teradata.

Teradata Corporation Global Privacy Policy

Effective Date: January 13th, 2025

Privacy Statement

Table of Contents

Introduction

This Privacy Statement provides clear and accurate information about the privacy and personal data protection ("Privacy") measures adopted by Teradata Corporation and its subsidiaries worldwide (collectively, "Teradata," "we," "us," "our"). It also explains how we process your Personal Data, including how we collect, use, access, retain, transfer, disclose, and handle it.

"Personal Data" means information that identifies you directly, like your name or email address. It also includes information that can be reasonably linked or combined with other information to identify you, like an account number or IP address. Some countries and privacy laws use terms like "Personal Information" or "Personally Identifiable Information" for the same types of information. In this Privacy Statement, we use the term Personal Data to mean all such terms. We are committed to transparency and ensuring you are fully informed of, and confident about, how we handle your Personal Data.

This Privacy Statement applies to all offline and online interactions across all channels with our Visitors, Customers, Partners, Applicants, Employees, and Others as those terms are defined below. Such channels include Teradata websites, social media sites, education and networking sites, mobile and desktop applications ("apps"), data analytics platforms and associated services and sites, other online portals, contacts, and communications between you and Teradata. This Privacy Statement also applies to any other scenario to which it is stated to apply or is incorporated by reference.

Who We Are

At Teradata, we believe that people thrive when empowered with trusted information. That's why we built the most complete cloud analytics and data platform for AI.

By delivering harmonized data, Trusted AI, and faster innovation, we uplift and empower our customers—and our customers' customers—to make better, more confident decisions. The world's top companies across every major industry trust Teradata to improve business performance, enrich customer experiences, and fully integrate data across the enterprise.

We drive positive impact for hundreds of millions of people every day around the world with faster, flexible data integration and trusted, cost-effective AI innovation.

We are a global organization with our corporate headquarters in Rancho Bernardo (San Diego), California. We are incorporated in the State of Delaware in the U.S. We own our Rancho Bernardo complex, while all other facilities are leased. We have employees worldwide, and as such, our information sources, data subjects, data flows, and supply chain span the globe.

Our Approach to Privacy

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

We have elected to adopt a globally uniform approach to Privacy, as set out in this Privacy Statement. In the unlikely case that applicable Privacy laws exceed the standards in this Policy, then we meet those standards. While we adopt a globally uniform approach to Privacy, your legal rights and remedies are exercisable to the extent provided by applicable law in the relevant jurisdiction where you reside.

To manage Teradata's Privacy program across a complex global landscape of Privacy laws, we have adopted a Privacy Program Framework that establishes a standard set of criteria, mapped to our various legal privacy requirements. We use this framework to implement, maintain, assess, and continually improve our Privacy program. Our Code of Conduct annual certification and other Privacy-related training include expectations of and commitments by all Teradata employees, contractors, and business partners to protect data and comply with Privacy laws. Additional privacy training is provided on an as needed based on role or topic. For example, individuals responsible for handling data subject requests trained on how respond to individuals exercising their rights under such laws.

Our Supplier Code of Conduct and our Business Partner Code of Conduct incorporate the principles of this Privacy Statement, the Teradata Code of Conduct, global Privacy laws, and standards and the principles of the United Nations Global Compact and the Responsible Business Alliance ("RBA," formerly the Electronic Industry Citizenship Coalition ("EICC")) Code of Conduct. For more information, please see our **Code of Conduct** and **Environmental and Social Governance page** (see particularly the "Teradata Corporate Social Responsibility Report" linked to that webpage).

Our Role in Processing Personal Data

Teradata typically acts as a data controller with respect to Personal Data that we collect and use for ourselves, as described in this Privacy Statement. Our service providers who handle Personal Data on our behalf typically serve as downstream data processors or subprocessors for us. Teradata also acts as a data controller for any Personal Data provided by customers in the course of doing business with us, such as customer contacts' names, email addresses, usernames, and usage details of our customers' use of our platforms.

Teradata typically acts as a data processor with respect to any Personal Data we process on behalf of our customers, including customer data processed within our platforms. Our customers typically serve as the data controller with respect to that Personal Data. Where we serve as a data processor for our customers, it is typically our customers' responsibility to specify their policies and regulatory compliance requirements, including Privacy compliance. We work with our customers to help ensure the data in their environments is stored, processed, and managed according to their specified contractual requirements. If contracted to do so, Teradata may also function in the role of consultant to our customers. In such cases, Teradata will help customers identify Privacy risks or non-compliance issues we notice in the normal course of business while providing services, hosted offerings, or cloud offerings. However, our customers retain ultimate responsibility for the compliance of their environments.

For more information about our roles in processing customer data and customer confidential information, please see our memo **How Does Teradata Process Customer Data?**

Whose Personal Data We Collect

Teradata may collect Personal Data from a variety of individuals, including:

- **Visitors**, including those who visit our physical locations and those who visit the websites, web portals, information exchange sites, blogs, wikis, social media sites, domains, downloadable applications, apps, surveys, questionnaires, webinars, events, conferences, network systems, or facilities we host, own or operate, or that are hosted or operated for us, as well as those who communicate with us, including by email or other electronic or digital means, and such as through help-lines, call-centers, telecommunications and the like ("Visitors" with the subset of those who do so through electronic or digital means being referred to as "Online Visitors").

