PRIVACY POLICY

10002358/1222/AD868

Contents

1. Important information and who we are

1.1 Purpose of this Privacy Policy

Welcome to Capital One (Europe) Plc's Privacy Policy. You trust us with your personal data and we want to be open about what we do with it. This Privacy Policy relates to our Range of Products and Services and aims to give you information on how we collect and process your personal data. It also outlines your privacy rights including how you can access your data, correct it, restrict use of it, erase it and/or object to it being processed. Please use the Glossary to understand the meaning of some of the terms used in this Privacy Policy.

1.2 What is Capital One's role?

Capital One (Europe) Plc is responsible for deciding why and how your personal data is collected and processed. This makes Capital One (Europe) Plc the Data Controller (referred to as "Capital One", "we", "us" or "our" in this Privacy Policy). Our contact details are: Capital One, PO Box 5281, Nottingham NG2 3HX. We have appointed a Data Protection Officer ("DPO") to help make sure we are transparent and fair about how we use your data and comply with any law that may affect your privacy. Our DPO contact details are: DPO Legal Dept, Capital One (Europe) plc, Trent House, Station St, Nottingham NG2 3HX. Email: dataprotection@capitalone.com. For any Subject Access Requests (SARs) or other data subject rights requests, please use these contact details; Capital One, PO Box 5281, Nottingham NG2 3HX. Email: sarsrightsrequest@capitalone.com

1.3 Changes to the Privacy Policy and your duty to inform us of any changes

You have a role to play in managing your data too! It is important that the personal data we hold about you is accurate and current so please let us know if your personal data changes during your relationship with us. From time to time we may make changes to this notice. The most recent version of this notice can be found on our website. This Privacy Policy was last updated on 21 December 2022 and historic versions can be obtained by contacting us.

2. The data we collect about you

2.1 What is personal data?

Personal data, or personal information, means any information about an individual from which that person can be identified (either on its own or when combined with other information). It does not include data where the identity has been removed (anonymised data).

We may Process different kinds of personal data about you, which we have grouped together as follows:

- **Identity Data** such as title, names, employment status, occupation, username or similar identifiers, marital status, date of birth;
- **Contact Data** such as addresses, email addresses and telephone numbers;
- **Credit File Data** collected from credit reference agencies (CRAs) – see section 6;
- **Financial Data** such as your income, credit card details, payment card details or details about other financial accounts that you may have;
- **Account Data** such as details of your account, history of changes, financial summaries, statements and account/user/policy or reference numbers;

- **Transaction Data** such as purchases / other transactions made on your account and payments to and from you;
- **Technical Data** such as device information and identifiers, internet protocol (IP) addresses, your login data, browser type/usage and versioning data based on the devices you use to access our digital platforms;
- **Profile Data** such as passwords on your accounts, preferences, feedback;
- **Survey and Research Data** such as your responses to questionnaires, surveys, feedback requests and design or research activities;
- **Usage Data** such as information about when and how you use our products, services processes or platforms (e.g. how often you use our mobile applications or how you use your credit card with us);
- **Marketing Data** such as your preferences on receiving marketing from us and information used in your interactions with us (or our partners) (e.g. cookie data used for behavioural advertising);
- **Communications Data** such as details about any contact made between you and us (e.g. phone calls made or received) and/or the content of those communications (e.g. call recordings);
- **Device Operations** information about operations and behaviour performed on the device, such as mouse movements or key strokes (which can help distinguish humans from bots and between individuals);
- **Special Categories of Personal Data** this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, criminal convictions and offences and data concerning your health and genetic and biometric data. We will only collect and use these types of data where we have obtained your explicit consent or if the law allows us to do so;
- We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature or our mobile app. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this Privacy Policy.

2.2 If you fail to provide personal data

We think it is important to tell you that where we need to collect certain personal data, and you fail to provide the data when requested, we may not be able to perform the contract we have or are trying to enter into with you. In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at that time.

3. How is your personal data collected?

We use different methods to collect data from and about you including through:

- **Direct interactions**. This is data that we collect directly from you and includes personal data you may provide or we may obtain when you:
    - apply or register for our products and services;
    - use our products and services;
    - use our website or mobile device applications;

- make contact with us (e.g. making a phone call);
- communicate with us (e.g. when you talk to us on the phone or send emails, letters or SMS);
- request marketing to be sent to you;
- enter a competition or promotion;
- give us feedback or take part in research or surveys.

- **Automated technologies or interactions**. As you interact with our website, telephony systems or mobile applications, we may automatically collect data including Technical Data about your equipment, browsing actions and patterns; and the telephone number from which you called us. This personal data may be collected by using cookies, web beacons and other similar technologies as well as by other technical methods. Please see our Cookie Policy for further details in relation to Cookies and similar tracking technologies;
- **Third parties or publicly available sources**. We may receive personal data about you from various third parties (and public sources) as set out in 'Our third parties';
- **Other**. We may receive personal data about you from individuals such as extra cardholders, people appointed to act on your behalf, family members, and others who are acting in your best interests or providing us with information in relation to your contact details.

