Effective date: 5 August 2025

Algbra FS UK Limited

Business Customer Privacy Notice

Version 1

TABLE OF CONTENTS

1. ALGBRA PRIVACY NOTICE

1.1. Algbra FS UK Limited ("Algbra") is committed to protecting and respecting your privacy. This policy notice (together with our terms and conditions) aims to give you information on how Algbra protects, collects, shares and uses your personal information when you visit our website, the Algbra app or use any other Algbra service.

1.2. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it. It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data.

1.3. This Privacy Notice applies to Algbra's website and app and all products and services offered by Algbra and by using any of these, you are agreeing to the policies described herein.

1.4. This privacy notice supplements any other policies or notices you may be provided with and is not intended to override them.

1.5. For the purpose of this notice and unless otherwise stated:

- "you" or "Authorised Person" refers to the individual(s) who access, use and/or operate the business account provided by Algbra on behalf of the business, or to an Authorised Employee (as defined below) to the extent Algbra is the controller of such Authorised Employee's personal data. If multiple individuals are authorised to do so, this term refers to any, both or all of those individuals;
- "Authorised Employee" refers to an employee of the business, and the business has invited that employee to use the Algbra business account;
- "Authorised User" refers to any Authorised Person and/or Authorised Employee; and
- "business" refers to the company that holds the Algbra business account.

2. WHO WE ARE

2.1. For the purpose of the General Data Protection Regulation, the data controller is Algbra FS UK Ltd with the registered address of 22 Upper Brook Street London | W1K 7PZ. References in this privacy notice to "we" or "us" are references to the controller.

2.2. If you are:

- an Authorised Person, Algbra is the controller of the Authorised Person's personal data when we provide the business with the Algbra business account; and
- an Authorised Employee, the business that holds the Algbra business account the Authorised Employee is using is usually the main controller of the Authorised Employee's personal data. Authorised Employees who may have questions about the processing of their personal data in relation to an Algbra business account should reach out to their employer in the first instance. In some cases, Algbra may also be a data controller of such Authorised Employee's personal data. This can happen, for example, if we ask this person for identification documents and 'selfie' photos or videos for Know-Your-Business

("KYB") checks.

3. PERSONAL DATA PROCESS

3.1. Data protection laws primarily apply to individuals. While these laws generally do not extend to legal entities themselves (such as limited liability companies), they do apply to the individuals associated with those entities. When providing Algbra business products, we process personal data related to Authorised Users, and this notice describes that processing. We may also process personal data about other employees and customers of the business that receives the Algbra business products.

3.2. Personal data, or personal information, means any information about an individual from which that person can be identified.

3.3. We may collect, use, store and transfer different types of personal data about you which we have grouped together as follows:

3.3.1 Information you give us: This is information about you that you give us when you:

- fill in any forms;
- correspond with us;
- register for the business to use the Algbra app;
- open an account on behalf of the business or use any of our services on behalf of the business;
- take part in online discussions, surveys or promotions;
- speak or interact with a member of our customer support team (either on the phone or through the Algbra app or through any other means by which our services are made available);
- enter a competition; or
- contact us for other reasons.

We will collect the following information:

- Your name, address, and date of birth;
- Your email address, phone number and details of the device you use (for example, your phone, computer or tablet);
- The business's Algbra username (this is random and is automatically assigned to you when you first join but you will be able to change it), password and other registration information, as well as any username specific to you;
- Details of the business bank account you are associated with, including the account number, sort code and IBAN;
- Details of the business's Algbra debit cards and credit cards (or other debit or credit cards you have registered with us), including the card number, expiry date and CVC (the last three digits of the number on the back of the card);
- Identification documents (for example, your passport or driving licence), copies of any documents you have provided for identification purposes, and any other information you provide to prove you are eligible to use our services;
- records of our discussions, if you contact us or we contact you (including records of phone calls);

- your image in photo or video form, and facial scan data extracted from your photo or video (known as 'biometric data'), to verify your identity during onboarding as part of our KYB checks, to authenticate you as an authorised user of our services, or to detect and prevent fraud; and
- information about other people (such as the company's shareholders, directors, employees, customers or business partners) where we are legally required to ask for such information (for example, as part of KYB checks or under anti-money laundering laws to verify the business's sources of funds).

If you provide personal data about anyone other than yourself, including business shareholders and directors, the Authorised Users to whom the business grants access to the Algbra business account, a payment counterpart, a friend you have recommended or any other person who has a relevant relationship with Algbra (a "connected person"), **you confirm on behalf of the business that it has their agreement or is otherwise entitled to provide this information to us and that they understand how we will use their personal data. That includes bringing this notice to their attention if legally necessary.**

3.2.2 Information about how you use the Algbra business account: When you use the Algbra business account, we get information about how you use the account on behalf of the business, any transactions made using the account, and your device (as explained below).

