Quick Car Credit Ltd
168 Crewe Road
Haslington
CREWE
CW1 5RN
Tel: 01270 501700
Fax: 01270 342717
Email: contact@quickcarcredit.co.uk
Web: www.quickcarcredit.co.uk

Data Protection Policy

REGISTERED OFFICE: 168 CREWE ROAD, HASLINGTON, CREWE, CW15RN

Introduction and Background

The purpose of this Policy is to outline how Quick Car Credit Ltd have established measures to maintain compliance with the EU General Data Protection Regulation (hereinafter referred to as the "GDPR").

Policy Principles

Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date, and that every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition, there is a requirement that "The controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Accountability and Governance

This Policy outlines comprehensive but proportionate governance measures designed to achieve and maintain compliance with the General Data Protection Regulation. These measures have been designed to minimise the risk of breaches and uphold the protection of personal data.

This section on accountability and governance considers:

- Roles and responsibilities – The responsibilities of Board Members, Directors and employees.
- Documentation – the firm's requirements in respect of documenting processing.
- Data protection by design and default – the firm's requirements for Data Protection Impact Assessments.
- Lawful basis for processing – the firm's Policy on determining the basis for processing.
- Security – Security Policy measures designed to protect information confidentiality, integrity and availability.
- Contracts – the measures that should be in place to ensure contractual relationships maintain GDPR compliance.
- Data Breaches – Principles for detecting and responding to data breaches.
- Compliance & Reporting – Principles and responsibilities surrounding compliance and reporting on the outcomes of compliance.
- Training & Awareness – Principles and measures to ensure that employees have knowledge to protect personal data sufficiently.

Roles and Responsibilities

While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. Quick Car Credit Ltd are expected to put into place comprehensive but proportionate governance measures.

Policy requirements:

The firm has defined Rob Hargreaves as the Data Protection Controller.

The Data Protection Controller responsibilities include:

- Informing and advising the firm and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, staff training and conduct including internal audits.
- Acting as the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).
- The Data Protection Controller reports to the Directors on a quarterly basis.
- The Directors responsibility is to provide effective governance over the firm's affairs for the benefit of the shareholders, including its customers, employees, suppliers and communities.
- Employees are obligated to report any breach to the Data Protection Controller as soon as they are aware of it.

Documentation

The GDPR contains explicit provisions about documenting the firm's processing activities. The firm must maintain records on several things such as processing purposes, data sharing and retention. The firm may be required to make the records available to the Information Commissioner Office (the "ICO") on request.

Policy Requirements:

- Where the firm is a controller for personal data, the firm maintains documentation in a manner consistent with Article 30(1) of the GDPR.
- Where the firm is a processor for personal data, the firm maintains documentation in a manner consistent with Article 30(2) of the GDPR.
- If the firm processes special category or criminal conviction and offence data, the firm will document.

- The condition for processing under the Data Protection Bill.
- The lawful basis for processing, and whether the personal data is erased and retained in accordance with the firm Policy.
- The firm conducts regular reviews of the personal data processed and updates documentation accordingly.

Data Protection by Design and Default

Under the GDPR, the firm has a general obligation to implement technical and organisational measures to show that the firm has considered and integrated data protection into processing activities.

Policy Requirements:

The firm carries out a Data Protection Impact Assessment ('DPIA') when:

- Using new technologies where the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
- Large scale processing of special categories of data or personal data relation to criminal convictions or offences. This includes processing a considerable amount of personal data at regional, national or supranational level that affects a large number of individuals and involves a high risk to rights and freedoms e.g based on the sensitivity of the processing activity.
- The decision of whether to conduct a DPIA is supported by a documented risk assessment and is endorsed by the Data Protection Controller.

