Workbooks

# GDPR Compliance FAQs

## Introduction

Our 'frequently asked questions' are answered in the context of our data protection compliance programme which is at the heart of our approach to data protection. The core elements of the compliance programme are as follows:

- Assessment
- Data Protection Policies
- Training and awareness
- Controls implemented to reduce and monitor risk
- Monitoring Compliance
- Reporting
- Annual Review Process

## Assessment

1. **What does the Workbooks service provide?**

   Workbooks delivers cloud-based CRM and business applications to growing and mid-market organisations.

   Workbooks extends beyond sales, marketing and customer support to include order management and fulfilment, invoicing and supplier management.

   Workbooks joins up the entire organisation around data and processes, promoting teamwork and collaboration. It provides a single 360° view of customers and the information is accessible anytime, anywhere.

   The full description of the Workbooks service can be reviewed here.

2. **What personal data is held within a typical Workbooks customer environment?**

   It is the customer as the Data Controller who decides what data is collected and held in the Workbooks customer environment as part of determining the purpose and means of processing the personal data.

3. **What steps have we taken to identify the data processing activities of our organisation?**

   We have undertaken a data inventory and data mapping to determine the following:
   - the types of personal data that are processed;
   - the categories of data subjects whose personal data are processed;
   - why the personal data is processed (in order to determine the lawful basis of processing);
   - how the personal data is processed;

- where the personal data is processed or stored geographically;
- third parties to whom personal data is sent to or shared with;
- how long the personal data is retained for; and
- identified the safeguards in place to protect the personal data.

As a result of the above undertaking we have reviewed and updated our records of processing activities, data protection procedures, documentation and privacy notices.

4. **Do we have a designated Data Protection Officer?**

Workbooks does not currently meet the mandatory criteria for appointing a DPO under the GDPR. In accordance with the GDPR we have carried out an assessment taking into account the relevant factors as to whether we should appoint a DPO on a voluntary basis.

We have concluded that at this time Workbooks processing activities does not warrant the voluntary appointment of a DPO, but fully recognise that these will change over time and therefore subject to continuous reassessment.

To contact the team that carries out the data protection functions and ensures compliance of the organisation with data protection regulations contact datarequest@workbooks.com.

## Data Protection Policies

5. **Does Workbooks have updated Service Terms in place to reflect its processing obligations under GDPR?**

We have updated our Terms of Service to reflect the new legal requirements. These are available here.

Rather than a single Terms of Service covering all solutions, we have a Master Services Agreement, which includes three different services terms:

- Workbooks CRM Service (including the Business Edition)
- Workbooks Marketing Automation Service
- Consulting Services (including training)

You will find the details of the service specific terms in the Master Services Agreement. The Master Services Agreement does not materially change the terms and conditions, but it does ensure that Workbooks meets its obligations under GDPR.

6. **What data protection policies do we have in place?**

   We have the following policies in place to support our data protection compliance program:

   - Data protection policy (Schedule 1 of the Master Services Agreement)
   - Privacy Notice
   - Information security policy
   - Cookie Policy
   - Sub-processors and Sub-contractors
   - Fair usage policy

   These policies can be accessed here.

7. **Where is data physically stored?**

   The Workbooks service data is stored in the UK.

   Details of our sub-processors are set out in our Sub-processors and Sub-contractors Policy.

8. **Who do we share data with, on what basis and where is it geographically located?**

   This will vary depending on the service that Workbooks is providing to the customer. We require organisations that we share data with to satisfy equivalent obligations as those required by Workbooks. This is set out in our Sub-processors and Sub-contractors Policy.

9. **How do we protect the data from unauthorised access or modification?**

   The way we do this is set out in the Data Processing Addendum of the Master Services Agreement.

10. **How will we communicate any changes to Service Terms, policies etc.?**

    This is covered in clause 19.4 of the Master Services Agreement.

**11. Do we test software using personal data?**

We don't use personal data for development or test, but it is used on beta testing to enable customers to test the system for themselves, using their own data, prior to a new release.

