

Security Policy



This page outlines the security measures and principles our team applies so you can be sure about your data safety. Your private data is safe while using the GrowthDot website and services. Our team takes several steps to ensure your privacy. While our data security measures adhere to legal requirements (such as the General Data Protection Regulation, etc.), they also stem from a moral and ethical obligation to safeguard privacy.

Trusted by the world's biggest brands



Security Levels

Protection at Every Level

Physical Security

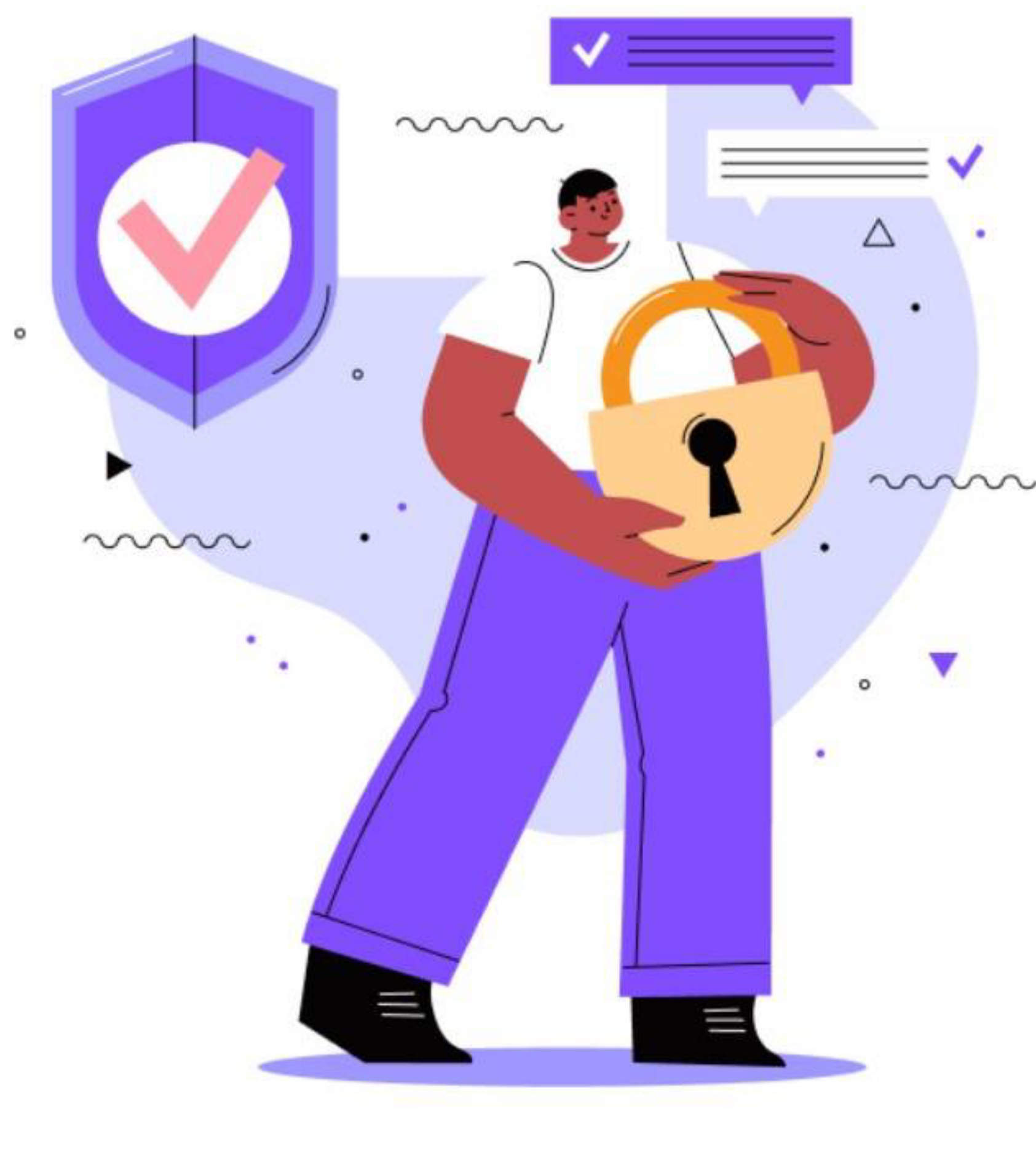
Our data centers are located in Germany and our hosting provider, AWS, takes the highest measures to provide the physical safety of the hardware. For example, only authorized personnel is able to access the data via electronic access control devices with an admission card or transponder key. Data storage parks are preserved from any natural disasters. These data center parks are also under 24/7 surveillance and which works in an autonomous mode using diesel power generators for any emergencies.

Network Security

The GrowthDot security team ensures your private data is protected from any kind of electronic attacks. To achieve this, we apply the best-proven practices across the entire network security infrastructure. Our network security measures include network firewalls, DDoS prevention, and network posture assessment.

