pipedrive

WHITEPAPER

SECURITY & PRIVACY

This document takes a deeper look at the security and privacy measures implemented at Pipedrive both in the application and the organization to ensure the safety of the data our customers entrust to us.

Mustamäe tee 3a, 10615
Tallinn, Estonia
pipedrive.com

Last updated on 28th August 2019. Content subject to changes.

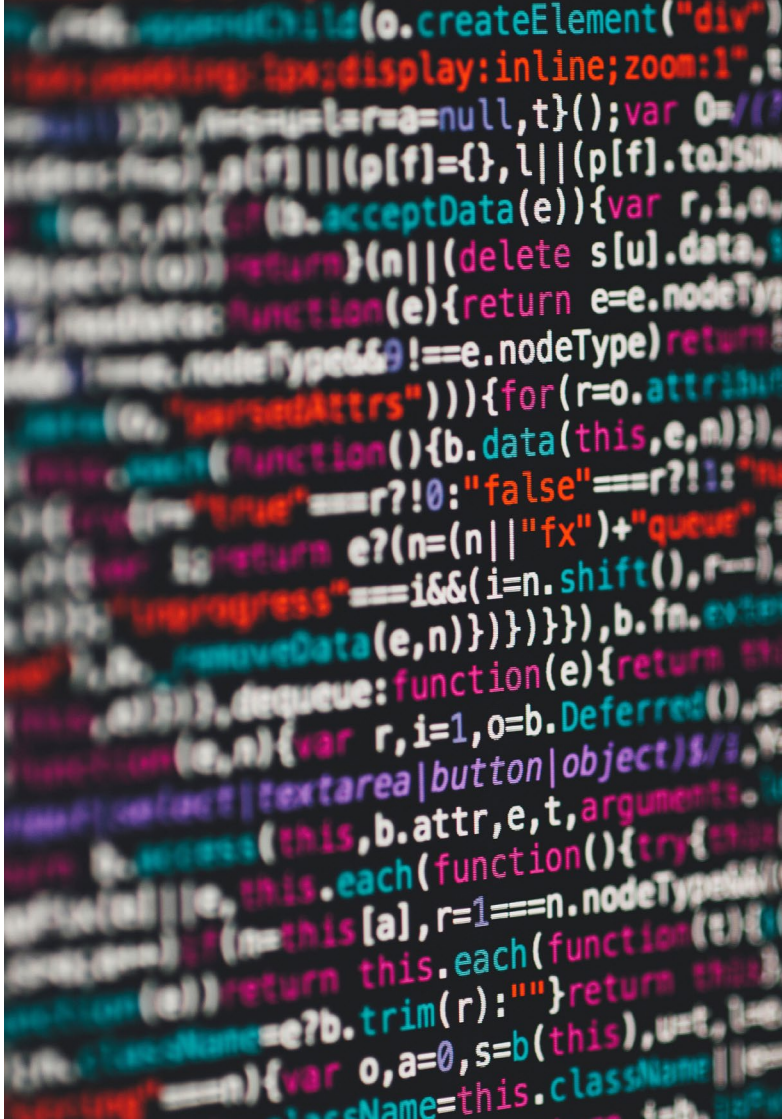

TABLE OF CONTENTS

PIPEDRIVE CRM

Pipedrive is a sales management tool designed to help sales teams manage intricate or lengthy sales processes.

Certifications:

- SOC 2
- Privacy Shield
- SOC 3
- GDPR Compliant

Product Offering:

You can choose between different plans based on the features you need to really make your sales team truly unstoppable.

ESSENTIAL	ADVANCED	PROFESSIONAL	ENTERPRISE
		Recommended	
Easily set up a clear sales process and get organized	Automate your sales process to spend less time on admin and close more deals	Ideal for managing teams and scaling sales performance to hit more targets	Customize Pipedrive for your business

TECHNOLOGY

Pipedrive is a cloud-based software platform that relies on state-of-the-art technologies for maximum security and availability.

Cloud Infrastructure

Pipedrive's production systems are hosted by Rackspace whose multi-layered approach to securing their cloud services and infrastructure meets the strictest industry standards.

Pipedrive's backups are hosted within Amazon Web Services (AWS) Elastic Compute Cloud (EC2) and Simple Storage Service (S3) and consist of a multi-tier virtualized architecture comprised of Linux-based application and database servers, storage and content delivery systems, and server and application monitoring and logging tools.

