



OneTrust Security, Privacy & Architecture Overview Whitepaper

Version 7.0 – January 2026



DISCLAIMER:

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue.

Executive Summary

OneTrust understands that its products must meet the highest standards for security and privacy. To achieve this, OneTrust's oversight and policy structures govern the people, process, and technology to ensure risks are identified and mitigated. Additionally, OneTrust has developed a comprehensive and rigorous software security assurance program that ensures and demonstrates the integrity of its products and addresses potential vulnerabilities.

OneTrust engages with independent third parties to give you greater assurance that the multiple layers of protection we have put in place will secure your data. By carrying out external penetration testing and reviews against the most widely accepted industry security and privacy standards, you can be confident that OneTrust is taking the necessary steps to protect your data.

OneTrust Information Security Governance & Compliance Program

Information Security Governance

Our security program begins with a strong governance foundation. OneTrust maintains a comprehensive suite of policies that define objectives, roles, and responsibilities for safeguarding information. These policies are formally approved by senior leadership and reviewed regularly to ensure alignment with evolving threats and regulatory requirements. Management's active involvement in day-to-day operations enables real-time oversight of internal controls, reinforcing a security-first culture across the organization.

OneTrust's approach to information security governance is based on ISO/IEC 27000 family of international standards in addition to targeted industry-standard certifications and accreditations. These require organizations to maintain a rigorous and continuously assessed security and privacy program, the features of which include but are not limited to:

- Policies - We have detailed internal policies and procedures explaining how security and privacy are managed, as well as what to do if incidents occur.
- Risk Management – OneTrust has established a systematic approach to managing information security and privacy risks, including internal and external security and privacy risk assessments, maturity modeling, impact analyses, privacy-by-design practices, architecture reviews, vendor risk reviews, vulnerability scanning, penetration testing, and more.
- Employee Training - All employees are trained in their security and privacy responsibilities. Employees that handle data receive additional training to better understand their position.
- Continuous Improvement – We have processes in place to encourage and document the ongoing evaluation and enhancement of our ISMS to adapt to new threats and changes.

OneTrust Security Policies

OneTrust has a comprehensive Information Security policy library which is centrally published for employees and undergoes periodic reviews at least annually or upon significant change to ensure adequacy and effectiveness.

OneTrust's policies and procedures contain guidance regarding aspects of information security best practices, mandates, and security compliance. OneTrust maintains and documents operating technology standards and procedures to provide staff with centralized up-to-date reference and training aids.

To that end, OneTrust maintains the following policies and procedures in support of its security program:

Information Security Policy

To serve as a top-level policy that defines the purpose, direction, principles and basic rules for information security and privacy management at OneTrust.

Acceptable Use Policy

To establish and maintain a culture of security and trust for all OneTrust workforce required to secure OneTrust's information in any form.

Access Control & Password Management Policy

To ensure that access to information systems and resources is granted to authorized users, based on their roles and responsibilities, while protecting confidentiality, integrity, and availability of organizational data.

Asset Management Policy

To establish framework for the proper classification, handling, and management of OneTrust Information Technology assets, from procurement to disposal.

Audit Logging & Monitoring Policy

To establish a framework for proper management of IT systems, including change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, and audit controls.

Business Continuity & Disaster Recovery Policy

To define how OneTrust shall recover its Business and IT services within set deadlines in the event of a disaster or other disruptive incident, and to define the activities and scope for planning and development of resilient business functions.

Configuration and Vulnerability Management Policy

To reduce the attack surface and mitigate the risks posed by unsecured and vulnerable endpoints, the OneTrust Configuration and Vulnerability Management Policy outlines controls for configuration and vulnerability management.

Data Protection & Privacy Policy

To establish compliance requirements to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and privacy and of any security or privacy requirements.

Endpoint Protection Policy

To security measures and requirements that OneTrust uses to protect its endpoint devices (laptops, desktops, servers).

Human Resources Security and Training Policy

To establish requirements for the entire Human Resources (HR) process, from pre-employment, during employment, and through termination, and empower workforce to make informed security decisions, reduce the likelihood of human error, and mitigate risks.

Incident Management Policy

To ensure a consistent and effective approach to managing information security events, including reporting, mitigating, and managing incidents and weaknesses, and designating roles and responsibilities

Mobile Device Security and Teleworking Policy

To define a framework to enable data protection and security when mobile devices are used to access business resources, and mitigate the risks associated with using mobile devices to access corporate data from unmanaged networks.

Network Protection Policy

To establish controls related to network security, privacy, segregation, network services, transfer of information, messaging, and more.

Physical and Environmental Security Policy

To prevent unauthorized physical access to, damage to, and interference with OneTrust's information and information processing facilities. To prevent loss, damage, theft, or compromise of OneTrust's assets, as well as to prevent interruption of its operations.