4. How we use your personal data

We collect and use your personal data for different reasons and we tell you what these are in this Privacy Policy. Most commonly, we will use your personal data in the following circumstances:

- Where it is necessary for us to perform the contract we are about to enter into or have entered into with you;
- Where it is necessary for our Legitimate Interests (or those of a third party) and your interests and fundamental rights do not override those interests;
- Where we need to comply with a legal or regulatory obligation;
- When you consent to it;
- In the case of Special Categories of Personal Data, where there is a Substantial Public Interest to process the data or we have obtained explicit consent to do so.

We're only allowed to use your personal data if we have legal grounds to do so. You can find out more about the types of legal ground that we rely on in the Glossary.

4.1 Purposes for which we will use your personal data

We have set out below a description of the ways we plan to use your personal data, the purposes for this usage and which of the legal grounds we rely on to do so. We have also identified what our Legitimate Interests are where appropriate. Note that we may process your personal data for more than one legal ground depending on the specific purpose for which we are using your data. If you had a loan product or are supporting our customers (e.g. powers of attorney) then the reasons we process your personal data are set out separately below.

Purposes and Legal Grounds

(a) We may process your information to:

(i) Understand how you use products, services, processes and related customer experiences provided by us and other organisations;

(ii) Inform the way that we manage our products, services, processes and platforms;

(iii) Develop, test and change our products, services, processes and platforms;

(iv) Invite you to provide customer feedback through surveys and forums to help us understand and improve the effectiveness of our products, services, processes and platforms;

(v) Monitor usage and performance of our products, services, processes and platforms; perform analysis (e.g. statistical, market, product analysis), reporting, forecasting and accounting;

(vi) Tell you about our products, services, events and activities that may be of interest to you;

(vii) Understand how you interact with our marketing; develop, test or change our marketing activities;

(viii) Communicate with our third parties to help them understand, improve and fulfil on marketing activities (including supporting behavioural advertising techniques e.g. use of cookie data);

(ix) Promote our products and services.

When processing your information for these purposes, we are relying on our Legitimate Interest to help us understand, develop, improve and market our products and services.

(b) We may process your information to:

(i) Allow you to begin using or register for our products or services;

(ii) Check your eligibility for our credit products; process your application and/or set up an account for you;

(iii) Uphold our lending criteria by performing creditworthiness, affordability and other checks including, but not limited to, fraud checks, anti-money laundering checks, vulnerability assessments, identity checks;

(iv) Report activities to credit reference agencies (CRAs), fraud prevention agencies (FPAs) and/or crime prevention agencies in line with our legal, regulatory or business requirements;

(v) Communicate with you to provide updates following a credit application or eligibility check;

(vi) Communicate with you to provide updates and information while you are using, registering or continuing to use one of our products or services;

(vii) Communicate with you for design or research purposes or to ask you about our current or potential products, services, processes and customer experiences;

(viii) Provide targeted communications via social media platforms (for example Facebook), by sending to them a hashed version of your personal information (which may be your email address, phone number and/or first name and surname) to provide you with information in relation to our current service availability and other relevant service and support information.

When processing your information for these purposes, we rely on our Legitimate Interest to allow you to access our products and services. In addition, in relation to some of the purposes, it is necessary for us to process your information for the Performance of the Contract between us.

(c) We may process your information to:

(i) Enable you to access and use our online services and functionality;

(ii) Understand how you use and navigate our online services;

(iii) Tailor online experiences or develop and/or change these services;

(iv) Service and fulfil on your products and services (e.g. processing transactions, managing account information and settings);

(v) Provide you with other suitable products, services or relevant information where we (or our partners) think you may be interested;

(vi) Manage potential Payment Protection Insurance (PPI) related activities on your accounts including activities relating to the potential miss-sell of PPI;

(vii) Keep our records up to date including updating preferences and making changes to your account;

(viii) Manage requests from you where you are exercising your data privacy rights;

(ix) Assess your personal circumstances while you are using our products and services and, potentially, taking actions on your account based on these circumstances (e.g. making changes to your account where you appear to be in financial difficulty);

(x) Communicate with you for any purpose relating to the servicing of your account;

(xi) Manage your accounts, products or services effectively (e.g. applying credit limit increases and decreases, updating your product terms);

(xii) Develop, improve or change the products and services that you are using;

(xiii) Offer you additional products, services and promotions;

(xiv) Assess, collect or recover outstanding debts from you;

(xv) Transfer ownership of your account to a third party. This may include activities we carry out with third parties including the assessment, pricing and handover of the debt;

(xvi) Inform strategies around how we collect, recover or sell outstanding debts. This may involve sharing data with third parties to help inform this strategy including which third parties we work with;

(xvii) Monitor usage and performance of our products, services, processes and platforms; perform analysis (e.g. statistical, market, product analysis), reporting, forecasting and accounting.