- **Customers and their related persons**, including the people and entities who are the visitors, employees, customers, partners, constituents, representatives, and other data subjects of our current and prospective customers, including those whose Personal Data is stored and processed on our solutions by or for our customers ("Customers").
- **Partners and their related persons**, including the people and entities who are the visitors, employees, customers, partners, constituents, representatives, and other data subjects of current and prospective suppliers, vendors, contractors, subcontractors, representatives, distributors, resellers, systems integrators, joint marketers, advertisers, sponsors, and services providers ("Partners").
- **Job Applicants**, including those who apply for a job or create a candidate profile in our career portal ("Applicants").
- **Employees**, including full and part-time employees, temporary and contract employees, former employees and retirees, and qualifying family members, beneficiaries, and insureds, such as those who receive or are eligible for benefits from or through us ("Employees").
- **Others**, including people who are or may be influencers related to our business or technologies, such as analysts, academia, members of the media, investors, members of subject-area communities, industry communities, and geographical or jurisdictional communities in which we operate, and those who do not fit into one or more of the preceding categories ("Others").

How We Collect Personal Data

We may collect Personal Data from a variety of sources depending on the ways you interact with us. Please read the relevant section(s) below for information about the sources from which we may collect your Personal Data.

Customers, Partners, Visitors, and Others

We may collect your Personal Data from the following sources:

- **When you submit it to us** or do business with us online or offline, such as:
    - When you register for an event, seminar, user group, conference, webcast, webinar, training program, or similar program.
    - When you subscribe to a newsletter, mailing, forum, blog, wiki, or request white papers or other information related to our business, products, or offerings.
    - When you contact us to request products or services or to receive offers or discounts.
    - When you request to participate in offers, surveys, questionnaires, polls, or contests that we conduct or sponsor.
    - When you contact us to submit feedback, ask a question, or raise a concern.
- **From the devices you use** to access our websites, applications, or online services, which may provide information to us, our service providers, or third parties, which may provide technical information to us via technologies such as cookies, web beacons, pixels, tags, and widgets. Please see the **Online Privacy** section below to learn more about the specific technologies used and how to adjust your preferences for these technologies.

- **From your employer**, if you work for a current or prospective Teradata Customer or Partner.
- **From your contacts at Teradata**, such as account managers or marketing personnel.
- **From your contacts**, when they provide your Personal Data to Teradata as part of our "refer a friend" or "forward to a friend" programs. See the **Customer Referrals** section below for more information.
- **From our service providers**, such as our web hosting partners and analytics providers.
- **From third-party data providers**, such as ZoomInfo, 6sense, LinkedIn, and TechTarget.
- **From publicly available information**, such as information you post on social media platforms or that is in the public domain.

Teradata offers no financial incentives in exchange for the collection or retention of Personal Data.

Customers Referrals

Certain communications and forums we operate in connection with our products, services, and business, or that 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 Personal Data or confidential information you do not have the legal right to share with or provide to us.

Where a law contractual obligation requires consent, 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 inform the referred person or party that you made the Referral to us.

Applicants

If you apply for a job with us, we may collect your Personal Data from the following sources:

- **When you submit it to us** through online or offline interactions with us. For example, when you fill out a job application or candidate profile, contact us regarding an application, or provide information during an interview.
- **From the devices you use** to access our career portal, which may provide technical information to us via technologies such as cookies, web beacons, pixels, tags, and widgets. Please see the **Online Privacy** section below to learn more about the specific technologies used and how to adjust your preferences for these technologies.
- **From our vendors and service providers**, such as our hosting partner for the career portal and analytics providers, who may provide us with information about you or your use of the career portal. We may also access information about you from service providers such as our background check and drug test providers, to the extent permitted by applicable law.
- **From third parties** such as your former employers or other references you provide.
- **From publicly available information**, including employment eligibility information and the information you choose to post publicly on social media. For example, if you use third-party social media sites, such as Facebook, LinkedIn, Google, or X (formerly Twitter), we may collect information that you make public on these third-party sites to enrich your contact profile.

- **From our employees** who provide your information to us as part of our employee referral program. Employees are responsible for informing you before sending us your Personal Data as part of an employment referral.

Employees

In the context of your employment with Teradata, we may collect your Personal Data from the following sources:

- **Directly from you**, such as when you submit it to our HR systems, interact with other systems, or through offline interactions with us.
- **From the devices you use** to access our networks and systems, which may provide technical information to us via technologies such as cookies, web beacons, pixels, tags, and widgets and other monitoring and security technologies to the extent permitted by applicable law. Please see the **Online Privacy** section below to learn more about the specific technologies used and how to adjust your preferences for these technologies.
- **From our vendors and service providers**, such as our hosting partners for our cloud systems and our background check and drug test providers, to the extent permitted by applicable law.
- **From publicly available information**, including the information you choose to post publicly on social media. For example, if you use third-party social media sites, such as Facebook, LinkedIn, Google, or X (formerly Twitter), we may collect information that you make public on these third-party sites to enrich your contact profile.

Types of Personal Data We Collect

Teradata may collect the following categories of your Personal Data depending on the circumstances of your relationship with us.

Customers, Partners, Visitors, and Others

- **Personal identifiers and details** such as your name, title, addresses, telephone numbers, email addresses, date of birth, gender, usernames, IDs, and social media handles, profiles, or account names.
- **Internet, network, and device activity** such as information about your browsing behavior, app activity, IP addresses, , and interactions with our websites, emails, and advertisements, including data from cookies, pixels, and tags as described in the **Online Privacy** section of this Privacy Statement.
- **Comments, posts, and profile details** if you participate in any forums we host or interact with our social media pages.
- **Information regarding your preferences**, business objectives, product and service interests, and similar characteristics to help us understand how we can best be of service to you.
- **Audio, video, and pictures**, such as recordings that you may be in when participating in calls or video meetings with recording enabled, CCTV footage when you visit our offices, or photos of you at events that you participate in.
- **Event and training** attendance records.

- **Professional information** such as your employer, title, job description, and certifications.
- **Educational information** such as your university affiliation, degrees, professors' names, courses, and enrollment status and performance.
- **Any other information** you voluntarily provide to us.

