Devo Security Data Platform
Technical & Organizational Measures (TOMs)

1 Products and Services

This document covers the technical, security, and privacy controls for the Devo Security Data Platform.

The Devo Security Data Platform, powered by our HyperStream technology, is purpose-built to provide the speed and scale, real-time analytics, and actionable intelligence that organizations require to unleash the potential of the SOC.

HyperStream provides visibility for customers by ingesting data from any source, at any volume. It fuels the end-to-end security capabilities of the Devo Security Data Platform – including advanced SIEM, SOAR, and UEBA capabilities. HyperStream enables an innovative set of capabilities, including AI-powered DeepTrace, which is Devo's autonomous threat hunting and investigation capability that augments security teams, and ML-powered Collective Defense, which uses Devo community threat intel insights to help customers keep pace with emerging threats.

The Devo Security Data Platform helps teams:

- **Improve visibility** as your infrastructure scales and evolves to help you have the full picture and act faster than certain threat actors.
- **Find threats** using streaming alerts. Devo also helps your security team pinpoint threat actor actions with context and precision while also assessing threat trends across your environment at scale.
- **Visualize your threat posture** and prove the efficacy of your security operations. Your security team can also obtain actionable intelligence with our attack-tracing AI and community-based threat intelligence.

2 Product Architecture

Key Capabilities

Data Ingestion

The Devo Security Data Platform gathers data from various sources, encrypts it, and prepares it for search. Data load balancers distribute the ingested events across the different data nodes (as data arrives at a data node, it is classified, compressed, and stored).

Storage and Search

Meta nodes distribute queries across associated data nodes and combine all results from each data node into datasets that are returned to the Devo Security Data Platform or an API, depending on where the request was made.

Security Operations Core Capabilities

The Devo Security Data Platform accesses stored information to run alert and correlation engines, advanced analytics, automated response, autonomous investigations, and interfaces to external data via APIs.

The Devo Security Data Platform Architecture

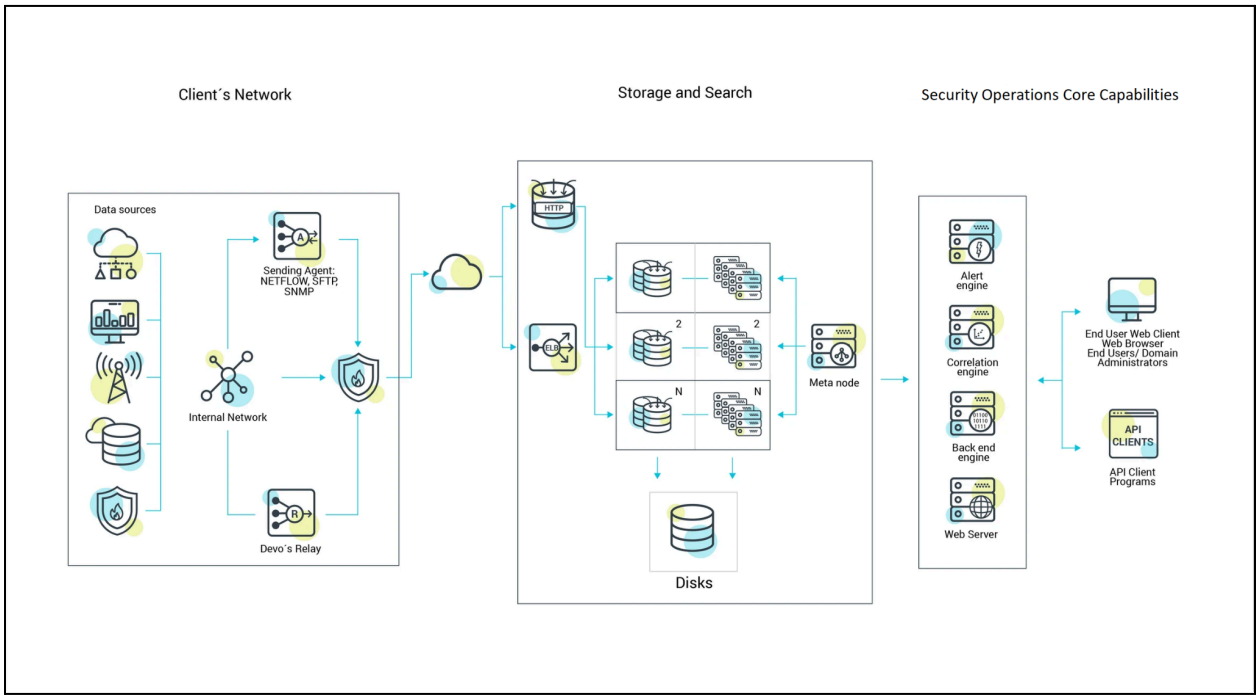
The Devo Security Data Platform enables data ingestion and querying, and adapts to the user's infrastructure for integration and scale.

