



Privacy Policy

1. Who are we?

We are GB Bank Ltd, formally known as The Model T Finance Ltd. Our data protection registration is ZA503192, which is renewed annually.

GB Bank Ltd is the data controller and has overall responsibility for your personal data (collectively referred to as "we", "us" or "our" in this privacy policy).

We have appointed a data protection officer, DPO, who is responsible for overseeing questions in relation to this privacy policy. If you have any questions about this privacy policy, including any requests to exercise your information rights, please contact our DPO using the details set out below.

Contact details:

Postal address: Data Protection Officer
 GB Bank
 73 Brook Street
 Mayfair
 London
 W1K 4HX

2. Purpose of this Privacy Policy

We respect an individuals' right to privacy and to the protection of their personal data. The purpose of this privacy policy is to explain how we collect and use personal data in connection with our business.

Personal data means any information about a living individual, who can be identified from that information, either directly or indirectly, e.g., when combined with other data.

This website is not intended for children as we will not be offering our services to anyone under 18 years of age.

3. What personal data do we collect about you?

We process your personal data in order for us to engage with you, the personal data processed will be dependent on the product you enquire about or apply for. We will also collect your name and contact information if you are acting on behalf of a customer.

We also have a legal obligation to prevent fraud and money laundering. We may therefore, collect, use, store and share the following personal data:

- **Basic Personal Data** which includes first name, last name, date of birth, passport information (or other identification information), financial information and employment information. This will help us verify your identity and meet our regulatory obligations. We may also request personal data i.e., first name, surname, and contact details of your next of kin. If you visit us in person, we will also collect your image via our in-house CCTV.
- **Special Categories of Personal Data** we may collect information that may reveal your racial and ethnic origin and data relating to the alleged commission or conviction of a criminal offence. We will only collect this data when it is absolutely necessary.
- **Contact Information** which includes, residential or business address, email address and telephone numbers.
- **Information Relating to your Tax Responsibilities**, this will help us comply with our obligations under the Foreign Account Tax Compliance Act ("FATCA") and the Common Reporting Standards.
- **Technical Information** which includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website.
- **Profile Data** includes your username and password.
- **Usage Data** includes information about how you use our website.
- **Telephone Recording** if you contact us by telephone, we may record your call with one of our representatives for training

purposes and to ensure we are meeting our regulatory obligations.

Where we need to collect personal data by law, due to the terms of a contract we have or are entering into with you, and you fail to provide that data when requested, we may not be able to perform the conditions of the contract. In these circumstances, we may have to cancel the product or service you have with us. We will notify you if this is the case.

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.

4. How is your personal data collected?

We use different methods to collect data from and about you, these being:

Direct interactions:

You may give us your identity and contact details by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:

- Create an account on our website
- Request marketing to be sent to you
- Give us feedback

Automated technologies or interactions:

As you interact with our website, we may automatically collect technical data about your equipment, browsing actions and patterns. We collect this personal data by using cookies and other similar technologies. Please see our cookie policy for further details [Cookie Policy – GBBank](#).

Third parties or publicly available sources:

We may obtain and receive personal data about you from various third parties and public sources as set out below:

- Credit reference agencies, see below for further information.
- Technical data from analytics providers such as Google based outside the EU.

- Identity and contact data from publicly available sources, such as Companies House and the Electoral Register.
- The Insolvency Register.

We will not commence gathering such data before you have been provided with the opportunity to read this privacy policy.

5. How will we use your personal data?

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need 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”.

6. For what purpose do we use your personal data?

We have set out below, a description of all the ways we plan to use your personal data, and which legal basis we rely on. Where appropriate, we have also identified what our legitimate interests are.

We may process your personal data for more than one lawful basis depending on the specific purpose for which we are using your data. Please contact our data protection officer on the above address if you need further information on the legal basis for processing your personal data.