Our cloud infrastructure providers maintain recognized security certifications and abide by key compliance frameworks including but not limited to:

- **ISO 9001, ISO 27001, ISO 27017, ISO 27018**
- **PCI-DSS**
- **SOC1, SOC2, SOC3**
- **Privacy Shield**

More information can be found at https://www.rackspace.com/security and https://aws.amazon.com/security

Sub-processors

Pipedrive engages only carefully selected sub-processors to best serve our customers. Vendors are required to enter into data processing agreements and undergo a security assessment by Pipedrive's Information Security team. We expect all sub-processors to have mature information security programs in place which are based on well-known standards such as SOC 2, CSA CAIQ, and ISO 27001 SoA.

In addition to the cloud infrastructure providers above, Pipedrive uses the following sub-processors:

Clearbit	Service provider for the Smart Data feature. Based in the U.S. (Privacy Shield certified). See Clearbit's Terms of Service and Privacy Policy.
SendGrid	Service provider for the Smart Email BCC feature. Based in the U.S. (Privacy Shield certified). See SendGrid's Terms of Service and Privacy Policy.
Google	Processes address data into Google Maps links. Based in the U.S. (Privacy Shield certified). Users are bound by the Google Maps/Google Earth Additional Terms of Service (including the Google Privacy Policy) Emails sent to Supplier are processed by Gmail in accordance with the Google Terms of Service.
Intercom	Service provider for customer support conversations, qualifying as a processor for Client Data only if you provide Client Data in conversations with our customer support specialists. Based in the U.S. (Privacy Shield certified). See Intercom's Terms and Policies.

TECHNOLOGY

Nylas	Service Provider for emailing features. Based in the U.S. (Privacy Shield certified). Service provided based on a Master Service Agreement and GDPR-compliant Data Processing Agreement.
Twilio	Service provider for the Caller feature. Based in the US (Privacy Shield certified).
Leadfeeder	Service provider for the LeadBooster feature. Based in Finland (GDPR compliant).
Akamai	Akamai is used to deliver content to you efficiently while protecting Pipedrive's infrastructure from DDoS and other cyber attacks. Based in the US (Privacy Shield certified).

SECURITY

Pipedrive has a comprehensive Information Security Program with SOC 2 compliant controls and processes.

Certifications

SOC 2 AND 3 COMPLIANT

Pipedrive undergoes annual SOC 2 and 3 audits conducted by reputable third-party auditors. Our latest SOC 3 report is freely available here. Should you require our SOC 2 Type II report, this can be provided by our Sales team under an NDA.

PRIVACY SHIELD

Pipedrive's U.S. entity is certified under the EU-U.S. Privacy Shield framework. Our certification is publicly listed at www.privacyshield.gov.

Preventive Security

AUTOMATED SCANNING

Pipedrive uses state-of-the-art automated code scanning tools to identify potential security issues before deployment. This helps prevent any malicious or accidental inclusion of vulnerabilities in our regular updates to the application.

SECURITY

DEPLOYMENT CHECKLIST

Pipedrive has adopted the OWASP Secure Coding Practices Checklist as a part of the development process. Pipedrive has also prepared a Privacy by Design checklist that product managers and engineers follow to design and build features in a secure and compliant manner. Teams complete this checklist to ensure that proper controls are in place for any project that they are working on.

BUG BOUNTY PROGRAM

Pipedrive maintains a private bug bounty program at HackerOne where experienced security researchers constantly attempt to identify vulnerabilities in the Pipedrive application and report any such instances to Pipedrive for a reward. These significant additional resources paired with Pipedrive's engineers and controls ensure a continually high level of application security.

PENETRATION TESTING

Pipedrive has successfully passed several penetration tests carried out by some of our more security-conscious customers with Pipedrive's permission. The results of the latest penetration test are available under an NDA.

Incident Response

Pipedrive has documented detailed procedures for handling any security incidents that might arise. Execution of and compliance with these procedures is regularly practiced with scenarios and exercises run by external security experts. This ensures that Pipedrive is prepared to promptly address all types of incidents by mitigating their impact, investigating the causes and applying corrective measures to prevent similar cases in the future.

DATA STORAGE & RETENTION

Pipedrive understands that your data is at the core of our business and, therefore, ensuring its confidentiality, integrity and availability is crucial to our success.

Encryption

DATA AT REST

Data at rest is encrypted with 256-bit Advanced Encryption Standard (AES-256).