3.2.3 Information from your device: Whenever you use our website or the Algbra app or any of our products and services, we may collect the following information:

- Technical information, including the internet protocol (IP) address used to connect your computer to the internet, your log-in information, the browser type and version, the time-zone setting, the operating system and platform, the type of device you use, a unique device identifier (for example, your device's IMEI number, the MAC address of the device's wireless network interface, or the mobile phone number used by the device), mobile network information, your mobile operating system, the type of mobile browser you use.
- Information about your visit, including the links you have clicked on, through and from our site (including date and time), services you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling and clicks), and methods used to browse away from the page.
- Information on transactions (for example, payments into and out of your account), including the date, time, amount, currencies, exchange rate, beneficiary details, details of the merchant or ATMs associated with the transaction (including merchants' and ATMs' locations), IP address of sender and receiver, sender's and receiver's name and registration information, messages sent or received with the payment, details of device used to arrange the payment and the payment method used.
- Information stored on your device, including if you give us access to contact information from your contacts list. The Algbra app will regularly collect this information in order to stay up to date (but only if you have given us permission).

3.2.4 Information from your employer: Where a business that holds an Algbra business account nominates you as an Authorised User, your employer will give us information about you. Typically, this will include your name and business contact details. In some cases, it may also include your employment status, salary details and tax information (for example, if your employer uses the account to administer its payroll).

3.2.5 Other types of data we collect/do not collect:

- If you are a "connected person" for an Algbra business customer, then that Algbra business customer may provide your personal data to us. For instance, if you're a payment beneficiary, data shared with us could include your name, account details, email, and additional verification information if necessary for fulfilling our legal obligations or requested by the recipient bank, or if you are an ultimate beneficial owner (UBO) data may include your name, date of birth, country of residence and a copy of your identity documents.
- 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.
- We collect personal data from third parties, such as official registers and databases, fraud prevention agencies or partners who help us to provide services, and occasionally publicly available information about you from social medial websites or apps to carry out enhanced due diligence checks.
- We do not collect any special categories of personal data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, political opinions, trade union membership, information about your health and genetic and biometric data).

4. WHAT ARE OUR PURPOSES AND LEGAL BASES FOR USING YOUR PERSONAL DATA?

We collect and process your personal data for the following purposes and legal bases:

Purposes	Legal basis	Explanation
To carry out the contract we have with the business	Contract necessity	We need certain personal data to provide our services, e.g. to make or receive payments, and cannot provide them without this personal data
To comply with our legal obligations to which we are subject	Legal Obligations	Where we have a legal obligation to process your personal data to comply with laws and regulations (such as collecting identification documents to comply with anti-money laundering laws)
To protect your interest or perform a task carried out in the public interest	Substantial public interest	We process your personal data to adhere to government

		regulations or guidance, such as our obligation to prevent fraud or to provide support if you are a vulnerable person
Where you have consented us to	Consent	Where you have given us your consent to process your data
Where we have a legitimate reason to process your personal data that is reasonable when balanced against your rights and interests	Legitimate interests	We may use your personal data to understand how our services are used by you so we can improve them

5. HOW WE USE YOUR PERSONAL DATA?

Examples of the purposes for which we may process your personal data include:

What we use your data for	The legal basis for doing so
To determine if the business is eligible for our services or products, and to verify your identity When a business signs up with Algbra, we carry out KYB checks to verify your identity or any other Authorised User's identity during onboarding in order to comply with anti-money laundering laws. This may include facial scan data extracted from any photo or video you submit ('biometric data').	Legal obligations Consent Substantial public interest
To provide our products and services to the business We use your data as necessary to provide the business with the Algbra services requested, including meeting our contractual and legal obligations, showing the geographic location of the business and/or helping you understand the business's usage and spending behaviour.	Contract necessity Legal obligations
For customer service and monitoring We use your data to provide you and/or the business with customer service support services, and to monitor or record any communications between you and us, including phone calls, for training and quality purposes.	Legitimate interests. It is in our legitimate interests to monitor service quality
To offer better support We use your data to help us identify if you and/or the business may need extra support. For instance, if we spot signs of vulnerability, we can offer better support.	Substantial public interest (if we process your sensitive personal data to keep to legal requirements that apply to us or to safeguard the economic well-being of certain individuals)

