



1. About this Privacy Statement

This is the Privacy Statement of SafeNed Limited, a company incorporated in England and Wales, whose registered number is 09220888, with a registered office located at 36 Old Jewry, 3rd Floor, Becket House, EC2R 8DD, London, United Kingdom ("**SafeNed**"). It applies to all subsidiaries and branches of SafeNed to the extent that they process personal data. SafeNed is supervised by the Financial Conduct Authority.

SafeNed treats personal data which it receives through its websites, portals and any other means with due care and is dedicated to safeguarding any personal data it receives. SafeNed is bound by the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") and the Data Protection Act 2018.

This Privacy Statement is designed to inform you about the type of information that SafeNed collects when using our website and our application and the purposes for which this information is being processed, used, maintained and disclosed (together the "**Services**").

This Privacy Statement aims to explain in a simple and transparent way what personal data we gather about you and how we process it. It applies to the following persons:

- the legal representatives and ultimate beneficial owners of all past, present and prospective commercial contracting parties. We are legally obliged to retain personal data of these persons, also for a certain period after the relationship has ended, in compliance with 'know your customer' ("**KYC**") regulations;
- all private persons with residence in a country in the European Economic Area that is interested in entering into an agreement with (financial) clients of SafeNed, for whom SafeNed provides inter alia customer due diligence services; and
- anyone visiting the SafeNed website.

We may amend this Privacy Statement to remain compliant with any changes in law and/or to reflect how our business processes personal data. This version was created on 25 February 2019. The most recent version is available at www.safened.com/documents/PrivacyStatement.pdf.

2. Personal Data

Personal data refers to any information that tells us something about you or that we can link to you. SafeNed processes any information we receive from you, including personal and financial information you provide to us including when you or your business: enquire or make an application for SafeNed's services, register to use and/or use any of our services and when you communicate with us through e-mail, SMS, WhatsApp, a website or portal, telephone or any other electronic means. Such information may include your:

- name including first name and family name, nationality, place of birth, date of birth, street name, street number, street number suffix, postal code, city, country of residence, phone number, e-mail address, gender, photograph, document type, ID document (picture), document number, issue date, expiration date, geolocation and a selfie.

SafeNed processes your personal data in accordance with the GDPR in the event at least one of the following applies:



- the data subject has given consent to the processing of his or her personal data for one or more specific purposes (refer to Article 6.1(a) GDPR). In the event you give your consent to the processing of your personal data for specific purposes, the processing is permitted on the legal basis of your consent, which consent is revocable at any time;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (refer to Article 6.1(b) GDPR). Personal data is processed to conduct financial services in order to fulfil our contractual and pre-contractual obligations. These actions are only taken when requested by you;
- processing is necessary for compliance with a legal obligation to which the controller is subject (refer to Article 6.1(c) GDPR) and processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (refer to Article 6.1(e) GDPR). SafeNed is subject to several legal obligations as well as regulatory requirements. Please refer to Section 5 (*Who we share your data with and why – government authorities*); and
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (refer to Article 6.1(f) GDPR). In we deem it is necessary, we will process your personal data beyond our contractual obligations in order to protect our legitimate interests or the legitimate interests of a third party.

By processing we mean everything we can do with this data such as collecting, recording, storing, adjusting, organising, using, disclosing, transferring or deleting. For more information about the way we use your personal data, please refer to Section 4 (*What we do with your personal data*).

You share personal information with us, for example when you: visit our website, complete a(n) (online) (application) form, sign a contract or contact us through one of our channels.

We also use data that is legally available from public sources such as commercial registers, the media, or data that is legitimately provided by other companies within the SafeNed Group or by third parties.

3. Sensitive data

We do not record sensitive data relating to your health, ethnicity, religious or political beliefs unless it is strictly necessary. When we do it is limited to specific circumstances.

4. What we do with your personal data

We only use your personal data for legitimate business reasons. This includes:

- **Administration.** When you provide us with information by filling in a form on our website or through the application we are legally obliged to collect personal data that verifies your identity (such as a copy of your ID card or passport) and to assess whether we can accept you or your company as a customer. We also need to know your address or phone number to contact you.
- **Managing customer relationships.** We may ask you for feedback about our products and services and share this with certain members of our staff to improve our offering.



We might also use notes from conversations we have with you online, by telephone or in person to customise products and services for you.

