PRIVACY NOTICE

This document describes how Capquest ('we, us, our') use and share personal data (also called 'Account data') they receive from you or other sources. This fully replaces all previous Fair Processing Notices.

1. WHO IS CAPQUEST?

Capquest Debt Recovery Limited are registered in England and Wales under company number 03772278 and have our registered office at Belvedere, 12 Booth Street, Manchester, M2 4AW. We are a limited company. We provide debt recovery services to our client(s) through engaging with their borrowers and establishing affordable and sustainable ways to repay their outstanding balances.

Capquest Debt Recovery Limited ("Capquest") is authorised and regulated by the Financial Conduct Authority for certain credit-related regulated activities and is registered on the Financial Services Register under registration number 721513.

Capquest Debt Recovery Limited is part of the Intrum Group, whose registered UK office is at The Omnibus Building, Lesbourne Road, Reigate, Surrey RH2 7JP.

In most instances, Capquest is the Data Controller for your account(s) for instances where we are not controller or the sole controller this will be specified in communications you may receive directly. Capquest is on the ICO's register under the reference number, ZB553871.

2. WHAT DO WE USE PERSONAL DATA FOR?

Customer and Account Information Accuracy

We, Capquest, maintain information, including personal data, for the purposes of managing accounts on behalf of the account owner. This could include activities designed to support:

- Making the utmost effort to ensure our customer and account information is accurate. This involves regular data quality reporting, investigating data inaccuracies and making corrections should they arise;
- Arrears Management;
- Processing statutory documents, including Statements, Notice of Sums in Arrears and Notices of Default.

Tracing and debt recovery

We use data from Credit Reference Agencies (CRAs) and other 3rd party data providers to trace people who are not responding using known contact details.

An example of a tracing activity could be when a customer moves home without informing us of their new address. We may then use the data we obtain from CRAs and other 3rd party data providers to inform our analytics to identify the customer's new address and contact details. We then use our analytics capability to help find missing individuals through updated addresses and contact details.

Credit reporting

We report the status of the accounts we own to the CRAs and any customer confirmed changes to contact details. The CRAs combine this data with that from other lenders to build

a credit profile of an individual which in turn may be used to help inform future lending decisions.

An example would be where a customer settles their account with us. This information would be reported back to the CRAs which may be used by other lenders to assess an individual's creditworthiness.

Statistical analysis, analytics and profiling

We will use and allow the use of personal data for statistical analysis and analytics purposes. Personal data can be used to create scorecards, models and variables in connection with the assessment of credit, fraud, risk or to verify identities. It can also be used to monitor and predict market trends, to allow use for refining recovery and trace strategies, and for analysis such as loss and revenue forecasting.

Database activities

We carry out certain processing activities internally which support databases effectiveness and efficiencies. For example:

- ***Data loading*****:** this is where data is supplied to us and is checked for integrity, validity, consistency, quality and age to help make sure it is fit for purpose. These checks pick up things like irregular dates of birth, names, addresses, account start and default dates, and gaps in status history.
- ***Data matching*****:** this is where data supplied to us is matched to existing databases to help make sure it's assigned to the right person, even when there are discrepancies e.g. spelling mistakes or different versions of a person's name. We use the personal data people give lenders together with data from other sources to create and confirm identities, which they use to underpin the services they provide.
- ***Data linking***: this is where we compile data into its databases and we create links between different pieces of data. For example, people who appear financially associated with each other may be linked together, and addresses where someone has previously lived can be linked to each other and to that person's current address.
- ***Systems and product testing*****:** this is where data is used to help support the development and testing of new products and technologies.

Uses as required by or permitted by law

Your personal data will also be used for other purposes where required by law, such as where we are obliged to provide data to the Law Enforcement and Government Agencies at their request.

3. WHAT ARE OUR LEGAL GROUNDS FOR HANDLING PERSONAL DATA?

We use the following legal grounds for handling personal data:

- Legitimate interests;
- Compliance with a legal obligation;
- Fulfilment of a contract;
- Consent; and
- Vital Interests.

Our primary grounds for handling data are the legitimate interests of our business, supplemented by both the compliance with our legal obligation to manage customers' accounts and fulfil the terms of such contracts.

