PRDUCT APS | SECURITY

Security overview

Version 1.0 | 10 September 2026 | https://prduct.com/security

A summary of the technical and organisational measures protecting customer data on the Prduct platform. The binding commitments are in the Data Processing Agreement and Schedule 1.

Prduct runs on AWS infrastructure inside the European Union. Traffic is encrypted with TLS 1.2 or higher, stored data with AES-256, and every access is logged. This page sets out which controls are in place today and which are still being built.

Measure	Detail
AWS regions holding customer data: Stockholm and Frankfurt	**2** EU regions
AES key length for data at rest, including backups	**256** bit
Target for notifying you of a personal data breach	**48** hours
Minimum password length on every account	**12** characters

1. Data residency

All customer data is stored and processed in AWS regions inside the European Union. Backups stay in EU availability zones, and no customer data is stored outside the EU.

- AWS regions eu-north-1 (Stockholm) and eu-central-1 (Frankfurt)
- Backup copies held in availability zones separate from the primary data
- An availability zone is one or more physically separate data centres with independent power, networking and connectivity
- Where a sub-processor processes data outside the EU, the EU Standard Contractual Clauses apply, listed in the sub-processor list
- Enterprise customers can agree specific data residency requirements in their enterprise agreement

2. Encryption

Traffic between your browser and the Platform is protected with TLS 1.2 or higher, and older protocols are refused. Stored data, uploaded documents, backups and log files are encrypted with AES-256.

- TLS 1.2 or higher on every connection, with weaker protocols blocked
- AES-256 encryption at rest for the database, file uploads, backups and logs
- Database access runs through an SSH-encrypted jumpbox, on top of standard authentication
- Encrypted storage means that compromised media stays unreadable without the keys

3. Access control

Every user has an individual account, every role is scoped to the data it needs, and administrative access requires two-factor authentication. Organisations can sign in with single sign-on through Microsoft Entra ID using OpenID Connect.

- Single sign-on through Microsoft Entra ID using OpenID Connect
- Two-factor authentication available to every user and required for all administrative access
- Individual accounts only; credentials are never shared
- Minimum 12-character passwords with complexity requirements and automatic session timeouts
- Role-based access control with least privilege, regular access reviews and immediate revocation when people leave
- Inside your workspace you set fine-grained permissions, including exactly what each supplier connection can see

4. Monitoring and logging

Authentication, data access, administrative actions, system errors and API patterns are logged, with continuous threat detection across the infrastructure through AWS GuardDuty and AWS Security Hub. Every file that enters the Platform is scanned for malware.

- AWS GuardDuty for continuous threat detection, with malware scanning of every uploaded file and every email attachment
- AWS Security Hub for centralised security findings
- Continuous monitoring for unauthorised activity, network intrusion detection and DNS query logging
- Audit trails covering logins, data access and modification, administrative actions and API access patterns
- Security patches applied on release, with a monthly review of advisories, IAM policies, security groups and network configuration

5. Backup and recovery

Backups are encrypted to the same standard as production data, held in availability zones separate from the primary data, and restoration procedures are tested. What you are entitled to depends on your subscription tier, as set out in Schedule 1.

Tier	Commitment	Detail
Starter and Plus	Encrypted backups	Regular automated backups held in separate EU availability zones.
Premium	Geo-redundant	Backups replicated across EU regions, in addition to encrypted storage.
Enterprise	365 days	Continuous backups, with recovery guaranteed for data from the preceding 365 days.

6. Compliance

Some of these commitments are ours and some are inherited from the infrastructure we run on. Each card says which.

Standard	Status	Detail
ISO 27001	In progress	Our security controls are built to the ISO 27001:2013/2022 framework. Formal certification is under way; this page carries the current status rather than our contracts.

