WHITEPAPER

Security and privacy

This document details the security and privacy measures implemented at Pipedrive – both the application and organization – to ensure the safety of the data our customers entrust to us.

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

Last updated September 2023. Content subject to changes

Table of contents

Pipedrive CRM

Technology

Security

Data storage & retention

Compliance

Authentication

Access controls

Audit capabilities

Pipedrive CRM

Pipedrive is a B2B, self-service customer relationship management (CRM) tool designed to help teams manage and improve sales processes.

Certifications

- ✓ SOC 2
- ✓ Privacy Shield
- ✓ SOC 3
- ✓ GDPR Compliant
- ✓ Data Privacy Framework (EU-U.S. DPF)
- ✓ ISO/IEC 27001

Product Offering

You can choose between different plans based on your needs and budget:

ESSENTIAL

Get organized and set up simple sales processes

ADVANCED

Scale quickly with easy-to-use email and automation functions

PROFESSIONAL

Recommended

Everything you need to boost performance and revenue

ENTERPRISE

Customize without limits and access unrivaled support

Technology

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

Cloud infrastructure

In Q4 2023, Pipedrive's production systems are hosted by Rackspace and Amazon Web Services (AWS), 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). These backups constitute a multi-tiered, virtualized architecture comprised of Linux-based application and database servers, storage and content delivery systems and server and application monitoring and logging tools.

By Q2 2024, Pipedrive's production systems and backups will be hosted by Amazon Web Services exclusively.

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

- ✓ **SO 9001, ISO 27001, ISO 27017, ISO 27018**
- ✓ **Data Privacy Framework (EU-U.S. DPF)**
- ✓ **PCI-DSS**
- ✓ **FEDRAMP SOC1, SOC2, SOC3**

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

Technology

Disaster recovery

Pipedrive conducts disaster recovery tests on a quarterly basis. During a disaster recovery test, we simulate destroying our databases and restoring their data from backups. Although the scope of the tests can change, the focus is always on rebuilding a selected region in a dedicated destination zone and restoring the databases. Pipedrive's databases contain all of Pipedrive's data, including customer data.

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.

In addition to the cloud infrastructure providers above, Pipedrive uses the following sub-processors: pipedrive.com/subprocessors.

Security

Pipedrive has a comprehensive information security program with ISO/IEC 27001- and SOC 2-compliant controls and processes.

Third-party certifications and attestations

ISO/IEC27001:2013

Pipedrive undergoes regular ISO/IEC 27001 audits conducted by reputable third-party auditors. Our latest certificate and statement of applicability are freely available here.

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. Contact our sales team for more information about our SOC 2 Type II report.

Data Privacy Framework (EU-U.S. DPF)

Pipedrive's US entity is certified under the Data Privacy Framework (EU-U.S. DPF). Our certification is publicly listed at www.dataprivacyframework.gov.

Security

Preventive security

Automated scanning

Pipedrive uses state-of-the-art automated vulnerability 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.

Deployment checklist

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

Bug bounty program

Pipedrive maintains a private bug bounty program at HackerOne, where experienced security researchers constantly attempt to identify app vulnerabilities and report them. These significant additional resources, paired with Pipedrive’s engineers and controls, ensure a continually high level of application security.

Penetration testing

Pipedrive has regular penetration tests (pentests) carried out by third parties. Pentests are performed annually. If an NDA is signed and a scope and time limit is defined for penetration testing, we allow customers to perform independent pentests. We also require that the results of this test be shared with us.

Security

Incident response

Pipedrive has documented and detailed procedures for handling potential security incidents. 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 incidents by mitigating their impact, investigating the causes and applying corrective measures to prevent similar cases.

Data storage & retention

Pipedrive understands that your data is at the core of our business. As such, ensuring its confidentiality, integrity and availability is crucial to the company's success.

Encryption

Data at rest

Data at rest is encrypted with a 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. Information transmitted over public networks is encrypted with 2048-bit TLS.