When processing your information for these purposes, we rely on our Legitimate Interest to fulfil on our products and services. In addition, in relation to some of the purposes, it is necessary for us to process your information for the Performance of the Contract between us.

(d) We may process your information to:

(i) Perform checks to prevent, detect, investigate and report fraud, crime and/or terrorist activity;

(ii) Carry out our obligations required by relevant laws and regulations including anti-money laundering (AML) checks, Her Majesty's Treasury (HM Treasury) and Office of Foreign Assets Control (OFAC) sanctions list checks, Politically Exposed Persons (PEP's) assessments and Transaction/Account monitoring and restriction;

(iii) Protect the security and resilience of our networks/applications and respond to technical and security incidents;

(iv) Devise defence strategies (e.g. in relation to fraud, crime, terrorist or cyber-attack risks) and develop, test or change our defences;

(v) Review and take appropriate action relating to threatening and abusive behaviour of customers to our agents whilst performing their day to day role;

(vi) To ensure we are able to offer our services in a secure manner by authenticating our customers and reducing the risk of fraud.

When processing your information for these purposes, we rely on our Legitimate Interest to manage risk, security and crime prevention. In addition, in relation to some of the purposes, we may process your information to comply with a Legal Obligation.

(e) We may process your information to:

(i) Improve, test, investigate and remediate any issues with our internal processes and practices;

(ii) Maintain your data and ensure the data that we hold about you is accurate and up to date.

When processing your information for these purposes, we rely on our Legitimate Interest to manage and improve our business processes.

(f) We may process your information to:

(i) Cooperate with (and respond to) requests from courts, regulators, law enforcement bodies and other institutions (e.g. fraud prevention agencies);

(ii) Appropriately handle and process complaints or disputes – this may include contacting relevant parties;

(iii) Exercise our rights in relation to complaints, disputes or litigation.

(iv) Manage policy affairs, public relations issues, media enquiries or customer interactions with the media;

(v) Manage complaints with third parties;

(vi) Manage disputes and charge backs;

(vii) Manage litigation against third parties;

(viii) Enable us to provide legal and/or regulatory advice in line with our business activities;

(ix) Share your online account information with regulated third parties, known as Account Information Service Providers (AISPs) where you have asked them to access this information.

When processing your information for these purposes, we rely on our Legitimate Interest to satisfy our industry, regulatory and legal requirements and exercise our rights. In addition, in relation to some of the purposes, we may process your information to comply with a Legal Obligation or it may be necessary to assist in relation to a task performed in the Public Interest.

We may use third parties for any of the purposes listed above.

Loan customers and those supporting our customers

If you had a loan product or are supporting one of our customers (e.g. powers of attorney) then we only process your data for the specific purposes set out below:

Loan Products Purposes and Legal Grounds

(a) We may process your information to:

(i) Manage potential Loan Protection Insurance (LPI) related activities including activities relating to the potential miss-sell of LPI;

(ii) Communicate with you for any purpose relating to the servicing of your products and services;

(iii) Manage requests from you where you are exercising your data privacy rights.

Where we process your information for these purposes, we rely on our Legitimate Interest to fulfil on our products and services. In addition, in relation to some of the purposes, it is necessary for us to process your information for the Performance of the Contract between us.

(b) We may process your information to:

(i) Appropriately handle and process complaints or disputes – this may include contacting relevant third parties to assist in their handling;

(ii) Exercise our rights in relation to complaints, disputes or litigation.

Where we process your information for these purposes, we rely on our Legitimate Interest to satisfy our industry, regulatory and legal requirements and exercising our rights. In addition, in relation to some of the purposes, we may process your information to comply with a Legal Obligation. We may use third parties for any of the purposes listed above.

Those who support our customers (e.g. powers of attorney)

Purposes and Legal Grounds

(a) We may process your information to:

(i) Communicate with you for any purpose relating to the servicing of the account.

(ii) Manage any rewards, offers or promotions;

(iii) Manage requests from you where you are exercising your data privacy rights.

Where we process your information for these purposes, we rely on our Legitimate Interest to fulfil on our products and services.

(b) We may process your information to:

(i) Perform checks to prevent, detect, investigate and report fraud, crime and/or terrorist activity;

(ii) Carry out our obligations required by relevant laws and regulation including anti-money laundering (AML) checks, Her Majesty's Treasury (HM Treasury) and Office of Foreign Assets Control (OFAC) sanctions list checks, Politically Exposed Persons (PEP's) assessments and Transaction/Account monitoring and restriction.

Where we process your information for these purposes, we rely on our Legitimate Interest to manage risk, security and crime prevention. In addition, in relation to some of the purposes, we may do so to comply with a Legal Obligation.

(c) We may process your information to:

(i) Improve; test, investigate and remediate any issues with our internal processes and practices;

(ii) Maintain your data and ensure the data that we hold about you is accurate and up to date.

Where we process your information for these purposes, we rely on our Legitimate Interest to manage and improve our business processes.