Key capabilities include

- No-index or normalization at ingestion
- Streaming architecture for real-time insights
- Enrich data on-query for context
- Query large amounts of data to help detect, investigate, and remediate cyber threats
- AI and ML enabler
- Cost-optimized architecture

For further details, please refer to Devo Documentation.

THE DEVO SECURITY DATA PLATFORM



3 Devo Platform Technical Security Controls

Devo employs technical safeguards aligned with industry standards appropriate to the nature and scope of the Services (as the term is defined in the Terms of Service[1]) designed to safeguard the Service infrastructure and data residing therein.

3.1 Logical Access Control

Logical access control procedures are in place, designed to prevent or mitigate the threats of unauthorized application access and data loss in corporate and production environments. Employees are granted minimum (or "least privilege") access to specified Devo systems, applications, networks, and devices as needed. Further, user privileges are segregated based on functional role and environment.

3.2 Perimeter Defense

Devo employs perimeter protection tools, techniques, and services that are designed to prevent unauthorized network traffic from entering our product infrastructure. The Devo network features web application firewalls and internal network segmentation. Cloud

resources also utilize a WAF and Distributed Denial of Service (DDoS) Protection. Critical system files are protected against malicious and unintended infection or destruction.

3.3 Data Segregation

Devo leverages a multitenant architecture, logically separated at the database level, based on a user's or organization's domain within the Devo Platform. Only authenticated parties are granted access to relevant accounts.

3.4 Physical Security

Office Locations

Devo is a remote-first organization. However, we have three office locations. Office headquarters are in Boston, MA, USA; Madrid, Spain; and Noida, India.

No product related customer data (eg, logs) is stored at these locations.

Data center Physical Security

Devo contracts with AWS data centers to provide physical security and environmental controls for server rooms that house production servers. These controls include:

- Video surveillance and recording
- Multi-factor authentication to highly sensitive areas
- Heating, ventilation, and air conditioning temperature control
- Fire suppression and smoke detectors
- Uninterruptible power supply (UPS)
- Raised floors or comprehensive cable management
- Continuous monitoring and alerting
- Protections against common natural and man-made disasters, as required by the geography and location of the relevant data center
- Scheduled maintenance and validation of all critical security and environmental controls

3.5 Data Backup, Disaster Recovery, and Availability

The Devo Disaster Recovery (DR) Plan consists of all actions taken to ensure service continuity after the occurrence of technology-related disaster conditions that unexpectedly affect customer business operations. Such actions include the deployment, maintenance, and utilization of alternative data storage installations.

Service restitution strategies, testing workflows, communications, and improvement actions are also included in the plan. Its completion requires human decision and supervision at all stages.

Customers can request access to Devo StatusPage to gain visibility of planned downtime or platform incidents. Planned maintenance notifications that will impact users are published a minimum of five (5) business days in advance. Urgent maintenance caused by factors outside of Devo's control (CSP hardware deprecation, et al) is rare but is published as far in advance as possible. Incidents related to availability and performance are posted as needed.

2.5.1 Devo Backups

The files containing Devo product customer data are held in persistent Amazon EBS storage systems - partitions, trunks - as part of the Datanodes. Backups of these file systems are located in a storage space different from the Datanode itself, mostly Amazon S3. Backups are incremental and performed daily as part of a set of routines dedicated to data consolidation, e.g., data compression and indexing. Vulnerabilities associated with current-day ingested data are covered since daily storage is duplicated, thus allowing the recovery of information lost due to failure conditions in a partition.