Applicants

When you apply for a job with Teradata or use our career portal, we may collect the following Personal Data:

- **Identifiers and contact details** such as your full name, aliases or nicknames, postal addresses, email addresses, phone numbers, fax numbers, social networking site user or account names, or other addresses at which you can receive communications, emergency contact details, driver's license number, passport number, national ID number, Social Security number, or other government identification number.
- **Demographic information** such as your age, date of birth, gender, nationality, place of birth, military service information, veteran status, and, where permitted by local law and you choose to disclose it, your race or ethnicity.
- **Professional, employment, educational, and background information** such as your educational background, transcripts, language skills, employment history, status, qualifications, certifications, skills, special competencies, or any other information included in your resume or CV, your salary and contract expectations, reasons for prior terminations, the names of relatives working at Teradata or individuals who may have referred you to a position, and, where permitted by local law, criminal background check information.
- **Citizenship and visa information** such as your citizenship country and status, visa information including issuing country, status, type, effective date, and expiration date, your current work status to work in a particular country, and whether you require sponsorship.
- **Preferences and other characteristics** such as your career interest areas and preferences, preferred work location and department, willingness to travel or relocate, and preferences regarding the types of information or communications you would like to receive from us.
- **Internet or other electronic network and device information** such as your username and password for the career portal, the IDs and IP addresses of the devices you use to access the career portal, and analytics data about your use of the career portal, such as the dates and times you access the career portal, browsing behavior, and other interactions with the career portal, including data from cookies.
- **Audio, video, and pictures** such as recordings of your video interviews, to the extent you provide consent to these recordings, and security footage that may include your image if you visit one of our facilities.
- **Health information** such as any disability that you self-identify for which you require accommodation and, where permitted by local law, drug test results.
- **Other information you choose to provide us** through your responses to our questions, supporting documentation attached to your application, or other interactions where you volunteer to share personal information.

Employees

Teradata may collect and process various categories of Personal Data about employees and persons related to employees, depending on local law, such as:

- **Contact information and identifiers** such as legal name, nickname or alias, gender, date of birth, home address or postal address, personal email address, personal phone number, photograph, national ID number, Social Security number, driver's license number, passport number, citizenship, immigration status documentation, visa information, and national insurance number.
- **Educational and professional background** such as academic and professional qualifications, professional registrations, education history, employment history, or resume, reference letters, interview notes, languages, sanctions with professional bodies, and criminal records data (for vetting purposes, where permissible and in accordance with applicable law).
- **Employment information** such as job title, office location, employee identification number, hire date, manager and functional area, contract details, benefits, pay grades, employment status and category, performance and disciplinary records, investigation records, termination date and reason, grievance procedures, training records, information regarding skills and development, career plans, workdays/hours and attendance, and sickness, holiday and leave records.
- **Family and beneficiary information** including marital status, emergency contact details, number of dependents, age of dependents or beneficiaries, and beneficiary details necessary for providing applicable benefits, such as name or gender.
- **Financial information** such as bank account details for direct deposit, tax information, payroll information, withholdings, salary or wage, compensation information, expense records, corporate credit cards, company allowances, and stock and equity grants.
- **Health information** such as information about short- or long-term disabilities or illnesses, particularly in relation to any accommodations required or leave of absence taken or requested, medical certificates, reports of the company doctor, and other documents required to confer special benefit status, such as information concerning pregnancy status and age of children, where applicable and permitted by applicable law.
- **IT information** required to provide access to, secure, and ensure the functioning of our IT systems and networks such as login credentials, IP addresses, device identifiers, login and access records, and network activity logs.
- **Vehicle information** such as year, make, model, license plate number and any other details necessary to issue parking permits.
- **Other information you choose to share with Teradata**, which may vary based on the context in which you share it.
- **Sensitive demographic information.** Where permitted or required by local law, Teradata may also collect certain demographic data that qualifies as sensitive Personal Data, such as race, ethnicity, sexual orientation, religion, and disability to help us understand the diversity of our workforce or comply with applicable law. This information is generally collected on a voluntary, consensual basis, and employees are not required to provide this information unless it is necessary for us to collect such information to comply with our legal obligations.

How We Use Personal Data

Teradata will process Personal Data in a way that is compatible with, and relevant to, the purpose for which it was collected or that you have authorized, or as we notify you if the purposes change. You have the right to object to or request that we restrict the processing of your Personal Data for such additional purposes.

Teradata may process Personal Data manually, automatically, or through responsible AI. We do not use sensitive Personal Data to infer characteristics about individuals, and we do not use automated processing of Personal Data for profiling purposes.

Please read the relevant section(s) below to learn how Teradata may process your Personal Data.

Customers, Partners, Visitors, and Others

Teradata may use the Personal Data we collect for the following purposes:

- To deliver our products and provide technical, maintenance, support, upgrade, back-up, recovery, diagnostic, security, consulting, implementation, and other related services both in the cloud and on customer premises.
- To enter into and fulfill business agreements with you.
- To respond to your requests, questions, or concerns that you send to us.
- To process orders, downloads, and requests, such as for product demonstration or evaluation.
- To complete online or offline transactions with you.
- To communicate with you about our business offerings and services through sales and marketing activities, including subscriptions to Teradata publications.
- To understand your experience with our products and recommend products, services, educational offerings, events, and other opportunities we believe you may be interested in.
- To provide, personalize, and analyze your access and use of our websites, Teradata platforms, and Teradata products and services, including via the use of cookies, tags, pixels, and related technologies as described in the **Online Privacy** section of this Privacy Statement.
- To communicate with you about policy changes, violations of the terms of use, data compromises, or other topics necessary for the administration of our products, services, and business.
- For purposes of research and development, such as benchmarking, testing, quality assurance, research, and product/offering strategy, development, and integration.
- To operate our networking sites, such as Peer Advantage.
- To provide customer or partner education or certification courses and, for certain courses, to confirm your eligibility for such courses. This includes courses provided via Teradata University/Teradata University for Academics or our Teradata Certified Professional Program.
- To plan and coordinate networking and other events.