Portable Media Security Policy

To provide the overall framework for the proper management of removable assets & media in OneTrust environments.

Risk Management Policy

To define the methodology and framework for identifying, minimizing, accepting, and treating risks that may impact an organization's platform and business processes.

System Development and Acquisition Policy

To define the minimum security and privacy requirements for the procurement and deployment of technology solutions as well as the requirements for internal development and support processes.

Third Party Assurance Policy

To provide a framework for OneTrust to perform vendor risk management, including due diligence, identification of contractually required privacy and security controls, and the management and monitoring of third-party suppliers/vendors/service providers.

Transmission Protection Policy

To protect data in transit by implementing security measures, such as encryption, secure network protocols, and firewalls. To establish requirements for proper encryption and key management.

Wireless Security Policy

To outline the requirements that wireless infrastructure devices must meet to connect to the network and the monitoring process for unauthorized devices that attempt to connect to the company's networks.

Information Security Compliance

Customers can now download a copy of our audit reports, certifications, and other security and compliance documents directly from the [OneTrust Trust Center](#).

ISO/IEC 27001 Information Security Management System Certification

OneTrust LLC's Integrated Management System (IMS) obtained an [ISO/IEC 27001:2022](#) (Information technology — Security techniques — Information security management systems — Requirements) certification, which can be [found here](#). The annual audit evaluates the operational efficiency of selected control areas within OneTrust's IMS.

ISO/IEC 27701 Privacy Information Management System Certification

OneTrust LLC's Integrated Management System (IMS) earned an [ISO/IEC 27701:2019](#) (Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines) certification, which can be [found here](#). OneTrust was the first organization in the world to achieve this certification, which provides guidance for establishing, implementing, maintaining, and continually improving a Privacy Information Management System.

ISO/IEC 27017 Cloud Security Management System Certification

OneTrust LLC's Integrated Management System (IMS) obtained an [ISO/IEC 27017:2015](#) (Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services) certification, which can be [found here](#). This certification provides guidance on security controls specifically for cloud service providers and cloud service customers, ensuring a secure cloud computing environment.

SOC 2 Type II Report Security Controls

OneTrust has completed a SOC 2 Type 2 audit for Service Organizations examination, which covers the period October 1, 2024, through September 30, 2025. The SOC 2 report was issued by independent CPA firm, Schellman & Company, LLC, and included an unqualified opinion that the design and implementation of the Company's controls are appropriate relative to the Security, Availability and Confidentiality Trust Services Principle and Criteria.

Payment Card Industry Data Security Standard (PCI-DSS) Certification

OneTrust has received a PCI-DSS v4.0.1 Attestation of Compliance (AOC) for Report on Compliance (ROC) effective December 1st, 2025. All sections of the PCI-DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby, OneTrust, LLC has demonstrated full compliance with the PCI-DSS.

OneTrust supports a segmented environment that can include customer-input cardholder data that supports customers with PCI-DSS compliance obligations. OneTrust does not collect or store cardholder data by default but recognizes that some customers may wish to include such data within the OneTrust platform to support other business cases. OneTrust offers a certified environment that meets the requirements of PCI-DSS v4.0.1.

HITRUST Risk-Based 2-Year (r2) Certification

OneTrust has received a HITRUST r2 validated assessment report with Certification, valid for the period of February 14, 2025 through February 14, 2027. HITRUST r2 is a two-year validated assessment that provides the highest level of information protection and compliance assurance, particularly for organizations needing to demonstrate regulatory compliance with standards like HIPAA and the NIST Cybersecurity Framework. HITRUST r2 is an updated version of the HITRUST Common Security Framework (CSF) that provides a comprehensive approach to managing data protection and compliance.

OneTrust Information Security Program

Organization of Information Security

OneTrust has cultivated a strong security culture that permeates every stage of the employee lifecycle. This begins with rigorous background checks during hiring and continues through onboarding, which includes non-disclosure agreements, acceptable use policies, and mandatory security training. Employees receive Information Security Awareness and Privacy training upon joining and annually thereafter. Ongoing awareness programs and leadership engagement ensure that security remains a shared responsibility across all teams.

Asset Management

We maintain a detailed inventory of all information assets and assign ownership to ensure accountability. Assets are classified based on sensitivity, and handling procedures are enforced throughout their lifecycle. Secure disposal practices prevent unauthorized access to retired assets, ensuring that customer data remains protected from acquisition to destruction.

Access Control

Access to systems and data is governed by strict principles of least privilege and role-based authorization. Multi-factor authentication is enforced for critical systems, and production environments are segregated from development and testing environments. Production access is limited to designated personnel and subject to strict audit controls. Remote access is secured through encrypted channels, and mobile devices are managed under stringent security policies to prevent unauthorized access.

No resources are shared between the production environment and lower environments where development, quality assurance, and integration testing occur. Production access is limited to the release manager and support engineers, and strict audited access controls are in place to ensure compliant segregation of duties. All production access is via a different channel than user access.