- **Providing you with the best-suited products and services.** When you visit our website, call our customer service centre or visit a branch we gather information about you. We analyse this information to identify your potential needs and assess the suitability of products or services. We assess your needs in relation to key moments when a specific financial product or service may be relevant for you. We assess your interests based on simulations you participate in on our website.
- **Improving and developing products and services:** Analysing how you use our products and services helps us understand more about you and shows us where we can improve. For instance, we analyse the results of our marketing activities to measure their effectiveness and the relevance of our campaigns.
- **Preventing and detecting fraud and data security:** We have a duty to protect your personal data and to prevent, detect and contain data breaches. This includes information we are obliged to collect about you, for example to comply with regulations against money laundering, terrorism financing and tax fraud.
 - We may process your personal information to protect you and your assets from fraudulent activities, for example if you are the victim of identity theft, if your personal data was disclosed or if you have been hacked.
 - We may use certain information about you for profiling (e.g. name, account number, age, nationality, IP address, etc.) to quickly and efficiently detect a particular crime and the person behind it.
- **Internal and external reporting:** We process your data for our operations and to help our management make better decisions about our operations and services. To comply with a range of legal obligations and statutory requirements (anti-money laundering legislation and tax legislation, for example).

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 by <https://www.cifas.org.uk/fpn>.

Data that we process for any other reason is anonymised or we remove as much of the personal information as possible.

5. Who we share your data with and why

Whenever we share personal data internally or with third parties in other countries, we ensure the necessary safeguards are in place to protect it. For this, SafeNed relies on:

- EU Model clauses, which are standardised contractual clauses used in agreements with service providers to ensure personal data transferred outside of the European Economic Area complies with EU data protection law.
- Privacy Shield framework that protects personal data transferred to the United States.

To be able to offer you the best possible services and remain competitive in our business, we share certain data both internally as well as outside of the SafeNed Group. This includes:



SafeNed entities

We transfer data across SafeNed businesses and branches for operational, regulatory or reporting purposes, for example to comply with certain laws, secure IT systems or provide certain services (see section 4 (*What we do with your personal data*)). We may also transfer data to centralised storage systems or to process it globally for more efficiency.

Government authorities

To comply with our regulatory obligations, we may disclose data to the relevant authorities, for example to counter terrorism and prevent money laundering.

In some cases, we are obliged by law to share your data with external parties, including:

- **public authorities, regulators and supervisory bodies** such as fraud protection agencies and the central banks of the countries where we operate;
- **judicial/investigative authorities** such as the police, public prosecutors, courts and arbitration/mediation bodies on their express and legal request; and
- **lawyers**, for example, in case of a claim or bankruptcy, trustees who take care of other parties' interests and company auditors.

Third party service providers

When we use other service providers we only share personal data that is required for the particular task we involve the service provider for. Service providers support us with activities like:

- performing certain services and operations;
- designing and maintenance of internet-based tools and applications;
- marketing activities or events and managing customer communications;
- preparing reports and statistics, printing materials and designing products; and
- placing advertisements on apps, websites and social media.

Business transfers

The SafeNed Group may buy or sell business units or affiliates. In such circumstances, we may transfer customer information as a business asset. Without limiting the foregoing, if our business enters into a joint venture with or is sold to or merged with another business entity, your information may be disclosed to our new business partners or owners.

With your permission

Your information may also be used for other purposes for which you give your specific permission, or when required by law or where permitted under the terms of the laws of the relevant jurisdiction.

6. Cookie Policy

SafeNed makes use of cookies and similar technologies throughout our websites to ensure your visit to our website goes smoothly.

Our websites (and some emails) use "cookies" and other technologies, which store small amounts of information on your computer or device, to allow certain information from your web browser to be collected. Cookies (and similar technologies) are widely used on the internet and allow a website/portal to recognise a user's device, without uniquely



identifying the individual person using the computer. These technologies help to make it easier for you to log on and use our websites and provide information to us, for example which parts of the website you visit.

For more information about cookies, including how to see what cookies have been set and how to manage, block and/or delete them, please refer to the below information about our Cookie Policy.

Cookies

SafeNed may use cookies or similar techniques whenever you interact with this website.

What are cookies?

Many of the websites you view place small text files on your computer. This enables the site to recognize your computer each time you visit. We call these text files 'cookies'. A cookie is sent by a web server to a web browser that enables the server to collect information back from the browser.

Which cookies are used and what do they do?

This website uses the following cookies:

1. Functional cookies

These cookies may store your browser name, the type of computer and technical information about your means of connection to this website, such as the operating system and the Internet Service Providers utilized and other similar information. This information is used to technically facilitate the navigation and use of this website. In addition, functional cookies may be used to store personal settings, such as language, or to remember your information for next visits if so requested.

3. Third-party/social media cookies

This website contains cookies from third-party websites, mainly social media cookies. When placed on your computer, they automatically activate handy extras, for example, a Facebook 'like' button or a Twitter messaging option. These cookies inform our website whether you are logged into such social media and they also enable you to share parts of this website on social media. When visiting this website, SafeNed will ask for your consent to use these cookies.

