

Frasers Plus Privacy Policy

Powered by Tymit

Introduction

This policy explains when and why we collect personal information about you, how we use it, the conditions under which we may disclose it to others and how we keep it secure. Tymit is committed to safeguarding the privacy of your information. By “your data,” “your personal data,” and “your information” we mean any personal data about you which you or third parties provide to us. We may change this policy from time to time, so please check this page regularly to ensure that you are happy with any changes.

Who we are

We are Tymit LTD (“we,” “our,” “us”) and operate under the name of Tymit. We are committed to protecting and respecting your privacy.

Tymit Ltd has partnered with Frasers Group Financial Services (Third Party Partner) to provide the Frasers Plus credit product. Tymit Ltd are the regulated lender for Frasers Plus, this means we are authorised to make, or take assignments of, regulated consumer lending as part of our regular business activities.

Tymit is the “data controller” for the Frasers Plus product, which means we retain and process the personal data you make available when applying for and using the Fraser Plus facility. This allows us to provide you with credit and service your agreement.

Tymit is also the “data processor” for the Frasers Plus Loyalty Programme, which means with your expressed consent, we will collect and share personal data such as your marketing preferences and information about your spending with Frasers Group Financial Services. Frasers Group Financial Services “they,” “them,” “their”]] act as data controller for relationship management, marketing, maintenance, and product development of the loyalty programme.

As the data controller and processor for the Frasers Plus product, Tymit are registered with the Information Commissioner's Office, registration number: ZA522915.

As the data controller for the Frasers Plus loyalty programme, Frasers Group Financial Services are registered with the Information Commissioner's Office under registration number Z6552731.

For more information about how Frasers Group use your personal information, view their [Privacy Notice](#).

*All links open in a new window; please note we cannot be responsible for the content of external websites.

If you have any questions about your personal information email us at privacy@tymit.com.

Information we collect about you

Tymit will request and process personal and/or special category information to deliver the Frasers Plus product and have the obligation to use personal data fairly and lawfully whilst ensuring it is kept secure. Individuals about whom the data relates to are referred as “data subjects.”

“Personal data,” or “personal information,” means any information we hold about you from which you can be identified. It does not include data where your identity has been removed (anonymous data).

We may collect, use, store and share different types of personal data about you to provide you with our products and services, such as:

- Identifiable information includes first name, last name, username or similar identifier, title, job title, date of birth, gender and visual or other identifiers (for example, photo on ID and photo for identification verification purposes).
- Contact Data includes billing address, email address and telephone numbers.
- Financial information includes salary, bank statements, financial accounts and credit referencing information.
- Technical Data 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 our app.
- Profile Data includes your username and password, the products, or services you have purchased from us, your interests, preferences, feedback, survey responses, and social media data including usernames/handles that you share with us.
- Usage Data includes information about how you use our products, and services.
- Marketing and Communications Data includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We may also collect, use, and share Aggregated Data such as statistical or demographic data for any purpose. Aggregated Data could be collected from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific app feature. 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.

Generally, we do not collect any Special Categories of personal data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data), but some sensitive data may occasionally be disclosed to us during your relationship with us that we may need to process to manage your agreement effectively. For example, a health condition that affects the way we communicate with you. If this is the case, we will ask you for your explicit consent to store, share and process this information and take additional measures to safeguard it.

How your personal information collected

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

- Direct interactions. You may give us your Identity, Contact and Financial Data by filling in forms (electronically or otherwise), or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:
 - apply for the Frasers Plus Product and our services.
 - upload content/documents onto our Site.
 - subscribe to our services or publications.
 - register for our newsletter.
 - request marketing to be sent to you; or
 - give us feedback or contact us.