2.5.2 Regular Backup Recovery Operation ('Standard' DR)

The detection of a failed disk in a Datanode involves an interruption of the ingestion process. This leads to an automatic redirection to a different volume to preserve ingestion continuity. By default, each customer is assigned at least two (2) Datanodes to ensure redundancy and ingestion/query load balancing. Devo has implemented these measures to enable continuity of ingestion since a minimum of 32 partitions are available to customers as part of Devo's standard service. Restoration is applied from the backup partition when recovery occurs within the same day, whereas data stored in repositories will be required in case of higher solution times.

In the case of total Datanode loss, incoming data flows would be automatically redirected to one of the customer’s redundant Datanodes.

Successful recovery of data requires:

1. bringing the affected Datanode back to a healthy condition, or
2. completing the full deployment of a new Datanode. Both options will lead to a significant impact on recovery times, which may affect customer service.

3.6 Malware Protection

Devo uses industry standards for endpoint management for all user endpoints and production-side malware protection with audit logging deployed.

3.7 Data Confidentiality and Authenticity

Devo maintains a cryptographic standard of TLS 1.2+, that aligns with recommendations from industry groups, government publications, and other relevant standards groups. The cryptographic standard is periodically reviewed, and selected technologies and ciphers may be updated in accordance with the assessed risk and market acceptance of new standards.

3.7.1 Data in Transit

Devo provides security measures for data in transit that are designed to protect against passive and active attacks against confidentiality, integrity, and availability.

All incoming and outgoing connections are encrypted with at least TLS 1.2.

For Data Load Balancers, passwords and secrets are encrypted from configuration. External TCP ports expecting to receive syslog over TCP use TLS encryption (TLSv1.2 or higher) with client certificates. External HTTP ports, such as the ones expecting to receive events via HTTP, use TLS encryption (TLSv1.2 or higher) and do not require client certificates.

Devo supports query signing. Query signing is used to secure certain sensitive administrative operations. Authenticity and integrity are validated, with keys secured in a Java KeyStore (JKS). Certificates with a strong cipher and key length are generated to support current industry best practices and TLS version 1.2+.

Devo enforces a 12-character password length and complexity per industry standards and uses SSO for both external access control and internal provider access through MFA.

Devo uses separation of duties for role-based access control and VPN authentication for privileged users to access the private VPC. The security administrator may reset all passwords, following the change control process and logging for audit. Storage permissions and encryption for storage outside EC2 and EBS are limited by RBAC.

For Relays, Devo encrypts all communications to a single aggregation instance (either cloud-based or on-premises) to maintain the security of data in transit. We use TLS 1.2

with a list of Devo nodes from our relays to our event load balancers. Each customer has a shared key established using a valid API request per relay during deployment. Devo uses OpenSSL library 1.1.1x for X.509v3 certificates and configurable key extensions based on security constraints. Customers may either use/generate a Devo-signed key (default) or specify their own if they have a certificate authority.

For Web access, Devo's user interface can be integrated with SSO technology. We recommend doing so as a best practice. Role-based access control for user interface-secured HTTPS access uses TLS 1.3 for web access. Authentication is configurable to use multifactor authentication using TOTP, time-based one-time password, or OAuth via HOTP (HMAC one-time password).

All passwords may be reset by the security administrator. We recommend adhering to security best practices and resetting passwords, following the change control process and logging for audit, as well as disabling users.

For their protection, Devo recommends that customers configure their browsers to use strong cryptography by default whenever possible and ensure that operating system and browser security patches are kept up to date.

Key creation is managed by Amazon Web Services (AWS). Devo does not allow Customers to "bring your own key" at this time.

3.7.2 Data at Rest Encryption and Protection

Devo Datanodes are configured with encrypted disks. Data is retained based on the storage used and duration of storage. We use AWS encryption for EBS volumes encrypted separately.

Backup and replication for dedicated data nodes copies Devo data node files in S3.

For dedicated data nodes, the backup S3 bucket is also dedicated for storage and restoration. All data stored at rest on data node-attached storage or ephemeral storage support cipher strength and key size appropriate in accordance with current industry best practices.

3.8 Vulnerability Management

Internal and external system and network vulnerability scanning is conducted at least weekly. Dynamic and static application vulnerability testing and penetration testing activities for targeted environments are performed periodically. These scanning and

testing results are reported into network monitoring tools and, where appropriate predicated on the criticality of any identified vulnerabilities, remediation action is taken.