Cryptographic Controls

OneTrust employs industry-standard server-side encryption to protect data in transit and at rest. For Azure deployments, Transparent Data Encryption (TDE) is applied to all databases and storage accounts, with AES-256 encryption ensuring robust protection. Each tenant database uses unique encryption keys, which are managed through Azure Key Vault with FIPS-140-2 Level 2 validated hardware security modules. Additionally, field-level encryption is implemented for all personally identifiable information (PII) within applicable modules in the OneTrust platform.

Physical and Environmental Security

Access to OneTrust facilities is controlled through physical security measures, and portable media is managed under strict protocols for secure transfer, storage, and destruction. Environmental safeguards, including redundant power and climate controls, ensure the integrity and availability of critical systems.

Operations Security

Operational resilience is achieved through documented procedures for configuration management, patching, and vulnerability remediation. OneTrust conducts automated vulnerability scanning on a regular cadence, both authenticated and unauthenticated, and applies patches promptly to minimize exposure. Our vulnerability management program leverages the OWASP Top Ten framework to prioritize remediation efforts. Anti-malware solutions and system hardening practices further reduce attack surfaces across the organization.

Penetration and Vulnerability Testing

OneTrust conducts annual penetration testing through an independent third party, covering web applications, infrastructure, and API endpoints. An Executive Summary of this test can be found on the [OneTrust Trust Center](#). In addition, our internal Application Security Team performs rotating penetration tests across all modules to ensure comprehensive coverage. Continuous attack surface monitoring and automated vulnerability scanning complement these efforts, reducing risk and strengthening our security posture.

OneTrust also has a robust vulnerability management program that utilizes the same scope as outlined for penetration testing on an ongoing basis. Automated vulnerability scanning is conducted at a regular cadence (both authenticated and unauthenticated), and operations teams work closely together to review potential risks, mitigate those risks, and ultimately reduce the attack surface across the organization. To assess and reduce risk, OneTrust's vulnerability management program primarily uses the [OWASP Top Ten](#) as the web application vulnerability framework.

Communications Security

All user access to the OneTrust platform occurs over HTTPS using TLS v1.2 or higher. Administrative access is restricted to secure channels via SSH with key-based authentication. OneTrust uses REST-based APIs to pull data into the OneTrust application. API security is enforced through OAuth 2.0 bearer tokens, cryptographically signed using RSA-256 keys, and integrated with role-based access control (RBAC). These measures ensure that data exchanges remain confidential and tamper-proof. For more information on API key management, please visit [Managing OAuth 2.0 API Keys](#).

System Development and Maintenance

Security is embedded into our software development lifecycle. Developers receive training on secure coding practices, and all new code undergoes peer review before deployment. Static and dynamic code analysis tools are used to identify vulnerabilities early in the development process. Virtual machines are regularly updated to mitigate operating system-level risks, and production environments remain isolated from development and testing environments to prevent unauthorized access.

Supplier and Third-Party Security

OneTrust employs a rigorous risk assessment framework for all sub-processors, evaluating potential impacts on confidentiality, integrity, and availability. Vendors undergo comprehensive security evaluations prior to contract execution, and annual audits verify ongoing compliance. Risk-based reassessments incorporate considerations for privacy and emerging technologies, including AI. All sub-processors adhere to contractual obligations that limit data processing to what is necessary for service delivery. For details on our subprocessors, please see our [list of sub-processors](#).

Incident Management and Notification

OneTrust maintains a formal incident response program designed to detect, contain, and remediate security events swiftly. In the event of a confirmed incident, customers are notified without undue delay and provided with relevant information to meet regulatory reporting obligations. We maintain responsibledisclosure@onetrust.com as a dedicated channel for reporting potential security events or vulnerabilities.

Business Continuity and Disaster Recovery

Our business continuity framework ensures resilience against disruptions. Backups are managed through Microsoft Azure, with full backups performed weekly, differential backups daily, and transaction logs every 5–10 minutes. Backups are encrypted using AES-256 and stored in geographically separate data centers. Azure provides a rolling 14-day continuous backup to prevent accidental data deletion. OneTrust maintains a disaster recovery environment and conducts annual tests of its business continuity and disaster recovery plans. Our Recovery Point Objective (RPO) is one hour, and Recovery Time Objective (RTO) is 48 hours, ensuring rapid restoration of critical services.

Compliance and Data Protection

OneTrust adheres to global privacy regulations, including GDPR, and conducts regular audits to validate compliance. Our Data Protection and Privacy Policy governs the handling of personal data, ensuring lawful processing and robust safeguards. Customers can trust that their data is managed in accordance with the highest regulatory standards.

Commitment to Continuous Improvement

Security is an ongoing journey. OneTrust continuously monitors emerging threats, reviews its controls, and implements enhancements to maintain alignment with best practices and regulatory changes. This commitment ensures that our security posture evolves alongside the threat landscape, delivering sustained protection for customer data.