- To engage in charitable activities.
- To manage investor relations and Teradata securities.
- To maintain the rights, safety, and security of Teradata and our websites, apps, products, databases, and other technology assets.
- To secure our facilities and protect the vital interests or safety of our employees and visitors.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations, including our transparency reporting obligations.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all our assets, whether as a going concern or as part of a bankruptcy, liquidation, or similar proceeding, in which Personal Data held by us is among the assets transferred.
- As otherwise described to you at the time we collect your Personal Data, or with your consent if not listed here.
- As otherwise required by law.

Applicants

When you apply for a job with Teradata or otherwise use our career portal, we may use your Personal Data for the following purposes:

- To process your employment application, including collecting relevant employment and skills data, assessing your suitability for the role, scheduling and holding conversations or interviews with you, and communicating with you about the status of your application and our hiring decisions.
- To perform background, including criminal record, checks, where permitted by law.
- To suggest job vacancies that may meet your skills or interests.
- To store your candidate profile information for future job applications and to meet our legal retention obligations, as described in the **Data Retention** section below.
- To send you alerts and newsletters about career opportunities with Teradata.
- To respond to your inquiries and requests.
- To maintain the rights, safety, and security of Teradata and our websites, apps, products, databases, and other technology assets.
- To secure our facilities and protect the vital interests or safety of our employees and visitors.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations, including our transparency reporting obligations.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all our assets, whether as a going concern or as part of a bankruptcy, liquidation, or similar proceeding, in which Personal Data held by us is among the assets transferred.

- To comply with applicable laws, regulations, industry codes of conduct, and Teradata's internal policies and procedures.
- As otherwise described to you at the time we collect your Personal Data, or with your consent if not listed here.

Employees

During your employment with Teradata, we may use your Personal Data for the following purposes:

- To manage your employment records, including your employment contract, time and attendance records, absences, and performance records.
- To calculate and administer payroll, compensation, and expense reimbursement, including withholdings, tax deductions, and allowances.
- To administer benefits and pensions to which you or your dependents or beneficiaries may be entitled.
- To conduct company elections and manage union or works council agreements, as applicable.
- To communicate with you and facilitate global collaboration and communication within Teradata.
- For financial planning, forecasting, budgeting, and resource management.
- To provide training, education, and certification relevant to your duties.
- To provide access to company resources necessary to perform your duties, including building access, network and system credentials, and company-issued IT devices, cars, and credit cards.
- To ensure the health and safety of our employees and visitors to our facilities.
- To maintain the rights, safety, and security of Teradata and our websites, apps, products, databases, and other technology assets.
- To secure our facilities and protect the vital interests or safety of our employees and visitors.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations, including our transparency reporting obligations.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all our assets, whether as a going concern or as part of a bankruptcy, liquidation, or similar proceeding, in which Personal Data held by us is among the assets transferred.
- To comply with applicable laws, regulations, industry codes of conduct, and Teradata's internal policies and procedures.
- As otherwise described to you at the time we collect or use your Personal Data for other purposes, or with your consent if not listed here.

Legal Basis for Processing

Teradata will only use or process your Personal Data if the use or processing is permitted by applicable Privacy laws in your jurisdiction. This is sometimes referred to as having a "legal basis" to use or process your Personal Data. The legal basis Teradata may rely on to process your Personal Data may include:

- **Necessary to Perform a Contract:** For example, to conduct our contractual obligations with you or your employer pursuant to a contract.
- **Necessary to Meet Legal Obligations:** For example, when we are required to disclose Personal Data pursuant to a lawful court order or subpoena.
- **With Your Consent:** For example, if you opt-in to receive marketing communications from us or otherwise provide your consent for us to process your Personal Data for purposes specified at the time we obtain your consent. If you provide your consent, you may withdraw your consent at any time. Please see the **Your Rights** section of this Privacy Statement to learn how to withdraw consent.
- **Legitimate Interests:** For example, to manage, operate, maintain, and secure our websites, network systems, and other assets. We rely on this legal basis only where we believe that our legitimate interests are not outweighed by your rights and freedoms under applicable law. If you wish to object to processing based on legitimate interests, please contact us as described in the **Contact Information** section of this Privacy Statement.
- **Vital Interests:** We may process Personal Data where it is necessary to protect the life or imminent safety of you or another individual, where no other legal basis applies.

How and Why We Share Personal Data

We share Personal Data with our affiliates and subsidiaries for the purposes described in this Privacy Statement. We may also share your Personal Data with third-party service providers that perform services and functions for us. In these situations, we will take reasonable steps to require the recipient to protect your Personal Data in accordance with applicable Privacy laws or regulations or otherwise take steps to help ensure your Personal Data is appropriately protected.

Teradata may share your Personal Data with third parties for the following purposes:

- With 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.
- With service providers who host or facilitate the delivery of technology services, online apps, training, seminars, and webinars, including but not limited to the providers of our Salesforce, Transcend, Microsoft, and Gr8 People databases and systems.
- With third parties who may assist in the delivery of marketing materials, technical support services, or other products, services, or other information.
- With authorized resellers, distributors, marketing partners, or our subsidiaries or branches so they may follow up with you regarding products and services.
- With our online advertising partners for the purpose of providing more relevant advertising to you, with your consent as described in the **Your Online Privacy Choices** section of this Privacy Statement.