(d) We may process your information to:

(i) Assess your personal circumstances in order to support you with the right outcome;

(ii) Appropriately handle and process complaints or disputes – this may include contacting relevant third parties to assist in their handling;

(iii) Exercise our rights in relation to complaints, disputes or litigation;

(iv) Manage policy affairs, public relations issues, media enquiries or customer interactions with media;

(v) Enable us to provide legal/regulatory advice in line with our business activities;

(vi) Cooperate with (and respond to) requests from other institutions, regulators, law enforcement bodies and other agencies (e.g. fraud prevention agencies).

Where we process your information for these purposes, we rely on our Legitimate Interest to satisfy our industry, regulatory and legal requirements and exercise our rights. In addition, we may process your information to comply with a Legal Obligation. We may use third parties for any of the purposes listed above.

Special Categories of Personal Data

Health Data

When we receive information concerning your health from you or someone else we may process it to provide a more appropriate service and/or protect your best interests as follows:

(a) Processing personal data relating to your health enables us or someone else to better protect you against potential harm, such as:

- Taking out credit that is not appropriate;
- Falling behind on debt repayments;
- Falling prey to fraud or financial abuse; or
- Otherwise not being able to protect your economic well-being.

(b) To ensure that we are able to send communications to you in an appropriate format or make other reasonable adjustments due to a condition.

(c) So that we can try and prevent fraud and/or where there may be suspicions of terrorist financing or money laundering;

We may also process your health data to establish, exercise or defend a legal claim.

Where we process this information we will usually do so on the basis of a Substantial Public Interest which has been set out in legislation, to perform or exercise obligations or rights which are imposed or conferred by law on us in connection with social protection or to exercise, establish or defend a legal claim.

If you do not want us to process information concerning your health, you may object to this processing as set out in Your legal rights. We will consider your request appropriately. If we stop processing your health data, we may still include a marker on your account to ensure that we are able to continue to protect your best interests.

Biometric Data

To ensure we are able to offer our services in a secure manner by authenticating our customers and reducing the risk of fraud, we process information about operations and behaviour performed on the device such as mouse movements and key strokes (Device Operations). In some circumstances this information is known as Biometric Data - where it is used to uniquely identify you.

Where we process this information we do so on the basis of a Substantial Public Interest which has been set out in legislation.

If you do not want us to process this information you may object to this processing as set out in Your Legal Rights. We will consider your request appropriately. If we stop processing this information, we will still need to protect the security of your account. We will do this in alternative ways available to us but this might change the overall standard of security that we can apply. You also might not be able to access your account and/or carry out transactions as quickly or easily.

We use third parties to fulfil this purpose on our behalf. The third parties do not process this data as Biometric Data but only as Device Operations.

They will:

- Use the Device Operations data to help us to understand whether you are the person using your device;
- Maintain the confidentiality and security of the information, including maintaining technical and physical safeguards that are designed to (a) protect the security and integrity of the information while it is within their systems and (b) guard against the accidental or unauthorised access, use, alteration or disclosure of information within their systems;
- Only retain the data for as long as is necessary to fulfil this purpose and delete once it is no longer needed for this purpose.

They will not:

- Share the information with any third parties;
- Use the information to append to other information to build profiles;
- Use the information to provide services to you.

4.2 Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising.

You will receive marketing communications from us if you have requested information from us or provided us with your details when you applied or registered for one of our products or services and, in each case, you have not opted out of receiving that marketing. However, you can ask us to stop sending you direct marketing at any time. When you ask us to stop, please note that this may not take effect immediately, since it takes time for the change to be processed in our systems.

If you ask us to stop sending you marketing messages, you will still receive communications pertaining to the servicing or fulfilment of your account, product, service or relationship with us (such as statements for your credit product, communications about your outstanding debts or relevant updates about the products or services that you are already using).

We may share information that we collect about you with third parties and we may also use third parties to conduct marketing activities on our behalf. In some cases, we do this to identify groups of similar audiences to target for advertising purposes. If you do not want us to share your personal information with third parties for this purpose, you can tell us not to.

4.3 Cookies and Online Marketing

For more information about the cookies we use for online marketing purposes, please see our Cookie and Online Marketing Policy.

Online advertising through pixels

We use targeting and advertising pixels on our website for various reasons, including to ensure you do not see advertisements that are not relevant or identify groups of similar audiences to target for advertising purposes.

We collect information about you using these pixels such as email addresses, names and telephone numbers and share this with our marketing partners such as Facebook, TikTok and Google. These can also monitor your online behaviour and identify website usage.

In some cases, we may also take your information to evaluate personal aspects about you. This is called profiling. We use data that you provide along with internal and third-party data to place you into groups with similar types of people.

If you have allowed us to use pixels for targeting and advertising, this information will be collected and sent through pixels to our marketing partners. For more information or to alter your cookie settings, please visit our Cookie and Online Marketing policy.