OneTrust Privacy & Compliance Program

OneTrust's Privacy Culture

As a privacy management software solution, OneTrust takes privacy seriously and strives to inculcate a culture of privacy. To that end, OneTrust encourages employees in obtaining the Certified Information Privacy Professional/Europe (CIPP/E) and the Certified Information Privacy Manager (CIPM) certifications from [the](#)

IAPP. In addition, all employees undergo continual privacy awareness training upon hire and annually thereafter for the duration of employment.

OneTrust Legal/Regulatory Compliance

OneTrust complies with all applicable privacy and data protection laws, including, the European Union (EU) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), as amended. To safeguard customer personal data and privacy in accordance with the applicable laws, OneTrust has implemented appropriate measures to meet legal and regulatory requirements and continually makes improvements based on regulatory changes and official guidance, as well as best practices.

Notice

OneTrust is committed to protecting the privacy of its customers. OneTrust's Privacy Notice details what personal data OneTrust collects as a data controller, for instance when individuals access or use the website, how OneTrust uses and discloses that information, and what rights individuals have with respect to their personal data. The Privacy Notice can be found at <https://onetrust.com/privacy-policy.html>. With respect to OneTrust's privacy commitment to protecting customer personal data in the OneTrust platform, the Data Processing Addendum (which is a part to any customer OneTrust contract) details the specifics of the processing and safeguards relating to it. The Data Processing Addendum can be found at <https://legal.onetrust.com/#dpa>.

Data Inventory

OneTrust performs data mapping exercises on an ongoing basis to build a data inventory and maintains accurate and up-to-date records of its processing activities. As a result, OneTrust knows all the data that it processes, how it uses that data, where it is stored, as well as any transfers within and without the organization.

Intellectual Property Rights and Data Usage

OneTrust customers own their data, and we commit to keeping customer data confidential and only using that data for purposes of providing the services. If customers delete their data, OneTrust commits to deleting it from our systems within 60 days. Finally, OneTrust enables data portability so customers may take their data with them if they choose to stop using our services, without penalty or additional costs imposed by OneTrust.

Data Subject Rights

Data subject and consumer rights are one of the most fundamental aspects of data protection and privacy law. The OneTrust Privacy Notice describes how individuals may exercise their rights. OneTrust also uses its own technology to enable easy submission of data subject requests via [this online "Exercise Your Rights" webform](#)

OneTrust has implemented internal policies to describe the process for handling the data subject requests it receives (from receiving the request and verifying the requester's identity, to implementing the request, (where applicable), and communicating with the data subject). We train our employees who are most likely to receive such requests, as well as those who are responsible for fulfilling the requests.

International Data Transfers

OneTrust customers may choose to have their environment hosted in a data center located in Europe, the US, Canada, Brazil, Australia and Asia. Please refer to the myOneTrust article on Hosting Options, Locations, and Back-up to learn more about customers' data center options. To ensure the highest quality of service, OneTrust's global support team works from the EU, the UK, and the US, which means that personal data of our customers may be transferred from the EU/EEA to the UK and the US, or from the UK to the US.

Cross-Border Transfers of Personal Data

To ensure personal data transfers from the EU and UK to third countries comply with global privacy laws, OneTrust relies on adequacy decisions issued by the European Commission and outlined in the UK adequacy regulations, where possible. For data transfers where adequacy is not an available transfer mechanism, OneTrust relies on approved standard contractual clauses (SCCs) as its lawful transfer mechanism, the International Data Transfer Agreements under the UK GDPR, and other global SCCs where relevant. In accordance with the GDPR, official court rulings, and official guidance, the OneTrust privacy team first reviews the adequacy of data protection in the third country (i.e., the destination country or country of the data importer) and applies appropriate measures (where necessary) to ensure that the personal data subject to the transfer still receives essentially equivalent protection. OneTrust regularly enters into SCCs with its customers that prefer to do so. OneTrust performs transfer impact assessments ("TIA") and continually monitors the circumstances surrounding such transfers to ensure that these maintain, in practice, a level of protection that is essentially equivalent to the one guaranteed by the EEA and UK data protection laws.

Data Privacy Framework

As part of OneTrust commitment to maintaining high data protection standards when transferring personal data between European Economic Area ("EEA")/UK/Switzerland and the US, we participate in the EU-US Data Privacy Framework ("EU-US DPF") as well as the UK Extension to the EU-US DPF and the Swiss-US Data Privacy Framework ("Swiss-US DPF"). The following US based entities are adhering to the EU-U.S. DPF Principles, including as applicable under the UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF Principles and are covered by OneTrust's DPF submission:

OneTrust LLC,

505 North Angier Avenue
Atlanta, Georgia 30308, USA

OT Technology Inc.,

505 North Angier Avenue
Atlanta, Georgia 30308, USA

To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

Accountability for Onward Transfers

OneTrust acknowledges its responsibility for the processing of Personal Information received and subsequently transferred to our Third Parties/Agents/Service Providers. OneTrust remains liable under the DPF Principles if a Third Party/Agent/Service Provider processes Personal Information in a manner inconsistent

with the DPF Principles, except where OneTrust can demonstrate that we are not responsible for the event giving rise to the damages.