Standard	Status	Detail
GDPR	In place	A published Data Processing Agreement, documented processing instructions, the EU Standard Contractual Clauses for any transfer outside the EU, and data protection impact assessments.
AWS certifications	Inherited	Our hosting inherits ISO 27001, 27017 and 27018, SOC 1, SOC 2 and SOC 3, PCI DSS and C5 from AWS, whose data centres provide multi-layer physical security.
Sub-processors	Published	Every third party that processes personal data on your behalf is listed with its purpose, processing location and scope, and changes are notified 30 days in advance.

7. Security testing

We would rather be precise about our maturity than imply a testing programme we do not yet run.

In place today

- Continuous vulnerability scanning through AWS Inspector
- Security reviews of infrastructure and applications
- Security code reviews
- Monthly review of security advisories, IAM policies and security groups
- Periodic AWS Security Hub assessment reviews and network configuration audits

Planned

- Annual third-party penetration testing
- Recurring formal vulnerability assessments
- External compliance audits, with reports available to Premium and Enterprise customers on request

8. Shared responsibility

We secure the Platform and the infrastructure it runs on. You decide who inside your organisation, and inside your supply chain, can see what.

What Prduct does

- Host your data in the EU and encrypt it in transit and at rest
- Scan every uploaded file and email attachment for malware
- Log access and monitor the infrastructure continuously
- Patch, review and audit the systems the Platform runs on
- Notify you of a personal data breach, with a 48-hour target
- Give 30 days' notice before a new sub-processor touches your data

What we ask of you

- Turn on two-factor authentication, or connect single sign-on through Entra ID
- Use strong, unique passwords and never share credentials
- Review roles and permissions, and remove leavers promptly
- Configure what each supplier connection is allowed to see
- Train your team and report anything suspicious to security@prduct.com

9. Reporting a security issue

If you believe you have found a vulnerability, write to us. We investigate every report and confirm receipt. Please give us a reasonable period to remediate before disclosing publicly, and do not access, alter or extract other customers' data while testing.

- Vulnerability reports: security@prduct.com
- Data protection and DPO: dpo@prduct.com
- Contracts and legal: legal@prduct.com

10. Questions we are asked

Where is our data stored?

In AWS regions inside the European Union: eu-north-1 (Stockholm) and eu-central-1 (Frankfurt). Backups are held in EU availability zones. No customer data is stored outside the EU.

Are you ISO 27001 certified?

Our controls are built to the ISO 27001 framework and formal certification is in progress. We publish the current status on this page rather than making a claim in our contracts, and we will confirm it in writing on request.

Do you run penetration tests?

We run continuous vulnerability scanning through AWS Inspector, security reviews of our infrastructure and applications, and security code reviews. Annual third-party penetration testing is planned rather than in place, and we say so rather than implying otherwise.

Are uploaded files scanned for malware?

Yes. AWS GuardDuty scans every file that enters the Platform, both documents uploaded by users and attachments that arrive by email, before they are made available in the workspace.

Can we audit you?

Yes. Section 11 of the Data Processing Agreement gives you an annual audit right with 30 days' notice, and more often after a breach or where a regulator requires it. We can also provide third-party certifications and assessments in place of an audit.

Who else processes our data?

Every sub-processor is listed with its purpose, processing location and scope on our sub-processor page. We give at least 30 days' notice before a new sub-processor begins processing, and you may object on data protection grounds.

How quickly are we told about a breach?

Without undue delay, with a target of 48 hours from becoming aware of it. The notification covers the nature of the breach, the categories and approximate number of people affected, the likely consequences and the measures taken.

Do you support single sign-on?

Yes. Single sign-on is available through Microsoft Entra ID using OpenID Connect, and two-factor authentication is available on every account. Contact us to set it up for your organisation.

11. Related documents

- Data Processing Agreement: https://prduct.com/data-processing-agreement
- Sub-processors: https://prduct.com/data-processing-agreement/sub-processors
- Schedule 1, Service Levels: https://prduct.com/service-levels
- Privacy Policy: https://prduct.com/privacy-policy
- All documents and versions: https://prduct.com/legal