

pipedrivenTM

REPORT ON PIPEDRIVE'S SALES MANAGEMENT SYSTEM
RELEVANT TO SECURITY, AVAILABILITY, CONFIDENTIALITY,
AND PRIVACY THROUGHOUT THE PERIOD OCTOBER 1, 2017 TO
SEPTEMBER 30, 2018



SKODA MINOTTI & CO.
CERTIFIED PUBLIC ACCOUNTANTS

Delivering on the Promise.

Acronym Table

➤ AICPA	American Institute of Certified Public Accountants
➤ AT-C	U.S. Attestation Standard– AICPA (Clarified)
➤ AWS	Amazon Web Services
➤ CEO	Chief Executive Officer
➤ CRM	Customer Relationship Management
➤ GAPP	Generally Accepted Privacy Principles
➤ HR	Human Resources
➤ IIS	Internet Information Services (Microsoft)
➤ IP	Internet Protocol
➤ IPS	Intrusion Prevention System
➤ IT	Information Technology
➤ NAT	Network Address Translation
➤ PII	Personally Identifiable Information
➤ Pipedrive	Pipedrive, Inc and Pipedrive OÜ
➤ QE	Quality Engineering
➤ RDS	Relational Database Service
➤ SDLC	Software Development Life Cycle
➤ SLA	Service Level Agreement
➤ SOC	System and Organization Control
➤ TLS	Transport Layer Security
➤ TSP	Trust Service Principles
➤ VM	Virtual Machine
➤ VP	Vice President
➤ VPN	Virtual Private Network

Assertion of Pipedrive Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Pipedrive, Inc.'s (Pipedrive's) Sales Management System (system) throughout the period October 1, 2017 to September 30, 2018, to provide reasonable assurance that Pipedrive's service commitments and system requirements relevant to security, availability, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented in section 3 and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2017 to September 30, 2018, to provide reasonable assurance that Pipedrive's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Pipedrive's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in section 3.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2017 to September 30, 2018, to provide reasonable assurance that Pipedrive's service commitments and system requirements were achieved base on the applicable trust services criteria.

/s / Timo Rein, Member of the Board
Pipedrive, Inc.
October 1, 2018

Independent Service Auditors' Report

To: Pipedrive, Inc.:

Scope

We have examined Pipedrive, Inc.'s (Pipedrive's) accompanying assertion titled "Assertion of Pipedrive Management" (assertion) that the controls within Pipedrive's Sales Management System (system) were effective throughout the period October 1, 2017 to September 30, 2018, to provide reasonable assurance that Pipedrive's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Pipedrive is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Pipedrive's service commitments and system requirements were achieved. Pipedrive has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Pipedrive is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Pipedrive's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Pipedrive's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the

applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Pipedrive's Sales Management System were effective throughout the period October 1, 2017 to September 30, 2018, to provide reasonable assurance that Pipedrive's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

SKODA MINOTTI & CO.

A handwritten signature in cursive script that reads "Skoda Minotti".

October 1, 2018
Tampa, Florida

Company Overview and Services Provided

Pipedrive is a software development company that implements CRM software for enterprise clients. Both co-founders are seasoned sales managers that recognized a need for a better CRM for the ground level sales personnel.

Pipedrive was founded in 2010 when the co-founders realized that the CRM landscape was populated by software designed to please upper management while ignoring the needs of the ground level sales representatives. After partnering with a talented developer and explaining their rooted philosophy of activity-based selling, the result was a CRM software known as Pipedrive. The Pipedrive software is utilized by over 75,000 companies around the world. Pipedrive is most widely used as a CRM program to drive sales and grow the bottom line but it has also seen success in recruiting and other facets. Pipedrive was founded in Tallinn, Estonia in 2010 and has since expanded to Tartu, Estonia, Lisbon Portugal, London England and New York, New York.

The Sales Management System SaaS product was developed with activity-based selling in mind. Activity-based selling is a sales management strategy that links the cause and effect relationship between sales activities and business results. In sales, the most desirable business result is closing a deal which translates to boosting revenue. But revenue is not a manageable metric and therefore, hard to control. Activity-based selling attempts to link what a sales team can control, inputs (sales pipeline activities), to the outputs, revenue.

The features included in the Sales Management System are what make it unique among other CRM programs. The Sales Management System offers clarity, is fully customizable at all levels, and is intuitive.