What we use your data for	The legal basis for doing so
To ensure account safety, including protecting you and/or the business against fraud We use your personal data to prevent, detect, or protect against actual or suspected fraud, unauthorised transactions, claims, liability, and financial or other crimes. In some cases this may include collecting biometric data.	Legal obligations Consent (for biometric data collection) Substantial public interest Legitimate interests (to develop insights and improve how we deal with financial crime)
Marketing and analytics We use your data to: • personalise your in-service experience and marketing messages about our products and services, including by sending alerts, updates, event invitations; • measure or understand the effectiveness of our advertising and how you use our products, services and your transactions; and • if you agree, we also provide you with information about other similar products and services we offer which we feel may interest you and/or the business.	Consent (where we are legally required to get your consent to send you direct marketing) Legitimate interests (to ensure our direct marketing is relevant to your and/or the business's interests, develop our services, and improve our efficiency about how we meet our legal and contractual duties)
To keep our services up and running, and ensure they are continually improving We may use your data to: • administer our services and internal operational, planning, audit, troubleshooting, data analysis, testing, statistical, and survey purposes; • undertake system or product development, including helping third party suppliers improve the services they provide to us and/or you and/or the business; • authenticate you as an Authorised User of our services when necessary; • tell you about changes to our services; • help keep our website, app and other platforms safe and secure; and • improve our services and ensure that they are presented in the most effective manner. This may include using Artificial intelligence ('AI') to improve our efficiency and effectiveness of our services and our financial crime prevention strategies.	Legitimate interests. It is in our legitimate interests to maintain, develop and improve our services Contract necessity Consent (where required by law)

What we use your data for	The legal basis for doing so
To comply with our legal, regulatory and risk management obligations, including helping detect or prevent crime; establishing, exercising or defending legal claims; protecting our rights, IP and products; investigating, managing and resolving complaints; and preventing and/or managing incidents of abusive or aggressive behaviour towards our employees We may also use your data to: • share it with other organisations (for example, government authorities, law enforcement authorities, tax authorities, fraud prevention agencies); • inform you or the business about our services, e.g. updates to the business account's terms and conditions; and • to take steps in relation to amounts owed to us including taxes, debts or damages from the business. For instance, if the business has a negative balance in its business account, we may allow a third party that incorrectly sent it money to recover the money sent in error to enforce our terms and conditions with the business. Sometimes, we are legally required to ask you to provide information about other people. For example, we might ask you to explain: • your relationship with somebody who pays money into the Algbra business account; and/or • how somebody got the money in the first place to pay it into the Algbra business account. If you, or the business, give us personal data about other people, it is your and the business's responsibility to ensure they understand how we will process their personal data.	Legitimate interests (for example, to protect us during a legal dispute or send you anti-fraud communications) Legal obligations Consent (where we are required to collect your consent by law)

6. COOKIES AND USE OF OUR WEBSITE

6.1. Our websites may use tools such as Google Analytics, a service provided by Google, Inc. that tracks and reports on the manner in which our websites are used. Google Analytics does this by placing small text files called "cookies" on your computer or other device. Cookies collect information about the number of visitors to the websites, the pages visited

and the time spent on the website.

6.2. You can set your browser 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 website may become inaccessible or not function properly.

6.3. Please read our Cookie Policy for more information about cookies. It is available here: https://www.algbra.com/cookies-policy/.

7. EMAILS

We may use your name and e-mail address(es) obtained from you to send you alerts, updates, event invitations and other information by e-mail. If you wish to receive marketing communications from us you have to opt-in to marketing communications. If you no longer wish to do so, you may unsubscribe at any time by following the link included in these e-mails.

8. SHARING YOUR PERSONAL INFORMATION WITH THIRD PARTY ORGANISATIONS

8.1. We may disclose your personal information:

8.1.1 to other Authorised Users to whom the business has granted access to its Algbra business account;

8.1.2 to beneficiaries whom may receive limited information when you initiate a payment transaction on behalf of the business;

8.1.3 in the event that we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets;

8.1.4 if Algbra substantially or all of its assets are acquired by a third party, in which case personal data held by us will be one of the transferred assets;

8.1.5 if we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply our terms of use and other agreements; or to protect the rights, property, or safety of Algbra, our customers, or others;

8.1.6 to fraud prevention agencies who will use it to prevent fraud and money-laundering and to verify your identity. If fraud is detected, you could be refused certain services, finance, or employment. Further details of how your information will be used by us and these fraud prevention agencies, and your data protection rights, can be found in Appendix 1 of this document;

8.1.7 in the event that we need to contact credit reference agencies for the purpose of assessing your credit score where this is a condition of us entering into a contract with the business;

