CASHCALC & GDPR FAQS

GENERAL

(1) Is your company aware of its responsibilities under the GDPR and is it ensuring compliance? Please describe what processes you are putting in place to ensure compliance.
Yes. We've undertaken a full review of the company's policies and procedures and adapted our processes accordingly.

(2) Name/ contact details of individual responsible for security/ data protection
Tom Roberts
Compliance Director
info@cashcalc.co.uk

1. SECURITY MEASURES TO PREVENT UNAUTHORISED OR UNLAWFUL PROCESSING

1.1 Is your firm certified under ISO27001 or accredited to any other security related standard/ code?

No, we are not currently certified under ISO27001. Security policies and procedures have been independently assessed and we are currently in the process of acquiring security accreditation via a qualified organisation.

1.2 Are all staff informed of their responsibilities in keeping data secure in accordance with users' requirements? If so, how?

Yes. This forms part of induction training when employees start work with CashCalc. Updates to security procedures, such as the introduction of GDPR is communicated in the form of training sessions with updates made to procedures as necessary.

1.3 Do such employees sign confidentiality undertakings?

Yes. This forms part of our recruitment procedure and is included within the contract employees sign upon commencement of employment with CashCalc.

1.4 How are your systems protected against newly discovered vulnerabilities or threats?

We regularly patch the server infrastructure when updates become available.

1.5 What computer operating measures are in place to protect data?

Passwords of users are hashed and are never stored in plain text, and never visible to CashCalc employees. Our system has an inactivity-timeout of 24 minutes and no “remember me” option. We have also put in place measures so that a user can never see the data contained on another user’s account.

1.6 Where data is held in manual form, is it identified in any way as being confidential data belonging to users?

We aim to keep all documents in electronic format and encrypted. If any documents are in hardcopy format they are securely stored and transferred to electronic form with the hardcopy destroyed as soon as possible.

1.7 Will manual data be kept secure at all times?

Yes.

1.8 Will data only be processed in a secure area? What precautions are taken to ensure that non-authorised personnel cannot access the area / premises in which data is processed?

Yes. Telephone support for users is only ever conducted in the CashCalc head office, which has a multitude of security measures in place to prevent unauthorised access. Computers are individually password protected, administrator CashCalc accounts are password protected and passwords are not auto-saved in any employee's web browser. Our head office is secured via a metal shutter as well as an alarm system, PIN code door entry as well as keyed entry.

1.9 Do you maintain a record of any data protection training provided?

Yes.

1.10 Describe what physical security measures you have in place for unauthorised access to any of your work space (i.e. key fob/ ID card)?

Our head office is secured via a metal shutter as well as an alarm system, PIN code door entry as well as keyed entry.

1.11 What measures do you have in place to prevent staff from installing potentially malicious software?

Staff are prohibited from the use of USB devices from an outside source within the office. Firewalls and anti-virus systems are installed on all devices to prevent the spread of malicious software on the internal network.

1.12 How many members of staff will have access to our data?

Currently we have 20 staff members within a single office with telephone support access

1.13 What measures are in place to prevent unauthorised access to data from outside hackers (e.g. firewalls) and to what extent is the adequacy of current precautions monitored?

Our server is protected by a managed firewall and measures to detect and stop any potential hack attempts. Our website is protected by requiring user authentication to access any client/user data.

1.14 Is there a formal policy on this?

Not at this time- it is currently being reviewed in our implementation of ISO 27001.

1.15 Do you enter into contracts with third parties for the provision of services which may involve intended or accidental access to user data e.g. software maintenance?

Yes, as outlined in our Privacy Policy: https://cashcalc.co.uk/privacy

1.16 If so, do these contracts include conditions requiring confidentiality in respect of data and compliance with the security provision of the Data Protection Act?

Yes, as outlined in our Privacy Policy: https://cashcalc.co.uk/privacy

1.17 How quickly can you react if a security vulnerability is identified in your product / service?

As soon we become aware of a security vulnerability we will act without delay to resolve the issue and suspend the service if necessary.

1.18 What are your timescales and costs for creating, suspending and deleting accounts?

An account can be created by a user with immediate access to a free trial. We can instantly suspend or delete any account without any costs being incurred.

1.19 Is all communication in transit encrypted?

All communication between browsers and our application servers is via SSL. We have an Extended Verification certificate provided by GeoTrust, which uses AES 256 encryption.

1.20 Do you encrypt all data 'at rest'?

Any data that we deem sensitive is encrypted at rest using the AES 256 encryption algorithm.

1.21 Will data be shared across other services you may offer?

No.

1.22 Do you have an Access Control policy (i.e. only certain members of staff can access certain information)?

No.

1.23 To what extent are users' system-use logged and monitored?

Abnormal activity (e.g. account sharing or hacking attempts) is notified daily. If a user has a concern, we can view the user's login and account activity.

