The Cashroom Limited (TCR)

Policy name	**Data protection policy**
Policy reference	
Policy owner	David Calder
Policy writer(s)	David Calder, Mike Touhey, Rachel Faris, Stuart Lockhart, Steven O'Day
Policy approver	Chief Operational Officer

Document control sheet

Version no.	Approved by	Date	Key changes	Sections affected
1.1	Mike Touhey	20/11/2018	1st full review Typing errors New Back up policy Changing names to job titles Ensuring consistency between linked sections Matching table of contents and headers	All areas. Specific changes made to; Schedule 2 part 6 (Back up Policy)
1.2	David Calder	16/11/2020	Full Review Changes to Physical security Changes to audit requirements	All areas. Specific changes made to: Schedule 1 part 1.2 (England & Wales office)
1.2	Steven O'Day	06/01/2022	No updates made	
1.3	Steven O'Day	07/02/2023	Admin account controls Backup Policy Change regs reference to UKGDPR	Schedule 2 1.21 Schedule 2 6
1.4	Steven O'Day		Update company name and role titles Internal Policies removed	All areas

Changes Log

Key Changes since last Version

Version no	Change	Reason for Change
1.1	Back up Policy	New back up strategy following change in IT Support Providers
1.2	Physical Security	New office in England & Wales
	Audit	Change to audit strategy
1.3	Backup Policy	Details removed to be included in design documents and disaster recovery plan
1.4	Schedule 1 and 2	Removed internal policies

Contents

DATA PROTECTION POLICY

1. Policy governance

This policy is owned by the Chief Operational Officer.

The policy owner is responsible for ensuring the following:

1.1 That this policy remains up to date.

1.2 That this policy is effectively implemented through appropriate process and procedural development, training and staff communication.

1.3 That any lack of compliance with this policy is appropriately raised and dealt with and that any breaches to the policy, reported by either the business teams or the data compliance team, are addressed and reported, as required.

This policy is designed to make clear to Cashroom's (also referred to as TCR) business teams and their business managers their data protection responsibilities.

1.4 The role of Cashroom's business teams is to ensure they understand their data protection responsibilities and act in accordance with Cashroom's data protection policy and procedures.

1.5 The role of Cashroom's business managers is to ensure the business teams comply with this policy and to report breaches to this policy in accordance with Cashroom breach procedures. This includes ensuring the business teams have appropriate knowledge of and training in their data protection responsibilities and knowledge of and training in how to raise and report breaches.

1.6 The role of Cashroom's data compliance team is to ensure it is carrying out effective monitoring to affirm that the standards laid down in this policy are being adhered to by the business teams and where they are not, to raise them as a matter of urgency with the board and any required regulatory authority.

2. Background

The purpose of this policy is to articulate Cashroom's approach to data protection - providing details of the principles, ethos and approach Cashroom takes to its data protection practices to ensure that it treats its customers and data subjects fairly. It also provides details of how Cashroom monitors its data protection activities to ensure it is meeting the Information Commissioner's Office (ICO) and other related regulatory standards.

The General Data Protection Regulations (GDPR) are enforceable in the UK from 25 May 2018. This was updated to the UK General Data Protection Regulation in January 2021. The GDPR are based on and builds out from the Data Protection Act 1998 (DPA). This policy is based on this legislation.

It is the responsibility of Cashroom's employees to ensure that they are complying with the policy. Managers are responsible for ensuring their teams understand and carry out the terms of the policy. It is also the responsibility of the Data Compliance Team in People Operations to raise and report any breaches to the operation or application of the policy to the Board.

3. Scope

This policy applies to all employees and agents of Cashroom who work with information, in any format, relating to our clients, their clients, our suppliers, our staff or any other partner for whom Cashroom has collected information in the normal course of its business.

4. Purpose

Cashroom is committed to collect, manage and store data on its customers and data subjects in a transparent manner that ensures that data is safe, protected and liable to cause no detriment to customers or data subjects.

