Plandek

Plandek Security

We know how important security is to our customers and that's why we follow security best practices and have strict processes to keep your data safe. We work with the industry leading cybersecurity team at Cure53.de to undertake regular penetration tests and source code audits of our software and infrastructure.

Data Protection

All access to customer services are performed over encrypted connections. We never write data to these services. Our analysis is performed on ephemeral Kubernetes pods and the raw data is purged after running. We store only metadata about your processes, but we never store ticket descriptions, source code, commit messages, pull request descriptions, titles or comments. Plandek only gathers the data which you request.

Protection of your access credentials

All access credentials which we hold are encrypted with Google Key Management Service.

Employee access to customer data

No Plandek employees will access your data unless it is necessary to support the service or to resolve an incident. We also respect the privacy of

our customers, so when it is necessary to access your data in Plandek, we will only view the minimum amount of data necessary to resolve the issue.

We limit the number of employees who have the ability to access customer data or production infrastructure to the minimum necessary to maintain and run the systems. We also require that employees with access to customer data are based in the EEA. All employees are also vetted before employment commences, and all contracts contain confidentiality clauses.

Authentication

Plandek supports authentication via Auth0, either with a username and password or via your own single sign on service. Our authentication system is built using Auth0. You can read more about Auth0's security here: https://auth0.com/security. Plandek supports fine grained role based authentication.

Uptime

The Plandek platform is designed for performance and resilience and our systems maintain over 99% uptime.

Application Security

Our platform is hosted on Google Cloud Platform in Belgium. We follow Google's best practices for configuration and security. Our infrastructure and software is audited and pentested by Cure53 on a regular basis and any issues that are identified are rapidly resolved. To read more about Google Cloud's security see: https://cloud.google.com/security

Only our web application is exposed on the internet, all other resources are firewalled and only accessible via Google Cloud Identity-Aware Proxy or our VPN.

The Plandek web application is only available via HTTPS, protected by TLS.

Data security

Our production database is Elasticsearch hosted by Elastic in Google Cloud Belgium. Elastic have an exemplary security model and we trust their ability to keep your data safe. See more about Elastic's security here: https://www.elastic.co/cloud/security

We store our metadata cache in Google Cloud Storage using customer supplied encryption keys and configuration in Postgres, encrypted at rest.

We never store or transmit data unencrypted.

Backups and Disaster Recovery

Our infrastructure covers multiple availability zones, and our databases are backed up and tested automatically daily.

Employee access

All access to internal systems and tools are only possible through either a VPN or Google Cloud Identity Aware Proxy and all employee devices are encrypted. We also mandate strong passwords and 2FA for employee accounts.

Pentests and Vulnerability scanning

We undertake a white box source code audit and penetration test annually with Cure53. This covers our web applications and backend services and the underlying infrastructure.

We also run automated vulnerability scans to identify risks and weaknesses in our systems on a continuous basis using intruder.io

Incident management

Plandek has a comprehensive and robust incident response plan for handling security incidents, from identification, to rapid mitigation to the post-mortem process.

Reporting an issue

If you believe you have identified a security issue, please contact security@plandek.com and the team will be in touch to learn more about it and work with you to reproduce and resolve the issue.

Any other questions

If you have any other questions or concerns about our approach to security, please get in touch at support@plandek.com and we will be happy to answer any questions.