- Automated technologies or interactions. As you interact with our Site or with us via the app, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. We may also receive Technical Data about you or your equipment, browsing actions and patterns if you visit other websites employing our cookies.
- Third parties or publicly available sources. We will receive personal data about you from various third parties (including public sources) as set out below:
 - Technical Data from parties such as analytics providers such as Google and Amazon Web Services which may be based outside the UK and/or the EU.
 - Financial data from Identity, Financial and Contact Data from credit reporting agencies such as Experian PLC.
 - Identity and Contact Data from publicly available sources such as Companies House and the Electoral Register based inside the UK.
 - Cifas, a not-for-profit fraud prevention membership organisation managing the largest database of instances of fraudulent conduct in the UK.
 - Regulatory Data Corp Inc which provides services relating to anti-money laundering, KYC (know your customer) compliance and identification of politically exposed persons.

How we use your personal information

We will only use your personal information for the specified purposes for which it was intended. Most commonly, we will rely on the following legal basis when we use your personal data:

- Contractual Necessity Where we need to perform the contractual obligations we are about to enter or have already entered with you.
- Legitimate Interest 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.
- Legal Obligation Where we are subject to regulation or national law enforcement, we may process your data to meet our legal and regulatory requirements.
- Consent Where we may ask you for your specific consent to process your data for specific purposes such as providing your marketing preferences to Frasers Group Financial Services.

You have the right to withdraw your consent at any time and can do so by opting out of future marketing materials as they arrive, via the Frasers Plus app or by emailing privacy@tymit.com.

Purposes for which we will use your personal data

We collect your personal information to:

- Make assessments of your eligibility for our products and services
- Make responsible lending decisions in accordance with our principles and regulatory obligations.
- Identify you and verify the personal data you have provided, including any other applications you make in the wider Tymit product range, to prevent fraud and identity theft.
- Satisfy our Financial Crime and Anti-Money Laundering obligations.
- Provide, process and service your Frasers Plus account.
- Provide you with access to, and use of our Frasers Plus app and other services.
- Process payments and manage transactions.
- Provide information to, and receive information from, Credit Referencing Agencies
- Debt tracing and recovery.

- Communicating with you about our products and services.
- Communicating with you about your account.
- Call recording for training and monitoring purposes.
- For direct marketing of other products and services that are aligned with the original purpose for which we initially collected the information.
- Enhance, modify, personalise, or otherwise improve our services and communications.

Who we share your personal information with

We may share your personal information with the following:

- Within the wider Tymit platform.
- The Frasers Group and all its subsidiaries.
- Any other third-party organisation we rely on to provide and service the Frasers Plus product.
- Any third party you give us explicit permission to share it with.
- Any authorities or regulators we are required to disclose your personal data to in compliance with laws or regulations.
- To enforce our Terms and Conditions or other agreement clauses.
- When there is a need to protect our rights, property, or safety, or that of our customers, or others.

We require all third parties to respect the security of your personal data and to treat it in accordance with the standards of data protection regulation. We do not allow our third-party service providers 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.

How Frasers Group Financial Services use your personal data

When you apply for the Frasers Plus product, your data will be processed by Tymit as the credit provider and service provider of the Frasers Plus app. Tymit will also store data about marketing preferencing and spending habits and share it with Frasers Group Financial Services for use in providing their loyalty programme and tailoring rewards and offers to you.

For more information about how Frasers Group Financial Services use your personal information use your personal information, view their [Privacy Notice](#).

*All links open in a new window; please note we cannot be responsible for the content of external websites.

Marketing Consent

Direct marketing

Tymit will not use your personal data to send you any marketing communications or materials. With your consent, we will share your preferences with Frasers Group Financial Services for marketing purposes and to manage and maintain the Frasers Plus Loyalty Programme.

We will ensure you are provided with enough information on the options available to you regarding certain personal data uses, to allow you to make your own informed choice prior to providing your consent.

Third-party marketing

We will get your express consent via a clear and affirmative act, freely given by you, (such as an 'opt-in' box) before we share your personal data with any third party or partner for marketing purposes.