Facebook is a joint controller with us when we process information we collect about you from your actions online or through the Facebook pixel on our website. This Joint Controller relationship is subject to Facebook's Controller Addendum. Facebook is the independent Data Controller once it is in receipt of that data. You can find more information about Facebook's processing at https://www.facebook.com/policy.php. To learn more about this type of processing please see our Cookie and Online Marketing Policy.

Data shared in other ways

We share information that we collect about you such as email addresses and telephone numbers with our third party partners such as Facebook, Google, TikTok, Microsoft and Yahoo. We do this so that we can identify groups of similar audiences to target for advertising purposes or ensure you do not see advertisements that are not relevant. We call these groups 'custom audiences'.

Yahoo

You can find more information about how Yahoo uses the data it receives here:
https://legal.yahoo.com/us/en/yahoo/privacy/index.html

Microsoft

You can find more information about how Microsoft uses the data that it receives here:
https://privacy.microsoft.com/en-gb/privacystatement

Google

You can find more information about how Google uses data that it receives here:
https://policies.google.com/technologies/partner-sites

TikTok Business Products

We use TikTok Business Products for the purposes outlined in this Section 4.3 above. TikTok is a joint controller with us when we process information we collect about you for this purpose. This Joint Controller relationship is subject to TikTok's Joint Controller Terms.

You can find more information about how TikTok processes personal data, including the legal basis TikTok relies on and the ways to exercise data subject rights against TikTok in the relevant TikTok inventory privacy notice here:
https://www.tiktok.com/legal/privacy-policy-eea?lang=en&selection=true

Facebook Custom Audience

When we use this feature, we "hash" your data locally before we pass it to Facebook. This is a process which turns your data into letters and numbers so that it is protected.

Facebook will:

- Use the hashed data for matching purposes; and
- Maintain the confidentiality and security of the hashed data and the collection of Facebook User IDs that comprise the customer audience created from the hashed data, including maintaining technical and physical safeguards that are designed to (a) protect the security and integrity of data while it is within Facebook's systems and (b) guard against the accidental or unauthorised access, use, alteration or disclosure of data within Facebook's systems.

Facebook will not:

- Share the hashed data with third parties or other advertisers and will delete the hashed data promptly after the match process is complete;
- Give access to or information about the custom audience(s) to third parties or other advertisers;
- Use custom audience(s) to append to the information it has about its users or build interest-based profiles;
- Use custom audience(s) to provide services to you.

For further details in relation to Facebook Custom Audience, please visit
https://www.facebook.com/legal/terms/customaudience.

When processing your information for these purposes we are relying on our Legitimate Interest to help us understand, develop, improve and market our products and services.

If you do not want us to share your personal information with third parties for this purpose, you can tell us not to. If you opt out after your data has been shared with the platform, your data will be removed from the custom audience.

4.4 Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal ground which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5. How we use your information to make automated decisions

Automated Decision Making, including profiling, is the processing of personal data (that we have collected or are allowed to collect from others) by automated means and without human involvement to evaluate personal aspects about you.

In particular, we may process data to analyse or predict (amongst other things) your financial situation, personal preferences, interests or behaviours. This means that automated decisions without human involvement could be made about you for example in relation to the products and services we offer you (e.g. credit limit change decisions or deciding which communications are suitable for you). Here are the types of automated decisions we make:

Making Lending Decisions

For our credit products, we use automated decision making when deciding whether to lend money to you and to determine the initial setup for our products (e.g. what credit limit you will be offered on your credit card). When you have an account with us, we may continue to use automated decision making where deciding whether to offer you additional credit (e.g. where offering you a credit limit increase).

Where making assessments of this type, we may use a technique known as "credit scoring".

Credit scoring uses data from several sources:

- Information you have provided;
- Information we may collect or already hold about you; and
- Information provided by third parties (including credit reference agencies).

We use data from these sources and our logic to predict behaviours (e.g. how well we expect you to manage your product and make regular payments), to group our customers (or potential customers) into 'customer segments' and to make our lending decisions (e.g. which applicants do we accept /decline).

This approach allows us to make quick, consistent decisions, uphold our lending requirements and ensure that we lend responsibly. These automated decisions may lead to your credit application being declined and may limit your ability to access further credit in the future.

Detecting Fraud

Where you apply for (or register for) one of our products or services, we use automated processes to detect and help prevent fraud.

We may automatically decide that you pose a fraud or money laundering risk if our processing reveals your behaviour to be consistent with money laundering or known fraudulent conduct; or is inconsistent with your previous submissions; or you appear to have deliberately hidden your true identity.

We may also continue to monitor your accounts, your product usage and your transactions to determine whether your account is being used for fraudulent activities.

We utilise data from several sources to help us identify fraud risks:

- Information you have provided;
- Information we may collect or already hold about you; and

- Information provided by third parties (including fraud prevention agencies).

We combine data from these sources and defined logic to identify threats and prevent fraud losses. If we think there is a risk of fraud, we may stop activity on your account and/or refuse access.