Vulnerabilities are also communicated and managed with monthly and quarterly reports provided to development teams as well as management.

3.9 Logging and Alerting

Devo collects identified anomalous or suspicious traffic into relevant security logs in applicable production systems. We use our proprietary platform, in an instance separate from our customer environments, to monitor our corporate environment 24/7/365. Due to the size of our organization, we have outsourced our SOC to a preferred MSSP partner.

In addition to security logging, Devo also monitors our infrastructure's performance through an industry-leading observability platform.

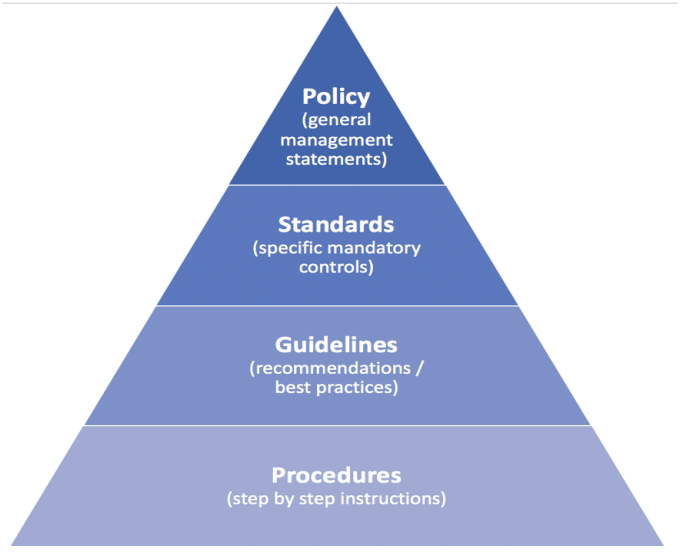
4 Organizational Controls

Devo operates a comprehensive set of organizational and administrative controls to protect the security and privacy posture of Devo.

4.1 Security and Privacy Policies

Devo maintains and implements a comprehensive set of security and privacy policies aligned with business goals, compliance programs, and overall corporate governance. These policies are periodically reviewed and updated as necessary to ensure ongoing compliance.

The documentation framework is aligned to internationally accepted control standards and ensures Devo is able to streamline processes to provide transparent insight to management on risks and issues pertaining to information security. Utilizing consistent control requirements assists leadership in identifying and remediating any potential control gaps. Our framework aligns our business to ISO 27001:2013 best practices. The diagram below demonstrates how Devo's security and privacy frameworks are established.



Policies

- Information Security Policy – a high-level policy that outlines Devo's commitment to Security and details the roles and responsibilities throughout the organization for ensuring compliance. This policy is the overarching security policy for Devo, and all security requirements fall beneath it. This must be signed by employees upon hire and annually thereafter.
- Acceptable Use Policy (AUP) - the set of mandatory rules and controls that every Devo employee, consultant, and contractor must abide by when accessing Devo information, the Devo network, and all Devo environments. This must be signed by employees upon hire and annually thereafter.
- Data Protection Policy - Outlines the mandatory privacy rights, protections, and obligations to protect data subjects from unlawful collection, processing, and disclosure.
- Privacy by Design Policy - Supports Devo's global data privacy program and compliance with applicable data protection laws, including the General Data Protection Regulation (EU) 2016/679 (GDPR), the California Consumer Privacy Act (CCPA), and other privacy laws that apply to the jurisdictions in which we operate.
- Risk Management Policy - Outlines Devo's commitment to risk management and the associated framework utilized by the company to identify and manage relevant risks within acceptable tolerance.
- Vendor Security Risk Assurance Policy - This document supports the overarching Procurement Policy managed by the finance team and is a part of the Information Security Framework. This policy outlines Devo's commitment to performing adequate vendor security risk due diligence.