DATA IN TRANSIT

Pipedrive uses HTTP Strict Transport Security (HSTS) to protect data in transit via Transport Layer Security (TLS) provided by HTTPS.

BACKUPS & MONITORING

Application data is continuously backed up to geographically redundant data centers, ensuring that our services remain available or are easily recoverable if necessary. Our servers are spread across multiple availability zones located in the United States and Germany.

Pipedrive maintains its own continuous monitoring services in order to ensure control and availability of customer data, including:

- Database monitoring
- Application monitoring
- Error reporting and monitoring

For visibility into our availability, we publish status, uptime, and incident reports at https://status.pipedrive.com.

DATA STORAGE & RETENTION

Accessibility

Pipedrive's product and processes are designed with the mindset that your data belongs to you. If you ever choose to move to another platform, we will not hold your data hostage. Our convenient export features allow you to generate and download .csv files or Excel spreadsheets of your deals, people, organizations, activities, notes and products, as necessary.

Pipedrive provides secure API access to all customers regardless of the chosen plan. This means that you are free to use the extensive set of endpoints for more complex actions on your data or to extract any and all data elements in your account. You can find our API reference here.

Data retention

Clear data retention rules are an essential part of minimizing the risk of sensitive data being compromised. By default, Pipedrive will keep your data as long as your account is open and for 3 months after it is closed. After that, the data will automatically cycle out of our daily backups within 3 months.

We keep your data to avoid complications if accounts are closed temporarily, due to expired payment methods, or otherwise inadvertently. If you would like us to permanently delete any data in your account, our customer support engineers will do this for you promptly with our purpose-built internal tools.

COMPLIANCE

Sales is a profession that relies on personal information which is subject to various laws and regulations. Compliance with these is a matter of focused efforts by the controllers and processors that handle this data.

Personally Identifiable Information or Personal Data

Pipedrive users store Personally Identifiable Information (a term commonly used in the U.S.) or Personal Data (a term commonly used in the EU) that is relevant to their sales process in our CRM application. The application has a certain amount of default fields like name, email address, phone number and address, which qualify as PII or Personal Data. Users can also create custom fields to save other necessary information.

Pipedrive also stores PII or Personal Data about its users, such as your name and email address to enable logging in and communication with Pipedrive. We also keep various metrics on product and website usage to facilitate improvements. We do not collect health data or other special categories of personal data.

Pipedrive always seeks to comply with national and international regulation or precedent pertaining to a person's rights and ownership over their own data. Moreover, we firmly respect privacy and your ownership of your data. Therefore, per our Terms of Service, Privacy Policy and internal policies, Pipedrive provides data subjects with the ability to request, rectify, or delete their personal information.

COMPLIANCE

GDPR Compliance

Pipedrive's core business is the processing of data on your behalf. As a GDPR compliant data processor we will keep the data entrusted to us safe using appropriate security measures and will always comply with your instructions as the data controller. To document this commitment, we offer our customers a Data Processing Addendum that directly addresses GDPR requirements. The main databases of EU customers are held in Frankfurt, Germany and any non-EU sub-processors that we engage must meet the strict data transfer requirements imposed by the GDPR.

We also believe that exceptional data processors provide added value to data controllers in their compliance efforts. This means that we design app features as well as internal processes to assist you in your compliance needs.

Pipedrive also recognizes its role as the controller of the personal data about its users. All our data handling practices are described in detail in our Privacy Policy and customer support has been trained on addressing all types of data subject access requests.

Pipedrive has also appointed a Data Protection Officer in accordance with the GDPR to oversee its internal processes through a data protection program and act as a liaison in interactions with data subjects and authorities.

AUTHENTICATION

As most security measures hinge on correct authentication of users at the start, it is important to get this step right. Pipedrive offers several options to provide a convenient yet secure way to access your account.

Login Options

Pipedrive is designed to serve companies of various sizes in any industry. This means that we also understand that our customers' needs, internal policies and processes as well as the sensitivity of the data held in their account may vary from one company to another. To meet these expectations, we have taken care to provide several options for user authentication ranging from the traditional password-based login to SAML based Single Sign-On.

PASSWORD

Authentication using only a password is the default option to help you get started quickly. It is important to understand that in this case your account's security depends largely on the complexity of your password. Due to this, we have set 8 characters as the minimum for any passwords used to access Pipedrive accounts. Also, we display a simple password strength indicator to give users immediate feedback when they are setting up their password and suggest ways to improve password security. Any and all credentials stored by Pipedrive are encrypted with 256-bit Advanced Encryption Standard (AES-256).