Providing you with access to products and services

When you apply (or register) for one of our products or services, we perform checks to ensure that these are suitable for your circumstances and that we manage our business risks.

To do so, we utilise data from several sources:

- Information you have provided;
- Information we may collect or already hold about you; and
- Information provided by third-parties (including fraud prevention agencies).

These checks may include (but are not limited to):

- Checks to ensure you meet conditions for opening an account (e.g. checking your age and residence);
- Checks based on your existing products with us (e.g. checking whether you already have an account with us and how it is currently being managed);
- Checks to identify money laundering, criminal / terrorist activity or cyber security threats that may pose a risk to you and our business.

Where we identify circumstances or threats that introduce a risk to you or our business, we may not be able to provide you with access to our products or services.

Managing, tailoring and marketing our products and services

Where we have an existing relationship with you, we may use profiling and automated decision making to help manage this relationship. We use these techniques to ensure that we manage your accounts, products or services appropriately; help you get the best out of your products and services; and provide you with promotions or offers that we think you will be interested in.

We use data that you provide along with internal and third-party data (which may include data from credit reference agencies) to place you into groups with similar types of people. We call these groupings 'segments' and these are used to help us understand, test and tailor our products, services and marketing more appropriately depending on identified segment types. Some examples of how we use profiling and decision making are:

Optimising and fulfilling on communications
Different communication approaches are suitable for different types of people so we use segmentation to provide you with the most appropriate communications for you;

Sending marketing and offers
Different marketing approaches may be used with certain segments where we think our marketing will perform more effectively;

Tailoring or managing products
We may tailor your accounts, products or services based on a segment that you are grouped into (e.g. changing product terms such as APR);

Deciding whether we need to help you
Certain details in your information may suggest that you are likely to become financially vulnerable and we may need to help you. For example, if we have information that shows you have moved from paying the full amount of your credit card to paying off only the minimum amount each month, this could be one sign that you may be having some financial difficulties and that we may be required to help you;

To take action in relation to your account
We may take action on your account such as restricting the use of your account or closing it due to inactivity.

This approach helps us to manage our accounts, products, services and marketing more effectively and meet industry and regulatory requirements (e.g. around customer indebtedness). This profiling and automated decision making may lead to changes on your account, product or service or in the way that we interact with you (communications or marketing).

Your rights in relation to automated decision making

You have rights in relation to certain automated decision making which means that before the end of the period of one month beginning with receipt of the automated decision you can request us to:

(i) reconsider the decision; or

(ii) take a new decision that is not based solely on automated decision making and ask that a person review it.

If these rights apply you will be notified. If you want to know more about these rights, please contact us.

6. Credit reference agencies (CRAs)

When you apply, use or register for our products and services, we may perform credit and identity checks on you with one or more credit reference agencies ("CRAs"). We may also make periodic searches at the CRAs to manage your account with us or fulfil our services. To do this, we will supply your personal information to the CRAs and they will give us information about you. We may share information that you give to us; information about your account; information about how you use our products and services and information about your financial situation and financial history. CRAs will supply to us both public (including the electoral register) and shared credit, financial history information and fraud prevention information.

We will use this information to:

- Assess your creditworthiness and whether you can afford to take the product;
- Verify the accuracy of the data you have provided to us;
- Confirm your identity and prevent criminal activity, fraud and money laundering;
- Manage your account;
- Trace and recover debts;
- Ensure any offers provided to you are appropriate to your circumstances;
- Provide you with access to your credit bureau data where you have asked us to;
- Ensure that you are aware of changes or offers which might be relevant to how you manage the product;

- Monitor your behaviour to inform our wider strategy.

We may continue to exchange information about you with the CRAs while you have a relationship with us in line with the product or service. We will also inform the CRAs about your settled accounts. CRAs will record your outstanding debts and this information may be supplied to other organisations by CRAs.

When CRAs receive an application search from us they will place a search footprint on your credit file that may be seen by other lenders.

The identities of the CRAs; their role also as fraud prevention agencies; the data they hold; the ways in which they use and share personal information; data retention periods and your data protection rights with the CRAs are explained in more detail at:

TransUnion
Equifax
Experian

7. Fraud prevention agencies (FPAs)

Before we provide products or services to you, we also undertake checks for the purposes of preventing fraud and money laundering, and to verify your identity. These checks require us to process personal data about you.

The personal data you have provided, we have collected from you, or we have received from third parties will be used to prevent fraud and money laundering, and to verify your identity.

Details of the personal information that will be processed include, for example: name, address, date of birth, contact details, financial information, and device identifiers including IP address.

We and fraud prevention agencies may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime.

We process your personal data on the basis that we have a Legitimate Interest in preventing fraud and money laundering, and to verify your identity, in order to protect our business and to comply with laws that apply to us. Such processing is also a contractual requirement of the products and services you have requested.

Fraud prevention agencies can hold your personal data for different periods of time, and if you are considered to pose a fraud or money laundering risk, your data can be held for up to six years.