Cashroom also understands the importance of designing its products and services in such a way that ensures its customers and data subjects privacy is assured and that they are 'private by default'. The Cashroom also understands the importance of ensuring data subjects and customers have effective access to their data and can easily and simply request their data be amended or erased where incorrect or inappropriately collected, managed or stored.

This data protection policy is written to be compliant with the UK General Data Protection Regulation (UKGDPR). Its purpose is to ensure that there is a usable reference guide to help direct their attitudes and behaviors in relation to the proper collection, management and storage of data as laid out in the DPA and UKGDPR. It builds specifically on the eight data principles listed in the DPA and the subsequent guidance detailed in the UKGDPR.

The outcome that this policy is designed to foster is the safe, transparent and effective collection, management and storage of data to ensure the risk of customer and/or data subject detriment is minimised in all Cashroom's services, products and activities.

5. Policy statement

Cashroom takes collecting, managing and storing personal data in a transparent, safe and effective manner very seriously.

Cashroom wishes to ensure that it is effectively collecting and protecting customer and Data Subject data in a manner that minimises the risk of detriment to those parties.

Cashroom wishes to ensure that its staff have access to this policy and have read and understood its contents and requirements. This is important to Cashroom as it expects all its staff to comply with the policy and its guidelines.

Cashroom is committed to developing effective data protection processes and procedures to enact the ethos and standards contained within this policy.

Cashroom is committed to ensuring that its staff are appropriately informed of and trained in the data protection activities associated with this policy.

Cashroom is committed to identifying, reporting and remediating any significant breaches to this policy to the data compliance team in People Operations, the board and any external regulators as detailed in the guidelines within this policy.

Cashroom will not tolerate a failure to abide by this policy and will take management action against those who fail to follow this policy and its guidelines.

6. Policy standards

Cashroom data protection policy has the following key policy standards.

6.1 Governance.

Cashroom commits to put in place effective governance arrangements to ensure the management of data protection activities. These include:

6.1.1 Discussion of Cashroom data protection activities at Board on a Quarterly basis.

6.1.2 Cashroom has appointed a Data Protection Administrator who has primary responsibility for enforcing this policy.

6.1.3 The development of and approval by the Board of Cashroom's data protection policy and associated processes that comply with the UKGDPR.

6.1.4 The set up and support of a suitable data compliance team to monitor data protection activities and report on compliance with the UKGDPR to the Board and, if necessary, following a significant breach to ICO, affected individuals and other regulated authorities within the timeframe specified within the UKGDPR.

6.2 Training.

Cashroom commits to training staff in the operation of this policy, and their responsibilities under the UKGDPR.

6.3 Data protection impact assessments.

Where there is a possibility that Cashroom will engage in a potentially high risk data processing activity (see UKGDPR guidelines) then Cashroom commits to undertake a data protection impact assessment (DPIA).

6.4 Lawful basis.

Cashroom also commits to reviewing, approving and documenting its 'lawful basis' for collecting data prior to collecting or processing new data sets

6.5 Purpose.

Cashroom commits to only using the data it collects from data subjects for the purpose(s) it was collected. Further consent will be sought if the data is to be used in a different manner

6.6 Rights.

Cashroom commits to respecting the rights of individuals in relation to the protection of their data as detailed in the UKGDPR and including:

6.6.1 **The right to be informed**

Where Cashroom is the Data Controller, when collecting data, it commits to inform individuals of the following:

6.6.1.1 The firm's identity

6.6.1.2 How the firm will use the information

6.6.1.3 The lawful basis under which the data is being collected

6.6.1.4 The duration the data will be retained for

6.6.1.5 The individuals' right to and process for complaining to ICO

6.6.2 **The right of access, rectification, erasure, object**

Cashroom commits to respond to and resolve a subject data requests:

5.6.2.1 within one month of receiving a request. If the requests are complex or numerous we will advise the Data Subject that we will deal with the request within 2 months, and explain why.