Privacy by Design

The OneTrust Privacy Program utilizes a “privacy by design” approach to ensure that key privacy principles and appropriate technical and organizational safeguards are considered and incorporated into its products, and to comply with the data protection by design and by default requirement of Article 25 of GDPR. This approach ensures that the OneTrust workforce examines the privacy and security of its products and services before they go live. As part of the program, the privacy team works with OneTrust’s engineers during product development to: (1) evaluate where security and privacy risks may emerge, including by working with product teams and conducting privacy impact assessments where appropriate; and (2) provide guidance for making critical changes in a timely fashion. This practice of reviewing privacy implications early in the development process has helped promote a privacy-conscious approach and culture.

Data Protection Impact Assessments

The GDPR and other global privacy laws require businesses to conduct data protection impact assessments (DPIA) before engaging in a processing activity that is likely to result in a high risk to the rights and freedoms of data subjects, such as where the activity involves the use of new technology or involves a very large amount of personal data).

The OneTrust privacy team developed its own threshold questionnaire to determine whether a full DPIA is required for new processing activities that might involve personal data (such as launching a new feature or module, or a new processing activity for marketing purposes). OneTrust has also created its own DPIA, which is based on relevant official guidance from global data protection authorities and covers all the mandatory elements. The privacy team leverages the OneTrust platform to launch the DPIA and engages the appropriate employee for assistance in completing the assessments. Using the automated workflow, the privacy team reviews the responses and determines the proper mitigating measures (where necessary) then generates a report containing all necessary information in the event evidence that must be provided to third parties (such as an EU supervisory authority). Finally, the OneTrust platform maintains records of all the DPIAs, thereby ensuring compliance with the GDPR’s accountability principle.

Controller-Processor/Business-Service Provider Relationships

Each controller-processor or business-service provider relationship must be governed by a contract addressing the minimum requirements set forth in Article 28 of the GDPR and/or in the CCPA and its implementing Regulations, respectively. OneTrust acts as a processor/service provider with respect to delivering its products and services to its customers and offers a data processing agreement addressing applicable data protection and privacy obligations to govern this relationship. Additionally, OneTrust has data processing agreements that satisfy applicable data protection and privacy obligations with its sub-processors/subcontractors to ensure that customer personal data receives the same level of protection.

To see OneTrust’s current subprocessors, please refer to the List of Subprocessors available at https://my.onetrust.com/s/article/List-of-Subprocessors?language=en_US.

Data Protection Officer

OneTrust has appointed a data protection officer (DPO) to support its privacy program globally and to provide data subjects with an easy point of contact for any questions they may have regarding the processing of their

personal data by OneTrust. OneTrust believes that individuals should easily be able to inquire about its processing activities, ensuring respect for their fundamental rights to privacy and data protection. For any privacy or data protection-related questions, please contact dpo@onetrust.com.

Personal Data Breach

Under the GDPR and other applicable data security breach laws, data controllers and organizations must keep a record of all personal data security breaches. In some jurisdictions, controllers must notify supervisory authorities and affected individuals of those breaches that are likely to result in risks to the rights and freedoms of individuals.

OneTrust has implemented breach prevention and detection controls and an information security incident management plan, which includes the steps needed to address applicable data breach notification requirements. OneTrust has invested in security technology and trained its teams to monitor and detect security incidents as early as possible. Employees are trained to report incidents or unusual activity to an Incident Response Team, who assess whether an incident constitutes a personal data breach that requires notification without undue delay. OneTrust's information security incident management plan details the steps to be taken when an incident occurs, including mitigating actions for the incident itself and actions to prevent incidents in the future, where applicable.

OneTrust's Government Data Request Policy

OneTrust does not voluntarily disclose any customer data/information to government entities (e.g., law enforcement officials) or otherwise grant them access to such data/information. However, OneTrust may receive a subpoena, writ, warrant, or other court order from a government agency requesting that it disclose customer data/information.

OneTrust's policy is to construe requests narrowly to limit the scope of the data/information provided, and OneTrust will only provide the requested data/information in response to formal and valid legal process. OneTrust's Transparency Report which outlines its policy on government data requests can be found at <https://www.onetrust.com/transparency-report/>.