The UK's data protection laws allow the use of personal data where the organisations legitimate interests aren't outweighed by the interests, fundamental rights or freedoms of data subjects (customers). The UK General Data Protection Regulation (GDPR) calls this the 'Legitimate Interests' condition for personal data processing. The below outlines the activities we undertake in relation to your data, the appropriate legal grounds for processing as well as an explanation of what our legitimate interests are when this is our reason for processing.

Purpose	**Legal Processing Condition**	**Explanation**
Managing your account	· Legitimate interests · Compliance with a legal obligation	We have an obligation to appropriately manage your account in line with any credit agreement, and with respect to our legal and regulatory obligations, such as those required by the Financial Conduct Authority (FCA).
Recovery of funds owed	· Legitimate interests · Compliance with a legal obligation	Our business is primarily the recovery of funds owed by individuals in the consumer credit market. As such, our customers typically have overdue funds that we are seeking to be repaid, either actively or by awaiting a change to customers' personal circumstances. This explicitly requires us to understand our customers and their circumstances in order to conduct ourselves in an appropriate way.
Promoting responsible lending and helping to prevent over-indebtedness	· Legitimate interests	Responsible lending means that lenders only sell products that are affordable and suitable for the borrowers' circumstances. We help to ensure this by sharing personal data about our customers, their circumstances where applicable, and their financial history with the CRAs. A comprehensive range of regulatory and statutory measures exists in the UK to underpin the UK's financial services industry, which helps address the balance of our legitimate interests so that they aren't outweighed by the interests, fundamental rights and freedoms of data subjects. Further explanation about this balance is set out below.
Complying with and supporting compliance with legal and regulatory requirements	· Legitimate interests · Compliance with a legal obligation · Fulfilment of a contract	We must comply with various legal and regulatory requirements and help other organisations comply with their own legal and regulatory obligations. For example, many kinds of financial services are regulated by the FCA or the Prudential Regulation Authority, who impose obligations to check that financial products are suitable for the people they are

		being sold to. The credit reference agencies provide data to help with those checks.
Maintenance of data for use in defending legal actions	· Legitimate interests · Compliance with a legal obligation	We need to be able to investigate and respond to customer claims and to provide appropriate disclosure in the event of proceedings being issued. This requires it to maintain information for a period after its original legitimate purpose has expired. This is subject to the retention of personal information, described below.
Training and Quality	· Legitimate interests · Compliance with a legal obligation	To ensure the good quality of the service we provide, customer data is used while training staff and reviewing the quality and output of ourselves and our partners.
Applying Forbearance and noting customer circumstances (health or other) Sharing critical data with relevant authorities.	. Consent . Vital Interests	We'll look for your consent to process personal information in relation to your health. This will only be in circumstances where you choose to share this information with us to help us understand your circumstances and appropriately manage your account. We seek explicit consent to record sensitive data in order to better process, handle and apply appropriate forbearance to your account. This will be used for no other purposes than managing your account and for training and quality purposes. You may withdraw consent by any means, at any time, effectively erasing our record of this data. In exceptional and very rare circumstances, we will use the lawful basis of vital interests to share your data with a charity or lawful authority in order to safeguard your well-being. This data is not stored but rather shared in the moment in cases of life-threatening situations we need to alert relevant organisations with due haste.

Our use of this personal data is subject to an extensive framework of safeguards that help make sure that people's rights are protected. These include the information given to you about how your personal data (including this privacy notice) will be used and how you can exercise your rights to obtain your personal data, have it corrected or restricted, object to it being processed, and complain if you are dissatisfied. These safeguards help sustain a fair and appropriate balance so that our activities don't override the interests, fundamental rights and freedoms of you, the data subject.

4. WHAT KINDS OF PERSONAL DATA DO WE USE, AND WHERE DO WE GET IT FROM?

We obtain and use information from different sources, so we often hold different information and personal data about each customer. All information we hold about our customers falls into the below categories:

Information Type	Description	Source
Key Customer Identifiers	We hold personal data that can be used to identify people; this includes: · Name, including Title, Forename and Surname. · Address, including current and previous addresses, if these are marked as no longer resident. Additionally, we will hold address confirmed as inaccurate to prevent these being reused. · Contact details, including telephone and email information, past and present. Additionally, we will hold contact details marked as inaccurate to prevent these being reused.	This personal data is included with all the other data sources. For example, names, addresses and dates of birth are attached to financial account data, so it can be matched and associated with all the other data Capquest holds about the relevant person. Data is first obtained from the lender of the debt prior to our acquisition. Data is also provided by customers directly in the daily interactions with ourselves or our agents. Data about UK postal addresses is also obtained from sources like Royal Mail. We also obtain copies of the Edited Electoral Register containing the names and addresses of registered voters from local authorities across the UK in accordance with specific legislation. We also have access to public data sources on people and businesses, including from the Insolvency Service, Companies House and commercial business directories. We also source data from third party sources including our Clients

		and Database providers such as Credit Reference Agencies.
Customer Circumstances	We hold personal data relating to individual's circumstances including mental and physical health, financial status (including hardship) and difficulties relating to communication. The purpose of this information is to ensure all circumstances are taken into account when managing your account(s).	This information will be obtained from: 1. You, the customer, during an interaction directly with Capquest 2. A 3rd party you have authorised to work on your behalf, or 3. You, the customer, directly during an interaction with an agency working on our behalf. We do not actively obtain data from external sources relating to customer circumstances. We will always obtain customer consent before recording information relating to personal circumstances such as health, or communication requirements.
Financial data	We receive information that includes personal data from credit accounts and other financial accounts that people hold with other organisations. This includes data about bank accounts, credit card accounts, mortgage accounts and other agreements that involve credit agreements such as utilities and communications contracts (including mobile and internet). The collected data includes the date the account was opened, the amount of debt outstanding (if any), any credit limits and the repayment history on the account, including late and missing payments. We may also receive data about financial accounts like current	Banks, building societies, lenders and other financial services providers supply data including personal data about people's financial accounts and repayments to CRAs. Other credit providers, such as hire purchase companies, utilities companies, mobile phone networks, retail and mail order, and insurance companies also provide this data when they agree credit facilities with their customers to the CRAs. These are then provided to us with regards to our customers, to assist us in our legitimate purposes.

	accounts, credit cards or loans and may receive payment information that businesses hold from the organisations who maintain other accounts belonging to you. We also use external data services from the CRAs to validate customers' stated income.	
Court judgments, decrees and administration orders	We obtain data about court judgments that have been issued. This may include, for example, the name of the court, the nature of the judgment, how much money was owed, and whether the judgment has been satisfied. Additionally, we may receive information about enforcement taken, such as Charging Orders on properties held by customers.	Judgments and some other decrees and orders are made publicly available through statutory public registers. These are maintained by Registry Trust Limited, which also supplies the data on the registers to the CRAs, and in turn Capquest. Charging Order information may also be provided by the Land Registry.
Bankruptcies, Individual Voluntary Arrangement (IVAs), debt relief orders and similar events	We obtain data about insolvency related events that happen to our customers and may also obtain this type of data about businesses. This includes data about bankruptcies, IVAs and debt relief orders, and in Scotland it includes sequestrations, trust deeds and debt arrangement schemes. This data includes the start and end dates of the relevant insolvency or arrangement.	We obtain this data from our customers, their representative (Insolvency Practitioner), The Insolvency Service, and the CRAs.
Search footprints	We have access to credit application information where a financial institution uses a CRA to make enquiries about a particular person, the CRA keeps a record of that enquiry which appears on the person's credit file. This includes the name of the application, the date, and the reason they gave for making the enquiry. Additionally, it may include such information as contact details,	CRAs generate search footprints when enquiries are made about a particular person by other lenders. The lender making the enquiry provides some of the data in the footprint (such as the reason for the enquiry). We in turn obtain this information from the CRAs.