**12. How does indemnity work in relation to data breaches?**

This is covered within clause 11 of the Master Service Agreement.

**13. How do we demonstrate compliance with the GDPR?**

Our data protection compliance programme is at the heart of our approach to data protection. At the core of the compliance program is our implementation of ISO 27001:2013 supported by robust policies which are available for review here.

**14. Do we have an Information Security Policy?**

Yes we do. This policy is accessible here.

**15. Please provide a copy of your ISO 27001 certificate**

Our ISO 27001 certificate is available here.

**16. Do our employment contracts require employees to comply with our data protection policies?**

Our employment contracts recognise that employees will have access to personal and sensitive personal customer data and they agree to comply with our Data Protection Policy at all times.

**17. How do we deal with Information Security incidents?**

We have information security incident management process within ISO 27001:2013.

## Training & Awareness

**18. What training do we undertake as part of our data compliance program?**

All staff receive information security awareness training on joining the company, refresher training throughout the year and role-specific information security training. We maintain records of all such training. We also vet all new employees using a third-party organisation.

**19. Have any staff undertaken GDPR specific training?**

Key members of staff have undertaken certified GDPR training at Foundation and Practitioner level. We give additional training in relation to the policies associated with protecting personal data, as well as non-compliance with the information security management system, breach and incident management. Employees are reminded that their contractual Confidentiality obligations remain in force post leaving the company.

**20. What training is done by Workbooks sub-processors?**

Workbooks requires its sub-processors to satisfy equivalent obligations which include providing regular training in security and data protection to personnel whom they grant access to personal data.

## Controls Implemented to Reduce & Monitor Risk

**21. What information does Workbooks process?**

We only process information under the strict instruction of the customer which are set out in a written contract as required under the GDPR.

**22. How do we assist the controller in demonstrating compliance with the GDPR?**

There is a requirement for us to assist the controller in demonstrating compliance (e.g. assisting in responding to subject access requests and permitting audits by the controller or its third-party auditors).

**23. How would Workbooks as a processor deal with a Subject Access Request?**

If the Data Subject clearly identifies the data controller in their request, we would promptly refer it to them upon receipt of the request.

If the Data Subject does clearly identify the data controller then we are limited to checking our own database and the search would be restricted e.g. employees of the data controller, third parties or parties to the Service Contract you have with us and therefore be Workbooks data subjects.

We would not check all customer databases for existence of that data subject.

**24. Would Workbooks provide us with the information to meet the Subject Access Request timeframes under the GDPR?**

There are tools in Workbooks for the customer to manage these requests themselves. We do not undertake fulfilment of Subject Access Requests on your behalf.

**25. How would the rights of the data subject be administered in the Workbook environment? Such as Right to be Forgotten, Right to Access, Right to Data Portability, Right to Rectification etc**

There are tools in Workbooks for the customer to manage these requests. We do not undertake fulfilment of 'Right to be Forgotten' on your behalf.

**26. What controls are in place to manage data encryption and access?**

Data is encrypted at rest, in addition to which data is spread across many disks which are held in secure data centres.

**27. Is Customer data kept segregated from data belonging to other customers?**

Data is held in separate databases and the credentials to access those databases are separate for each customer.

**28. What mechanisms are in place to prevent this segregation from being compromised by an authorised user?**

All security sensitive configuration can only be changed by users with the appropriate capabilities. These are carefully managed and only granted to the small set of users that need them. The segregation is fundamental to the platform and it is not possible to share one end-user customer's database with another end-user customer.

**29. How does access control work?**

Multiple levels of authorisation exist to permit access to data, including user and group row-level security, and database access controls utilising a unique per-database access token.

**30. How is the data protected from disclosure to unauthorised parties during transmission?**

All data transfer happens over encrypted links (HTTPS etc.) utilising strong cryptographic algorithms.

**31. How does Workbooks manage backups?**

Backups of a database in one production site are automatically made in both that site and the other production site.