If OneTrust receives a request for data/information, then its legal team reviews the request to ensure that it satisfies applicable legal requirements and OneTrust's policies. For OneTrust to produce any data/information, the request must (a) be made in writing and on official letterhead, (b) identify and be signed by an authorized official of the requesting party and include official contact information, including a valid email address, (c) indicate the reason for, and nature of, the request, (d) identify the customer or customer account that is the target of the request, (e) describe with specificity the data/information sought and its relationship to the investigation, and (f) be issued and served in compliance with applicable law.

Requests from U.S. government authorities must be sent to OneTrust's U.S. offices in Atlanta, GA, while requests from UK or EU government authorities must be sent to OneTrust's UK offices in London. All other requests from foreign government authorities must be issued by a federal court in the U.S. pursuant to an official legal mechanism, such as a Mutual Legal Assistance Treaty.

Where OneTrust receives legal process for a customer's account, its policy is to notify the customer via email before disclosing any information. This notice gives the customer an opportunity to pursue a legal remedy, such as filing an objection with a court or the requesting party.

Exceptions to the government request policy:

- A statute, court order, or other legal limitations may prohibit OneTrust from notifying the customer about the request, but OneTrust will make reasonable efforts to provide notice once the prohibition requirement ends
- OneTrust might not give notice to the customer in exceptional circumstances involving imminent danger of death or serious physical injury to any person or to prevent harm to OneTrust's services
- OneTrust might not give notice to the customer when it has reason to believe that the notice would not go to the actual customer account holder, for instance, if an account has been hijacked
- Where OneTrust identifies unlawful or harmful activity or suspects any such activity related to a customer's account, it might notify appropriate authorities, such as in cases of hacking.

OneTrust Platform Hosting Options

Shared Cloud Environment

OneTrust cloud hosting is provided by Microsoft Azure. OneTrust clients can select hosting locality from many regions around the globe, including the United States, United Kingdom, Germany, France, Switzerland, Australia, Singapore, Canada, Brazil, Japan, India, and United Arab Emirates. This includes a multi-tenant cloud environment with dedicated tenant databases. Backups for cloud-hosted implementations are managed, performed, and tested by Microsoft Azure. Azure provides a 14-day backup to prevent accidental data deletion.

Dedicated Cloud Environment

For an additional cost or for clients holding OneTrust Premier Support, potential clients and current clients can choose to have a dedicated public cloud environment.

A small percentage of OneTrust clients choose to have a dedicated cloud environment hosted through Microsoft Azure, instead of our multitenant cloud environment, also hosted in Microsoft Azure. OneTrust clients leverage our platform for various use cases, and some of these use cases may involve processing more sensitive information in the application. Some clients will have more stringent security and compliance requirements before onboarding a vendor, as well. OneTrust's multitenant public cloud environment has been purchased by more than 14,000 clients globally, and approximately .01% of our current client base has purchased the dedicated cloud option.

In both hosting options, client data is segregated to your own database (logically segregated in public cloud option) with a unique encryption key per client. OneTrust's security certifications also cover both.

For clients who are anticipating a very high volume of traffic, such as capturing Consent receipts via API, a dedicated cloud guarantees dedicated infrastructure and services for that client environment.

Additional features in our dedicated environment:

- Configurable upgrade schedule and maintenance windows to fit your organization's business needs
- Customizable OneTrust application URL
- Option to configure VPN access to OneTrust by your organization's internal business users
- Lower RTO than public cloud environment; requires additional SKU to be added to Order Form

- Support for configuring [Cross-Tenant Customer-Managed Keys \(CMK\)](#)

To see if choosing a dedicated cloud environment hosted through Microsoft Azure is the right option for your organization, please contact your OneTrust Account Executive.

HIPAA Cloud Environment

OneTrust offers a HIPAA-compliant hosting option for U.S. companies that need OneTrust to host Protected Health Information (PHI), as it is defined under the Health Insurance Portability and Accountability Act (HIPAA).

This segregated environment is hosted through Microsoft Azure’s HIPAA cloud hosting option from the rest of the OneTrust platform. This environment employs the same security controls as all other production environments available through OneTrust, with enhanced controls in place under our HIPAA program.

These enhanced controls include segregated audit logging from this environment to our SIEM, which are retained for six years to meet compliance requirements; and enhanced HIPAA training for OneTrust employees supporting this segregated environment, which include how to handle healthcare information. This program is designed to address the administrative, physical, and technical safeguards of the security rule.