	address information, income and employment situation of the applicant when they applied for the credit.	
Scores and ratings	We will use the data they receive to produce scores and ratings including potential affordability, risk, fraud and identity checks, screening, collections, litigation and insolvency scores about our customers.	We produce their scores and ratings using the data available to them detailed in this section only. This is sometimes supplemented by CRAs' own scores.
Public interest data	We receive data from commercial sources which includes lists of politically exposed persons (PEPs) and sanctions data; this is to ensure we meet our regulatory requirements in relation to identifying and appropriately managing such individuals.	We receive this data from reputable commercial sources as agreed from time to time.
Other derived data	We produce other kinds of data ourselves to manage our databases efficiently and ensure that all the relevant data about a person is on the correct credit file. **Address links:** when we detect that a person seems to have moved to a different residence, it may create and store a link between the old and new address. **Flags and triggers:** through analysis of other data, we can add indicators to a customer's account file. These aim to summarise particular aspects of a person's financial situation. For example, a Potential Insolvency flag protects those who may be insolvent, and invites additional checks as a defence against further fraud risk.	Capquest generates this data from the data sources available to them.
Criminal Conviction data	Through the course of our operation we may obtain data relating to criminal conduct or historic convictions. This data is only on record for screening activities for financial	Capquest obtains this data via public record, customer disclosure or through acquisition of accounts/communications with Third Party firms.

	crime risks, ensuring we recognise power of attorney (in case of incarceration of account holder), and to recognise any impacts or vulnerability this may have on your account.	

5. SPECIAL CATEGORY DATA

We acknowledge and store Special Category Data which if defined by UK GDPR sensitive data which requires extra protection including but not limited to: 'data revealing ethnic or racial origin, political opinions, biometric data, data concerning health etc.' For more information on types of Special Category please visit the ICO's guidance here.

In other words, this is data which if made public could have adverse impact on a data subject hence the need to ensure extra safeguards.

We only store health data which, as outlined above, is gained through your explicit consent. We recognise that through the course of your interactions with us there may be vital need to inform us of your conditions or circumstances.

We store this data on our systems often tagged on your account, only approved and trained agents and support staff have access to this information.

We recognise that not all data stored under this lawful basis will be considered as 'Special Category' however considering the needs for the data is only in the customer's interest we operate to this high-standard and will process any withdrawals of Consent you may ask for.

In rare circumstances, we will utilise vital interest processing for life-threatening situations to inform emergency services or charities and share your special category data to safeguard your well-being.

6. WHO DO WE SHARE PERSONAL DATA WITH?

This section describes the types of recipients we share data with and our process for ensuring it is an appropriate organisation.

In some cases, some organisations have the ability to compel us, by law, to disclose certain data for certain purposes.

Members of the credit reference agency data sharing network

We share information with CRAs as part of our obligation to ensure appropriate lending for consumers and help ensure the health of the UK financial services industry.

Each organisation that shares financial data with the CRAs is also entitled to receive similar kinds of financial data contributed by other organisations. These organisations are typically banks, building societies, and other lenders, as well as other credit providers like utilities companies and mobile phone networks.

In the UK we use the following CRAs:

Credit reference agency	**Contact details**

TransUnion	**Post:** One Park Lane, Leeds, West Yorkshire, LS3 1EP **Web Address:** https://www.transunion.co.uk **Phone:** 0113 388 4300
Equifax Limited	**Post:** Equifax Ltd, Customer Service Centre PO Box 10036, Leicester, LE3 4FS **Web Address:** https://www.equifax.co.uk **Phone:** 0333 321 4043 or 0800 014 2955
Experian Limited	**Post:** Experian, PO BOX 9000, Nottingham, NG80 7WF **Web Address:** https://www.experian.co.uk **Phone:** 0344 481 0800 or 0800 013 8888

The Credit Reference Agency Information Notice ('CRAIN') describes how the three main credit reference agencies in the UK use and share personal data. The CRAIN is available on the credit reference agencies' websites:

TransUnion: www.transunion.co.uk/crain

Equifax: www.equifax.co.uk/crain

Experian: www.experian.co.uk/legal/crain

Partners

We may entrust your account for management by one of our Partner companies, who will operate as our agent. We use market leading partners, and we rely on their expertise in their fields to manage your account efficiently on our behalf. Our partner network includes Debt Collection Agencies, Legal Firms and Specialist firms (specialising in insolvency or deceased accounts). We will communicate with you at the time should this outsourcing take place.

Information Technology Processors

We will use other organisations to perform tasks on their own behalf (for example, IT service providers, call centre providers, and postal couriers) in order to assist us with running our business. These providers will always act as our agents, should we instruct them to contact you.

Court Service

If proceedings are issued against you or enforcement activity is taken, we will provide information to the relevant Court service.

Payment Processors

If you have chosen to make payments via Debit or Credit Card, we'll provide relevant information to payment processing companies to facilitate the transaction.