Purpose/Activity	Type of data	Lawful basis for processing your data
To register you as a customer of our services. (This includes the contact details of those acting on a customer’s behalf).	<ul style="list-style-type: none"> • Identity data (this may include special category of personal data) • Contact 	<ul style="list-style-type: none"> • Performance of a “contract” with you • Necessary to comply with a “legal obligation”

Processing data, (including sharing), which may identify criminal activity in order to stop and detect crime, to obey laws relating to money laundering, fraud, and terrorist financing.	<ul style="list-style-type: none"> • Identity data (this may include special categories of data) • Contact • Transactional data 	<ul style="list-style-type: none"> • Necessary to comply with a "legal obligation". • Necessary for ours and the wider public's "legitimate interests".
<p>To manage our relationship with you which will include but is not limited to:</p> <ul style="list-style-type: none"> • Notifying you about changes to our terms or privacy policy 	<ul style="list-style-type: none"> • Identity • Contact • Profile • Marketing and Communications 	<ul style="list-style-type: none"> • Performance of a "contract" with you • Necessary to comply with a "legal obligation" • Necessary for our "legitimate interests" (to keep our records updated and to study how investors use our services)
For assessment and testing of our systems to ensure we continue to provide a high standard of service to our customers.	<ul style="list-style-type: none"> • Identity • Contact 	<ul style="list-style-type: none"> • Necessary for our "legitimate interests", (to develop, build improve our systems, products, and services)
To enable you to complete a survey	<ul style="list-style-type: none"> • Identity • Contact • Profile • Usage • Marketing and Communications 	<ul style="list-style-type: none"> • Performance of a "contract" with you • Necessary for our "legitimate interests" (to study how investors use our services, to develop them and grow our business)
To administer and protect our business	<ul style="list-style-type: none"> • Identity 	<ul style="list-style-type: none"> • Necessary for our "legitimate

<p>and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)</p>	<ul style="list-style-type: none"> • Contact • Technical 	<ul style="list-style-type: none"> • interests” (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) • Necessary to comply with a “legal obligation”
<p>To deliver relevant website content to you</p>	<ul style="list-style-type: none"> • Identity • Contact • Profile • Usage • Marketing and Communications • Technical 	<ul style="list-style-type: none"> • Necessary for our “legitimate interests” (to study how investors use our services, to develop them, to grow our business and to inform our marketing strategy)
<p>To use data analytics to improve our website, services, marketing, investor relationships and experiences</p>	<ul style="list-style-type: none"> • Technical • Usage 	<ul style="list-style-type: none"> • Necessary for our “legitimate interests” (to define types of investors for our services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
<p>To make suggestions and recommendations to you about services</p>	<ul style="list-style-type: none"> • Identity • Contact 	<ul style="list-style-type: none"> • Necessary for our “legitimate interests” (to develop our services

that may be of interest to you	<ul style="list-style-type: none"> • Technical • Usage • Profile 	and grow our business)
If you visit us at our office in person	<ul style="list-style-type: none"> • Your image via CCTV 	<ul style="list-style-type: none"> • Necessary for our "legitimate interests" (for safeguarding and the prevention and detection of crime)

7. Change in purpose?

We will only use your personal data for the purpose(s) for which we collect it, unless we consider that we need to use it for another reason, and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us at the above address.

Where permitted by law we can process your personal data without your knowledge or consent. If we do need to use your personal data for an unrelated purpose, and where the law permits, we will notify you to explain the legal basis which allows us to do so.

8. Will we share your personal data?

We may need to share some or all your data with third parties, however this will only be to the following third parties and under the following circumstances:

Law enforcement and other external parties:

- To authorities that identify and stop financial crime, money laundering, terrorism, and tax evasion if the law says we have to, or if it's necessary for other reasons.
- To the police, courts, or dispute resolution bodies if we are required to do so by law or it is in ours or a third parties' legitimate interest.
- To other banks to help trace money if you are a victim of fraud or other crimes or if there's a dispute about a payment.

- To any other third parties where necessary to meet our legal obligations.
- To partner agencies where there is a contractual requirement to do so, or a legitimate interest has been identified.
- We may also share your details with people or companies if there's a corporate restructure, merger, acquisition, or takeover.

Credit reference agencies:

Credit reference agencies (CRAs) give lenders information about borrowers to help them make responsible lending decisions. Banks also share details about their customers to help CRAs maintain up-to-date information about people's financial status.

In order to process your application with us we will provide your personal information to a CRA. This includes:

- Your name, address, and date of birth.
- It may also include additional information such as previous residential addresses, and other information you provide as part of your loan application.

The CRA will match this information to the records they hold about you, and provide in return, both public information (including the electoral register) and shared credit, financial situation, and 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.
- Prevent criminal activity, e.g., fraud and money laundering.
- Manage your account(s).
- Trace and recover any debts; and

- Ensure any offers provided to you are appropriate to your circumstances.