Do you object to cookies?

Cookies generally process your IP-address, but they do not save your personal information like e-mail address or phone number. If you do not want to have cookies stored on your computer or want to remove cookies that have already been stored, you can arrange this via your browser settings. You can find more information concerning the removal of cookies on the website [all about cookies](#).

7. Your rights and how we respect them



We respect your rights as a customer to determine how your personal information is used. These rights include:

Right to access information

You have the right to ask us for an overview of your personal data that we process.

Right to rectification

If your personal data is incorrect, you have the right ask us to rectify it. If we shared data about you with a third party that is later corrected, we will also notify that party.

Right to object to processing

You can object to SafeNed using your personal data for its own legitimate interests. There is a list of contact details at the end of this Privacy Statement. We will consider your objection and whether processing your information has any undue impact on you that requires us to stop doing so.

You can also object to receiving personalised commercial messages from us. You cannot object to us processing your personal data if we are legally required to do so, even if you have opted out of receiving personalised commercial messages.

Right to object to automated decisions

We sometimes use systems to make automated decisions based on your personal information if this is necessary to fulfil a contract with you, or if you gave us consent to do so. You have the right to object to such automated decisions (for example requiring a new passport copy if the one we have on file for you as representative of your company is no longer valid) and ask for an actual person to make the decision instead.

Right to restrict processing

You have the right to ask us to restrict using your personal data if:

- you believe the information is inaccurate;
- we are processing the data unlawfully;
- SafeNed no longer needs the data, but you want us to keep it for use in a legal claim; and/or
- you have objected to us processing your data for our own legitimate interests.

Right to data portability

You have the right to ask us to transfer your personal data directly to you or to another company. This applies to personal data we process by automated means and with your consent or on the basis of a contract with you. Where technically feasible, we will transfer your personal data.

Right to erasure

You may ask us to erase your personal data if:

- we no longer need it for its original purpose;
- you withdraw your consent for processing it;



- you object to us processing your data for our own legitimate interests or for personalised commercial messages;
- SafeNed unlawfully processes your personal data; and/or
- a law of the European Union or a member state of the European Union requires SafeNed to erase your personal data.

Right to complain

Should you for any reason be unhappy with the way SafeNed treats your personal data, you can file a complaint with SafeNed's Compliance Officer via info@safened.com. You can also contact the data protection authority in your country.

Exercising your rights

How you can exercise your rights depends on the type personal data SafeNed processes. It could be through our website, by fulfilling our KYC obligations or by processing a transaction. We aim to respond to your request as quickly as possible.

In certain cases, we may deny your request. If it's legally permitted, we will let you know within a reasonable timeframe why we denied it.

If you want to exercise your rights or submit a complaint, please contact us via the e-mail address provided below.

8. Your duty to provide data

There is certain information that we must know about you so that we can commence and execute our duties as a payment institution and fulfil our associated obligations. There is also information that we are legally obliged to collect. Without this data we may for example not be able to enter into an agreement with you.

9. How we protect your personal data

We apply an internal framework of policies and minimum standards to keep your data safe. These policies and standards are periodically updated to keep them up to date with regulations and market developments. More specifically and in accordance with the law, we take appropriate technical and organisational measures (policies and procedures, IT security etc.) to ensure the confidentiality and integrity of your personal data and the way it's processed.

In addition, SafeNed employees are subject to confidentiality and may not disclose your personal data unlawfully or unnecessarily.

10. What you can do to help us keep your data safe

Unfortunately, the transmission of information via the internet in general is not always completely secure. Although we will do our best to protect your personal information, we cannot guarantee the security of your information transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

We do our utmost to protect your data, but there are certain things you can do too:



- install anti-virus software, anti-spyware software and a firewall on your computer and keep them updated;
- do not leave verification tokens or your credit card) unattended;
- keep your passwords strictly confidential and use strong passwords, i.e. avoid obvious combinations of letters and figures; and
- be alert online and learn how to spot unusual activity, such as a new website address or phishing emails requesting personal information.

11. How long we keep your personal data

SafeNed will store and process your personal data only as long as it is necessary to perform our obligations under the agreement with you or as long as the law requires to store it. Therefore, we keep your personal data as long as you are using our Services and for seven (7) years after termination of the agreement to comply with the law. There may be circumstances (e.g. fraud or anti-money laundering) whereby we are obliged to store your personal data even longer.

12. Contact us

If you want to know more about SafeNed's data policies and how we use your personal data, you can send us an e-mail at the following dedicated e-mail address: [\[info@safened.com\]](mailto:info@safened.com)