EU General Data Protection Regulation Policy

(Cheetah Money 006 - Data Protection Policy)

Effective Date:	**22/12/2017**
Next Review Due Date:	**03/05/2019**

Document Control

Contents

Document Control

Version no.	Date	Details of Change	Updated by	Approved By
V1	22/12/2017	Separated out from Compliance Manual as standalone policy	Fiona Carton	Pat Patterson
V2	3/05/2019	Update for GDPR	Fiona Carton	Valerie Moran

Introduction

Cheetah Money needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

Purpose

This data protection policy ensures the company:

- Complies with data protection law and best practice for data collection
- Protects the data rights of staff, customers and partners
- Is transparent about how it processes and stores individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

The EU General Data Protection Regulation (GDPR) 2018 which comes into force on 25th May 2018, replaces the previous Data Protection Acts 1988. This describes how organisations must collect, process and store personal information including increased rights for data subjects. These rules apply to all methods of data storage whether data is stored electronically, on paper or on other materials. To comply with the law, personal data must be collected and used fairly, stored safely and not disclosed unlawfully.

Policy scope

This policy applies to:

- The head office of Cheetah Money
- All offices of Cheetah Money
- All staff of Cheetah Money
- All contractors, agents, suppliers and others working on behalf of Cheetah Money

It applies to all data that the company holds relating to identifiable individuals. This can include:

- Names of individuals

- Postal addresses
- Email addresses
- Telephone numbers
- Any other sensitive information relating to data subjects

This policy should be read in conjunction with the associated Subject Access Request procedure, the Data Retention and Destruction Policy and the Data Breach Notification procedure.

Data Protection Risks

This policy is to protect Cheetah Money from data security risks, including:

- Breaches of confidentiality if information is given out inappropriately.
- Risk of litigation if data subject suffers loss due to breach of data
- Failing to offer choice or consent, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage if the company suffers any successful hacking of sensitive data.

Roles and Responsibilities under the General Data Protection Regulation

Cheetah Money is a data controller, and in some cases a data processor, under the GDPR. Senior Management and all those in managerial or supervisory roles throughout Cheetah Money are responsible for developing and encouraging secure information handling practices. Responsibilities are set out in individual job descriptions.

Everyone who works for or with Cheetah Money has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

In general terms, staff members should consult with the Data Protection Officer to seek clarification.

These roles have key areas of responsibility:

- The **Board of Directors** is ultimately responsible for ensuring that Cheetah Money meets its legal obligations.
- The **Data Protection Officer (DPO)** is responsible for:
    - Keeping the executive board updated about data protection responsibilities, risks, breaches and issues;
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule and any changes in regulation;
    - Arranging data protection training and advising on the policy; ○ Handling data protection queries from staff and anyone else covered by this policy; ○ Dealing with requests from individuals to see what data Cheetah Money holds about them; ○ Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data;
    - Overall responsibility for the Data Protection across the business.
- The IT **Security Manager** is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
    - Performing regular checks and scans to ensure security hardware and software is functioning properly;
    - Evaluating any third-party services that the company is considering using to store or process data. For instance, cloud computing services.

General Guidelines

- Access to data covered by this policy should only be given to those who need it for their role;
- Data should not be shared informally or externally. When access to confidential information is required, employees can request it from their line managers;
- Cheetah Money will provide training to all employees to help them understand their responsibilities when handling data;
- Employees should keep all data secure, by taking reasonable precautions and following the guidelines below;
- Strong passwords must be used, and they should never be shared;
- Personal data should not be disclosed to unauthorised people, either within the company or externally;
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of;
- Employees should request support from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Cheetah Money's policies and procedures are designed to ensure compliance with the below principles.

