kahootz

Secure cloud collaboration, the safest way to work across organisations online

Kahootz & the GDPR

A overview of how Kahootz meets the UK General Data Protection Regulation (UK GDPR)

T: +44 (0)1488 648 468
E: info@kahootz.com
W: kahootz.com

Kahootz,
Gladstone House, Hithercroft Road,
Wallingford, Oxfordshire, OX10 9BT

Contents

1 Introduction 2

2 Basic Principles 2

3 Information Security 3

3.1 Our Security Accreditations 3

3.1.1 ISO27001 3

3.1.2 Cyber Essentials+ 3

3.1.3 3.1.3 IT Health Check 4

3.2 Our Information Security Policy 4

3.2.1 Incidents and Weaknesses 4

3.3 Our Employees 4

3.4 Access to Your Data 5

3.5 Security Review and Audit 5

3.6 Data Destruction 6

4 Data Protection in General 7

4.1 Data Protection Officer 7

4.2 Data Processor Agreements 7

4.3 Sub-Contractors 7

4.3.1 Amazon Web Services (AWS) 7

4.4 Data Processing Instructions 7

4.5 Data Breaches 8

4.6 Site Terms & Conditions and Privacy Policy 8

1 Introduction

Kahootz has been supplying cloud services to the UK public sector and private enterprises since 2002. We are absolutely committed to keeping your data secure, providing a well-supported, highly-available service and of course complying with applicable legislation.

Kahootz is provided as a software-as-a-service (SaaS), also known as a 'cloud service'. There isn't really the concept of a SaaS being GDPR compliant – it's all about the organisations that provide and consume the service and the rights of the people that use the service. This document is about how Kahootz – the organisation – is compliant with the GDPR.

If you need any more information, please contact the support desk – support@kahootz.com – and we will help where we can.

For the avoidance of doubt: Kahootz is a trading name of KAHOOTZ LIMITED and our registered company number is 04228932.

2 Basic Principles

With respect to the Kahootz service:

You (the Kahootz client) are the **Data Controller**:

> the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

You are responsible for (and must be able to demonstrate compliance with) the principles relating to processing of personal data. These are: lawfulness, fairness and transparency, data minimization, accuracy, storage limitation and integrity, and confidentiality of personal data.

We (Kahootz) are the **Data Processor**:

> a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

We must guarantee to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of GDPR and ensure the protection of the rights of the data subject.

3 Information Security

3.1 Our Security Accreditations

Kahootz has several security accreditations, which are independently audited to demonstrate that our organisation and service are secure:

- ISO27001 – the internationally recognised security standard
- Cyber Essentials+
- An annual IT Health Check to CHECK standards
- BS7858 for staff vetting

We have a separate publicly available document that describes the security measures we take. It's called "How Kahootz meets the 14 Cloud Security Principles".

3.1.1 ISO27001

Kahootz has been certified to ISO27001 since December 2012 and we have been audited annually since then. Importantly, our ISO27001 is UKAS accredited.

We have an excellent audit record to demonstrate that our security policies and procedures are robust and that we follow them precisely. This includes zero failures, zero recommendations and zero observations.

The scope of our ISO27001 certification was agreed with a CESG pan-Government Accreditor. It specifically covers the operation and support of our services and information assets such as client data.

We have a very complete control set: we have only opted out of 3 Annex A controls (because they are not applicable to us) and have added 2 additional controls.

We are happy to provide a copy of our latest accreditation certificate.

3.1.2 Cyber Essentials+

Kahootz has been accredited to Cyber Essentials+ (CE+) since October 2017.

The CE+ scheme is an independent audit to show that we have good policies and procedures in place to prevent attacks against our own office IT systems. It involves a penetration test of our office infrastructure as well as on-site testing of office IT equipment.

A mandatory test for CE+ is that all IT equipment is up-to-date with operating system and software patches.

It's an important link in our service security because it demonstrates that our office IT systems cannot be used as an easy way to access Kahootz.

We are happy to provide a copy of our latest accreditation certificate.

3.1.3 IT Health Check

The IT Health Check (ITHC) is an exhaustive and rigorous test, undertaken by security experts, to ensure that the service is secure against a determined hacker.

The ITHC tests that our service infrastructure and code are both secure, using a combination of automated and manual testing.

Our ITHC is done to CHECK standards and was scoped by a pan-Government accreditor within CESG. Amongst other things it checks that:

- The service authentication is robust
- The service is secure against attacks such as Cross-Site Scripting, Cross-Site-Request-Forgery, SQL Injection, Click-Jacking, and Frame-Embedding
- There service does not exhibit Sensitive Data Exposure or any security misconfiguration

We can share the residual risk register from our ITHC on request, under a non-disclosure agreement.

3.2 Our Information Security Policy

As part of our ISO27001 accreditation, we have detailed documented information security policies and procedures.

We do not make our security policies and procedures available outside the organisation, but if you are interested in a specific policy, we might be able to share this with you, under a non-disclosure agreement.

Within our Information Security Policy is an obligation to proactively follow applicable legislation and that of course includes Data Protection.