Clients

We will share our data with clients who may conduct audits of our activities. These reviews would include personal data which may have originated from the client or is data associated with their historic customer base.

Law enforcement & Emergency Services

At the request of law enforcement (Police, local authority or the Courts) we will supply them with your personal data once proper request and procedure is followed. Furthermore, we reserve the judgement to share your data with emergency services if we have strong reason to believe your life or well-being is at risk. This is covered by our use of vital interests described above.

Individuals

People are entitled to obtain copies of the personal data the Capquest holds about them. You can find out how to do this in Section 11 below.

7. WHERE IS PERSONAL DATA STORED, SENT & SECURED

Where we send the data

As Capquest is part of the Intrum Group, we may transfer your data to another country outside of the UK and European Economic Area (EEA). If we do so, we will ensure there are suitable safeguards in place to comply with GDPR and the Data Protection Act 2018. Generally, your personal data will not be transferred outside of the UK and EEA. However, in cases of international debt collection, your personal data may be transferred to one of our representatives working in the relevant country.

We also use third party service providers to store or who may access your data which may be located outside of the UK and EEA. These transfers are subject to special rules under European and UK data protection law. This means we can only transfer your personal data to a country or international organisation outside the UK/EEA where:

The European Commission has issued an ‘adequacy decision’ in relation to that country or international organisation; or

There are appropriate safeguards in place, together with enforceable rights and effective legal remedies for data subjects; or a specific exception applies under data protection law.

Transfers under an exception

In the absence of an adequacy decision or appropriate safeguards, we may transfer personal information to a third country where an exception applies under relevant data protection law, e.g.:

you have explicitly consented to the proposed transfer after having been informed of the possible risks;

the transfer is necessary for the performance of a contract between us or to take pre-contract measures at your request;

the transfer is necessary for a contract in your interests, between us and another person; or

the transfer is necessary to establish, exercise or defend legal claims

We may also transfer information for the purpose of our compelling legitimate interests, so long as those interests are not overridden by your interests, rights and freedoms. Specific conditions apply to such transfers, and we will provide relevant information if and when we seek to transfer your personal information on this ground.

We may also disclose information to help prevent financial crime, such as fraud or money laundering, or if required to do so by law to a relevant law enforcement agency such as the National Crime Agency or Government agency such as the His Majesty's Revenue & Customs (HRMC).

Where we store the data

We store data on various systems all on servers located within the United Kingdom and the EEA.

How We Protect Your Data

At Capquest, we prioritise the security of your personal data by adhering to key information security principles and implementing a robust Information Security Management Framework (ISMF). Our approach is designed to ensure the confidentiality, integrity, and availability of your data through a comprehensive set of controls aligned with the international standard ISO 27001.

- **Confidentiality:** We implement stringent measures to protect your information from breaches, unauthorised disclosures, loss, or unauthorised viewing
- **Integrity:** We maintain the integrity of your information to ensure it is accurate and unaltered:
- **Availability:** We ensure your data is available when needed, protecting it from disruptions and denial of service attacks.

8. FOR HOW LONG IS PERSONAL DATA RETAINED?

In general, we will retain all information held about our customers for as long as they continue to have an active account with us. This will include for as long as funds are owed to us. This is in line with our legitimate interests (Please see Section 3 – for our lawful basis breakdown) and to fulfil any legal obligations we may have towards other entities.

Once the account is closed and no funds are considered owed, we will continue to retain all data for a period of six years from closure. The criteria used to determine the storage period will include the legal limitation of liability period, agreed contractual provisions, applicable regulatory requirements and industry standards. Additionally, any right to erasures submitted during this period are likely to be rejected as we maintain the exception to enable defence of any complaints submitted to institutions such as the Financial Ombudsman Service (FOS).

Exceptions to this standard six-year approach are detailed below:

Credit Balances

In the rare situations where customers' accounts have some form of overpayment, the data is kept for as long as the account remains in credit and for six years from the date these monies are re-paid to the customer.

Voice Recordings

Voice recordings of telephone conversations with customers will be held for three years after the call has taken place. We store this for training and monitoring purposes on our staff primarily and do not share this information unless Law enforcement request it. Where relevant, personal data including payment details is not recorded as we suspend recording payment information if taken over the phone.