Application Security Layer

Our firewalls expose only necessary posts through the Internet and between different online servers. All requests are validated to ensure the security of the application level. Our service transfers data from the visitor's browser to our system via HTTPS. The data being transferred is encrypted by SSL protocol and ciphered.



Data Principles

Your Security, Our Priority

Data Location

All data is stored in Germany on the AWS electronic data center. Only authorized staff can access the data. No external sources are allowed to access the database.

Data Ownership

Your data is exclusively yours, ensuring utmost privacy and control. It is never sold or used beyond what is outlined in our agreement, preserving your rights and confidentiality.

Data Access

Access to data is limited to our employees. Only our authorized tech engineers can access your private data storage to provide the required services to your account.

Data Storage

We maintain data on our premises strictly for the specified duration and under your direct control.

Why do we need specific permissions?

Connecting Your Account Safely

We need these specific permissions to be able to connect to your current account and provide the required services. After establishing the connection, we can access the data needed to provide certain services, and without these access permissions, it is impossible.



Certification and Compliance

Security You Can Trust



ISO/IEC 27001:2013

GrowthDot data centers comply with ISO/IEC 27001:2013 since our hosting provider has achieved this certificate.



Data Privacy Regulations

GrowthDot complies with relevant EU (GDPR) and US (CCPA) data privacy requirements.



AWS

Utilizing AWS infrastructure, GrowthDot adheres to rigorous SOC, PCI DSS, and ISO certifications.



PCI DSS

GrowthDot conducts regular compliance checks to ensure adherence to our rigorous security standards.



PCI DSS

GrowthDot uses 2Checkout and PayPro to accept payments. Both providers are certified PCI Level 1 Service Providers, the most stringent level of certification available in the payment industry. You can verify this by checking 2Checkout's fraud protection policy and PayPro's compliance page.



SLA

GrowthDot establishes Service Level Agreements (SLAs) that articulate the precise service standards, encompassing performance, availability, and support.

Security Measures

Advanced Threat Protection

AWS Infrastructure

Our security posture benefits from the robust features of AWS, including dedicated security groups and firewalls. It is further enhanced by CloudWatch's real-time monitoring and GuardDuty's proactive threat detection, offering unwavering security for your data.

Cloudflare WAF Deployment

We have integrated Cloudflare's Web Application Firewall (WAF) to shield our platform against prevalent web vulnerabilities and evolving threats. This WAF constantly adapts and protects your data from malicious bots and unauthorized access attempts, providing an extra layer of security.

Data Encryption

We adhere to industry-standard encryption protocols to fortify data security within our infrastructure, ensuring robust protection for information stored and processed in our systems. This encryption guarantees comprehensive security measures during storage and processing stages within our controlled environment.