We will continue to exchange information about you with the CRA while you have a relationship with us. We will also inform the CRA about your settled accounts. If you borrow and do not repay in full or on time, the CRA will record the outstanding debt. This information may be supplied to other organisations by the CRA we use.

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

If you are making a joint application we will link your records together, so you should make sure you discuss this with the third party involved, and share with them this information, before lodging the application. CRA will also link your records together and these links will remain on yours and their files until such time as the third party successfully files for a disassociation with the CRA to break the link.

To better understand how the credit reference agency we obtain information from, uses, and shares personal data please refer to the following Credit Reference Agency Notice, ("CRAIN") www.equifax.co.uk/crain.

Fraud prevention services

When you apply for an account the personal information we collected from you will be shared with fraud prevention agencies, like Cifas, who will use it to verify your identity. If you are seeking to use our lending services, fraud prevent agencies will also use your data to prevent fraud and money laundering. Further details of how your information will be used by fraud prevention agencies, can be found at [Fair Processing Notices for Cifas' Databases | Cifas](#)

Once you have opened an account with us, we may process your personal information in systems that look for fraud by studying patterns in the data. This may indicate that there is a risk that fraud or money-laundering may be occurring against a customer or the bank. If we or a fraud prevention agency notice that an account is being used for fraud or money laundering, we may stop activity on your account or block access.

Third parties working on behalf of GB Bank:

We will share your data with third parties who are acting on our behalf and are referred to as data processors i.e., contractors (including sub-contractors). Some of our data processors are based outside of the UK

however they are all within the European Economic Area, EEA. We do not allow our data processors (including sub processors) to use your personal data for their own purposes, they are only permitted to process your personal data for a specified purpose(s) and in accordance with our instructions.

Your personal data may also be shared with professional advisers acting as data processors or joint controllers, these include lawyers, bankers, auditors, and insurers based within the UK and the EEA.

9. How do we store and transfer your personal data?

We will process and store your personal data on servers managed by our hosting providers, who we refer to as data processors.

The hosting servers are cloud based with some being hosted outside the UK, but within the EEA. We will only allow your personal data to be hosted by our data processors if we are assured that they will protect your data as we do, and in accordance with the applicable law, i.e., Data Protection Act 2018 and the UK General Data Protection Regulation, UK GDPR.

GB Bank will not transfer your personal data outside the EEA; however, fraud prevention agencies may allow the transfer of your personal data outside of the UK. This may be to a country where the UK Government has decided that your data will be protected to UK standards, but if the transfer is to another type of country, then the fraud prevention agencies will ensure your data continues to be protected by ensuring appropriate safeguards are in place. Cifas has published more [information about data transfers](#).

10. Automated decision making

Automated decision-making is the process of making a decision by solely automated means i.e., without any human involvement.

We may complete automated decision making when you request to open a savings account with us. This will be done by gathering information from you and third parties i.e fraud prevention agencies, which is then used to complete identity verification and anti-fraud checks. However, if we believe the checks we have completed may lead to us refusing you a savings account then we will have a member of staff review the information gathered and make the decision on your application.

GB Bank do not complete automated decision making on applications for our lending products.

11. Consequences of processing

If when completing background checks, we or a fraud prevention agency detect fraud or decide that you pose an unacceptable level of fraud or money-laundering risk, you may be refused our services and it could also result in other organisations refusing to provide you their services, financing, or employment. Further details of how your information will be used by fraud prevention agencies, and your data protection rights, can be found by [Fair Processing Notices for Cifas' Databases | Cifas](#)

Those checks which help us identify fraud or money laundering include but are not limited to.

- Behaviours which are known to be consistent with that of known fraudsters or money launderers; or
- Your submission is inconsistent with previous submissions; or
- It would appear that you have deliberately hidden your identity.

A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, who can hold your information for different periods of time. If you are considered to pose a fraud or money laundering risk, your data can be held for up to six years.

12. Marketing

We strive to provide you with choices regarding the use of some of your personal data. Particularly around marketing and advertising.

We may use your identity, contact, technical usage, and profile data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products and services may be relevant for your circumstances; we call this marketing.

You will receive marketing communications if you have requested information from us previously or invested with us. You can "opt out" of receiving marketing material at any time by contacting us at [the above address](#). In addition, all marketing material issued to you will provide you with the opportunity to "opt-out" and explain how this can be done.