- With your professors or teaching assistants if you are a student registered in Teradata University or Teradata University for Academics.
- In the event we undergo a business transition, such as a merger, acquisition by another company, bankruptcy, reorganization, or sale of all or a portion of Teradata's assets.
- With law enforcement or governmental agencies to comply with a lawful court order, subpoena, legal or regulatory requirement, or other legal process, including to respond to a lawful government or regulatory request, as described in the **Law Enforcement Requests** section below.
- To prevent or investigate a possible crime, including but not limited to identity theft, fraud, hacking, cyber-attacks, phishing attempts, or other cyber-crimes.
- If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of Teradata, our customers, or others. This includes sharing information with other organizations for the purposes of fraud protection and credit risk reduction.
- To protect the vital interests or life of you or another individual.
- To any other third party with your affirmative consent.

Law Enforcement Requests

We may be required to provide certain Personal Data to public authorities to meet legally mandated reporting, disclosure, or other legal process requirements, including to comply with national security or law enforcement requests. To date, we have not received any such requests, and Teradata commits to updating this Privacy Statement if we receive such a request in the future to the extent that we are legally permitted to do so.

Cross-Border Data Transfer

Teradata's Privacy practices are designed to help protect Personal Data all over the world. At times, Personal Data may be transferred to service providers or systems in countries whose laws may not offer a level of data protection equivalent to that in your country. Where such cross-border transfers occur, we take reasonable steps to require the recipient to protect Personal Data in accordance with applicable Privacy laws and our Privacy standards.

We take a multi-dimensional approach to Privacy compliance by implementing at least one of several different legally recognized mechanisms for all cross-border data transfers. This includes mechanisms to permit the export of Personal Data from the European Union ("EU"), the European Economic Area ("EEA"), the United Kingdom ("UK"), and Switzerland, among other countries.

Adequacy

Teradata may share Personal Data with its affiliates, subsidiaries, and third-party partners located in countries that have been deemed to ensure an adequate level of data protection. When we send or receive Personal Data to or from such "adequate" countries, we rely on these adequacy decisions as the basis for the cross-border transfer of Personal Data.

Data Privacy Frameworks

Teradata's U.S. entities (Teradata Corporation, Teradata Operations, Inc., Teradata US, Inc., Teradata International, Inc., and Teradata Government Systems LLC) comply with and have certified to the U.S. Department of Commerce that we adhere to the EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF ("UK-U.S. DPF") and the Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF"). These frameworks are the cross-border data transfer mechanisms on which we rely when the Personal Data of individuals residing in the EU, EEA, UK, or Switzerland is transferred to Teradata in the United States.

Where we transfer Personal Data to a third party located in the United States that also certifies to these frameworks, we rely on these frameworks as the basis for those transfers as well.

If there is any conflict between this Privacy Statement and the EU-U.S. DPF Principles, the UK-U.S. DPF Principles, or the Swiss-U.S. DPF Principles, the applicable DPF Principles will govern. To learn more about the Data Privacy Framework program and to view our participation status, please visit **https://www.dataprivacyframework.gov/**.

In compliance with the EU-U.S. DPF, the UK-U.S. DPF and the Swiss-U.S. DPF, Teradata commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities ("DPAs"), the UK DPAs, and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning its handling of human resources data received in reliance on the EU-U.S. DPF, the UK-U.S. DPF and the Swiss-U.S. DPF in the context of the employment relationship.

Teradata has committed to refer all unresolved DPF-related Privacy complaints/disputes from EU, EEA, UK, or Swiss citizens or residents to an independent dispute resolution services provider and dispute resolution mechanism. If you have a complaint, dispute, or problem related to the Data Privacy Framework that Teradata does not timely acknowledge or satisfactorily address within 45 days of receiving notice from you, you may initiate the independent dispute resolution process described in the **Complaints** section of this Privacy Statement.

Data Transfer Agreements and the Standard Contractual Clauses

Where Teradata sends or receives Personal Data to or from countries that do not have an adequacy decision, and we are unable to rely on an applicable Data Privacy Framework, we enter into government-approved data transfer agreements as the basis for the cross-border transfer of Personal Data. These data transfer agreements include the European Commission's Standard Contractual Clauses ("EU SCCs") and the UK Addendum to the EU SCCs ("UK Addendum").

Where necessary, Teradata will take appropriate supplementary measures to ensure an essentially equivalent level of data protection to that guaranteed in the EEA, in accordance with European Data Protection Board ("EDPB") recommendations.

Transfers Within the Teradata Group of Companies

Teradata has executed written intra-group data protection agreements among various Teradata subsidiaries and entities around the world that incorporate the necessary government-approved data transfer agreements, including the EU SCCs and UK Addendum, to permit the cross-border transfer of Personal Data within the Teradata group of companies. We review and update these intra-group data protection agreements as our business and the requirements of applicable Privacy laws evolve.

Online Privacy

Cookies and Online Tracking

We use cookies and similar technologies on our websites and other online services, including email and other digital communications. These technologies include:

- **Cookies:** A cookie is a small element of data that a website may send to your browser and is then stored on your system. The distinct types of cookies we use and why are described below. You may set your web browser to block cookies or warn you before you accept a cookie.
- **Pixels or Web Beacons:** Pixels and web beacons are tiny graphics with unique identifiers, similar in function to cookies, and are used to track users' online movements. 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.
- **Tags:** A tag is a piece of code inserted into a webpage used to either gather data from or add functionality to the webpage.

We use these technologies to secure and operate these services, provide enhanced functionality, analyze the services' usage, provide personalized advertising, help serve you better as you navigate the websites, and remember your preferences and choices each time you return. We also may use this 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.