Archived data

We will hold archived data in both physical and digital formats for business continuity purposes. Where data is retained in archives for longer than the periods described above, it will not be accessible to unauthorised staff and in the case of digital backups data is encrypted. We will take steps to ensure that, if such archives are required to be accessed, we will have all personal information no longer required removed.

9. WHAT RIGHTS DO I HAVE UNDER DATA PROTECTION REGULATION?

Right	**Description**	**Section**
Right to be informed	You have the right to be informed about how we collect and use your personal data. This has been described within this Privacy Notice.	All
Rights related to automated decision making	You have rights in relation to any automated decision-making and/or profiling that has legal or similarly significant effects on you.	10
Right of access	You have the right to access your personal data and supplementary information held by us.	11
Right to data portability	In certain circumstances, you have the right to obtain and reuse your personal data for your own purposes across different services.	12
Right of rectification	You have the right to have inaccurate personal data rectified, or updated if it is incomplete.	13
Right to object	You have the right to object to the processing of your personal data.	14
Right of erasure	In certain circumstances, you have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.	14

Right to restrict processing	In certain circumstances, you have the right to request us to 'block' or suppress processing of personal data.	15

If you wish to exercise any of these rights, you can contact us at SARS@capquest.co.uk

10. HOW DO YOU MAKE DECISIONS ABOUT ME ("RIGHTS RELATED TO AUTOMATED DECISION MAKING")?

Scores and ratings

We use the data we hold on the accounts we own along with data from the CRAs and other 3rd party data providers to produce various scores such as risk, fraud, affordability, collection, litigation and/or insolvency scores to profile accounts and customers. The following factors are likely to impact these scores:

- How long the person has lived at their address;
- The number and type of credit agreements and how they use those credit products;
- Whether the person has been late making payments;
- Whether the person has had any court judgments made against them;
- Whether the person has been bankrupt or had an IVA or other form of debt-related arrangement.

These scores will inform appropriate actions to manage customers' accounts with us and ensure appropriate steps are taken with respect to personal circumstances. An example would be where we use the insolvency scores and data to place an account with a specialist insolvency practitioner.

Where automated decisions are made with regards to account treatment or placement, customers have the right to appeal and request for human oversight and intervention. In this instance a staff member will review your account journey and determine whether the automated process was correct in its decision making.

11. WHAT CAN I DO IF I WANT TO SEE THE PERSONAL DATA HELD ABOUT ME ("RIGHT OF ACCESS")?

You have the right to ask us what data we hold about you. This is known as a Data Subject Access Request (DSAR). You can do this either by emailing your request to SARS@capquest.co.uk or by writing to us at:

Capquest (SARS)

Capella Building 60 York St, Glasgow, G2 8JX

This right or request enables you to receive copies of your personal data, whether all or specific items a data subject can tailor their request. A DSAR provides copies of your data held by us as Data Controller.

What a DSAR does not provide:

1. Copies of corporate documents or contracts that does not contain your personal data.
2. Private and business sensitive information or communications that are reserved under legal privilege.
3. Copies of data belonging to another party unless they provide written agreement and sufficient ID to prove their identity.

We are required to provide a copy of your personal data in a secured format (often reciprocal to your chosen method of request i.e. DSAR sent to us via post will be provided by post) within one calendar month.

In the event your DSAR is considered complex (i.e. requiring extensive resource to complete) we will advise you of that outcome and extend the deadline to a maximum of three calendar months. We reserve the right to charge a small admin fee or require ID in limited cases where repeated DSARs are issued for the former and whether we have doubts about your identity for the latter.

12. DO I HAVE A 'PORTABILITY RIGHT' IN CONNECTION WITH MY DATA ("RIGHT TO DATA PORTABILITY")?

New data protection legislation also contains a right to data portability that may give consumers a right in some data processing contexts, to receive their personal data in a portable format when it's processed on certain grounds, such as consent. This is not a right that will apply to Capquest data because this data is processed on the grounds of legitimate interests.

13. WHAT CAN I DO IF MY PERSONAL DATA IS WRONG ("RIGHT TO RECTIFICATION")?

When we receive personal data, we perform a number of checks on it to try and detect any defects or mistakes. Ultimately, we rely on our suppliers and our customers to provide accurate data to us.

If you think that any personal data we hold about you is wrong or incomplete, you have the right to request this is updated.