Consequences of Processing

A record of any fraud or money laundering risk will be retained by fraud prevention agencies, and may result in others refusing to provide products or services to you.

Data Transfer

Whenever fraud prevention agencies transfer your personal data outside of the UK, they impose contractual obligations on the recipients of that data to protect your personal data to the standard required by the UK. They may also require the recipient to subscribe to “international frameworks” intended to enable secure data sharing.

8. Credit card networks (Visa and Mastercard)

We use credit card networks such as Visa and Mastercard to process transactions with merchants. The purpose of credit card networks is to control where credit cards are accepted and to facilitate transactions between merchants and credit card issuers such as Capital One.

As well as processing your information to process transactions, credit card networks also aggregate and anonymise data in its network - so you are no longer identifiable - which may be used and/or shared where deemed appropriate with third parties for the following purposes:

- Billing purposes;
- Product enablement and build;
- Testing or product improvement purposes;
- To reply to requests from public authorities;
- Analysed by Visa and its partners for offers or promotional activities that cardholders have entered or agreed to be a part of;
- To support loyalty programs, promotional activities or other services offered by a network member, Visa or its partners including by determining eligibility and identifying qualifying transactions;
- Authentication, security, dispute resolution, managing risk and preventing fraud;
- Keeping Personal Data up-to-date;
- Data modelling, analytics, business intelligence and insights.

Data Transfer

- Whenever credit card networks transfer your personal data outside of the UK, they impose contractual obligations on the recipients of that data to protect your personal data to the standard required by the UK.

Visa Account Updater (VAU) and Mastercard Automatic Billing Updater

Once you receive a replacement or new card from us, any merchant with which you have an existing relationship (specifically where you have stored your card details for recurring or future payments) can request your new card details so that those card payments can continue. An example of this would be a monthly music subscription. You can opt out of this service at any time by contacting us.

9. Credit brokers

On occasion, we issue our cards through a credit broker who introduces you to us - for example the Post Office, Ocean Finance, ThinkMoney, the Very Group and Littlewoods. In these circumstances, they will have their own Privacy Policy which sets out how they process your personal data. To ensure that the credit broker has up to date and accurate information, we will share your contact details with them. We also share with them the fact that you have been accepted for a card.

10. Disclosures of your personal data

We may share personal data about you with various third parties and public sources as set out in 'Our third parties' for the purposes set out in paragraph 4 above.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers in their capacity of Data Processor to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

11. Our third parties

We use third parties to enable, perform or improve a range of our business processes. These may require us to share your data with third parties and/or they may share your data with us. These third parties may include (but are not limited to):

(a) Third parties that enable us to understand, develop, improve and market our products and services

(i) Product, marketing and industry monitoring services and tools;

(ii) Market research, surveying, consultancy and benchmarking services;

(iii) Product/service/communications design and development services;

(iv) Marketing partners, affiliates and intermediaries;

(v) Analytics and incident management services;

(vi) Regulated Open Banking entities.

(b) Third parties that enable us to uphold our lending, usage or registration criteria by supporting creditworthiness, affordability and other checks – for example:

(i) Credit reference agencies (CRAs);

(ii) Fraud detection and prevention tools, services, bodies or agencies;

(iii) Cyber threat detection tools or services;

(iv) Parties providing additional data or services for our credit underwriting;

(v) Regulated Open Banking entities;

(vi) Third parties used to meet our legal and regulatory requirements (e.g. anti-money laundering (AML) checks, Her Majesty's Treasury (HM Treasury) sanctions list checks).

(c) Third parties that work with us to help us fulfil on and service your accounts, products or services:

(i) Communications fulfilment or development service providers;

(ii) Customer account management services;

(iii) Customer servicing (service agents, support and tools);

(iv) Payment services, payment schemes and network services;

(v) Transaction enablement and dispute services;

(vi) Payment Protection Insurance (PPI) services including the ongoing management and activities relating to the potential miss-sell of PPI.

(d) Third parties that support the running of our business processes:

(i) Business process systems and support providers;

(ii) Technical platforms, software and tools providers (e.g. tools that we use to optimise

and test on our website or mobile applications);

(iii) Platform management and support services;

(iv) Data storage, transfer and processing services;

(v) Disaster recovery solution services;

(vi) Public relations support and consultancy services.

(e) Third parties that work with us to ensure we reach the best possible outcome:

(i) Regulators, advisory entities and consumer rights/advice bodies;

(ii) Customer complaints and dispute resolution services.

(f) Third parties that support with debt management, debt placement, debt collection, debt advice and potential purchasers (for assessment and transfer of accounts).

(g) Third parties that provide reporting, banking or tax management services and enable us to manage our business financials and performance.

(h) Other third parties, bodies or institutions where we are required by regulation, law, industry practices or to detect/prevent fraud, crime, terrorist activity or business risks e.g. regulators, law enforcement bodies, crime prevention bodies and sharing information with other institutions to help detect and prevent fraud.