Frameworks and standards

- Security Standard – documents the minimum controls required to set a baseline for Devo to achieve and then measure itself against security maturity. Exceptions to these requirements are allowed but must follow the established risk governance process.
- Technical Privacy Standard – detailed controlled standard aligned to applicable privacy laws and standards, which supports Devo's Privacy Policy. It defines the principles and minimum controls necessary for protecting: (i) Personally Identifiable Information (PII), (ii) Personal Data, and (iii) Devo Information classified as Confidential, including customer content or employee personal information and Devo systems. The standard is designed to support and supplement the security framework.
- Incident Response Plan – plan to ensure a consistent and effective approach to the management of information security Incidents, including stakeholder communication on security events and weaknesses. This Incident Response Plan is intended to instruct Devo employees on appropriate steps and responsive actions to be taken when a "Security Incident" is detected and/or reported internally or externally by a third party.
- Guidelines – high-level instructions created by departments/functions on how to meet the minimum requirements in the Security Standard or the Technical Privacy Standard.
- Procedures – documents that provide step-by-step procedures, created by departments/functions with support from the Security Team, supporting the Information Security Framework.

4.2 Standards Compliance

Devo complies with applicable legal, financial, data privacy, and regulatory requirements and conforms with compliance certification(s) and external audit report(s) including but limited to the following:

- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Type II attestation report incl. American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Type II attestation report[4];
- FedRAMP, Federal Risk and Authorization Management Program, Moderate Authorization to Operate, December 26, 2023
- TX RAMP, Texas Risk and Authorization Management Program, and Texas Senate Bill 475
- General Data Protection Regulation, 2018

- EU-U.S. Data Privacy Framework (EU-U.S. DPF) and, as applicable, the UK Extension to the EU-U.S. DPF
- UK Data Protection Act of 2018
- Privacy and Electronic Communications Directive (2002) (ePrivacy Directive);
- Canadian Anti-Spam Legislation (CASL) of 2014; and
- Spam Act 2003 of Australia.

Note that Devo's FedRAMP Moderate Authorized environment is separate from the commercial Devo environment described herein and is not represented in this document. For more information on FedRAMP or to verify Devo's authorization, visit https://marketplace.fedramp.gov/products and search for Devo.

4.3 Security Operations and Incident Management

Devo's Security Operations Center (SOC) is outsourced to a preferred MSSP Partner. The SOC uses our proprietary Devo Platform, security sensors, and analysis systems to identify potential issues and has developed an Incident Response Plan that dictates appropriate responses.

The Incident Response Plan is aligned with Devo's critical communication processes, the Information Security Policy Framework, and associated standard operating procedures. It is designed to manage, identify, and resolve suspected or identified security events across its systems and services, including the Devo Security Data Platform.

Per the Incident Response Plan, technical personnel are in place to identify potential information security-related events and vulnerabilities and to escalate any suspected or confirmed events to management when appropriate. Employees can report security incidents via email and/or ticket, according to the process documented on the Devo SOC Team Confluence site and other associated staff sites. All identified or suspected events are documented and escalated by standardized event tickets and triaged based on criticality.

Customers can report events and vulnerabilities through two (2) formal channels: Devo Support and Devo's Vulnerability Disclosure Program.

Customers can create a support case and share relevant technical details about suspected vulnerabilities. Devo will need to know:

- the steps to reproduce the findings,
- how it was discovered, including screenshots, and
- what part of the product it affects.

If a customer has discovered a vulnerability in a Devo-hosted product (e.g., CSS in a feature of the web app), Devo Support will escalate it to the appropriate channels (CISO team, Product). If a customer has discovered a vulnerability in a Devo product running in their environment, we suggest upgrading to the latest version, if applicable - else Devo Support will again escalate to CISO and Product teams.

Devo is not responsible for OS-level vulnerabilities on instances/machines in a customer's environment that hosts Devo software. This is because Devo does not issue the virtual machine images to customers; Customers bring their own devices and pull down code from the Devo Repository.

Devo's external https://www.devo.com/responsible-vulnerability-disclosure-program/ is available to all customers and researchers to submit potential security issues to Devo directly. The rules are listed on the web page.

4.4 Application Security

3.4.1. Authentication Controls

Multi-Factor Authentication (MFA)

Devo has implemented MFA and Single Sign On (SSO) to critical applications and systems to add an extra layer of security by requiring users to provide multiple forms of identification.

Strong Password Policies

Devo enforces complex password requirements, including a minimum length of twelve (12) characters for user accounts and sixteen (16) characters for administrator accounts, use of special characters, and regular password changes.

