IKIGAI PRIVACY POLICY

Welcome to Ikigai Invest Services Ltd's ("**Ikigai**") privacy policy ("**Privacy Policy**").

Ikigai respects your privacy and is committed to protecting your personal data. This Privacy Policy will inform you as to how we look after your personal data when you:

- Visit our website www.ikigai-invest.com ("**Site**");
- Open an account with Ikigai ("**Ikigai Account**");
- Use our Ikigai mobile application ("**App**") once you have downloaded a copy of the App onto your mobile telephone or handheld device in connection with your Ikigai Account;
- Use any of the services accessible through the App or the Site (the "**Services**"); and

tell you about your privacy rights and how the law protects you.

1. Important information and who we are

1.1. Purpose of this Privacy Policy

This Privacy Policy aims to give you information on how Ikigai, the Ikigai prepaid debit card issuer, PayrNet Limited ("**PayrNet**"), the Ikigai digital wallet technology provider Railsbank Technology Ltd ("**Railsbank**") and the Ikigai custody provider, Third Platform Services Limited ("**TPS**"), collect and process your personal data through your use of our Site or App, including any data you may provide through our Site or App when you subscribe to our Services pursuant to the Ikigai Terms & Conditions, search for a product, take part in a competition, promotion, or survey or sign up to our newsletter or waiting list.

Our Site and App are not intended for children and we do not knowingly collect data relating to children.

It is important that you read this Privacy Policy together with any other privacy policies or fair processing notices 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. This Privacy Policy supplements the other notices and is not intended to override them.

1.2. Purpose of this Privacy Policy

Ikigai is the controller and responsible for your personal data (also referred to as "we", "us" or "our" in this Privacy Policy) that is generated in connection with your Ikigai Account on our Site and our App and in any contact we have with you, throughout the course of our relationship.

PayrNet, Railsbank and TPS are partners of Ikigai ("**Partners**"). All details about how the Partners will hold and process your data are set out in paragraph 11 of this Privacy Policy.

Ikigai has appointed a data protection officer ("**DPO**") who is responsible for overseeing questions in relation to their processing of personal data in accordance with this Privacy Policy. If you have any questions about this Privacy Policy, including any requests to exercise your legal rights. Please contact the DPO using the details set out below.

1.3. Contact details

Our full details are:

Full name of legal entity: Ikigai Invest Services Ltd

Name or title of DPO: Data Protection Officer for Ikigai Invest Services Ltd

E-mail address: privacy@ikigai-invest.com

Postal address: 41 Corsham Street, N1 6DR, London, UK

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

1.4. Third-party links

Our App and our Site may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our App or our Site, we encourage you to read the privacy policy of every website you visit our website application you use.

2. The data we collect about you

Personal data, or personal information means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

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

Identity Data includes your full name, username or similar identifier, date of birth, gender, nationality, personal description, photograph, video and photograph or video of your identification documents (for example a passport or a driving licence).

Contact Data may include contact address, email address and telephone numbers.

Contractual Data includes details about the contractual agreement we have in place with you.

Data on relationships with legal entities includes data submitted by you or obtained from public registers or through third party on representatives, directors and beneficial owners of a legal entity subscribing to our Services.

Financial Data includes information related to your Ikigai Account, the related debit card(s), your goals and investments made via Ikigai, their performance and your answers to the financial personality test available in the app.

Transaction Data includes details about the use of your Ikigai Account, debit card(s) and other details of products and Services you have obtained from us.

Due Diligence Data includes information we are required by law to process about you to comply with our obligations in relation to illegal activities involving money (for example, fraud, money laundering and terrorist financing) or in compliance with international sanctions, which processing data about the origin of funds and/or transaction parties, the purpose of our business relationship, account usage behaviour, political exposed status (i.e. are you a politically exposed person or PEP).

Technical Data includes Internet Protocol (IP) address, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, your login data, unique device identifier (for example, the IMEI number of any device you use to access our Site and/or App ("**Device**"), the MAC address of the Service's wireless network interface, or the mobile phone number used by the Device) and other technology on a Device.

Locational Data includes information about your geographical location, this information may be provided by your mobile phone, the address where you connect a Device to the internet (internet protocol (IP) address), or a shop, where you buy something with the pre-paid card associated with your Ikigai Account ("**Ikigai Card**").

Contractual Data includes details about the products and Services we provide to you and the terms under which we provide these.

Usage Data includes information about how you use our Site, App, products and Services.