Backups and monitoring

Application data is continuously backed up to geographically redundant data centers, ensuring that Pipedrive's services remain available or are easily recoverable if necessary. The company's data centers are spread across the US and Europe.

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

- Database monitoring
- Application monitoring
- Error reporting and monitoring

Data storage & retention

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

Accessibility

Pipedrive's product and processes are designed with data security in mind. If you choose to move to another platform, we will not retain your data. 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 their chosen plan. This means that you are free to use an extensive set of endpoints to conduct more complex actions on your data or extract any and all data elements in your account. You can find our API reference here.

Data retention

Clear data retention rules are integral to minimizing the risk of sensitive data being compromised. By default, Pipedrive keeps customers' data as long as their account is active and for six months after its closing. Free trialists' data is kept for 60 days. After that, data is automatically cycled out of Pipedrive's daily backups within three months.

We keep customers' data after temporary account closing to avoid legal ramifications such as expired payment methods. 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 rules requires focused efforts by the controllers and processors that handle this data.

Personally Identifiable Information or Personal Data

Pipedrive users store Personally Identifiable Information (PII) or Personal Data 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 users' names and email addresses, to enable logins 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 regulations or precedents pertaining to a person's rights and ownership over their own data. Moreover, we firmly respect privacy and your ownership of your data. Therefore, in accordance with 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

Sensitive information

Pipedrive services are not designed or intended for the processing of sensitive data.

Pipedrive services are not designed to comply with industry-specific regulations such as the Health Insurance Portability and Accountability Act (HIPAA) or the Federal Information Security Management Act (FISMA). As such, clients may not use Pipedrive services where their communications would be subject to such laws. In addition, clients may not use Pipedrive services in a way that would violate the Gramm-Leach-Bliley Act (GLBA).

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 and internal processes to assist you in your compliance needs.

Pipedrive also recognizes its responsibility to look after users' personal data. All our data handling practices are described in detail in our Privacy Policy, and our customer support team has been trained to address 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 the 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 and 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's 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 eight characters as the minimum for any passwords used to access Pipedrive accounts. 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 (AES256).

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 in to Pipedrive will prompt an email to be sent to the email address you use to log in to Pipedrive. This email will contain 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.

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 new joins. To help you save onboarding time and overheads, we have developed a SAML 2.0 protocol-based single sign-on, which is available on all Pipedrive plans. Since setting up single sign-on requires some technical expertise, we recommend that you ask your internal IT teams for their assistance in providing the necessary information for the SAML configuration.

Devices

Pipedrive keeps a record of the devices that you regularly use to access the app.
This allows 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 to vital data in the best possible way for your business.

Visibility groups

Limiting users' access to various information serves the dual purpose of ensuring confidentiality where needed and de-cluttering the user interface, allowing users to conveniently see relevant information. To help you achieve this, Pipedrive offers the visibility groups feature that affords you control over which data is visible to particular users. The level of flexibility you have with your visibility groups is dependent on the 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 which actions they will be allowed access to, Pipedrive offers permission sets. These sets give you total control over which actions users can perform with the data and which features they can use.

- **The Essential and 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 admin user and regular user permission sets, plus two additional, custom permission sets. Both the regular sets and custom sets are customizable.

Access controls

- **The Power plan** has admin user and regular user permission sets, plus an additional ten custom permission sets.
- **The Enterprise plan** has further permissions, which include all of the above, plus an unlimited amount of additional custom sets.

Every permission set is fully customizable (except for admins, 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 rule. It also 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, ensuring that you always know what's happening. 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 deal from the point of creation, navigate to the relevant details page, where all the interactions are provided in a convenient feed.

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 two weeks so that you can check which data was exported.

Access log

A history of logins with relevant device data is available for each individual user on all plans. In addition, on the Enterprise plan, you can see a full history of all user logins. This overview lets you identify any anomalies and serves as the starting point for any investigations if an incident occurs.

Audit capabilities

Security event log

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

Note: Customers can’t integrate a security dashboard that allows access to data via any external application.

Security assessment

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