The categories of purposes for the technologies we use on our websites include:

- **Strictly necessary (essential)** – These are required for the operation of our websites, such as enabling you to log into secure areas of our websites, helping us choose the right language for you, or protecting the website against fraud, security threats, or other malicious activity.
- **Analytical/performance** – These allow us to recognize and count the number of visitors and to see how visitors move around our websites. This helps us to improve the way our websites work, for example, by ensuring that users find what they are seeking easily.
- **Functionality/personalization** – These are used to recognize you when you return to our websites. This enables us to personalize our content for you and remember your preferences.
- **Advertising** – These allow us and third parties to provide more relevant advertisements to you and other visitors to our websites when you visit other websites or use public search engines.

Please see the **Your Online Privacy Choices** section of this Privacy Statement to learn how we gather consent for these technologies and how you can prevent the collection of your Personal Data via these technologies.

Third-Party Cookies, Advertising, and the "Sale" or "Sharing" of Personal Data

Some of our business partners, internet advertisers, ad servers, and ad networks may use cookies, web beacons, and other tracking technologies to collect information about users' behavior from our websites and online services and use that information for analytics and to serve targeted ads to those users on other websites or online services (i.e., cross-context behavioral advertising).

While Teradata's business model does not include sharing or selling your Personal Data for money, under certain U.S. state laws, the collection of your Personal Data via such third-party cookies and related technologies may be considered a "sale" or "sharing" of your Personal Data, which you have a right to opt out of. To opt out of such sale or sharing of your Personal Data, please click **this link** and select "Don't Personalize." You can also access this option by clicking the "Tracking Consent" link in the footer of any page on our websites. You may also contact us at **privacy@teradata.com** with any questions about this process.

In the 12 months preceding the Effective Date of this Privacy Statement, Teradata has only sold or shared Personal Data with third parties, as defined under applicable U.S. laws, via these third-party cookies and tracking technologies. Teradata does not and has not otherwise shared or sold your or anyone else's Personal Data.

Chatbot

We use chatbot technology on some of our website(s) to optimize user experience and deliver personalized content. To provide this technology, our third-party chatbot Drift, owned by Salesloft, collects and processes IP addresses and any Personal Data provided to the chatbot for the sole purpose of providing the chatbot service. Please see Salesloft's platform privacy notice at **https://www.salesloft.com/legal/platform-privacy-notice** for more information about their Personal Data handling practices within the chatbot platform.

Hosted Services

Some of our customers and their business partners may use cookies, web beacons, and other tracking technologies and analytics in connection with their Teradata environments. We have no access to or control over these third-party tracking technologies and no responsibility for them or with respect to the deployment or use of those kinds of analytic technologies by or for another.

Web Server Logs

These logs collect information about the devices that interact with our systems. They provide usage information such as what types of browsers are accessing our websites, what pages receive high traffic, the domains from which our online visitors arrive at our websites, and the times of day our servers experience significant loads.

We use IP addresses collected in these logs to analyze trends, administer, and secure websites and internet-connected systems, track users' movements though our websites, gather broad demographic information for aggregate use, and improve the content and navigation features of our websites.

Links to External Websites

Our websites and Teradata platforms may contain links to external websites. A link to such websites does not imply Teradata's endorsement of such websites. This Privacy Statement does not apply to those external websites, and you should review the privacy notices of such external websites to learn about their Personal Data collection and handling practices.

We are not responsible for the content or behavior of any outside third-party websites or their users.

Forums

Information posted to or shared via bulletin boards, blogs, wikis, chat rooms, exchanges, share sites, social media platforms, and similar "forums" (whether operated by or for us, or otherwise) may be accessible to others and may be open to the public. Your participation and disclosures in such forums in such forums is your choice. If you choose to include your Personal Data in your posts, it may lead to the use of your Personal Data by others. We are not responsible for any information you make available on or through such forums, nor for any contact by others because of your participation in or your disclosures on or through such forums.

We reserve the right to monitor any 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 through such forums. To the extent that such forums are hosted on third-party platforms, such as our social media pages, the third-party platform provider may also collect and use Personal Data other than as described in this Privacy Statement. Please review the privacy notices of such websites to learn about their Personal Data collection and handling practices.

Social Plug-Ins and Share Buttons

We also may use social plug-ins on or in connection with some of our websites. When you visit a website 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 and then receives information about your access to and activity on the website.

Our websites currently include plug-ins from Instagram, Facebook, LinkedIn, X (formerly Twitter), and YouTube. If you would like to prevent these social plug-ins from gathering your Personal Data, please click **this link** and select "Don't Personalize." You can also access these options by clicking the "Tracking Consent" link in the footer of any page on our websites. Then, please avoid clicking the social plug-in icons on our websites.

We have no influence over a social network's use of the data gathered via a plug-in. For the purpose and scope of data collection and the further processing and use of Personal Data by these social networks, as well as ways to exercise your Privacy rights with them, please see the privacy notices of the respective social networks.

Your Online Privacy Choices

Depending on your location and applicable law, we will ask you for your explicit consent prior to using these technologies and will not use them without your consent or for longer than necessary. For all visitors, if you would like to limit the use of these technologies to those that are strictly necessary, you may do so by clicking **this link** and selecting "Don't Personalize." You can also access these options by clicking the "Tracking Consent" link in the footer of any page on our websites. Please note that if you select "Don't Personalize," any cookies placed prior to this selection will remain on your browser or device. You may clear these cookies through your browser's privacy or security settings.

For more information about cookies, including how to set your internet browser to reject all cookies, please go to **www.allaboutcookies.org**. Please note that if you set your browser to block all cookies, some elements of our websites may be inaccessible or not function correctly.

Do Not Track

Currently, Teradata does not respond to Do Not Track ("DNT") signals. All About Do Not Track, a Future of Privacy Forum website, has more information about DNT signals and is located at **https://allaboutdnt.com/**.