HTTPS Protocols

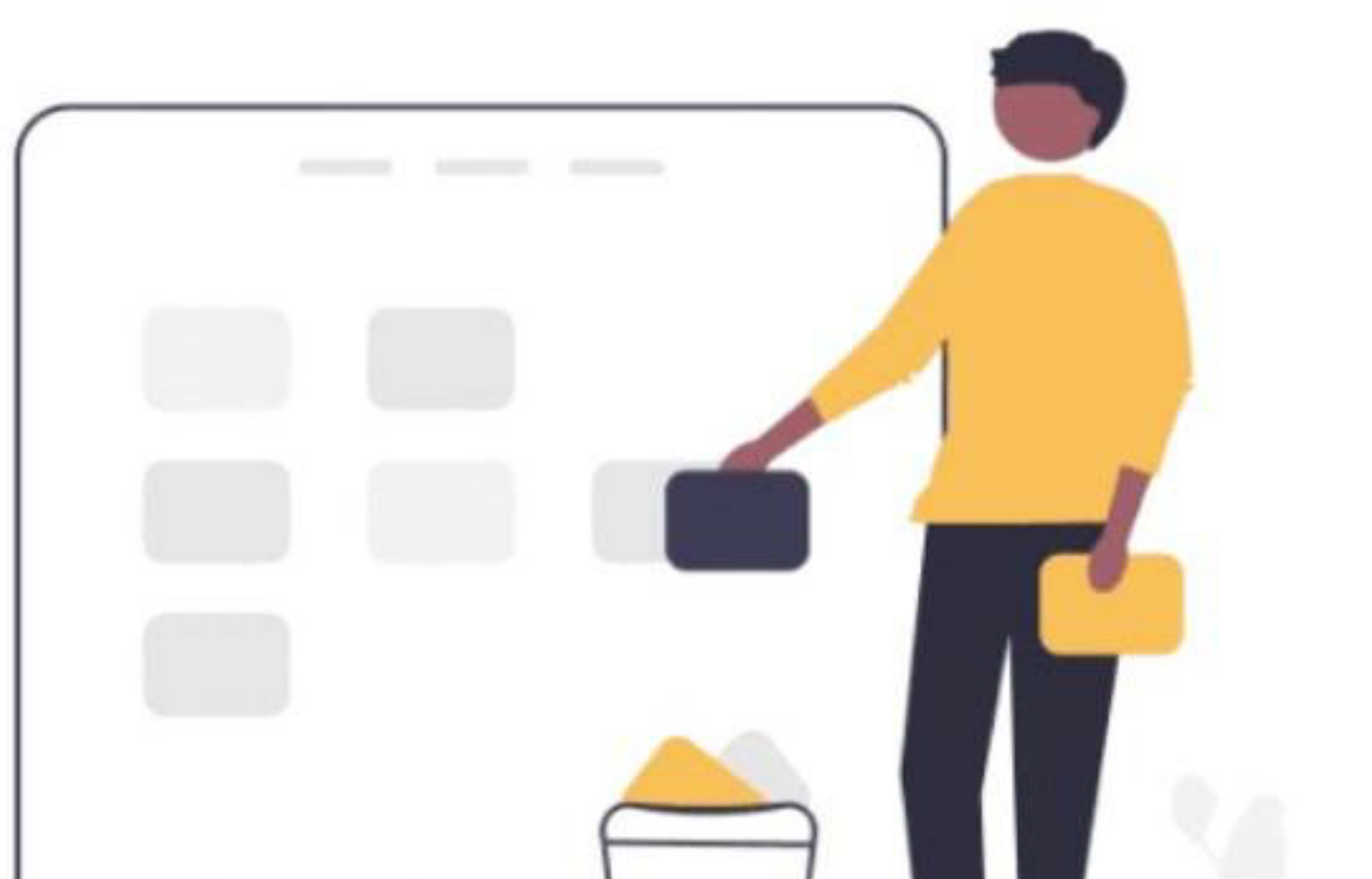
We prioritize secure communication channels by communicating with your platform exclusively through HTTPS connections, safeguarding data integrity, and preventing interception.

Data Deletion

Transparent Data Management

As GDPR and CCPA compliant, we empower our customers to exercise complete control over their data, including the ability to delete it anytime.

Upon a customer's request to delete all private information, we provide a secure deletion certificate as verifiable proof of data erasure. This certificate confirms the complete and irreversible removal of their data in accordance with our security policy and relevant regulations.



Data Storage After App Deletion

After deleting any Growthdot application, your data will be stored for 30 days if you want to return to utilizing our app without losing any important information. Otherwise, after 30 days, all data will be entirely removed from the plugin.

Organizational Protection Measures

Risk Assessments

GrowthDot leverages rigorous annual risk assessments to evaluate our security posture comprehensively. We meticulously analyze critical assets, vulnerabilities, and threat vectors, utilizing penetration testing, code reviews, and vulnerability scans to identify potential security gaps.

Vendor Security Checks

We enforce strict security clauses in vendor contracts, specifying data handling, access controls, and breach procedures. Regular reviews evaluate vendor performance against our standards and agreed security metrics.

Disaster Recovery

Our team has a meticulously crafted plan outlining procedures for every conceivable disaster, from natural events to power outages and cyberattacks. We strategically maintain redundant infrastructure across secure locations, safeguarding data integrity and availability even during localized disruptions.

Security Training & Confidentiality

GrowthDot empowers its team with regular security training, fostering a culture of awareness and responsibility when handling sensitive data. To safeguard confidentiality and comply with regulations, all our employees sign comprehensive non-disclosure agreements, ensuring information entrusted to us remains protected.

MDM Solutions

At GrowthDot, we prioritize comprehensive data security, even on our team's corporate laptops. That's why we utilize leading MDM solutions to safeguard sensitive information on every device. Automated software updates and policy enforcement further strengthen our security posture, minimizing vulnerabilities and ensuring device compliance.

Proactive Vulnerability Detection

Emergency Change Control

Our Emergency Change Control process enables rapid deployment of critical changes while maintaining rigorous security protocols.

Docker Image Scanning

Each Docker image undergoes rigorous security scanning before entering production, ensuring compliance with our internal and external policies.

Access Control & Accountability

Authorization Protocols

Before granting access, we meticulously ensure comprehensive authorization protocols for IT systems and networks.

Password Security Measures

We enforce the use of complex passwords and implement multi-factor authentication across all corporate IT systems and laptops.

Personalized Accounts

Each of our employees is equipped with personalized user accounts, fostering traceability and accountability within production systems.

How to report a security vulnerability?

In case you've noticed any possible security vulnerability in our service, please inform us at (link/email to support). Please, include the following points to help us complete the case investigation:

- Description of the location of the vulnerability and its potential impact;
- A detailed description of the steps required to represent the vulnerability (e.g. screenshots, POC scripts, etc.)