Opting out

You can request for Frasers Group Financial Services to stop sending you marketing messages at any time by following the opt-out links on any marketing communications sent to you, or by contacting us at any time to exercise your right to object and withdraw your consent.

Where you opt out of receiving marketing messages, this will not apply to personal data you provided to us as a result of a product/service purchase, product/service experience or other transactions.

If you choose to object to the communications, unsubscribe or withdraw your consent, this will not make our processing of your personal data before you withdrew your consent unlawful.

Cookies and other similar technologies

You can set your devices to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of our app or Site may become inaccessible or not function properly. For more information about the cookies and other similar technologies we use, please see our [Cookie Policy](#).

Change of purpose

We will only use your personal data for the purposes for which we collected 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.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis 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.

Automated decision-making

Automated decisions are made by technological means, mostly based on algorithms subject to predefined criteria. Such automated decision-making, taken solely by technological means without any human intervention, may have legal effects or similarly significant effects on you.

By using our Site and/or our services, you are giving us your explicit consent to make automated decisions. If you do not consent to us making automated decisions, you must not use our Site or services.

Our Site may use your personal data to make decisions entirely or partially based on automated processes according to the purposes outlined in this privacy policy. Our Site adopts automated decision-making processes as far as necessary to enter or perform a contract between you and us (where you are looking to be our customer), or for our legitimate interests or based on your consent where consent is required by the law.

The rationale behind the automated decision-making is:

- so that we can assess whether it is suitable for us to offer our services/products to you (for example, in determining your credit worthiness).

- to enable or improve the decision-making process.
- to grant you fair and unbiased treatment based on consistent and uniform criteria.
- to reduce the potential harm derived from human error, personal bias and the like which may potentially lead to discrimination or imbalance in the treatment of individuals etc; or
- to reduce the risk of you failing to meet your obligation under your contract with us.

Your rights as a result of automated decision-making

Where you are subject to automated decision-making processes, you are entitled to exercise specific rights aimed at preventing or limiting the potential effects of the automated decisions taken.

In particular, you have the right to:

- obtain an explanation about any decision taken as a result of automated decision-making and express your point of view regarding such decision.
- challenge such a decision by asking us to reconsider a decision or take a new decision on a different basis; or
- request for human intervention to review your application if we decline it.

Please contact us if you want to find out more about the purposes and/or the third-party services we use which makes automated decisions (if any), and any specific rationale for automated decisions used within our Site.

How do we work with Credit Reference Agencies

To process your application, we will perform credit and identity checks on you with one or more credit reference agencies ("CRAs"). Where you take services from us, we may also make periodic searches at CRAs to manage your account with us. To do this, we will supply your personal information to CRAs, and they will give us information about you. This will include information from your credit application and about your financial situation and financial history. CRAs will supply to us both public (including the electoral register) and shared credit, financial situation and financial history information and fraud prevention information.

This information will be used for:

- Assessing your creditworthiness and whether you can afford to take the product.
- Verifying the accuracy of the data you have provided to us.
- Preventing criminal activity, fraud, and money laundering.
- Managing your account(s).
- Tracing and recovering debts.

Transferring and storing personal information to another country

We share your personal data within the Tymit Group. This may involve transferring your data outside the UK and/or the EU (as applicable).

Many of our selected and external third parties are based outside the UK and/or the EU so their processing of your personal data will involve a transfer and/or storage of personal data outside the UK and/or the EU.

Whenever we transfer your personal data out of the UK and/or the EU (as applicable), we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data.
- Where we use certain service providers outside of the UK and/or the EU (as applicable), we may use specific contracts approved for use in the UK and/or the EU (as applicable) which give personal data the same protection it has in the UK and/or the EU (as applicable).

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the UK and/or the EU.

Personal Information Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used, accessed, altered or disclosed in an unauthorised way. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a legitimate need to use it.

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.