Your Marketing Choices

Marketing Communications

We will respect your preferences and choices about how we communicate with you for marketing and promotional purposes. We will only contact you with such messages when you have provided your affirmative consent or when it is in our legitimate business interest to do so, depending on the law in your jurisdiction. We may obtain your Personal Data for marketing purposes directly from you, such as when you subscribe to an email list or newsletter, or from the contact information we receive as part of a business relationship with you or your employer. In some cases, we may receive Personal Data for marketing purposes from third parties such as ZoomInfo, 6Sense, LinkedIn, or TechTarget.

If you are receiving marketing communications about our products, services, or offers but no longer wish to receive these types of communications, you always have the option to unsubscribe from some or all these communications. To do so, please click the "unsubscribe" or "preferences" link in the communication and follow the instructions to change your marketing preferences. You may also contact us at **privacy@teradata.com** to opt-out or withdraw your consent for marketing communications.

Please note that if you unsubscribe from marketing communications, we may still send you communications as needed to provide our products and services and to fulfill our contractual obligations to you and your employer.

Advertising Cookies and Similar Technologies

As described in greater detail in the **Online Privacy** section of this Privacy Statement, you may limit the use of advertising cookies and similar technologies on our websites by clicking **this link** and selecting "Don't Personalize." You can also access these options by clicking the "Tracking Consent" link in the footer of any page on our websites.

Your Rights

Many Privacy laws provide certain rights for individuals regarding their Personal Data. Your rights with respect to your Personal Data may include the following, depending on the circumstances and where you are located:

- **Withdraw Consent.** If we use or share your Personal Data based on your consent, you may withdraw your consent at any time by contacting us as described in the **Contact Information** section of this Privacy Statement. To withdraw your consent for marketing communications from Teradata, you may alternatively follow the process described in the **Your Marketing Choices** section of this Privacy Statement.
- **Access.** You may request to access or obtain a copy of your Personal Data that Teradata processes. You may also request information about what types of Personal Data we hold about you, the purposes for which we process it, and who has received access to or a copy of your Personal Data in the past year.
- **Correction.** You may request that we correct your Personal Data if you think it is inaccurate or incomplete.
- **Deletion.** You may request that we erase or delete your Personal Data. Teradata may satisfy such requests by anonymizing the information in cases where it is not technologically or reasonably feasible to erase the data. Please note that there may be overriding legal obligations that prohibit us from deleting Personal Data in certain cases.

- **Restrict Processing.** You may request that we restrict certain ways we process your Personal Data in certain circumstances.
- **Data Portability.** You may request that we provide the Personal Data we hold about you in a machine-readable format to you or another entity.
- **Object to Processing.** You may object to our processing of your Personal Data for certain purposes. Please note that if we have compelling, legitimate grounds for the processing that override your Privacy interests, we may continue to process your Personal Data even after you object to the processing.
- **Not to be Subject to Adverse Decisions from Automated Processing.** You may object to a material decision that significantly negatively or adversely affects you that you believe has been taken solely by a computer or other automated process. We will review, assess, and respond to your concerns through human engagement.

To exercise these rights, please send an email to **privacy@teradata.com** with the details of your request or contact us using any of the other communication methods listed in the **Contact Information** section of this Privacy Statement. You will not receive discriminatory treatment if you exercise your rights as set out in this Privacy Statement or applicable law.

Please note that we may not be able to fulfill some requests, in whole or in part, depending on the requirements and restrictions of the laws applicable to your situation or if doing so would infringe the rights and freedoms of others. If we are unable to fulfill your request, we will explain why.

We will maintain a record of all requests we receive as part of our recordkeeping obligations.

Identity Verification

Depending on the nature of your request and applicable law, we may need to verify your identity before fulfilling your request. We do so to protect your Personal Data from unauthorized disclosure, modification, deletion, or restriction.

If you update your Personal Data directly using self-help tools available when you log in to your account with us, such as a customer account, career portal account, or HR system account, no additional identity verification is necessary. Similarly, if you send us a message from your account requesting to exercise your rights, we will not need to further verify your identity if we can confirm you were logged into the account when you sent the message.

Otherwise, to verify your identity, we will usually request that you provide two to three pieces of Personal Data for verifying your identity and match the information you provide to the data we maintain in our systems.

If you designate an authorized agent to submit such a request for you, we may also need to verify the identity of that agent and their authority to act on your behalf.

Where Teradata deems it necessary, we may also require you to provide a signed declaration under penalty of perjury that it is your Personal Data that is the subject of the request. Teradata will maintain all signed declarations as part of our recordkeeping obligations.

Complaints

If you believe that Teradata has not handled your Personal Data in accordance with this Privacy Statement and applicable laws, please contact us by the appropriate means identified in the **Contact Information** section of this Privacy Statement. All complaints will be taken seriously.

You may also have the right to lodge a complaint directly with the regulatory authority for Privacy in your country or state if you have concerns about our Personal Data collection and handling practices.

Data Privacy Framework Complaints and Disputes

Teradata has committed to refer all unresolved DPF-related Privacy complaints/disputes from EU, EEA, UK, or Swiss citizens or residents to an independent dispute resolution services provider and dispute resolution mechanism. If you have a complaint, dispute, or problem related to the Data Privacy Framework that Teradata does not timely acknowledge or satisfactorily address within 45 days of receiving notice from you, you may initiate the independent dispute resolution process by contacting the International Center for Dispute Resolution ("ICDR") of the international division of the American Arbitration Association ("AAA").

The ICDR/AAA is the provider for such disputes, 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. and EU-UK DPF Procedures or applicable Swiss-U.S. DPF Administrative Procedures.

Consistent with the principles of the EU-U.S. DPF, the UK-U.S. DPF, and the Swiss-U.S.DPF, if you are subject to such a framework, you may initiate and proceed with this dispute resolution mechanism without bearing any filing fees or administrative costs from the dispute resolution provider. In other words, Teradata will be responsible for all filing fees and administrative costs from the dispute resolution provider). There is the possibility, under certain conditions, for you to invoke binding arbitration.