We do not participate in third-party marketing and will therefore never share your personal data with any company outside of GB Bank. However,

if we do decide to participate in third-party marketing in the future, we will seek your “consent” before sharing your personal data for this purpose.

13. How long do we keep your information for?

We will not retain your personal data for longer than is necessary for the purpose described in this privacy policy.

Regulatory requirements dictate that we should keep your personal data for seven years following the closure of your account, however in certain circumstances we may have to store your data for a longer period.

In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes. We may therefore use this information indefinitely without further notice to you.

If we, or a fraud prevention agency believe that you pose a fraud or money laundering risk not only may we refuse to provide our services or products but a record of any fraud or money laundering risk may also be retained by us and fraud prevention agencies and could result in financial companies, including GB Bank, refusing to provide you with their services and products in the future.

14. 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 any applicable regulator of a breach where we are legally required to do so.

15. Your legal rights in relation to your personal data

The Data Protection Act 2018 and the UK General Data Protection Regulation, UK GDPR, provides a number of rights for individuals over their personal data. These being:

Right to be informed – This places an obligation on us as a data controller to tell you how we obtain your personal data and describe how

we will use, retain, store, and who we share it with. We have written this privacy policy to explain how we will process your personal data and advise you what your rights are under data protection law.

Right of access – This is commonly known as subject access and is the right which allows you access to your personal data and to supplementary information. This right is subject to certain restrictions.

Right to rectification – You have the right to have your personal data rectified if it is inaccurate or incomplete.

Right to erasure – The right to erasure is also known as “the right to be forgotten”. This right enables you to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Right to restrict processing – You have the right to request your personal data be “blocked” or suppressed. When processing is restricted, organisations are permitted to store personal data but not to further process it.

Right to data portability – This allows you to obtain and reuse your personal data for your own purposes across different services.

Right to object – You have the right to object to the processing of your personal data under certain circumstances, these being:

- The processing of your personal data for direct marketing purposes, including the profiling of data for direct marketing purposes. This is an absolute right and processing must cease on the receipt of an objection.
- The processing of your personal data based on legitimate interests (or those of a third party) or a performance of a task in the public interest. The right to object when personal data is processed under this legal basis is not absolute. You must provide us with specific reasons why you object. We will consider your request and decide if our legitimate grounds for processing override your interests, rights, and freedoms. Any decision made will be explained to you in writing.

Rights relating to fully automated decision making – Fully automated individual decision making, is a decision made by automated means without any human involvement.

Individuals have the right not to be subject to automated decision making if to do so would impact on their rights or freedoms unless it is based on one of the following criteria:

- Necessary for the entry into or the performance of a contract; or
- Authorised by domestic law applicable to the controller; or
- Based on the individual's explicit consent.

In all cases you have the right to request a human review of any fully automated decision.

16. Making an information rights request

If you wish to exercise any of the rights set out above, please contact us at the above address.

Please provide us with as much information as you can as this will help us process your request as quickly as possible. We may need to request specific information from you to help us confirm your identity. 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.

You will not normally be required to pay a fee to access your personal data, or to exercise any of your other information rights, however we may charge a reasonable fee if your request is considered as manifestly unfounded, repetitive, or excessive. Alternatively, we may refuse to comply with your request in these circumstances. We will advise you as soon as possible if this is the case and explain our reason why.

We will provide you with an outcome to your request within one calendar month. In certain circumstances we can extend the time period to respond to your request by a further two calendar months. This will be when the request is complex, or we have received a number of requests from you. We will inform you as soon as possible if we are extending the time limit and provide an explanation why.

17. Lawful basis explained

Lawful Basis	Meaning
"Legitimate Interest"	Means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. 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 for our legitimate interests. 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). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.
Performance of "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.
Comply with a "legal or regulatory obligation"	Means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

18. Changes to the privacy policy and your duty to inform us of changes

We may update our privacy policy from time to time, the updated privacy policy will be published on our website. It is important that you visit our website regularly to stay informed as to how we process your personal data and to understand your information rights under the Data Protection Act 2018 and the UK General Data Protection Regulation, UK GDPR.

It is also important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

19. Information Commissioner

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk or call them on 0303 123 1113). However, we would appreciate the opportunity to deal with your concerns

before you approach the ICO. Please contact our data protection officer at: GB Bank, 73 Brook Street, Mayfair, London W1K 4HX.

This version of our privacy policy was last updated November 2024.