data will be stored;
- 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 personal data we hold about you;
- Request erasure of personal data (except to the extent as may be limited, excused or prohibited by applicable law) without undue delay. Where permitted by, and at all times to the standard required by applicable law, Teradata may satisfy such requests by anonymisation and/or pseudonymisation where it is not reasonably viable to achieve absolute deletion;
- Restrict data processing where you contest the accuracy of the personal data, the processing is unlawful but you oppose the erasure of the data, the controller no longer needs the personal data 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 and/or pseudonymisation;
- 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,
- Object to the processing of your personal data;

- Request data portability;
- A copy of your personal data undergoing processing, as long as that does not adversely affect the rights and freedoms of others.

10.3 Breaches of GDPR and Other Applicable Laws

If you consider that Teradata has not handled your personal data in accordance with the requirements of the GDPR or other applicable laws, then please contact the EEA Data Protection Officer identified in the "Contact Us" section above. Any alleged breach will be taken seriously. You also have the right to lodge a complaint directly with the supervisory authority for privacy in your country.

10.4 EEA Job Applicants

Where Teradata handles recruitment directly with you as a candidate, it may do so via various means, including the use of suppliers who collect your personal data and transfer it to Teradata and the use of third party technology. In such situations, Teradata Corporation or the Teradata subsidiary to which you have provided your personal data is the data controller of your personal data, and will process personal data (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 personal data in an appropriate and lawful manner, in accordance with the GDPR and all applicable laws.

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

Teradata may use external companies to manage our recruitment activities for us. In such a case, such an external company would be the data controller of your personal data, and you should only provide your personal data to it if you agree with its privacy policy/notice. Such external companies may share your personal data with Teradata for the purposes specified in this Privacy Policy.

10.4.1 The Type of Personal Data We Hold About You

We will collect, store and use the following categories of personal data 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 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

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

10.4.2 How We Will Use Information About You

We will process personal data 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 will only process your personal data 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 personal data 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 personal data 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.

10.4.3 Recipients of your personal data

The following categories of recipients may collect and/or receive your personal data: our enterprise hiring management providers, our 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.

10.4.4 Period of Storage

Your personal data 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, but not longer than for a period of five years. Data will be destroyed, erased, or pseudo/anonymised from or in our systems when it is no longer required.

10.5 EEA Employees, Contractors and Workers

As your employer, Teradata Corporation is the controller of your personal data 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 personal data (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 personal data in an appropriate and lawful manner, in accordance with the GDPR and all applicable laws.

10.5.1 The Type of Personal Data We Hold About You

We will collect, store and use the following categories or personal data 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
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Start date
- Location of employment or workplace
- Copy of driving licence
- 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
- Performance information
- Disciplinary and grievance information
- CCTV footage and other information obtained through electronic means such as swipecard records
- Information about your use of our information and communications systems
- Photographs

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

- 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

You can always access the then-current version of this Privacy Policy via Teradata website or internal employee portals, currently Teradata Connections. If you are unable to do so or wish to receive a copy of an earlier version, please request such through one of the channels identified in the "Contact Us' section of this Privacy Policy and we will provide such to you within no later than 30 days after our receipt of your request.

10.5.2 How We Will Use Information About You

We will only process your personal data where the processing is necessary for the performance and efficient administration of your employment contract and to enable us to meet our legal obligations as an employer, for example to pay you, monitor and manage your performance and salary, and to administer and confer benefits in connection with your employment. In other cases, we may process your personal data 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), 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 personal data" 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.

10.5.3 Recipients of your personal data

The following categories of recipients will receive your personal data: our third-party enterprise system management provider(s), pension providers, pension trustees and their legal and financial advisors, health insurance providers, life assurance providers, other insurance 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 personal data. 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.

10.5.4 Period of Storage

We will not keep your personal data 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.

10.6 EEA Marketing Activities

Marketing is important to allow Teradata to efficiently address the markets it serves. To do so, Teradata will collect, store and use the following categories of personal data.

10.6.1 The Type of Personal Data We Hold About You:

We may collect, store and use some or all of the following categories of personal data 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

This will occur when you submit such personal data to Teradata, for example via website form submissions and subscriptions or via your personal contacts at Teradata, such as account managers or marketing personnel. In these situations, Teradata Corporation is the controller of your personal data, and this means we are responsible for deciding how we hold and use personal information about you. We will process personal data (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 personal data in an appropriate and lawful manner, in accordance with the General

Data Protection Regulation (GDPR) and all applicable laws. We may also obtain and process such personal data 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 personal data 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.

10.6.2 How We Will Use Information About You:

We will usually only process your personal data where you have given your consent or where we have a legitimate interest to process your personal data - 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 our products and services. In other cases, we may process your personal data 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.

10.6.3 Recipients of your personal data:

The following categories of recipients may receive your personal data: our enterprise customer relationship management and marketing automation tools providers from time to time, 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.

10.6.4 Period of Storage

We will not keep your personal data 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.

10.7 Miscellaneous Other Processing Situations

We, or third parties who administer on our behalf, may also collect personal data of EEA persons (usually limited to name, job title, contact details and where applicable university affiliation) when you log on to our networking sites, such as Peer Advantage, enroll 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, or when you submit incidents via our customer services incident

reporting portal, currently called Teradata@YourService, or when 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 will only use your personal data 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. Your personal data 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.

END OF DOCUMENT