

Privacy Statement

1. About this Privacy Statement

This is the Privacy Statement of Fourthline B.V., a company incorporated in the Netherlands, whose registered number is 58905413, with a registered office located at James Wattstraat 77-R, 1097 DL Amsterdam, the Netherlands ("Fourthline", "We", "Our", "Us"). This Privacy Statement applies to all subsidiaries and branches of Fourthline to the extent that they process personal data.

Fourthline 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. Fourthline is bound by the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), the Dutch GDPR implementation Act (Uitvoeringswet Algemene verordening gegevensbescherming) and the Data Protection Act 2018. This Privacy Statement is designed to inform data subjects ("You", "Your") about the type of information that Fourthline collects when using its website and its application and the purposes for which this information is being processed, used, maintained and disclosed (together the "Services").

We may amend this Privacy Statement to remain compliant with any change in law and/or to reflect how we process personal data.

This Privacy Statement aims to explain 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 that are onboarded as a (prospective) Fourthline Client ("Client"), persons We process the payment data of when providing payment services, persons We process the personal data of when We improve Our services and persons We process the personal data of in order to detect and prevent fraud;
- Anyone visiting the Fourthline website.

2. Categories of personal data, purpose and legal grounds for processing

Personal data refers to any information that tells Us something about You or that We can link to You. Fourthline processes any information We receive from You, including personal and financial information You provide to Us including when You or Your business: inquire or make an application for Services, register to use and/or use any of Our services and when You communicate with Us through email, SMS, WhatsApp, a website or portal, telephone or any other electronic means. We may receive Your personal data either directly by You or through Our Business Partner with whom you wish to enter into a business relationship with. In addition, we may also receive Your personal data by consulting Sanctions/Terrorism lists or lists for politically-exposed persons provided to us by data service providers.

Onboarding and maintaining of relationship with Clients

If We want to establish and maintain a client relationship with You, We need to collect and process an extensive amount of personal data from You. This is due to the fact that, as a payment institution, We need to comply with KYC rules laid down in amongst others the Dutch Prevention of Money Laundering and Terrorism Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme) and the Dutch Sanctions Act (Sanctiewet). We may process the following personal data for this purpose: last name, first name, date of birth, place of birth, ID document issue date, ID document expiration date, ID document issuing authority and ID document number, address, geolocation, device language, device model, region and country code of phone number and biometric data. We will also verify whether You are a politically-exposed person or on a Sanctions list. In addition, We may verify whether there are any adverse media results for You to determine whether We want to provide services to You.

We also create risk profiles for every prospective client for the following parts of Our onboarding process: Identity verification, Client Authentication and Document Authentication. Datapoints related to a prospective Client are assigned a predetermined weighted score. This leads to an overall risk score based on which You may be either accepted or rejected as a Client.

Our legal ground for processing such personal data is legal obligation and legitimate interest. To the extent biometric data is included, the applicable exception to process such a special category of personal data is substantial public interest i.e. to authenticate You and for related security purposes.

Fourthline may perform Your onboarding in an automated manner. The automated onboarding is based on the above risk profile. If your risk profile is unacceptably high,

We may reject Your application. The processing of Your personal data in the above manner is based on the legal ground performance of contract and to the extent biometric data is included the applicable exception to process such a special category of personal data is substantial public interest i.e. to authenticate You and for related security purposes.

Payment transaction data

When performing payment services We need to process certain personal data. This may include: first name, last name, address, IBAN, and transaction indicators and related information. The legal ground for such processing is performance of contract.

Personal KYC Vault

As part of the Services, We offer You a secure personal KYC Vault in which You can store Your personal data. We may process the following personal data for this service: last name, first name, date of birth, place of birth, ID document issue date, ID document expiration date, ID document issuing authority and ID document number, address, geolocation, device language, device model, region and country code of phone number. The legal ground for processing such personal data is performance of contract.

Improvement of Fourthline services

As criminals continuously step up their game We also need to step up ours. This entails that We need to improve Our Services on a continuous basis. We continuously work on improving the user experience. In addition, We gather insights on how the Services perform and train Our IT systems, which may include AI systems. We may use the following personal data for these purposes: last name, first name, date of birth, place of birth, issue date, ID document expiration date, ID document issuing authority and ID document number, address, geolocation, metadata (such as operating system, browser details, system, device sensors, battery, network) and pictures. In the event We process pictures for the training of Our AI systems, We convert the pictures to datapoints called vectors which are created and subsequently permanently deleted in a fraction of a second. Our legal ground for processing such personal data is consent and/or legitimate interest.