If our data does turn out to be incorrect, we will update our records accordingly. If we still believe our data is correct after completing our checks, we will continue to hold and keep it - although you can ask us to add a note to your file indicating that you disagree or providing an explanation of the circumstances. Additionally, we will need to keep a copy of the incorrect record but solely for auditing purposes.

If you'd like to request an update of your data, please contact us.

14. CAN I OBJECT TO THE USE OF MY PERSONAL DATA (“RIGHT TO OBJECT”) AND HAVE IT DELETED (“RIGHT TO ERASURE”)?

As an individual you have specific rights under the UK General Data Protection Regulation. You have the right to object to our use of your personal information, or to ask us to delete, remove, or stop using your personal information if there is no need for us to keep it. This is known as the ‘right to object’ and ‘right to erasure’.

Section 4 of this notice details what information we process, and why we need this information within our organisation in relation to the activities we undertake. This is why your right to erasure doesn’t automatically lead to deletion of your information or prevent its processing with the right to object, but we will deal with every request we receive and if we cannot delete or stop processing your information, we shall inform you and explain why we cannot.

Generally, your right to erasure or right to object will be rejected if you have an open account with us with a balance owed. Furthermore, due to regulatory obligations we retain your information for 6 years past that date therefore your data will not typically be deleted until after that time expires.

There are exceptions, such as we may possess your data and you are not a customer i.e. an authorised third party or carer however this would be limited information, in these cases and no third-party authority remains active we can comply with your request. Moreover, although we strive to take every care in handling your data and making it relevant to our business if we have mistakenly contacted you and you owe no funds or hold an account with us your right of erasure will be processed in line with the timescales afforded by the Information Commissioner’s Office.

Withdrawal of your prior consent, in cases where you have shared sensitive information, in confidence, would also act as a right of erasure which we will comply with.

15. CAN I RESTRICT WHAT YOU DO WITH MY PERSONAL DATA (“RIGHT TO RESTRICT PROCESSING”)?

In the following circumstances:

- You contest the accuracy of the personal data we hold on you, or
- The data we are processing is done illegally and you prefer to restrict rather than erase, or
- We no longer need the data but you ask us to keep it for an anticipated or ongoing legal matter or,
- You have invoked your right to object and we must restrict processing your data while we consider your request.

You can ask us to restrict how we use your personal data. This is not an absolute right, and your personal data may still be processed where certain grounds exist. These grounds include:

- With your consent;
- For the establishment, exercise, or defence of legal claims;
- For the protection of the rights of another natural or legal person;

- For reasons of important public interest.

Only one of these grounds needs to be demonstrated to continue data processing. We will consider and respond to requests we receive, including assessing the applicability of these exemptions.

Please note that given the importance of complete and accurate records, for purposes outlined above, it will usually be appropriate to continue processing data. In particular, to ensure appropriate management of your account.

16. WHO CAN I COMPLAIN TO IF I'M UNHAPPY ABOUT THE USE OF MY PERSONAL DATA?

We try to deliver the best customer service levels, but if you're not happy you should contact us so we can investigate your concerns.

Name	**Contact Details**
Capquest	**Post:** Complaints Team Capella Building, 60 York St, Glasgow G2 8IX Telephone: 0333 999 7217 Email: complaintsin@capquest.co.uk

If you are unhappy with how we have investigated your complaint, you have the right to refer it to the Financial Ombudsman Service (Ombudsman) for free. The Ombudsman is an independent public body that aims to resolve disputes between consumers and businesses like us. You can contact them by:

1. Phone on 0300 123 9 123 (or from outside the UK on +44 20 7964 1000)

2. Emailing them at: complaint.info@financial-ombudsman.org.uk

3. Writing to them at: Financial Ombudsman Service, Exchange Tower London E14 9SR

4. Going to their website at: www.financial-ombudsman.org.uk

You can also refer your concerns to the Information Commissioner's Office (or ICO), the body that regulates the handling of personal data in the UK. You can contact them by:

- Phone on 0303 123 1113
- Writing to them at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF
- Going to their website at www.ico.org.uk.

Capquest's data protection officer can be contacted by emailing DPO@capquest.co.uk or by writing to us at Belvedere, 12 Booth Street, Manchester, M2 4AW.