1.24 Are failed login attempts recorded and viewed on a regular basis?

Yes, we use a daily notification system to allow us to see if there have been cases of multiple logins to help protect accounts from logins from unknown IP addresses.

1.25 How do you protect information taken offsite?

Data relating to users should never be accessed by CashCalc staff outside of the head office. We keep activity logs of all telephone support logins.

1.26 Do you have a procedure in place to ensure users are notified without delay of a data breach concerning the personal data of users and/ or clients?

Yes, users will be notified within one working day of the discovery of any data breach.

1.27 What back-up systems are in place to prevent loss of data caused by system crashes?

Backups of the database are regularly taken and can be quickly switched across in the event of a database failure. Server images are also regularly taken to provide a quick recovery in the event of a DDoS attack or similar.

2. DATA OWNERSHIP/ RETENTION AND DISPOSAL

2.1 Do you have a Data Retention policy?

We hold the data entered by our subscribers for an indefinite period.

3. LOSS, DESTRUCTION OF, OR DAMAGE TO DATA

3.1 Do you have a business continuity plan in place to deal with any interruptions to data processing/ breach of data protection legislation?

Yes.

4. DEALINGS WITH THE DATA PROTECTION/ INFORMATION COMMISSIONER

4.1 Are you aware whether you have breached the DPA 1998 in the last 3 years and if so was the breach reported to the affected data subjects/Information Commissioner?

No.

5. TRANSFER OF DATA

5.1 Will there be any circumstances in which data may be processed/ transferred to countries outside UK/ EEA?

Yes, for the purposes of email marketing, billing and Google Analytics for statistics and geographic data handling where there is compliance with the EU-US Privacy Shield Frameworks.

5.2 Do you have safeguards in place at each location where data will be processed?

The physical datacentre where data is held by CashCalc is constantly secured by our hosting providers 1&1. Personal data is encrypted at rest using AES-256 and is only shown to authenticated users. When data is input, each webpage is secured via an EV SSL certificate.

6. DATA OWNERSHIP/ RETENTION AND DISPOSAL

6.1 Do you delete data completely if users delete it from the application?

Yes, if requested data is erased from the CashCalc servers, unless we are subject to any legal requirement for us to retain the data.

7. DISPOSAL OF DATA

7.1 Is data removed from all equipment before that equipment is disposed of?

Yes. Any associated applications are removed and wiped by our web development team. Hard drives are removed and correctly disposed of.

7.2 How is data in manual form, disposed of?

Any print-outs are securely shredded by use of an industrial cross-cut shredder.

8. CHANGES TO APPLICATION/ SERVICES

8.1 Approximately, how often do you make upgrades to your application/ services?

Weekly.

8.2 Will these upgrades impact use of your services?

Our upgrades will only enhance usability of CashCalc and security. Any impact this may have on services will be explained and notified accordingly.

8.3 How and when will you notify users about any scheduled maintenance?

As and when required. If it affects the service we provide, you will be provided with advanced notification.

8.4 How easy is it to export data from your service when moving to a new service?

We can provide an export of your data if you request it from us.

8.5 Can users obtain a copy of their data in a usable format?

Yes, upon request.

8.6 What happens to user data if use of CashCalc is discontinued? Do you delete all data immediately and securely?

All data is kept secured in our databases and is deleted on request in accordance with our Terms of Business: https://cashcalc.co.uk/terms

9. LOSS, DESTRUCTION OF, OR DAMAGE TO DATA

9.1 How many copies of data are backed-up?

Two copies are kept in the form of a slave database and a backup to restore that in the event of an emergency.

9.2 How often are back-ups performed?

Daily

9.3 What back- up systems are in place to prevent loss of data caused by events such as fire, flood and burglaries?

Via MySQL hosting. Manual back up to local protected server.

9.4 Is your computer equipment on which data is processed protected from power failure or electrical disturbances?

Yes. All electronic appliances used in our office are subject to annual PAT tests, and all computers are powered by back-up power supplies providing a limited duration of power in the event of a power failure.

9.5 Are all areas in which data is processed suitably protected from damage by fire, flood or similar disasters?

Yes.

9.6 How quickly will you be able to restore data, without alteration, from a back-up if you suffered a major data loss?

During normal working hours this may take approximately one hour.

10. AVAILABILITY

10.1 Do you have sufficient capacity to cope with a high demand from a small number of other users?

Yes.

10.2 Could the actions of other users impact on the quality of your service?

No, we safeguard against all reasonable events and scenarios.

10.3 Can you guarantee that users can access data and services whenever needed?

We aim to provide an uninterrupted service; however, this may be suspended for maintenance as necessary in accordance with our Terms of Business: https://cashcalc.co.uk/terms