



Security and Data Compliance Document

Introduction

This document provides a comprehensive overview of PlannerPal's security measures, data protection policies, and compliance standards. It is designed to assist users in their due diligence and compliance sign-off.

This document is available for download by registered users via the PlannerPal website upon signing up in the Help section or at the footer of the website. For further questions, please contact us at team@plannerpal.co.uk.

General Security and Data Compliance Information

1. Who is responsible for PlannerPal's information security and data protection obligations?

Shoomon Perry, Co-Founder/CPTO. Contact details: shoomon@plannerpal.co.uk.

2. Is PlannerPal registered under the Data Protection Act with the Information Commissioner's Office (ICO)?

Yes, PlannerPal is registered with the ICO. Registration number: ZB533595.

3. Is PlannerPal certified under any security-related standards or codes?

Yes, PlannerPal is accredited under Cyber Essentials certification (achieved in March 2023 and renewed until March 2026). The ISO 27001 certification process is in progress, with target completion later in the year.

Security Policies and Measures

1. Does PlannerPal have a security policy in place for handling personal data?

Yes, PlannerPal has a comprehensive [Privacy Policy](#) available which can be viewed once signed into your PlannerPal account on the website footer.

2. What computer operating system measures are in place to protect data?

- Data is encrypted in transit and at rest, securely stored on AWS servers in the UK.



- Authentication is managed through AWS Cognito, adhering to the Principle of Least Privilege.
- Multi-factor authentication (MFA) is used for user logins, with the option of biometric authentication for mobile access.
- Account policies include complexity requirements and expiration policies, and session time-outs are enforced to prevent unauthorized access.

3. What measures are in place to prevent unauthorized access to data from outside hackers?

- PlannerPal uses industry-standard firewalls and intrusion detection systems to prevent unauthorized access.
 - Employees can only access PlannerPal data via password and authentication codes using an authentication app.
 - Devices adhere to Cyber Essentials accreditation standards.
 - Security audits and continuous monitoring of system activity ensure compliance and protection.
-

Employee Screening and Training

1. How does PlannerPal ensure the trustworthiness of employees with access to data?

- All employees undergo a rigorous screening process before being granted access to data.

2. Are staff informed of their responsibilities in keeping data secure?

- Yes, all staff receive regular training sessions on security responsibilities.
 - Employees are required to sign confidentiality agreements as part of their employment contracts.
-

Data Processing and Transfer

1. Which countries does PlannerPal process data in?

Data is processed in the UK, Ireland, Sweden, and Germany.

2. Will data ever be processed or transferred to countries outside the UK?

Yes, data is processed by third-party providers such as:

- AssemblyAI (Ireland) – Transcription services



- Microsoft Azure OpenAI (UK, Sweden, and Germany) – AI functionalities
- AWS Bedrock (UK, France, and Germany) – AI functionalities

All data processing locations operate within the European Economic Area (EEA) or the UK, ensuring compliance with GDPR and UK data protection laws. Standard Contractual Clauses (SCCs) are in place where necessary to maintain regulatory compliance.

- 3. Can PlannerPal ensure the rights and freedoms of data subjects are protected?**
Yes, through GDPR compliance at all processing locations, encryption protocols, and robust security measures.

Data Deletion and Retention

1. What are PlannerPal's data deletion and retention timescales?

- Data is retained based on legal and business requirements.
- Users can request data deletion via support channels.
- End-of-life destruction involves secure methods, including multiple overwrites and cryptographic techniques.

3. What is PlannerPal's process for securely deleting user data upon request or account termination?

- Upon request, data is permanently erased using secure deletion methods compliant with GDPR and industry best practices.
- This includes multiple overwrites and cryptographic deletion techniques.

Incident Response and Business Continuity

1. Does PlannerPal have a business continuity plan in place?

Yes, PlannerPal has a business continuity plan, including:

- Regular data backups
- Disaster recovery procedures
- Secure off-site storage

2. How quickly can PlannerPal react to a security vulnerability?

- PlannerPal has immediate measures in place for containment and remediation.
- Response time is minimised to ensure rapid resolution.



3. Does PlannerPal have a disaster recovery plan?

Yes, including regular testing and verification to maintain data integrity and quick recovery from disruptions.

Audit Trails and Monitoring

1. Does PlannerPal have audit trails in place to monitor data access?

Yes, PlannerPal maintains detailed audit trails that log all access and activity. These logs are regularly reviewed to ensure compliance and detect unauthorized access.

Third-Party Assessments

1. Does PlannerPal conduct regular third-party assessments of its data security arrangements?

Yes, PlannerPal conducts annual third-party security assessments covering:

- Data encryption
- Access controls
- Vulnerability management
- Incident response protocols

Any identified security gaps are promptly remediated to maintain the highest level of data protection.

Conclusion

PlannerPal is committed to maintaining the highest standards of data security and compliance. This document provides an overview of our security measures, data protection policies, and compliance standards to assist users in due diligence and compliance sign-off.

For further information, please see PlannerPal's [Subscription Terms](#) or contact us at team@plannerpal.co.uk.