5.6.2.2 Without charge, unless the request is manifestly unfounded or excessive

5.6.2.3 Without refusal unless a clear and compelling reason for the refusal can be provided and details of the process for complaining are provided with the refusal.

6.6.3 **The right to restrict processing**

Cashroom commits to restrict the processing of any information within one month of it being acknowledged as necessary to do so by Cashroom

6.6.4 **The right to data portability**

Cashroom commits to provide agreed personal data in a structured commonly used and 'machine readable' form, on request

6.6.5 **Rights in relation to automated decision making and profiling**

Cashroom does not use personal data to make automated decisions or complete individual profiling.

6.7 Consent.

Cashroom commits to ensure that, where consent is the lawful reason for processing, all data is collected with appropriate consent. Specifically that when data is collected the consent obtained is:

6.7.1 Specific and granular in nature

6.7.2 Clearly articulated in plain English

6.7.3 Prominent within the collection process and documentation

6.7.4 Requires the individual giving consent to opt-in

6.7.5 Properly documented and stored

6.7.6 Easily withdrawn

6.7.7 Not gained from children under the age of 16 without the consent of a parent or guardian

6.8 Duration.

Cashroom commits to keeping its data in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed, or for other lawful reasons

6.9 Quality.

Cashroom commits to keep accurate data and will take reasonable steps to ensure that personal data that is inaccurate with regard to the purposes for which it is processed, is erased or rectified within one month of being recognised as such.

6.10 Information security.

Cashroom commits to ensure the appropriate security of the personal data it collects, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by using appropriate technical or organisational measures. Further details of these policies are contained in the Schedules to this policy.

6.11 International data.

Cashroom commits to the guidelines provided in UKGDPR and the DPA with regard to sharing data internationally and recognises that the level of protection afforded by UKGDPR must not be undermined if any personal data is transferred outside of the United Kingdom.

7. Policy controls and processes

7.1. Monitoring structure

7.1.1 It is the responsibility of Cashroom's staff (the first line of defence) to ensure that it is enacting and following the policy guidelines and meeting the policy standards.

7.1.2 It is also the responsibility of the first line of defence to raise and report any breaches to the operation or application of the policy to the DPA (via the Portal or dataprotection@thecashroom.co.uk), and the Board.

7.1.3 To support the first line of defence the DPA (the second line of defence) will carry out additional monitoring activities on both a scheduled and unscheduled basis:

7.1.3.1 The scheduled monitoring will take place every 12 months as detailed in the data protection compliance monitoring plan and will review the first line of defence's records, documents and knowledge of the data protection arrangements.

7.1.3.2 The unscheduled monitoring is likely to be triggered by a specific incident (e.g. a specific breach) and will review and assess compliance with any relevant aspects of the data protection policy or process.

7.2. Reporting procedures

Cashroom takes seriously the reporting of management information in relation to the carrying out of its data protection activities. It is committed to reporting significant breaches of the regulations to ICO within 72 hours after the breach has come to the attention of TCR staff. The standards for reporting data breaches are contained within Cashroom's breach management policy.

Cashroom also acknowledges that on occasions it may also need to inform Data Subjects if they are impacted by a data breach and that Cashroom is committed to ensuring it has the procedures in place to be able to carry this out if required.

Cashroom expects, that in addition to the normal flow of management information (detailing any data related risks and issues) from the business areas handling data that the Cashroom Board will receive a written report from the data compliance team detailing the risks and issues generated by the monitoring it has completed in relation to Cashroom's data protection activities. They will receive that report at least every 6 months.

7.3. Policy communication and training

This data protection policy is stored in the GDPR folder on the company File Share and can be accessed by all employees.

In addition to the initial post-recruitment training provided by the People Operations Team to all staff, Cashroom commits to provide annual refresher training in data protection for all its staff.

The data compliance team will be asked to provide evidence on the quality and coverage of the requisite training as part of its reports to the board.