Some of our third parties may be international. See 'International transfers' to understand how we manage our data internationally.

12. International transfers

Capital One (Europe) Plc is based in the UK and we keep our main databases here. However, we do have operations inside and outside the UK and your data may be transferred to, or accessed from, those locations.

Specifically, Capital One has operations in the US, Canada and India.

As well as other Capital One operations, the service providers we share your data with may have operations in the UK and elsewhere in the world.

While some countries - including those in the European Economic Area ("EEA"), are recognised as having the same high standard of data protection as offered here in the UK, other parts of the world may not guarantee that same level of protection. When we share your data with anyone outside of the UK, where necessary, we always put in place the safeguards required by law to ensure that a consistent high level of protection travels with your data.

If you want to learn more about the specific legal safeguards we use to transfer your data, see below.

Before we share your data outside the UK and outside the EEA, we must assess the risks of transferring the data and make sure there are safeguards in place which provide adequate protection of your data. Where adequate safeguards are established, your rights as a data subject continue to be protected even after your data has been transferred outside the UK.

As part of the safeguards, we put in place a data transfer agreement or "standard contractual clauses" with the third party receiving the data outside the UK containing obligations on the service provider to protect the data.

We transfer some of your personal data to our US parent. We have a Data Transfer Agreement in place with our US parent which sets out terms upon which they can process your data.

If you would like more specific details about the safeguards in place when transferring your data outside the UK, please email DataProtection@capitalone.com.

13. Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and the Information Commissioner's Office of a breach where we are legally required to do so.

14. How long will you use my personal data for?

There are a number of reasons why we need to keep hold of your personal data and our aim is to only retain it for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

How long we keep it for depends on the type of data we're holding and why we need it. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

If you apply and/or register for one of our products and/or services, we will retain your personal data for up to seven years after your relationship with us ends.

If your application for one of our products is declined or you decide not to progress with the application, we will retain your personal data for up to 18 months after your application or quotation search was made.

We may keep your data for longer than explained above if we cannot delete it for legal, regulatory or technical reasons. If we do, we will continue to make sure your privacy is protected.

15. Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data.

- Right of access to your personal data
    - Right of access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you.
- Right to rectification
    - Right to rectification of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected. However, please note that we may need to verify the accuracy of the new data you provide to us.

- Right to erasure ("right to be forgotten")
    - Right to erasure of your personal data (also known as the "Right to be forgotten").

This enables you to ask us to delete or remove personal data in the following circumstances:

- Where the personal data is no longer necessary for the purpose for which it was collected;
- Where we have requested your consent to process your information and you wish to withdraw consent;
- Where you have successfully exercised your right to object to processing of your personal data;
- Where we may have processed your information unlawfully or where we are required to erase your personal data to comply with a legal obligation.

Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

- Right to object
    - Right to object to processing (including profiling) of your personal data where we are relying on a Legitimate Interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms. You have the right to object where we are processing your personal data for direct marketing purposes.
- Right to restriction of processing
    - Right to restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

      (a) if you want us to establish the data's accuracy (see Right of rectification);

      (b) where our use of the data is unlawful but you do not want us to erase it;

      (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or

      (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it (see Right to object).
- Right to data portability
    - Right to data portability of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- Right to complain to the ICO
    - Right to make a complaint to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues, at any time https://ico.org.uk/global/contact-us/ We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

- Right to object to direct marketing
    - Right to object to direct marketing at any time by following the opt-out links on any marketing message sent to you or by contacting us.
- Right to withdraw consent
    - Right to withdraw consent at any time. In certain circumstances, we may need to get your consent before we can access or process your personal data. If this happens, we will always ask for your consent first. If you have given us consent in the past but subsequently change your mind, you can withdraw your consent at any time.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests in relation to your legal rights within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Contact Us

If you wish to exercise any of the rights set out above, please contact us at Capital One, PO Box 5281, Nottingham NG2 3HX.

Email: sarsrightsrequest@capitalone.com

16. Glossary

Biometric Data means data which relates to the specific physical, physiological or behavioural characteristics of an individual and which can be processed in a way that allows that particular individual to be uniquely identified.

Comply with a Legal Obligation means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

Legitimate Interest means we have business or commercial reasons to use your data. We can use your data to pursue Legitimate Interest of our own or of other service providers. When we rely on our Legitimate Interest, we make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

Performance of the Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Process means anything we do with your data such as collecting, using, storing, sharing, monitoring, analysing and deleting it.

Public Interest means the processing is necessary for either carrying out a specific task in the public interest which is laid down by law, or exercising official authority, e.g. a public body's task, functions, duties or powers which is laid down by law.

Range of Products and Services means our website or tools available on our website (e.g. QuickCheck). It would also include our current lending products (e.g. our Classic Credit Card) or historic products (e.g. loan products or our Aspire World Credit Card). We also have services available to help you manage your account (e.g. Web Servicing platform and Mobile Applications).

Substantial Public Interest means those laid down in data protection laws.