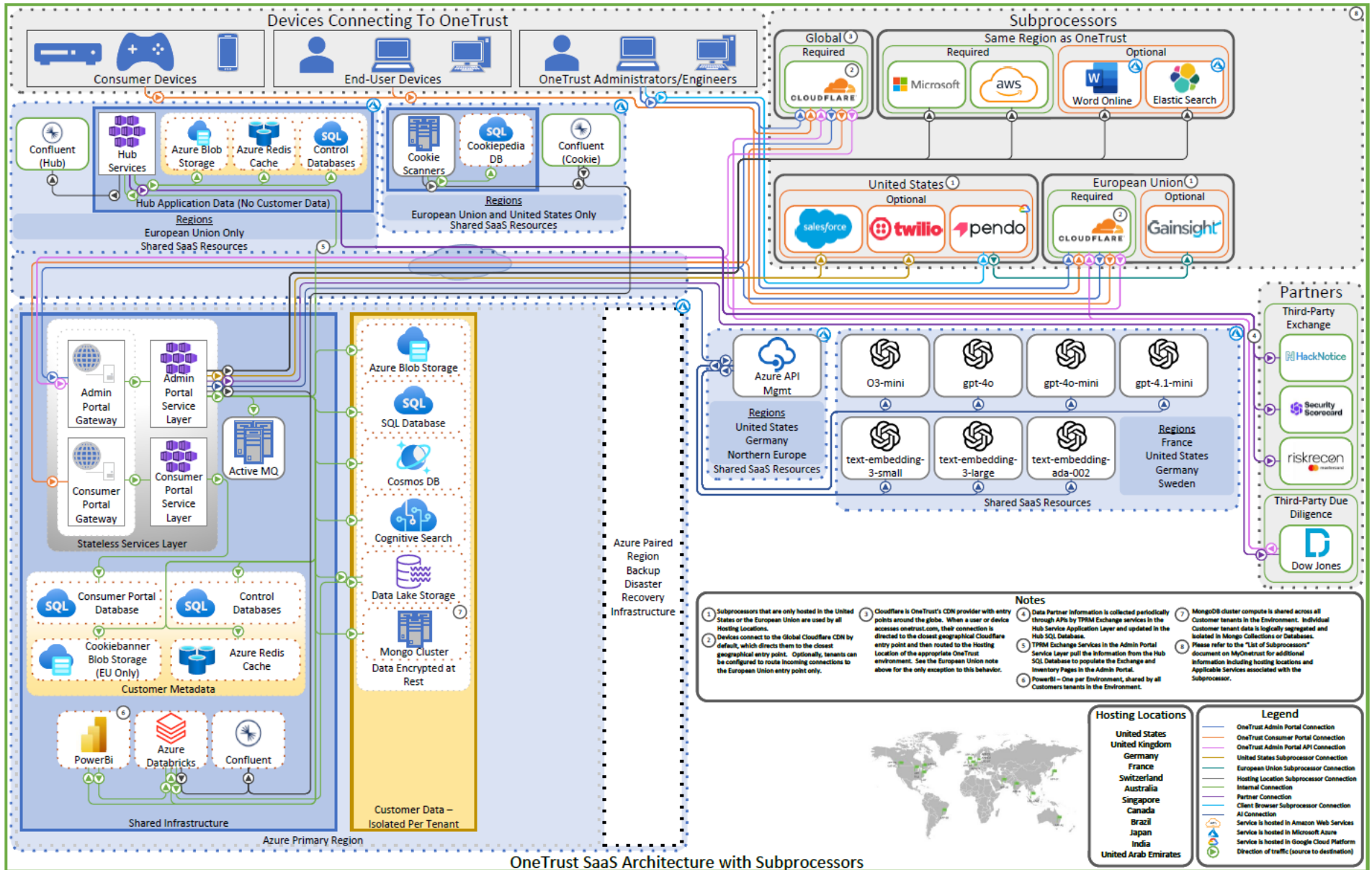
Customer data is stored and hosted in the Azure data centers located in Washington State, with backups stored in Wyoming. OneTrust requires our business associate agreement (BAA) to be signed by the client when the HIPAA hosting environment is selected, and an additional cost is associated with this hosting option. For any further questions, please contact your OneTrust Account Executive.

Cloud Hosting Location Options

In OneTrust’s cloud environment, each tenant has its own database, reducing the risk of one customer seeing another customer’s data. OneTrust uses Microsoft Azure data centers located around the world to support our global customers’ needs. Please see the table below for all hosting options OneTrust supports.

Country	Primary Hosting Location	Disaster Recovery Hosting Location
United States	Iowa	Virginia
Canada	Toronto	Quebec City
United Kingdom	Cardiff	London
Germany	Frankfurt	Berlin
France	Paris	Marseille
Switzerland	Zurich	Geneva
India	Pune	Chennai
Australia	New South Wales	Canberra
Brazil	Sao Paulo State	Texas, USA
Asia Pacific	Singapore	Hong Kong
Japan	Tokyo, Saitama	Osaka
United Arab Emirates	Dubai	Abu Dhabi