A weekly backup is taken plus a journal of all changes since that backup; this occurs in two locations and a restore of this data to a separate test system is done on a weekly basis. Each database is maintained in the second location through the replay of that journal and continuous integrity checks confirm that the two copies are identical.

Backups are secured behind several layers of access controls and encrypted at rest.

**32. How does Workbooks implement firewalls (between the public internet and the hosting server(s) and network)?**

In addition to perimeter firewalls we have multiple firewalls within the service and a layered architecture.

We restrict outbound traffic as well as inbound. We automatically parse logs for intrusion attempts.

Firewall changes are managed by a formal change management process.

**33. Can we (or one of our nominated security individuals) review the firewall rules and request changes to the configuration?**

No. This is sensitive information.

**34. Do we run any network intrusion detection systems?**

No. The set of externally-accessible ports and services is tightly restricted, as is the set of internally-usable ports and services. We automatically parse logs on our service hosts; these logs include firewall log output.

**35. Do we run any host-based intrusion detection systems?**

No. We automatically parse logs on our service hosts; these logs include firewall log output.

Critical file integrity is checked automatically including the monitoring of update timestamps.

**36. Does Workbooks undertake our own vulnerability scanning including application vulnerability scanning?**

We implement our own tools including a variety of source code scanning tools focussed on issues such as SQL injection vulnerabilities.

**37. Does Workbooks provide a managed AV (antivirus, antimalware etc) solution for all hosting servers?**

No. Workbooks does not provide a general hosting service; it is a specific application service.

**38. How does Workbooks carry out penetration testing against the servers, applications, and perimeter hardware?**

Workbooks contracts with a leading penetration testing company to carry out such checks on an annual basis.

**39. Does Workbooks permit penetration testing against the servers, applications and perimeter hardware.**

Workbooks contracts with a leading penetration testing company to carry out such checks on an annual basis. We do not allow customers to do this themselves.

**40. What access controls are in place at the datacentre?**

Access to Workbooks hardware is restricted to a small number of operations engineers and access requires pre-booking, biometric checks, multiple doors with key cards, and is monitored using CCTV.

**41. What technical certifications does the hosting company hold?**

As of the time of writing, our hosting company has the following certifications:

- SOC 1 Type II
- SOC 2 Type II
- ISO 27001
- PCI DSS
- ISO 45001
- ISO 9001:2015
- ISO 22301
- ISO 14001
- ISO 50001

**42. How does patch management work?**

Critical patches are installed very rapidly, often within a few hours. In order to minimise impact on service availability and integrity other patches are run alongside other system changes with full QA process of the service and deployed at the appropriate time. We have a pre-production environment which is used to validate patches and a series of Confidence and Automated tests which are run on this.

**43. How long do you retain each item of our data for and the justification for the retention period?**

The retention period is the responsibility of the customer based on the type of data that is held within the Workbooks solution. If you terminate your agreement with Workbooks we automatically delete your database(s) after 90 days.

**44. When do you notify us if you become aware of a data protection breach by your company or a sub-contractor?**

The GDPR requires us to notify you 'without undue delay'.

## Monitoring Compliance

**45. What checks are undertaken on sub-processors?**

We ask all suppliers to complete an information security questionnaire in accordance with our supplier management policy.

**46. How do we monitor compliance with GDPR?**

We continually monitor non-conformance with the ISMS in accordance with ISO 27001:2013. Additionally, we receive continual updates on evolving data protection law and guidance from the UK Regulator – the Information Commissioners Office.

## Reporting

**47. How do we report on activities and compliance issues discovered?**

A report is compiled by the privacy team in relation to any data privacy and information security issues such as breaches, complaints, guidance from regulators, and it is circulated to middle, senior & the board of directors for action.

## Annual Review Process

**48. What do we review on an annual basis?**

On an annual basis we review issues of noncompliance over the preceding 12 months, as well as any changes in the law and regulations and the impact on processing also any changes in data processing activities within the organisation such as the introduction of biometric data, mobile apps etc.