Account Lockout Policies

Devo has implemented policies that automatically lock user accounts after a specified number of failed login attempts to prevent brute force attacks.

3.4.2 Authorization Controls

Role-Based Access Control (RBAC)

Devo utilizes RBAC to assign permissions based on job roles, ensuring that users only have access to the functionalities necessary for their responsibilities in our Devo Platform.

Least Privilege Principle

Devo applies the principle of least privilege to grant users the minimum level of access required to perform their tasks.

3.4.3. Application Development Controls

Secure Coding Standards

Establish and enforce secure coding standards to ensure that developers write code with security considerations in mind.

Static Application Security Testing (SAST)

We use an industry-leading tool to analyze source code for security vulnerabilities during the development phase.

4.5 Personnel Security

Background checks, to the extent permitted by applicable law and as appropriate for the position, are performed globally on new employees prior to the date of hire. Results are maintained within an employee's job record. Background check criteria will vary depending upon the laws, job responsibilities, and leadership level of the potential employee and are subject to the common and acceptable practices of the applicable country.

4.6 Security and Privacy Awareness and Training Programs

New hires are informed of security and privacy policies and the Devo Code of Conduct and Business Ethics at orientation. Additionally, new hires are required to complete privacy and security training within two weeks of their start date. The security and privacy training is provided annually and managed by the Training and Development with support from the security team.

Devo employees and temporary workers are informed regularly about security and privacy guidelines, procedures, policies, and standards through various mediums, including new hire onboarding kits and awareness campaigns.

Developer Training Programs

Devo provides ongoing security training for developers to keep them informed about the latest security threats and best practices. The training includes but is not limited to, OWASP Top 10, Capture the Flag challenges, and Java, Python, and Javascript best practices.

Devo Employee Awareness Programs

Devo educates employees on a continuous basis about social engineering attacks, phishing, and the importance of secure behavior through training exercises and awareness campaigns targeting all staff.

5 Privacy Practices

Devo takes the privacy of its customers and employees very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

5.1 Privacy Policies and Statement

Devo discloses the types of information it collects and uses to provide, maintain, enhance, and secure its services in its Privacy Statement on our public website and in customer contracts[2]. Devo may occasionally update the Privacy Statement to reflect changes to its information practices and/or changes in applicable law but will provide notice on its website for any material changes before any such change takes effect.

Devo has an internal Data Protection Policy applicable to all employees and a Privacy by Design applicable to employees who design, build, and support our platform.

5.2 GDPR; ePrivacy Directive

The General Data Protection Regulation (GDPR) is a European Union (EU) law on data protection and privacy for individuals within the European Union. GDPR aims primarily to give control to its citizens and residents over their personal data and to simplify the regulatory environment across the EU. Devo's services are compliant with the applicable provisions of the GDPR. For more information, please visit www.devo.com/privacy.

5.3 UK Data Protection Act 2018

The UK Data Protection Act 2018 is a United Kingdom law on data protection and privacy for individuals within the UK after the UK's exit from the EU. The Data Protection Act aims to give control to its citizens and residents over their personal data and to continue GDPR protections. Devo is registered with the UK's Information Commissioner's Office. For more information, please visit www.devo.com/privacy.

5.4 CCPA/CPRA

Devo is in compliance with the California Consumer Privacy Act and California Privacy Rights Act (CCPA and CPRA), and has implemented and maintained the necessary controls to adhere to the applicable provisions of CCPA and CPRA. For more information, please visit https://www.devo.com/legal-hub/personal-data-processing/.

5.5 Singapore Personal Data Protection Act (PDPA)

Singapore's Personal Data Protection Act (PDPA) regulates the collection and use of Singaporean personal data. Devo has implemented the necessary controls to adhere to the applicable provisions of PDPA. For more information, please visit https://www.devo.com/legal-hub/personal-data-processing/

5.6 Canada Personal Information Protection and Electronic Documents Act (PIPEDA)

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a federal Canadian law regulating how entities collect, process, and disclose personal information in commercial contexts. Devo has implemented the necessary controls to adhere to the applicable provisions of PIPEDA. For more information, please visit https://www.devo.com/legal-hub/personal-data-processing/.