8. Policy review and update process

Events that will trigger a policy review are detailed below. The DPA will ensure the Data Protection Policy is reviewed, as required.

Standard triggers:

8.1 Calendar-based

If no other trigger results in a policy review then the policy will be reviewed on an annual basis.

8.2 Business change-based

The policy will be reviewed following changes to business strategy or policies that relate to this policy

Emergency triggers:

8.3 Incident-based

The policy will be reviewed as a result of identifying a major issue either during the monitoring process or as the result of an incident or breach that is the outcome of a weakness in the policy

8.4 Ad-hoc Improvement based

The policy will be reviewed as a result of a suggestion for an improvement

8.5 Regulatory-based

The policy will be reviewed as a result of the implementation of new regulation

8.6 Customer sensitivity based

The policy will be reviewed as a result of customer perceptions changing that may require the policy to drive different outcomes or behaviours

DATA PROTECTION SCHEDULE

This Schedule sets out the detail of how Cashroom complies with its obligations. It is divided into 7 parts.

1. **Use of Client Data.** This part describes the data we collect from clients and sets out our reason for processing, explains how we keep the data safe, how long we keep it for, and when we destroy or return that data.
2. **Use of Employee Data.** This part describes the data we collect from Employees and sets out our reason for processing, explains how we keep the data safe, how long we keep it for, and when we destroy or return that data.
3. **Use of Marketing Data.** This part describes the data we collect from contacts and potential clients, and sets out our reason for processing, explains how we keep the data safe, how long we keep it for, and when we destroy or return that data.
4. **Suppliers Data.** This part lists the Data Processors and Sub-processors we use.
5. **Data Protection Impact Assessments.** This part explains how and when we carry out Data Protection Impact Assessments.
6. **Data Breach Management and Reporting.** This part explains our Breach Notification Policy and the management and reporting in data incidents.
7. **Data Protection Compliance Monitoring Policy.** This sets out our internal and external audit process.

PART 1 – USE OF CLIENT DATA

Broadly we gather 2 types of data from our Clients; data about our client's clients, and data about our clients and their business. The data is collected and processed in line with the bases for processing outlined in the UKGDPR. The bases that Cashroom rely on are contract, legal obligation and legitimate interest.

More information can be found in our Client Privacy policy, available on our website.

PART 2 – USE OF EMPLOYEE DATA

The data is collected and processed in line with the bases for processing outlined in the UKGDPR. The bases that Cashroom rely on are contract, consent, legal obligation and legitimate interest. Use of employee data is further set out in our Employee Privacy policy. This is accessible to all staff.

PART 3 – USE OF MARKETING DATA

We collect data as part of our marketing and business development activities. Where consent and legitimate interest have been used as our basis for processing, we have processes in place to ensure continued compliance with UK GDPR and the protections that they grant to data subjects.

PART 4 – USE OF SUBPROCCESSORS

During the course of our business, we share data with a number of suppliers. We do so to allow us to provide a better service to our clients and help us to fulfil our obligations to Employees.

The UKGDPR requires us to ensure that any supplier, who processes personal data on our instructions provides sufficient guarantees that the requirements of the UKGDPR will be met and the rights of data subjects protected. We are also under an obligation to advise Data Controllers, for whom we are Data Processors, of the suppliers who have access to personal data.

We have risk assessed all our suppliers into low, medium and high risk based on the impact a data breach would have. The “guarantees” obtained are greater depending on our risk assessment.

A list of the sub-processors who have access to personal data provided by clients can be requested via the DPAdmin (dataprotection@thecashroom.co.uk).

PART 5 – DATA PROTECTION IMPACT ASSESSMENTS

A Data Protection Impact Assessment (DPIA) is a process to help Cashroom identify and minimise the data protection risk of a project.