Our Information Security Policy is reviewed annually, and our data protection policy is reviewed every two years, or sooner if there is a trigger to do so, such as a change in legislation or a security incident.

3.2.1 Incidents and Weaknesses

Our Information Security Policy contains a detailed Incident management procedure. All security incidents and security vulnerabilities are logged. We identify a short-term solution, a long-term solution and adjust our security procedures to ensure that a similar incident cannot happen again.

We regularly review our security incidents to see if anything could be done better and adopt a cycle of continuous improvement.

3.3 Our Employees

All employees are vetted to BS7858 standard and are contractually obliged to comply with our Information Security Policy and our Data Protection policies.

All staff are trained annually on our Information Security Policy and Data Protection, and this is recorded in our ISO27001 logs.

We have detailed procedures to manage new and departing staff, to ensure that appropriate access to information is granted and revoked.

All staff have a confidentiality clause in their contract which obliges them not to disclose our and your confidential information.

We have a detailed staff handbook which contains a documented disciplinary procedure to deal with staff issues, including security breaches.

3.4 Access to Your Data

Our Information Security Policy contains a detailed access control policy. Client data is given an information classification of “Confidential” and the highest possible risk assessment scores for confidentiality, integrity and availability. This means:

- We keep it secret from anyone who does not have an absolute requirement to access it.
- We take appropriate measures to keep the information safe.
- We take appropriate measures to keep the information available to those that need it – primarily our clients.

Our access control policy together the access rights of individual staff are reviewed annually.

The only staff members at Kahootz who can access client data are those in the operational and technical support team, and they may only do so to deliver the service that we are contracted to deliver.

Your data is only stored in our Data Centre and not within the Kahootz offices. If your data leaves our Data Centre, it’s only in response to a request by you, and we have a documented procedure to ensure the security of the data in transit.

3.5 Security Review and Audit

The Kahootz service keeps an audit trail of user actions within the service. In particular:

- Failed login attempts by users
- The actions and logins of our admin users

These are periodically reviewed.

3.6 Data Destruction

Your data will be deleted from our servers 1 month after the end of your license to use Kahootz expires, or sooner on demand. It can take up to 1 additional month for your data to be removed from our backups.

Apart from end-of-contract, we do not apply our own data retention policies to your data.

Our Information Security Policy contains detailed procedures to ensure that end-of-life media is disposed of securely. We keep a record of all media and media disposals.

4 Data Protection in General

4.1 Data Protection Officer

Kahootz has a board-level Data Protection officer who has overall responsibility for both security and data protection and ensuring that any updates are communicated effectively to staff.

We are registered under the UK Data Protection Act (registration reference: Z8289153).

4.2 Data Processor Agreements

We have a standard data processor agreement which we deem you have accepted by continued use of the service. The data processor agreement has obligations for both parties and, like most organisation's agreements, ours is mostly a restatement of the GDPR.

4.3 Sub-Contractors

To deliver our service, Kahootz uses Amazon Web Services (AWS) as our primary infrastructure provider.

Assessing sub-contractor security and performance is a key requirement of our ISO/IEC 27001 Information Security Management System. AWS is GDPR compliant, operates to a high level of security, and maintains a wide range of certifications including ISO/IEC 27001, SOC 1/2/3, PCI-DSS, and CSA STAR.

A data processing agreement is in place with AWS, and we ensure that any additional sub-processors are also GDPR compliant. In order to deliver our service in the most efficient and effective way, we request general consent from our customers to appoint new sub-processors. We will notify customers in advance of any changes.

4.3.1 Amazon Web Services (AWS)

AWS provides the cloud infrastructure on which the Kahootz service runs. This includes compute (EC2, ECS), storage (S3, EFS), databases (RDS), networking (Route 53), and monitoring (CloudWatch).

All data is hosted within AWS UK regions, ensuring compliance with UK data protection laws. AWS staff do not have access to Kahootz application data, and all access to the infrastructure is tightly controlled by Kahootz using AWS Identity and Access Management (IAM).

More information about AWS compliance and security can be found at: https://aws.amazon.com/compliance/

4.4 Data Processing Instructions

Apart from the normal operation of the service, we do not and will not do any processing of your data without your expression written instruction.

We keep a record of any such activities and we will inform the ICO if we are asked to undertake any processing of information that breaches the GDPR.

4.5 Data Breaches

Our servers employ pro-active monitoring to identify any suspicious behaviour that would identify a potential breach. We have a high level of logging and the logs are monitored.

Our Data Protection Policy documents the actions to take after a breach, including forensics and contacts. In particular:

- We will notify you as soon as possible, and within 24 hours of being aware.
- We will notify the ICO and the National Cyber Security Centre if applicable.

Kahootz has never had a data breach to date.

4.6 Site Terms & Conditions and Privacy Policy

Kahootz has a default set of Terms and Conditions and Privacy Policy:

https://signup.kahootz.com/connect.ti/system/text/terms

https://signup.kahootz.com/connect.ti/system/text/privacy

We encourage clients to use their own T&C and Privacy Policy. As the Data Controller, it's you telling your users what you do with their data.