8.1.8 if required by professional advisers including lawyers, bankers, auditors and insurers

some based UK and some based outside EEA, who provide consultancy, banking, legal, insurance and accounting services; necessary to the performance of our contractual obligations to the business;

8.1.9 if we are under a duty to HM Revenue & Customs, fraud prevention agencies, regulators and other authorities based in the United Kingdom who require reporting of processing activities in certain circumstances;

8.1.10 if we engage with companies we have a joint venture or agreement to co-operate with; or

8.1.11 where requested by the person or companies you ask us to share your data with. For example, where you ask us to transfer money to a person or a company on behalf of the business, we may need provide the recipient with certain of your details alongside your payment. Where receiving money on the business's behalf, we may provide the payer with your details (e.g. your name and the IBAN of the Algbra business account).

8.2. We will also share your personal data with our group companies, as well as our partners and our suppliers who help to provide our services to you. The table below explains which suppliers we normally share your personal data with:

Type of supplier	**Why we share your personal data**
Suppliers who provide us with IT, artificial intelligence, payment and delivery services	To help us provide our customer services to you and support operational efficiency and risk management
Our banking and financial services partners and payments networks, including Visa and Mastercard	To help us provide our services to you and/or the business. This includes banking and lending partners, banking intermediaries and international payment service providers
Identity verification, KYB service providers, sanction screening and transaction monitoring	To help us verify your identity before onboarding and ensure compliance with the applicable AML/CTF laws
Card manufacturing, personalisation and delivery companies	To create and deliver your personalised Algbra card
Analytics providers and search information providers	To help us improve our website or apps
Customer-service providers, survey providers and developers	To help us to improve our services to you and/or the business

8.3. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Notice and our Cookie Policy; and that those we share data

with adhere to similar exacting standards.

9. TRANSFER OF PERSONAL DATA OUTSIDE OF THE UK

9.1. Although we are a business based in the UK, due to the international nature of Algbra's operations and for the purposes of providing the services to you (for example, if you make an international payment, we will send funds to banks outside of the UK), any personal information that we hold and the data we collect from you may be transferred to, and stored at, a destination outside the UK for the following purposes:

- keep to global legal and regulatory requirements;
- provide ongoing support services;
- fraud prevention agencies, regulators or law enforcement authorities; and/or
- enable us to provide you with products or services you have requested.

If we transfer your personal data to another country that doesn't offer a standard of data protection equivalent to the United Kingdom or EEA, we will make sure that your personal data is sufficiently protected. For example, we'll make sure that a contract with strict data protection safeguards is in place before we transfer your personal data. In some cases, you may be entitled to ask us for a copy of this contract.

9.2. By submitting your personal data, you agree to this transfer, storing and processing by us. We will take all steps reasonably necessary to ensure that such transfers comply with applicable data protection law and that your data is treated securely and in accordance with this Privacy Notice and our Cookie Policy. This may include entering into data transfer agreements with recipients.

10. DATA ABOUT THIRD PARTIES

If, and to the extent, you provide personal data relating to any third party to us, you confirm that they have appointed you or the business (on whose behalf you act) to act on their behalf, you or the business (on whose behalf you act) has obtained their consent to pass their personal data to us and for us to process that personal data in the manner and for the purposes described in this Privacy Notice.

11. HOW WE RETAIN YOUR DATA

11.1. We will only retain your personal data 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.

11.2. We are required to keep certain personal data for specified time periods by KYB, anti-money laundering, banking and e-money laws. These time periods vary from country to country. For example, if you use Algbra services in the United Kingdom, we will keep personal data for no more than 7 years after our agreement ends.

12. YOUR RIGHTS

12.1. Under UK data protection laws, you have rights as an individual which you can exercise

in relation to the information we hold about you. You are entitled to ask for details of the personal data we hold about you and how we process it and to receive a copy of your personal data. You may also have your data rectified or deleted, restrict our processing of that information, and object to the processing of your personal data. You may also choose to withdraw your consent. You can read more about these rights here: https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly/

12.2. If you are an Authorised Employee or a customer of a business that holds an Algbra business account, the business, rather than Algbra, is primarily responsible for helping you with your request.

12.3. You have the right to be told about how we use your personal data

- We provide this Privacy Notice to explain how we use your personal data.
- If you ask, we will provide a copy of the personal data we hold about you. We can't give you any personal data about other people, personal data which is linked to an ongoing criminal or fraud investigation, or personal data which is linked to settlement negotiations with you. We also won't provide you with any communication we've had with our legal advisers.