Marketing and Communications Data includes your preferences in receiving marketing communications from us and our third parties, your communication preferences and what we learn about you in relation to marketing from letters, emails and conversations between us.

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 Site and/or 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.

Some of the personal data we collect is classified as **Special Categories of Personal Data** (also known as sensitive personal data, for further details see the Glossary in section 10). In particular, we may process personal data that relates to biometric data (voice and face recognition only) and any criminal convictions and offences. Where we process such sensitive personal data (for example, during video calls and recordings of

phone conversations or when we are collecting Due Diligence Data), we will usually do so on the basis that it is necessary for reasons of substantial public interest, to meet regulatory requirements relating to unlawful and dishonest acts, to establish, exercise or defend any legal claims, or in some cases, with consent. In any case, we will carry out the processing in accordance with applicable laws.

2.1. If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with products or Services (i.e. access to our Site or App)). 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 the time.

3. How is your personal data collected?

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

Direct interactions. You may give us your Identity, Contact, Financial and Due Diligence Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:

- download or register the App
- create an Ikigai Account on our App;
- enter into any transactions via the App;
- subscribe to our Service or publications;
- apply for our products or Services (including but not limited to answering the financial personality test or creating an investment goal);
- request marketing to be sent to you;
- enter a competition, promotion or survey;
- use social media functions on our Site or App; or
- communicate with us via email, on-line chat, and/or phone call or give us some feedback.

Automated technologies or interactions. As you interact with our Site and/or App, we may automatically collect Technical Data about your equipment like the type of Device you use, your Device's operating system, browsing actions and patterns, App activity and version. We collect this personal data by using cookies, App session logs and other similar technologies. We may also receive Technical Data about you if you visit other websites and/or apps employing our cookies. Please see our Cookie Policy for further details.

Third parties or publicly available sources. We work closely with third parties who may provide us with Identity, Contact and Due Diligence Data (including, for example, business partners based inside and outside the UK and EU, sub-contractors in delivery services and advertising networks based inside and outside the UK and EU, analytics providers based inside and outside the UK and EU, search information providers such as Google based outside of the UK and EU, fraud prevention agencies based inside and

outside the UK and EU, customer service providers based inside and outside the UK and EU, social media organisations such as Facebook or Twitter based outside of the UK and EU). We will also receive Identity, Contact and Due Diligence Data about you from third parties we use to screen you for PEP status, screen sanctions lists, perform criminal history checks and verify your identity based inside and outside the EU.

Technical Data from the following parties:

- analytics providers such as Google and Branch Metrics Inc based outside the UK and EU;
- advertising networks such as Google based outside the UK and EU; and
- search information providers such as Google based outside the UK and EU.

Identity, Contact, Diligence, Financial and Transaction Data from providers of technical and payment services (including domestic, European and international payment systems), such as SWIFT based inside and outside of the UK and EU.

Identity, Contact Data and Due Diligence Data from publicly available sources such as Companies House and the Electoral Register based inside the EU.

4. How we use your personal data

We will only use your personal data when the law allows us to do so. 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 in our legitimate interests to detect, prevent and investigate fraud, money laundering, terrorist financing and other crimes.
- Where we need to comply with a legal or regulatory obligation, for example, to cooperate with our regulators and/or law enforcement bodies.
- In the case of Special Categories of Personal Data, where processing of such data is in the substantial public interest (for example, for us to comply with our regulatory requirements).

Generally, we do not rely on consent as a legal basis for processing your personal data other than in relation to certain marketing activities. You have the right to withdraw consent to marketing related processing at any time by visiting the settings section in our App.

4.1. Purposes for which we will use your personal data

We use your personal data in the following ways:

personal data that you provide to us is used to:

- provide you with the information, products and Services that you request from us (including access to your Ikigai Account on our App and our money management and investment services services)
- perform payment transactions requested by you on your Ikigai Account via both national and international payment systems - comply with rules and obligations

specified in card certification schemes such as when a chargeback request is filed, or a card related dispute has been lodged

- to protect against fraud and comply with our regulatory and anti-financial crime regulations
- manage and administer our business
- perform customer surveys, market analyses and statistics so we can improve our Services and user experience, and develop new offerings based on our customers preferences and feedback
- notify you about changes to our Services and help you to solve any difficulties you may encounter while using our products and Services
- assess the quality of our customer services and to provide staff training. Calls to our customer support may be recorded and monitored for these purposes
- perform analysis on customer complaints for the purposes of preventing errors and process failures and rectifying negative impacts on customers
- provide you with information about new products and Services including personalised offers and information about upcoming campaigns in accordance with your marketing preferences and location (see Marketing)
- attract customers with similar preferences and interests as yourself via retargeting/remarketing campaigns by means of Facebook custom audiences. Some of the data that we disclose to Facebook is Aggregated Data or anonymised data. We will only disclose your personal data to Facebook if we have your consent or it is in our legitimate interests to do so.
- personal data that we receive from third parties is combined with the personal data that you provide to us and used for the purposes described above.