Lawful basis for Processing

Under the GDPR, there are six available lawful bases for processing. The firm has documented the relevant lawful basis for processing and the purpose of that processing in its Information Asset Register.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever the firm processes personal data:

- Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Policy Requirements

- The lawful basis for processing must be considered and documented in line with the 'Data Audit'.
- With new systems or processes, the firm must determine the lawful basis and purpose of processing before beginning processing (usually as a part of the DPIA).
- The firm's public privacy notice includes the lawful basis for processing as well as the purposes of the processing.
- If the firm is processing special category or criminal offence data, both a lawful basis for processing and a special category condition for processing must be documented in the Data Audit document and DPIA. The firm should document both the lawful basis for processing and the special category condition to demonstrate compliance and accountability.
- The firm obtains the consent of possible candidates to process the application through the website.

Security

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

Policy Requirements:

- The firm has defined and implemented an IT Security Policy and supporting management system to maintain effective and proportionate security.

Contracts

The GDPR requires diligence and clarity in entering into third party relationships. Whether the firm is a processor or controller, there are mandatory requirements relating to the contracts that are in place.

Policy requirements:

- Whenever the firm acts as a controller a written contract must be in place with the processors. Standards to be applied to the contracts have been defined by the Information Commissioner's Office.
- Whenever the firm acts as a processor, the firm must only act on the documented instructions of a controller (as specified in a valid written contract). Standards to be applied to the contracts have been defined and are documented by the Information Commissioner's Office.
- On an annual basis, the Data Protection Controller will review third party relationships to determine the risk posed by processing. This will be documented as a part of a DPIA.
- Based on this assessment, the Data Protection Controller will determine the most appropriate means to validate that contractual obligations in relation to data processing are being adhered to.
- The Data Protection Controller will present this assessment, and the results of compliance visits, to the Directors at least annually.

Data Breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.
The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority. In some cases, organisations will also have to report certain types of data breach to the individuals affected.

Policy Requirements:

- The Data Protection Controller must be notified of all breaches to this Policy as soon as possible.
- TheData Protection Controller must record breaches and work with the information owner to consider the likely impact of the breach.
- Where a breach is considered notifiable to the Information Commissioner, the Data Protection Controller must immediately inform the Directors.
- A notifiable breach has to be reported by the Data Protection Controller to the relevant supervisory authority within 72 hours of the firm becoming aware of it.

The notification must contain:

- The nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned, the categories and approximate number of personal data records concerned, the name and contact details of the data protection or other contact point for more information.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.
- Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the firm will notify those concerned directly.
- The Data Protection Controller must present an analysis of breaches and near misses to the directors at least annually.
- All employees must be trained to recognise and escalate breaches.
- The detailed Data Breach Policy is to be followed when a breach or potential breach occurs.

Compliance and Reporting

Monitoring compliance with the GDPR is a key role of the Data Protection Controller. The Data Protection Controller must also report compliance to the Directors.

Policy Requirements:

- The Data Protection Controller is responsible for developing a compliance monitoring plan for this Policy.
- The compliance monitoring plan should be submitted to the Directors for approval at least annually.
- Progress to deliver the plan, exceptions noted, breaches and near misses and updates on progress to address material deviations from compliance with the Policy must be reported to the Data Protection Controller and to the Directors at least quarterly.

Training & Awareness

Employee awareness of the GDPR, and their role to protect the privacy of data subjects, is core to the firm's compliance program.

Policy Requirements:

- Employees must be trained on the requirements of this Policy at least annually through the annual Compliance Training and the induction training for new joiners.

Individual Rights

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Right to be Informed

The right to be informed encompasses the firm's obligation to provide 'fair processing information' typically through a privacy notice.

Policy requirements:

- The firm maintains a privacy notice and publishes this for all potential customers.

Right of Access

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Under the GDPR, individuals will have the right to obtain:

- Confirmation that their data is being processed.
- Access to their personal data, and other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

Policy requirements:

All requests from subjects for access to their data should be submitted immediately to the Data Protection Controller by submitting the Subject Access Request Form. The Data Protection Controller must log the request and will:

- Consider whether the request is manifestly unfounded or excessive
- Request copies of information held from information owners within the firm
- Review the information to ensure it does not impair the privacy of another data subject
- Consider whether the request warrants a fee (if it requires a significant amount of data)
- Respond to the formal request

A response to the request must be provided without delay and at the latest within one month of receipt. In the event the request is particularly complex or numerous, the period of compliance can be extended by a further two months. If this is the case, the Data Protection Controller must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Performance against the response target of one month must be reported to the Director by the Data Protection Controller at least annually.