Fraud detection and prevention

Because criminals also want to use bank accounts and other financial systems they sometimes try to access a financial account in a fraudulent manner. In order to detect such fraud and prevent it, either for ourselves or to the benefit of a third party such as a financial institution, We may process the following personal data: last name, first name, date of birth, place of birth, ID document issue date, ID document expiration date, ID document issuing authority and ID document number, address, geolocation, metadata, biometric data and personal data relating to an offense. Whenever Our IT systems have established that a Client file is likely to be fraudulent, a Fourthline analyst will perform a manual check to ascertain whether the client application is indeed fraudulent or linked to fraud in any other way. Once fraud has been established by a Fourthline analyst and the Fourthline analyst has ascertained that the relevant personal data are from a perpetrator, such personal data related to an offense will be stored by Fourthline for a period of up to eight years. Our legal ground for processing such personal data is legitimate interest. The exception relied on by Fourthline to process Your biometric data and personal data relating to an offense where the beneficiary of such processing is a third party is: explicit consent. If the processing of Your personal data relating to an offense pertains to the provision of Our Services to You, the exception to process such personal data is: to determine whether or not to provide a service to You as a (prospective) Client and for the protection of Fourthline's interest with regard to criminal violations that have been or may potentially be committed against Fourthline. In order to ensure that the personal data related to an offense are accurate, the Fourthline quality assurance team performs regular sample checks of personal data relating to an offense.

3. 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. The sharing of personal data is based on adequacy decisions, EU-U.S. Data privacy Framework or EU Model Standard Contractual Clauses. In order to offer You the best possible services, We share certain data both internally as well as outside of the Fourthline Group. This includes the following parties.

Fourthline entities

We transfer data across Fourthline businesses and branches for operational, regulatory or reporting purposes, for example to comply with certain laws, secure IT systems or provide certain services. We may also transfer data to centralized storage systems or to process it globally for more efficiency.

Business Partners

We may share Your personal data with a Business Partner. We will do so if You wish to obtain products and/or services from such Business Partner. This could pertain to any of the personal data mentioned in this privacy statement.

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.
- 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 such as cloud storage, analytics and KYC analysis;
- 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;
- Placing advertisements on apps, websites and social media.

Business transfers

The Fourthline 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.

4. Cookie Policy

Fourthline makes use of cookies and similar technologies throughout its websites to enhance Your user experience of Our website. 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 recognize 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.

Which cookies are used and what do they do?

Our 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 Our 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 Our 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.

2. Third-party/social media cookies

Our 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 Our website on social media. When visiting Our website, Fourthline will ask for Your consent to use these cookies.

3. Do you object to cookies?

Cookies generally process Your IP-address, but they do not save Your personal information like email 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 www.allaboutcookies.org.

5. 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 the following.

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 to 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 Fourthline 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.

Rights related 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 in order to take steps at Your request prior to entering into a contract or if You gave Us consent to do so. You have the right to obtain human intervention by one of Our KYC analysts, to express Your opinion with respect to such automated decision and to contest an automated decision. You can do so by [sending an email to the Fourthline Data Privacy Officer](#).

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.
- Fourthline no longer needs the data, but you want Us to keep it for use in a legal claim.
- 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. 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 personalized commercial messages.
- Fourthline unlawfully processes Your personal data.
- A law of the European Union or a member state of the European Union requires Fourthline to erase Your personal data.

Right to complain

Should You for any reason be unhappy with the way Fourthline treats Your personal data, You can file a complaint with Fourthline's Compliance Officer via dpo@fourthline.com. You can also contact the data protection authority in Your country or the lead supervisory authority which is the [Dutch authority for personal data](#) (Autoriteit Persoonsgegevens)

Exercising your rights

How You can exercise Your rights depends on the type of personal data Fourthline processes. 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.

6. 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.

7. How we protect your personal data

We apply an internal framework of policies, procedures and 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 organizational measures (policies and procedures, IT security etc.) to ensure the confidentiality and integrity of Your personal data and the way it is processed. This includes clean room policies and access restriction. In addition, Fourthline employees are subject to confidentiality and may not disclose Your personal data unlawfully or unnecessarily.

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

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.
- Be alert online and learn how to spot unusual activity, such as a new website address or phishing emails requesting personal information.

9. How long we keep your personal data

Fourthline 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 Us to store it. We are obliged to keep Your personal data pertaining to Your onboarding as a customer for five years after termination of Our business relationship with You or five years after execution of a transaction pursuant to the Dutch Anti-money laundering and prevention of financing of terrorism Act (Wet ter voorkoming van witwassen en financieren van terrorisme). There may be circumstances (e.g. fraud, anti-money laundering, law enforcement investigation or exercise of legal claims) whereby We are obliged to store Your personal data even longer. We may keep Your personal data relating to an offence in cases of fraud for up to eight years.

10. Contact us

If you want to know more about Fourthline's data policies, how We use Your personal data or you wish to receive a copy of the international transfer safeguards, You can send Us an e-mail at the following dedicated email address: dpo@fourthline.com