Personal information Retention Periods

Tymit will only keep personal data for as long as necessary, for the purposes for which it was gained and only where we continue to have a legal basis for doing so. We will review the personal data we hold for our customers in line with our Storage and Retention policy, to check for accuracy and relevancy and to ensure we continue to have a legal basis for processing.

If the personal data is no longer necessary, or where we no longer have the legal basis for processing, we will delete or fully anonymise the data we hold for a customer, in line with our Data Protection Policy. If customer data becomes inaccurate, Tymit will update it accordingly. Otherwise, Tymit will retain personal data for the following periods:

Product/Process Name	Retention Period
Fraser's Plus Credit Account	6 years from the termination of the contract to which customer is a party.
All declined applications	6 years from date at which customer is informed of our decision to decline their application. We will cease contact 1 year after customer is informed of our decision unless we gain the customer's explicit consent to continue processing their data.
All cancelled applications	6 years from date at which customer is informed of our decision to approve their application. We will cease contact 1 year after customer is informed of our decision unless we gain the customer's explicit consent to continue processing their data.

Your Legal Rights

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

Request 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 and to check that we are lawfully processing it. In circumstances where your right to access some or all of your data could have adverse effects of the freedom of others or the law requires us not to comply with your request, we are within our rights to refuse your request to access your personal data.

Request correction of the personal data

This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data

This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with applicable law. 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.

Object to processing of your personal data

This allows you to object to us processing your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request 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:

- if you want us to establish the data’s accuracy
- where our use of the data is unlawful, but you do not want us to erase it.
- 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
- you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party

We will provide 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.

Withdraw your consent to process data

At any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before the you withdrew your consent. If you withdraw your consent, we may not be able to provide certain services to you. We will advise you if this is the case at the time you withdraw your consent.

Notification of changes to your data

We will notify everyone we have given your personal data to in circumstances where we amend, delete or agree to restrict our use of your personal data.

Request for human intervention

You may request human intervention to review your application where we have made a decision using automation and have declined your application.

If you wish to exercise any of the rights set out above, please contact us. Please note, we may not always be able to comply with your request because we:

- have a legitimate ground for using your personal data which overrides your rights and freedom; or
- we need to retain your personal data by law.

We are here to help if you have any further questions about privacy at Tymit or if you would like to raise a complaint as a result of how we have handled your personal data. Please contact us at: privacy@tymit.com.

You also have the right to make a complaint at any time to the Information Commissioner's Office ("ICO"), who is the UK supervisory authority for data protection issues at:

Information Commissioners Office: Wycliffe House, Water Lane, Wimslow, SK9 5AF.
Telephone number: 03031231113. Website: www.ico.org.uk.

We would appreciate the chance to deal with concerns before you approach the ICO so please contact us in the first instance.

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 could 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 to data requests

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

Complaints

We hope that our Data Protection Team can resolve any query or concern you may raise about our use of your personal information. The General Data Protection Regulation also gives you right to lodge a complaint with a supervisory authority, in the European Union (or European Economic Area) state where you work, normally live or where any alleged infringement of data protection laws occurred.

The supervisory authority in the UK is the Information Commissioner's Office (ICO). You also have the right to make a complaint at any time to the Information Commissioner's Office ("ICO"), who is the UK supervisory authority for data protection issues at:

Information Commissioners Office: Wycliffe House, Water Lane, Wimslow, SK9 5AF.
Telephone number: 03031231113. Website: www.ico.org.uk.

We would appreciate the chance to deal with concerns before you approach the ICO so please contact us in the first instance.

Other websites

Our website may contain links to other websites. This privacy policy applies only to our website, so we encourage you to read the privacy statements on any other websites you visit. We cannot be responsible for the privacy policies and practices of other sites even if you access them using links from our website.

Changes to this policy

Any material changes we make to our privacy policy in the future will be posted on this page and, if appropriate, sent to you by email.

How to contact us

If you have any questions about our privacy policy or the personal information which we hold about you or, please send an email to our Data Protection Team privacy@tymit.com.