We will carry out a DPIA when we

1. Use new technologies
2. Combine, compare or match data from multiple sources
3. Process personal data without providing a privacy notice directly to the individual

We will consider carrying out a DPIA when we are:

1. Evaluating or scoring
2. Automatic decision making with significant effects
3. Processing sensitive data or data of a highly personal nature
4. Processing data on a large scale
5. When using Innovative technologies or organisational solutions
6. In any major project involving the use of personal data
7. Where there is a change to the nature, scope, contexts and purpose of our processing

If we decide not to use a DPIA we will document our reasons

A DPIA will

1. Describe the nature scope context and purpose of the processing
2. Assess necessity, proportionality and compliance measures
3. Identify and assess risks to individuals; and
4. Identify any additional measures to mitigate those risks.

If we complete a DPIA that identifies a high risk, and we cannot take any measures to reduce that risk, we will consult the ICO, and will not carry out the processing until we have done so.

We have trained our staff to recognise when a DPIA is necessary.

Primary responsibility for carrying out a DPIA rests with the project lead and will be overseen by our Data Protection Administrator.

PART 6 – DATA BREACH MANAGEMENT AND REPORTING

The Cashroom is under an obligation to report Personal Data Breaches.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

ALL CASHROOM EMPLOYEES ARE RESPONSIBLE FOR REPORTING DATA BREACHES TO THE DATA PROTECTION ADMINISTRATOR (DPAdmin - dataprotection@thecashroom.co.uk).

The DPAdmin will report the breach to the Chief Operational Officer and initiate an investigation of the breach. If the DPAdmin and the Chief Operational Officer believe that a data breach has occurred, the following process(es) will be implemented.

1. Data Breaches Register

The Cashroom maintains a Data Breaches Register to record all data breaches.

2. Reporting a Data Breach to Data Controllers

Where we are a Data Processor, for example, where we process our client's clients' data, we must report the data breach to the Data Controller (here, our client) immediately. It is then for the Data Controller to decide whether to report the breach to ICO, or to the Data Subjects.

3. Reporting a Data Breach to ICO

Where we are the Data Controller, we are under an obligation to report a data breach to ICO where the data breach is likely to result in a risk of adversely affecting individuals' rights and freedoms. This is a decision for the Chief Operational Officer, and they will make that decision based on all relevant factors.

Where a decision is made not to report a data breach to ICO, the reason for not reporting the breach is recorded in the Data Breaches Register.

A data breach must be reported within 72 hours of becoming aware of the breach. The report must contain

3.1. A description of the nature of the Personal Data breach including the individuals concerned

3.2. The name and details of the Data Protection Administrator

3.3. A description of the key consequences of the personal data breach

3.4. A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including where appropriate the measures taken to mitigate any possible adverse effects.

4. Reporting a Data Breach to Individuals

Where we are the Data Controller, we are under an obligation to report a data breach directly to Data Subjects where the data breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms. This is a decision for the Chief Operational Officer, and they will make that decision based on all relevant factors.

The main reason for informing individuals as quickly as possible is so they can take steps to protect themselves from the effects of a breach.

Where a decision is made not to report a data breach to individuals, the reason for not reporting the breach is recorded in the Data Breaches Register.

A data breach must be reported without undue delay. The report must contain

4.1. A description of the nature of the personal data breach

4.2. The name and details of the Data Protection Administrator

4.3. A description of the key consequences of the personal data breach

4.4. A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including where appropriate the measures taken to mitigate any possible adverse effects.

PART 7 – DATA PROTECTION COMPLIANCE MONITORING

To ensure compliance with our DPP, Cashroom will train its staff in their obligations and monitor compliance.

1. Staff Training

All new staff will receive training on their obligations under the UKGDPR, and under our DPP within 1 month of starting with Cashroom. In addition, all staff will receive yearly update training.

2. Internal Audit

The Data Protection Administrator is responsible for carrying out an internal compliance audit with our DPP every 12 months.

The DPADMIN will report the outcome of that audit to the Board, along with any recommendations on changes and updates to the policy.