personal data about your use of our Site and App is used to:

- to provide you with our Services (including money management)
- administer our Site and App and for internal operations, including troubleshooting, data analytics, testing, research, statistical and survey purposes
- to improve our Site and App to ensure that content is presented in the most effective manner for you and for your Device.
- to allow you to participate in interactive features of our Site and App, when you choose to do so
- as part of our efforts to keep our Site and App safe and secure
- to protect against fraud and comply with our regulatory and anti-financial crime regulations to measure or understand the effectiveness of advertising we serve to you and others, and to deliver relevant advertising to you based on your preferences (also see Marketing)

personal data that we collect from your Device (for example, location data) is used to:

- protect against fraud and other financial crime
- to provide you with our money management services
- to deliver any relevant marketing to you based on your location

Fraud Prevention Agencies

The personal information we have collected from you will be shared with 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 under paragraph 12.

We will always tell fraud prevention agencies if you give us false or fraudulent information. They will also allow other organisations (in the UK or abroad), including law enforcement agencies, to access this information to prevent and detect fraud or other crimes.

You can ask us for the details of the fraud prevention agencies we share information with.

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.

4.2. Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. We have established the following personal data control mechanisms:

Promotional offers from us

We may use your personal data and location 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, Services and offers may be relevant for you.

You may receive promotional communications from us via email, SMS, in-app messages, telephone or post if you have requested information from us or signed up to use our Services, or if you provided us with your details when you entered a competition or registered for a promotion and, in each case, you have not opted out of receiving that communication.

Third-party marketing

We will not share your personal data with any company outside of the Ikigai group of companies for marketing purposes.

Retargeting

Sometimes we use social media sites to retarget/remarket our products and Services to a similar audience as that of our existing customer base. Some of the data that we disclose to social media sites is Aggregated Data or anonymised data. We will only disclose your personal data to social media sites if we have your consent or it is in our legitimate interests to do so.

Opting out

You can ask us to stop sending you our marketing messages at any time by logging into our App and checking or unchecking the relevant options under account settings (found in the More section of the Ikigai App), to adjust your marketing preferences or by following the opt-out link on any marketing message sent to you or by contacting us at any time here.

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

4.3. Cookies

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 Site may become inaccessible or not function properly. For more information about the cookies we use, please see our Cookie Policy.

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 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 privacy@ikigai-invest.com.

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.

5. Disclosure of your personal data

We may have to share your personal data with the parties set out below for the purposes set out in paragraph 4 above.

Internal Third Parties as set out in the Glossary.

External Third Parties as set out in the Glossary.

Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this Privacy Policy.

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 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.

If we are under a duty to disclose or share your personal data to comply with any legal or regulatory obligation, we will only disclose to the extent required to comply with such obligation.

6. International transfers

Some of our external third parties are based outside the European Economic Area ("**EEA**") so their processing of your personal data will involve a transfer of data outside the EEA.

Whenever we transfer your personal data out of the EEA, 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 by the European Commission. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries.
- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, see European Commission: Model contracts for the transfer of personal data to third countries.
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US. For further details, see European Commission: EU-US Privacy Shield.

Where we share data with fraud and crime prevention agencies and fraud and/or criminal history checking service providers in the EEA, they may transfer your data outside of the EEA, in this case they impose contractual obligations on the recipients of that data to protect your personal data to the standard required in the EEA and/or they may require the recipient to subscribe to certain standards, intended to enable secure data sharing.

Please contact us at privacy@ikigai-invest.com if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

7. Data security

We have put in place appropriate physical and technological 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.

Our internal control systems regarding information security are fully ISO standard 27001:2013 (Information Security Management) compliant.

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.

8. Data retention

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. By law we have to keep basic information about our customers (including contact, identity, financial and transaction data) for six years after they cease being customers for tax purposes, and we may also use such data to enable us to respond to any future complaints, or to share information with the Financial Conduct Authority who regulate us.