12.4. You can ask us to correct your personal data if you think it's wrong. You can have incomplete or inaccurate personal data corrected. Before we update your file, we may need to check the accuracy of the new personal data you have provided.

12.5. You can ask us to delete your personal data if:

- there's no good reason for us to continue using it;
- you gave us consent (permission) to use your personal data and you have now withdrawn that consent;
- you have objected to us using your personal data;
- we have used your personal data unlawfully; or
- the law requires us to delete your personal data.

12.6. We may in some cases not be able to agree to your request for us to delete certain of your personal data. As a regulated financial services provider, we must keep certain customer personal data even if you ask us to delete it (we've explained this in more detail below). If the business has closed its Algbra account, we may not be able to delete its entire file because our regulatory responsibilities take priority. We will always let you know if we can't delete your information.

12.7. You can object to us processing your personal data for marketing purposes and can tell us to stop using your personal data for marketing.

12.8. You can object to us processing other personal data (if we are using it for legitimate interests)

- If our legal basis for using your personal data is 'legitimate interests' and you disagree with us using it, you can object.
- However, if there is an overriding reason why we need to use your personal data, we

will not accept your request.

- If you object to us using personal data which we need in order to provide our services, we may need to close the business account as we won't be able to provide the services.

12.9. You can ask us to restrict how we use your personal data. You can ask us to suspend using your personal data if:

- you want us to investigate whether it is accurate;
- our use of your personal data is unlawful but you do not want us to delete it;
- we no longer need the information, but you want us to continue holding it for you in connection with a legal claim; or
- you have objected to us using your personal data (see above), but we need to check whether we have an overriding reason to use it.

12.10. You can ask us to transfer personal data to you. If we can, and the regulatory requirements that apply to us allow us to do so, we will provide your personal data in a structured, commonly used, machine-readable format.

12.11. You can withdraw your permission

- If you have given us any consent we need to use your personal data, you can withdraw your consent at any time by changing your privacy settings in the Algbra app or otherwise contacting us through the provided channel.
- You can ask us to carry out a human review of an automated decision we make about you. If we make an automated decision about you that significantly affects you, you can ask us to carry out a manual review of this decision.
- Your ability to exercise these rights will depend on a number of factors. Sometimes, we will not be able to agree to your request (for example, if we have a legitimate reason for not doing so or the right does not apply to the particular information we hold about you).

12.12. How do I exercise my rights?

- To exercise any of your rights set out in the previous section, you can contact us via the Algbra app or any other channels provided to you.
- For security reasons, we can't deal with your request if we are not sure of your identity, so we may ask you for proof of your ID.
- Algbra will usually not charge you a fee when you exercise your rights. However, we are allowed by law to charge a reasonable fee or refuse to act on your request if it is manifestly unfounded or excessive.
- If you are unhappy with how we have handled your personal data, you can complain to your local data protection authority. In the United Kingdom, this is the ICO (see here: https://ico.org.uk/make-a-complaint/).

12 CHANGES TO OUR PRIVACY NOTICE

Any changes we may make to our Privacy Notice in the future will be posted on this page and/or, where appropriate, notified to you.

13 CONTACT

13.1 Questions, comments and requests regarding this privacy notice are welcomed and should be addressed to:

Algbra FS UK Limited
Registered Address: 22 Upper Brook Street, London, W1K 7PZ
Tel: 44 0 808 258 4888
Email: info@algbra.com

Appendix 1

Fair Processing Notices for the National Fraud Database

GENERAL

1. Before we provide services, goods or financing to you and/or the business, we 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.
2. 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.
3. Details of the personal information that will be processed include, for example: name, address, date of birth, contact details, financial information, employment details, device identifiers including IP address and vehicle details.
4. We and fraud prevention agencies may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime
5. We process your personal data on the basis that we have a legitimate interest in preventing fraud and money laundering, and to verify 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 services or financing you have requested.
6. 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.

AUTOMATED DECISIONS

7. As part of the processing of your personal data, decisions may be made by automated means. This means 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. You have rights in relation to automated decision making: if you want to know more please contact us using the details above.

CONSEQUENCES OF PROCESSING

8. If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to provide the services or financing you have requested, or to employ you, or we may stop providing existing services to you.
9. A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services, financing or employment to you. If you have any questions about this, please contact us on the details above.

DATA TRANSFERS

10. 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.

YOUR RIGHTS

11. Your personal data is protected by legal rights, which include your rights to object to our processing of your personal data, request that your personal data be erased or corrected, and request access to your personal data.
12. For more information or to exercise your data protection rights, please contact us using the contact details above.
13. You also have a right to complain to the Information Commissioner's Office, which regulates the processing of personal data.