Principal Service Commitments and System Requirements

Pipedrive designs its processes and procedures related to its Sales Management System to meet its objectives. Those objectives are based on the service commitments that Pipedrive makes to user entities, the laws and regulations that govern SaaS providers, and the financial, operational, and compliance requirements that Pipedrive has established for the services. The CRM services of Pipedrive are, inter alia, subject to the GDPR due to the jurisdictions in which Pipedrive operates.

Security commitments to user entities are documented in customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Sales Management System that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect customer data at rest and in transit.

Pipedrive establishes operational requirements that support the achievement of security, availability, confidentiality, and privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Pipedrive's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Sales Management System.

Infrastructure

The infrastructure supporting the Sales Management System consists of the following:

- Debian and Ubuntu production application servers
- A load balancer located within Rackspace to distribute traffic to Sales Management System web application servers
- MySQL Server database server to support the Sales Management System web application
- Jenkins automation server for continuous deployment
- Consul for service discovery
- Docker Swarm for clustering and scheduling docker containers
- A batch server to run schedule jobs
- Cisco AnyConnect VPN server appliance

The Pipedrive Sales Management production SaaS System is entirely hosted within Rackspace. The Sales Management web application is written in PHP that runs on multiple Linux servers within Rackspace. Pipedrive utilizes a cloud load balancer that distributes traffic to application servers running the Sales Management website application. There is also a batch server which is used to run various scheduled jobs. Database services are provided by a MySQL database servers. The system utilizes a Cisco VPN communications server to establish an IPsec VPN tunnel between the Tallinn office and the New York office as well as the IPsec VPN tunnel from Tallinn and Tartu to Rackspace in Chicago. Backups are stored within the AWS US East region in S3. No connection between the Rackspace Chicago and AWS US East exists. The AWS environment houses the development, testing, and staging environments. The testing and staging environments share hardware and a load balancer. The development environment consists of one server which replicates all aspects of the production environment except for the production database contents.

Software

The following provides a summary of the systems used to deliver the Sales Management System:

- MySQL Server is the relational database management system.
- Confluence team collaboration software stores and organizes Pipedrive's policies and procedures.
- Bamboo stores the organizational hierarchy and made available to employees.
- 7 Geese store HR documentation and personnel files such as employee contracts and evaluations.
- Jira ticketing software is used to track and respond to development issues, requests, and bugs.
- Github is used for version control software utilized in the development process.
- Carbon Black CB Defense is utilized for antivirus protection.
- Jenkins automation server for continuous deployment
- Consul for service discovery
- Docker Swarm for clustering and scheduling docker containers

People

People involved in the operation and use of the system are:

- The CEO, who is responsible for general oversight of the day-to-day operations of Pipedrive and the design of the corporate culture
- VP of Engineering, who is responsible for oversight of the development team as well as project management and business analysis for the Sales Management application
- Developers and Business Analysts, who are responsible for the support and development of the Sales Management application
- Head of QE, who is responsible for quality assurance and system testing
- Head of Information Security (Governance, Risk, Compliance), who is responsible for security awareness and overall compliance

Procedures

Executive and Operations Management personnel maintain documented operating procedures involved in the operation of the Sales Management System:

- Access Controls Policy
- Account Management Policy
- Backup and Recovery Policy
- Business Continuity Policy
- Data Integrity and Privacy Policy
- Electronic Data Disposal Policy
- Firewall Management Policy
- Incident Report and Response Policy
- Information Classification Policy
- Information Security Policy
- Information Security Program Policy
- Log Management and Monitoring Policy
- Media Re-Use and Disposal Policy
- Physical Security Policy
- Privacy Policy
- Privacy and Security Responsibilities Policy
- Risk Management Policy
- SDLC Policy
- Security Training Program
- Third Party Security Review and Risk Management Lifecycle Policy
- Vendor Validation and Monitoring Policy

Data

Pipedrive's Sales Management System provides CRM and sales management designed to help small sales teams manage intricate or lengthy sales processes. The Sales Management System was designed with the sales representatives in mind with easy tracking and reporting capabilities to help increase efficiency with the many customer relationships and sales data representatives are required to maintain. Some of the data maintained within Pipedrive's Sales Management System would include prospective clients' contact information, potential contract prices and realization, description of business, and much more. Access to customer data in Pipedrive's Sales Management System is restricted to appropriate IT personnel, approved customer personnel, and certain business partners.