9. Your legal rights

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

- Request access to your personal data.
- Request correction of your personal data.
- Request erasure of your personal data.
- Object to processing of your personal data.
- Request restriction of processing your personal data.
- Request transfer of your personal data.
- Right to withdraw consent.

See the Glossary for further details. If you wish to exercise any of the rights set out above, please contact us at privacy@ikigai-invest.com.

If you are unhappy about how your personal data has been used please refer to our complaints procedure in our Terms & Conditions (paragraph 10). Privacy-related complaints can be sent to: privacy@ikigai-invest.com. You also have a right to complain to the Information Commissioner's Office (www.ico.org.uk) which regulates the processing of personal data.

9.1. 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.

9.2. 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.

9.3. Time limit to respond

We try to respond to all legitimate requests 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.

10. Glossary

10.1. Lawful basis

Performance of a 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.

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 at privacy@ikigai-invest.com.

10.2. Ikigai Card

Ikigai Card is a prepaid debit card related to your Ikigai Account pursuant the Account Terms and & Conditions.

10.3. Special Categories of Personal Data

Includes data 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).

10.4. Third parties

I**nternal Third Parties** - Group companies, affiliates and branches of Ikigai Invest Services Ltd of which there is currently only one: Ikigai Invest Ltd, UK (Registry number: 11845555).

External Third Parties

Service providers acting as processors based in the EU who provide:

- IT and system administration services such as analytics and search engine providers
- Data storage, server, hosting and security providers
- Delivery service providers
- Payment service providers and processors and providers of technical and payment services (including domestic, European and international payment systems)
- Customer service and support systems providers, so we can communicate with you via email, chat, video or phone call.
- Third parties who assist with our marketing communications and who provide automation and analytics platforms
- Criminal history check providers and verification of identity providers

We will share your Identity, Contact, Transaction, Contractual and Usage Data with PayrNet, Railsbank and TPS. PayrNet is a separate controller of your Identity, Transaction and Usage Data. In order to provide you with the Ikigai Card, PayrNet will share your Identity and Transaction Data with its service providers based in the EU and US, including Visa, card manufacturers, suppliers of identity validation services and us. Railsbank is a technology platform to provide the Everyday Banking services. TPS is a technology platform to provide the Invest services.

Advertisers and advertising networks and social media companies based in EU and/or US that require some personal data to select and serve relevant adverts to you and others. We limit the information about identifiable individuals that we disclose to our advertisers. For example, we may provide them with a hashed ID (data hashed by modern pseudonymous methods, including MD5 and SHA-256 double-hashing processes) which is used to match with data already held by the advertiser, advertising network or social media company (as opposed to providing your Contact Data).

The Financial Conduct Authority ("**FCA**") acting as processor, joint controller or controller based in the United Kingdom for the purposes of compliance with the Electronic Money Regulations 2011 and related legislation and policies. Please be aware that the FCA has a legal duty to co-operate and exchange information with other government and regulatory agencies in the UK and internationally.

Fraud Prevention Agencies in UK, for example, National Crime Agency and CIFAS and providers we use to process and check Due Diligence Data based in the UK, EU and US, including compliance system providers for sanctions and politically exposed persons (PEP) checks.

HM Revenue & Customs, The Financial Ombudsman Service, the UK Financial Services Compensation Scheme or other government or regulatory agencies acting as processors, joint controllers or controllers based in the United Kingdom.

If you ask us to, we will share information with any third party that provides you with account information or payment services. Where you ask us to do this, you are allowing that third party to access information relating to your account. We are not responsible

for any such third party's use of your account information, which will be governed by their agreement with you and any privacy statement they provide to you.

10.5. Your legal rights

You have the right to:

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.

Request correction of the personal data that we hold about you. 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 local 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 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. 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: (a) if you want us to establish the data's accuracy; (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.

Request the transfer 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.

Withdraw consent 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 you withdraw your consent. If you withdraw your consent, we may not be able

to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

11. Fair processing for sharing data with fraud prevention agencies

Before we provide services, goods or financing to you, 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.

WHAT WE PROCESS AND SHARE

The personal data you have provided, we have collected from you, or we have received from third parties may include your:

- name
- date of birth
- residential address and address history
- contact details such as email address and telephone numbers
- financial information
- employment details
- identifiers assigned to your computer or other internet connected device including your Internet Protocol (IP) address

When we and fraud prevention agencies process your personal data, we do so 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.

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

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

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 that of known fraudsters or money launderers; 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

If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to provide the services and financing you have requested, or to employ you, or we may stop providing existing services to you.

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

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