AUTHENTICATION

TWO-FACTOR AUTHENTICATION

To further protect your account, we recommend using the two-factor authentication feature, which is available under all our plans. When enabled, logging into Pipedrive will prompt an email to be sent to the email address you use to log into Pipedrive, with a verification link that will allow you access to your Pipedrive account. Pipedrive has chosen email-based two-factor authentication because it has been proven to be more secure than SMS-based systems. That same email will provide you with information about where that verifiable login occurred in the world.

GOOGLE ACCOUNT

If you use a Google account for work, you can conveniently sign up and log in through that, saving you from having to remember a separate password for Pipedrive. If you've enabled two-factor authentication, this will be enforced in addition to the Google login.

SINGLE SIGN-ON

If you have a big team, you know the pain of creating multiple new accounts every time someone joins your team. To help you save on-boarding time and overheads, we have developed a SAML 2.0 protocol based Single Sign-On — or "SSO" — in the Advanced, Professional & Enterprise plans of Pipedrive. Setting up SSO requires some technical expertise, so we suggest speaking to your internal IT teams for their assistance in providing the necessary information for the SAML configuration.

DEVICES

On the Professional and Enterprise plans Pipedrive keeps a record of the devices that you normally use to access the app in order to allow us to notify you if a new device is ever used to log in to your account.

ACCESS CONTROLS

Pipedrive offers a variety of security and privacy features to manage access and vital data in the best possible way for your business.

Visibility groups

Limiting users' access to various information serves a dual purpose of ensuring confidentiality where needed and de-cluttering the user interface so users can conveniently see just the information that is relevant for them. To help you achieve this, Pipedrive offers the visibility groups feature that afford you control over which data is visible to particular users. The level of flexibility you have with your visibility groups is dependent on which subscription plan your company account is using in Pipedrive.

Permission sets

When managing a team, there will be occasions when you will want certain users to not perform certain tasks, to reduce the chance of mistakes or duplication of a user's workload. To allow you to categorize your users and dictate what actions they will be allowed access to, Pipedrive offers Permission Sets. This way you have total control over what actions users can perform with the data and which features they can use.

• **The Essential & Advanced plans** have two permission sets — Admin User and Regular User. The Regular User permission set can be customized for specific permissions.
• **The Professional plan** has three permission sets — Admin User, Manager, and Regular User. Both the Manager and Regular User sets are customizable, like above.
• **The Enterprise plan** has further permissions — all of the above, plus additional custom sets. Every permission set is fully customizable (except for Admins, of course, who have all permissions in the account regardless of settings).

AUDIT CAPABILITIES

Users' awareness that there is a way to trace back actions and processes relating to your data encourages adherence to your internal data handling rules and allows you to identify where and why any misstep happened.

Comprehensive and easy-to-read logs

Pipedrive keeps a detailed record of the actions taken within your account. This ensures that you always know what's going on in your account in general and with a particular record specifically. We have taken care to make the logs easy to understand and place them in locations where you would expect to see them.

FULL HISTORY OF CONTACTS AND DEALS

To see the full history of a contact or a deal from the point of creation, you simply navigate to the relevant details page where all the interactions are provided in a convenient feed.

USER ACTIONS LOG

The users' statistics pages have a tab that shows you the recent actions of that specific user within your Pipedrive account. This page is available to admin users by default but access can be shared further to regular users on the Basic and Advanced plans and other groups as well on the Professional and Enterprise plans.

EXPORT LOG

Pipedrive logs all exports of data from your account. Admins can export the contents of your account into convenient .csv or .xls files and may also delegate certain exporting rights to other users. Copies of the export files are kept for 2 weeks so you can check which data was exported.

AUDIT CAPABILITIES

ACCESS LOG

A history of logins with relevant device data is available to to Professional and Enterprise customers on the Settings page in Pipedrive to identify any anomalies and to serve as the starting point for any investigations if an incident occurs.

SECURITY EVENT LOG

For Professional and Enterprise accounts, Pipedrive logs 57 different authentication, permissions, visibility, export and user management events which admins can always review on the Settings page.

SECURITY ASSESSMENT

Administrators on the Professional and Enterprise plans have access to a summary assessment of security-related aspects of the account such as user password strength, adoption of security-enhancing features, and a reminder of permissions that have been granted.