For online access to information about the ICDR/AAA EU/UK/Swiss-U.S. DPF or to initiate a complaint under the ICDR/AAA EU/UK/Swiss-U.S. DPF, please visit **https://go.adr.org/dpf_irm.html**.

Rights to Restrict Sharing or Selling Personal Data

While Teradata's business model does not include sharing or selling your Personal Data for money, Teradata may "sell" or "share" Personal Data as defined under certain U.S. state laws when we use third-party cookies and tracking technologies to identify and place advertisements targeted to users who visit Teradata platforms. Please see the **Online Privacy** section of this Privacy Statement for more information about our use of these technologies.

To opt out of such sale or sharing of your Personal Data, please click **this link** and select "Don't Personalize." You can also access this option by clicking the "Tracking Consent" link in the footer of any page on our websites. You may also contact us at **privacy@teradata.com** with any questions about this process.

Data Security

Teradata will take reasonable steps to ensure that Personal Data is accurate, complete, current, secure, and reliable for its intended uses as described in this Privacy Statement. We employ reasonable physical, administrative, procedural, and technical security measures to protect Personal Data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction.

Some of the security measures we employ include, 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 have also designated a Chief Security Officer with ultimate responsibility for managing our global information security program.
- **Access control.** We limit access to Personal Data only to those individuals who have an authorized purpose for accessing that information. We terminate those access privileges and credentials following job changes that no longer require such access and upon employment termination. We also have designated local or organizational data protection officers, stewards, or managers for various locations and organizations of Teradata and otherwise as and where required by applicable law.
- **Data encryption.** Our policies and procedures require that, wherever practicable, we use encrypted connections for any electronic transfers of Personal Data.

Unfortunately, no security measures can be guaranteed to be 100 percent effective, and no website, system, or network can be completely secure or "hacker proof," "cyber-attack proof," or "cyber-crime proof." Please guard against unauthorized access to your passwords and the unauthorized use of computers and other electronic/data-access devices you own or control.

You might find **Stay Safe Online**, powered by the National Cyber Security Alliance, and its *"Stop. Think. Connect."* initiative helpful and informative.

For more information about our security policies and practices, please visit our Trust Center.

Data Retention

Teradata will retain your Personal Data for as long as reasonably necessary for the purposes described in this Privacy Statement or as required by law. Personal Data will be kept until it is no longer necessary to provide our products and services, to fulfill our contractual agreements with you or your employer, to comply with applicable law, to protect Teradata's rights and interests (e.g., where the retention is necessary for the establishment, exercise, or defense of legal claims), or as otherwise needed for lawful purposes. In determining this period, and where your employer is a Teradata customer or customer prospect, we take into consideration the duration of your tenure with your employer and the duration of our legal and contractual obligations and potential business relationship with your employer. Once Personal Data is no longer needed for these purposes, we will destroy, erase, or anonymize it.

Privacy Statement for Children

The Websites and Teradata platforms are not intended to be directed to children younger than sixteen. Teradata does not knowingly collect or intend to collect Personal Data from anyone younger than sixteen years of age. In the event we learn we have collected Personal Data from a child without parental consent, we will delete that information. If you believe we might have any information from or about a child under sixteen, please contact us at **privacy@teradata.com**.

Enforcement

Teradata maintains procedures for verifying compliance with the commitments we make in this Privacy Statement. To do this, we complete one or more relevant Privacy compliance assessments at least annually and make improvements based on the results thereof.

We provide the resources identified in the **Contact Information** section of this Privacy Statement so you may raise Privacy-related questions or concerns with us. For disputes related to the EU-U.S. DPF, the UK-U.S. DPF, and the Swiss-U.S.DPF, we also provide the dispute resolution process noted in the **Complaints** section of this Privacy Statement so that you have a process and mechanism to enforce compliance with the standards set forth in this Privacy Statement.

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 Personal Data, such as Personal Data in HR data. Teradata commits to cooperating with EU Data Protection Authorities and the Swiss Federal Data Protection and Information Commissioner and complying with the advice given by such authorities regarding HR data transferred from the EU and Switzerland in the context of the employment relationship.

Changes and Supplemental Terms

We are committed to notifying data subjects regarding a change in this Privacy Statement in a timely manner. To that end, we will post a public notice via the **Effective Date** written at the top of this Privacy Statement and for at least 30 days afterward when we materially update or modify this Privacy Statement. You may request a file showing the changes from the last version by emailing **privacy@teradata.com**.

From time to time, we may supplement or amend this Privacy Statement and other Privacy terms with website- or interaction-specific information and terms ("Supplemental Privacy Terms"). If so, we will notify you of any such applicable Supplemental Privacy Terms and give you the choice to consent or not consent to them.

Contact Information

You may contact our Ethics, Compliance & Privacy Office or our Data Protection Officer using the contact details below to exercise your Privacy rights or with any requests, questions, or concerns regarding your Personal Data or Teradata's handling of Personal Data. Questions or concerns specific to Information Technology ("IT") Security may also be directed to our Global Information Security Office.

Teradata Ethics, Compliance & Privacy Office

Attn: Chief Ethics, Compliance and Privacy Officer
Teradata Corporation
17095 Via del Campo
San Diego, CA 92127
USA
+1 855-729-4835
privacy@teradata.com

Teradata's Data Protection Officer

Amy Worley
DPO@teradata.com

Global Information Security Office

Attn: Chief Security Officer
Teradata Corporation
17095 Via del Campo
San Diego, CA 92127
USA
+1 866-455-0993
information.security@teradata.com
https://tdhelp.alertline.com/gcs/welcome