Right to Rectification

The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete.

Policy requirements:

Requests for rectification must be treated in the same way as requests for access. The following additional measures will apply:

- If the firm has disclosed the personal data in question to third parties, the Data Protection Controller must inform them of the rectification where possible.
- TheData Protection Controller must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.
- The information owner will be responsible for ensuring the request for rectification is actioned on the information they are responsible for.
- The Data Protection Controller will be responsible for validating whether requests for rectification have been properly addressed.

Right to Erasure

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'.

Individuals have a right to have personal data erased and to prevent processing in specific circumstances. These circumstances include:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.

Policy requirements:

The firm can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- Archiving purposes in the public interest, scientific research, historical research or statistical purposes, or the exercise or defence of legal claims.

Requests for erasure of data should be submitted immediately to the Data Protection Controller and will follow the same principles as for right to access and right to rectification.

If the firm has disclosed the personal data in question to third parties, the Data Protection Controller must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Right to Restrict Processing

Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, the firm is permitted to store the personal data, but not further process it.

The firm is required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, the firm should restrict the processing until the firm has verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the firm considers whether its legitimate grounds override those of the individual.
- When processing is unlawful, the individual opposes erasure and requests restriction instead.
- If the firm no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Policy requirements:

Requests to restrict processing will be submitted to the Data Protection Controller and will follow the same principles as for right to access and right to rectification, with the following additional requirements:

- The Data Protection Controller must inform individuals when the firm decides to lift a restriction on processing.

Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability applies:

- To personal data an individual has provided to a controller;
- Where the processing is based on the individual's consent or for the performance of a contract, and when processing is carried out by automated means.

Policy requirements:

- Requests for data under the right to data portability must be submitted to the Data Protection Controller.
- The Data Protection Controller is responsible for recording these and requesting the information from the information owner(s).
- The Data Protection Controller will also review the data to ensure the privacy of other data subjects is not adversely impacted.
- The Data Protection Controller will provide the personal data in a structured, commonly used and machine-readable form, submitted using a secure transfer mechanism.
- The information will be provided within one month of the formal request.
- Performance against this timescale must be reported by the Data Protection Controller to the Board at least annually.

Right to Object

Individuals have the right to object to:

- Processing for purposes of scientific/historical research and statistics.

Policy requirements:

- Requests that object to processing must be submitted to the Data Protection Controller
- The Data Protection Controller is responsible for recording and assessing these.
- Where instructed by the Data Protection Controller the firm must immediately stop processing the personal data unless there are demonstrable and compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual, or the processing is for the establishment, exercise or defence of legal claims.
- The firm must inform individuals of their right to object "at the point of first communication" and in its privacy notice.

Personal Data Breach

With regard to Personal Data Breach caused by the firm, the firm shall:

- In accordance with GDPR Article 33 and 34, (i) notify the data subject without undue delay in the event of any Personal Data Breach involving Personal Data and (ii) provide reasonable assistance to you when you are required to communicate a Personal Data Breach to a Data Subject.
- Use reasonable efforts to identify the cause of such Personal Data Breach and take those steps as the firm deems reasonably practicable in order to remediate the cause of such Personal Data Breach.
- Provide reasonable assistance and cooperation as requested in the furtherance of any correction or remediation of any Personal Data Breach.

Complaints

In the event that a customer, supplier, business contact or an employee would like to make a complaint about their personal data has been processed by the firm or how their complaint has been handled, they have the right to lodge a complaint directly with the supervisory authority and the firm's Data Protection Controller.

To do so, please contact the Data Protection Controller by email at rob@quickcarcredit.co.uk