1 - Personal data must be processed lawfully, fairly and transparently

The specific information that must be provided to the data subject must, at a minimum, include:

- The identity and the contact details of the controller and, if any, of the controller's representative;
- The contact details of the Data Protection Officer;
- Where possible, the informed consent of the Data Subject will be sought before their data is processed;
- Where it is not possible to seek consent, Cheetah Money will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- The period for which the personal data will be stored;
- The existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- The categories of personal data concerned;
- The recipients or categories of recipients of the personal data, where applicable;
- Where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- Any further information necessary to guarantee fair processing.

2 - Personal data can only be collected for specific, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of Cheetah Moneys GDPR register of processing. The Cheetah Money Privacy Procedure sets out the relevant procedures.

3 - Personal data must be adequate, relevant and limited to what is necessary for processing

- ➢ The Data Protection Officer is responsible for ensuring that Cheetah Money does not collect information that is not strictly necessary for the purpose for which it is obtained.
- ➢ All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the Data Protection Officer.
- ➢ The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive.

4 - Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

- ➢ Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate;
- ➢ The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it;
- ➢ It is also the responsibility of the data subject to ensure that data held by Cheetah Money is accurate and up to date;
- ➢ Cheetah Money should be notified of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Cheetah Money to ensure that any notification regarding change of circumstances is recorded and acted upon;
- ➢ The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors;
- ➢ On at least an annual basis, the Data Protection Officer will review the retention dates of all the personal data processed by Cheetah Money, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Data Retention and Disposal of Data Procedure;
- ➢ The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month as per the Subject Access Request Procedure. This can be extended to a further two months for complex requests. If Cheetah Money decides not to comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy;
- ➢ The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction of the personal data to the third party where this is required.

5 - Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

- ➢ Where personal data is retained beyond the processing date, it will be encrypted in order to protect the identity of the data subject in the event of a data breach;
- ➢ Personal data will be retained in line with the Data Retention Procedure and, once its retention date is passed, it must be securely destroyed as set out in the procedure;
- ➢ The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in Data Retention Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

6 - Personal data must be processed in a manner that ensures the appropriate security

The Data Protection Officer will carry out a risk assessment taking into account all the circumstances of Cheetah Money controlling or processing operations. In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to data subjects if a security breach occurs, the effect of any security breach on Cheetah Money itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the Data Protection Officer will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to Cheetah Money.

When assessing appropriate organisational measures the Data Protection Officer will consider the following:

- The appropriate training levels throughout Cheetah Money
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper-based records;
- Adoption of a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

7 - The controller must be able to demonstrate compliance with the GDPR's other principle, accountability

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements.

The accountability principle requires Cheetah Money to demonstrate that we comply with the principles and states explicitly that this is our responsibility.

Cheetah Money will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

Subject access requests

All individuals who are the subject of personal data held by Cheetah Money are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

Please see the Cheetah Money Subject Access Requests Policy and Procedure for further information on dealing with subject access requests.

International Transfers

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined. Where Cheetah Money transfers personal data to third countries, we ensure that the third party has adequate data protection controls in place in their country. A list of the third parties is available from the DPO.

Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Cheetah Money will disclose requested data. However, we will ensure the request is legitimate, seeking assistance from the board and from the legal team where necessary.

Providing information

Cheetah Money ensures that individuals are aware that their data is being processed, and that they understand:

- How the data is being processed and used
- How to exercise their rights in relation to the processing of their data

Cheetah Money has a Privacy Policy on the website, setting out how data relating to individuals will be used by us.

Compliance With GDPR

As a Data Controller, Cheetah Money ensures that any entity which processes personal data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation. Failure of a Data Processor to manage Cheetah Money's data in a compliant manner will be viewed as a breach of contract and may be pursued through the courts. Failure of Cheetah Money staff to process personal data in compliance with this policy may result in disciplinary proceedings.

Complaints from Data Subjects

Data subjects whom express a wish to lodge a complaint with Cheetah Money Data Protection Officer you are able to do so by emailing ronanfarrelly@cloudpayments.ie the Data Protection Officer for resolution. Please refer to the Cheetah Money Data Protection Complaints Procedure.