OneTrust Platform Architecture



Azure Primary Region

Shared Infrastructure

- Stateless Services Layer – No customer data stored in components that exist in this layer.
 - Admin Portal Gateway: The OneTrust web site where all administrative tasks are performed by OneTrust users.
 - Admin Portal Service Layer: Azure Kubernetes Cluster containing all the services that make up the OneTrust application.
 - Consumer Portal Gateway: Where all traffic originating from a DSAR webform, cookie banner, or consent preference center is sent.
 - Consumer Portal Service Layer: Azure Kubernetes Cluster containing all the services that make up the Consumer Portal.
- ActiveMQ – message broker utilized to foster communication within Shared infrastructure
- Customer Metadata
 - Consumer Portal Database: Contains metadata used to help serve requests to our customers.
 - Control Database: Contains metadata and seed data that is not specific to any customer.
 - Cookie banner Blob Storage: Storage for our customers' cookie banners (when that product is purchased).
 - Azure Redis Cache: Used as a temporary store of metadata to accelerate the application and take load off the databases.
- Confluent: Messaging service used for communication between modules in the OneTrust application.
- Azure Databricks: Azure Databricks is a unified, open analytics platform for building, deploying, sharing, and maintaining enterprise-grade data, analytics, and AI solutions at scale. The Databricks Data Intelligence Platform integrates with cloud storage and security in your cloud account and manages and deploys cloud infrastructure on your behalf. Azure Databricks is used to provide data from the Data Lake to OneTrust Insights reporting which is driven by PowerBI.
- PowerBI: Presentation layer for analytics and reporting.

Customer Data – Isolated per tenant

- Data Encrypted at Rest
 - Azure Blob Storage: Used to store documents, attachments, and other files.
 - SQL Server: Primary data store for the OneTrust platform.
 - Cosmos DB: High scale store for certain use cases.
 - Cognitive Search: Index used to support the data discovery product.
 - Data Lake Storage: Used as a store for analytics and reporting.
- Mongo Cluster: Legacy datastore for reporting and analytics prior to adoption of the Insights product.

Disaster Recovery Infrastructure

See [Business Continuity and Disaster Recovery](#) section above.

Shared SaaS Resources

Hub Application Data (EU Region only)

- Hub Services (Application Layer): Provides global services to all OneTrust environments, no customer data.
- Azure Blob Storage: Supports global services running in hub.
- Azure Redis Cache: Supports global services running in hub.
- Control Database: Supports global services running in hub.

Cookie Scanner Azure Region (EU and US Regions only)

- Cookie Scanners: Used as part of discovering cookies for customers on their websites.
- Cookiepedia Database: Supports the Cookiepedia product.
- Confluent for Cookies: Provides Kafka service to Cookie Scanner environment.
- Confluent for Hub: Provides Kafka service to Hub environment.

Artificial Intelligence Models

- Azure API Management: Azure service which manages routing to Azure OpenAI models for AI processing of customer data.
- Azure OpenAI models are deployed in-region where possible. Where not possible, they are deployed to the relevant Data Zone for a region. This keeps customer data which is operated on by the models within regulatory boundaries.

Responsible AI

OneTrust is dedicated to building and maintaining a culture of trust. Our vision for artificial intelligence (“AI”) embeds our responsible standards into the design, delivery and use of AI solutions and services. OneTrust does not utilize customer data to train our models.

Additionally, OneTrust's AI Governance Committee Team has developed a Global AI Use Policy to govern and guide our employees on their usage of AI internally. This Policy and our AI governance systems enable our technical, business, and legal teams to successfully leverage AI tools consistent with our standards and the rule of law. We believe that a trustworthy AI system is explainable, secure, has a positive purpose, is inclusive, and uses data responsibly.

OneTrust utilizes Azure OpenAI models to power AI functionality within the platform, and the location of the AI features will be the hosting location specified within customer agreements with OneTrust. In certain regions outside of the European Union where the specified location is not available, OneTrust may use Azure regions outside the hosting location specified in the agreement.

OneTrust has published an [AI Transparency Report](#) in the [My.OneTrust.com](#) customer documentation portal, which includes details of current and forthcoming projects, and will be maintained with future updates.

Subprocessors

For more detailed information on our subprocessors, please visit the knowledge base article that contains our [List of Subprocessors](#)

Partners

- HackNotice: Provides updates and alerts on security breaches or hacking incidents relevant to third parties
- Security Scorecard: Risk and vulnerability information relevant to third parties
- RiskRecon: Risk and vulnerability information relevant to third parties
- DowJones: Vendor screening as a part of the Third-Party Due Diligence module to help identify risks such as adverse media, politically exposed persons (PEPs), and sanctions data.

Conclusion

The protection of customer data is the primary consideration for all OneTrust's infrastructure, applications, and operations. As a result, OneTrust makes extensive investments in technology, resources, and expertise that support security and privacy, as well as compliance.

OneTrust strives to build products that its customers trust. OneTrust has established oversight and policy structures that identify and mitigate potential product security risks during development and has instituted programs and practices that drive software security initiatives and awareness across the enterprise. OneTrust will continue to invest in security and privacy to allow our customers to benefit from our services in a secure and transparent manner.