5.7 The Australian Federal Privacy Act 1988 (Cth) (Privacy Act) and the Australian Privacy Principles

The Australian Federal Privacy Act 1988 regulates the collection and use of Australian personal data and implements the Privacy Principles. Devo has implemented the necessary controls to adhere to the applicable provisions of the Privacy Act. For more information, please visit https://www.devo.com/legal-hub/personal-data-processing/.

5.8 Transfer Frameworks

Devo's privacy program and contracts have been designed to account for shifts in the regulatory landscape to avoid impacts on our ability to provide our services to you. Devo offers the following Transfer Framework.

5.7.1 Standard Contractual Clauses

The Standard Contractual Clauses (or "SCCs") are standardized contractual terms recognized and adopted by the European Commission, whose primary purpose is to ensure that any personal data leaving the EEA will be transferred in compliance with EU

data protection law. Devo has invested in a world-class data privacy program designed to meet the exacting requirements of the SCCs for the transfer of personal data.

Devo offers customers SCCs, sometimes referred to as EU Model Clauses, that make specific guarantees around transfers of personal data for in-scope Devo services as part of its global DPA.[4] Execution of the SCCs helps ensure that Devo customers can freely move data from the EEA to the rest of the world where necessary.[3]

For more information on how Devo uses your data, please refer to your Data Protection Addendum (DPA).

5.7.2 Data Privacy Framework

Devo has certified to the Department of Commerce that we adhere to the Data Privacy Framework Principles ("Principles") of the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework, as further described in the Devo Data Privacy Framework Notice, and Devo complies with all its obligations under the Principles. Please note this certification is pending acceptance by the US Federal Trade Commission.

5.9 Retrieval and Deletion of Customer Data

Customers can request the deletion of their data by contacting legal@devo.com. Devo will delete the data within the timeframe required by contract or applicable law, whichever is shorter. Upon request, Devo will provide certification of such deletion.. Devo will also provide instructions on how to retrieve data.

5.10Sensitive Data

While Devo aims to protect all customer content, regulatory and contractual limitations require us to restrict the use of Devo for certain types of information. Unless the customer has written permission from Devo, the following data must not be uploaded or generated to Devo:

- Government-issued identification numbers;

- Information related to an individual's health, including, but not limited to, Personal Health Information (PHI) identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA) and related laws and regulations.
- Information related to financial accounts and payment instruments, including, but not limited to, credit card data. The only general exception to this provision extends to explicitly identified payment forms and pages that are used by Devo to collect payment; and
- Any information especially protected by applicable laws and regulation, specifically information about an individual's race, ethnicity, religious or political beliefs, organizational memberships, etc.

5.11 Tracking and Analytics

Devo continuously improves its websites and products using various third-party web analytics tools, which help Devo understand how visitors use its websites and desktop tools, what they like and dislike, and where they may have problems. For further details, please reference our Privacy Statement.[2]

6 Third Parties

6.1 Use of Third Parties

As part of the internal assessment and processes related to vendors and third parties, vendor evaluations are performed by multiple teams depending upon relevance and applicability. Devo's security team evaluates vendors that provide information security-based services including the evaluation of third-party hosting facilities, that have access to, process, store, or transmit customer Information, Devo information, and/or access Devo networks. Legal and Procurement evaluate all contracts per internal processes. Appropriate compliance documentation or reports are obtained where necessary and evaluated at least annually to ensure vendors and third parties maintain an acceptable security and technical privacy posture.

6.2 Contract Practices

To ensure business continuity and that appropriate measures are in place to protect the confidentiality and integrity of third-party business processes and data processing, Devo reviews third parties' terms and conditions and either utilizes Devo-approved procurement templates or negotiates such third-party terms, where deemed where necessary.

7 Contacting Devo

Customers can contact Devo at support@devo.com or sales@devo.com for privacy-related questions.

8 References

[1]	Devo Terms and Conditions of Service, https://www.devo.com/legal-hub/devo-terms-of-service/
[2]	Devo Privacy Statement, https://www.devo.com/privacy/
[3]	Devo, Annex B, Standard Contractual Clauses, https://www.devo.com/legal-hub/personal-data-processing/
[4]	Devo Public Facing SOC3 Report, https://www.devo.com/legal