Fourthline Privacy Statement

1. About this Privacy Statement

This is the Privacy Statement of the Fourthline Group. This Privacy Statement applies to all entities that form part of the Fourthline Group to the extent we process personal data.

There are two controllers of the Fourthline Group that are of relevance to data subjects visiting the Fourthline Group website or applications ("you", "your"). The first is Fourthline B.V. whose registered number is 58905413, with registered office at James Wattstraat 77-R, 1097 DL Amsterdam, the Netherlands ("Fourthline"). The second is Fourthline Payments B.V. whose registered number is 96263253, with registered office at James Wattstraat 77-R, 1097 DL Amsterdam, the Netherlands ("Fourthline Payments", each of these Fourthline Group entities separately "we", "our", "us").

The Fourthline Group treats personal data that it receives through its websites, portals, and applications (together "Websites") and any other means, with due care. We are 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. 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 is intended to inform you about the type of data that the Fourthline Group processes when providing its services to you ("Services").
Fourthline Payments is the relevant controller for all processing of your personal data related to your onboarding as a client of Fourthline Payments (“Client”) and improvement of Services.

Fourthline is the relevant controller for all processing of your personal data related to the improvement of Services.

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

Personal data refers to any information that tells the Fourthline Group something about you or that we can link to you. We process any data we receive from you, including personal and financial data, that you provide to us including when you or your business:

- Inquire about or apply for Services;
- Register to use and/or use any of our Services;
- Communicate with us through email, SMS, WhatsApp, our Websites, telephone, or any other electronic means.

We may receive your personal data either directly from you or through companies who use our Services ("Business Partners") with whom you want to enter into a business relationship. In addition, we may also receive your personal data by consulting sanctions, terrorism, or politically exposed person lists provided to us by data service providers.

Onboarding and maintaining relationships with Clients

If we want to establish and maintain a Client relationship with you, we need to collect and process an extensive amount of your personal data. This is due to the fact that, Fourthline Payments, as a payment institution, needs 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 1977). We may process the following personal data for this purpose:

- Your last name, first name, date of birth, place of birth, address, and biometric data;
- Your ID document's issue date, expiration date, issuing authority, and document number;
- Your device's geolocation, language, model, and region and country code of phone number.

We always check whether you are on a sanctions, terrorism, or politically exposed persons list. In addition, we may check whether there are any adverse media articles about 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. Data points related to a (prospective) Client are assigned a predetermined weighted score. This leads to an overall risk score based on which we either accept or reject you as a Client. Our legal ground for processing such personal data is legal obligation and legitimate interest. To the extent that biometric data is included, the applicable exception to process such a special category of personal data is substantial public interest, i.e. for authenticating you and for related security purposes.

We may perform your onboarding in an automated manner including through the use of various AI systems, based on your risk profile. If your risk profile is unacceptably high, we may reject you as a Client. Our legal ground for processing such personal data in this manner is performance of contract and, to the extent that biometric data is included, the applicable exception to process such a special category of personal data is substantial public interest, i.e. for authenticating you and for related security purposes.

Payment transaction data

When Fourthline Payments is providing payment services, it needs to process certain personal data, which may include:

- Your first name, last name, address, and international bank account number (IBAN);
- Transaction indicators and related information.

Our legal ground for processing such personal data is performance of contract.

Personal KYC Vault

As part of our Services, Fourthline Payments offers you a secure personal KYC Vault in which you can store your personal data. We may process the following personal data for this Service:

- Your last name, first name, date of birth, place of birth, address, and picture;
- Your ID document's issue date, expiration date, issuing authority, and document number;
- Your device's geolocation, language, model, and region and country code of phone number.

Our legal ground for processing such personal data is performance of contract.

Improvement of Fourthline Group's Services

As criminals adopt ever-more sophisticated techniques to abuse the financial system, the Fourthline Group also needs to continually improve its Services and the user experience. In addition, we gather insights on how the Services perform in order to train our IT systems, which may include AI systems. We may use the following personal data for these purposes:

- Your last name, first name, date of birth, place of birth, address, and picture;
- Your ID document's issue date, expiration date, issuing authority, and document number;
- Your device's geolocation and metadata, such as operating system, browser details, system, device sensors, battery, and network.

In the event that we process pictures for training our AI systems, we convert the pictures into data points 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 or legitimate interest.

Fraud detection and prevention

Criminals who want to use bank accounts and other financial systems for illegal activity sometimes try to access a financial account in a fraudulent manner. In order to detect such fraud and prevent it, either for our own benefit or that of a third party such as a financial institution, we may process the following personal data:

- Your last name, first name, date of birth, place of birth, address, biometric data, and any personal data relating to an offense;
- Your ID document's issue date, expiration date, issuing authority, and document number;

- Your device's geolocation and metadata.

Whenever our IT systems indicate that a Client file is likely to be fraudulent, a Fourthline Group analyst performs a manual check to ascertain whether such file is indeed fraudulent or linked to fraud in any other way. If the analyst establishes that fraud has taken place and that the relevant personal data belong to a perpetrator, we store such personal data relating to an offense for a period of up to eight years.

Our legal ground for processing such personal data is legitimate interest. The exception we rely on 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 to protect our interests with regard to criminal violations that have been or may potentially be committed against the Fourthline Group. In order to ensure that the personal data relating to an offense are accurate, our Quality Assurance Team regularly performs sample checks of such personal data.

Marketing and communication

We may use personal data relating to our Business Partners' representatives, prospective business customers, and other professional contacts to send information about our products, services, and related updates, such as newsletters, event invitations, and similar communications. This marketing is not directed at end users of our Services.

Our legal ground for processing such personal data is consent or legitimate interest.

You may object to receiving marketing communications at any time by using the unsubscribe option included in our messages or by contacting us using the details set out below.

Back-ups and business continuity

We create and maintain back-ups of our systems to ensure data security, integrity, availability, and business continuity, including the ability to restore systems in the event of an incident.

Personal data contained in such back-ups is processed only for these purposes and is subject to appropriate technical and organisational measures. Back-ups are retained for a limited period and are not used for any other purposes.

Our legal ground for processing such personal data is legitimate interest.

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, the EU-US Data Privacy Framework, or EU 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 listed below in this section 3.

Fourthline entities

We transfer data across the Fourthline Group for operational, regulatory, and reporting purposes, for example to comply with certain laws, to secure our IT systems, to improve the Services including AI systems or to provide certain Services. We may also transfer data to centralized storage systems or process it globally for greater efficiency as set out in the below table of processors under section "Third-party service providers".

Business Partners

We may share your personal data with a Business Partner if you want to obtain products and/or services from such Business Partner. This may pertain to any of the personal data mentioned in this Privacy Statement.

Government authorities

To comply with Fourthline Payments' 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. This includes the following list of processors.

Processor	**Personal Data type**	**Purpose**	**Location of processing**

Amazon Web Services EMEA S.a.r.l.	All personal data processed by Fourthline	Cloud hosting services	Ireland, Germany
Genpact (UK) Limited	KYC data including: Name, Surname, Gender, Date of Birth, Place of Birth, Nationality, Address, ID document information, picture	Provision of trained analysts for case review and related support services	Romania
Google Cloud EMEA Limited	Location data such as address	Google Maps Platform	United States, Chile, Belgium, Netherlands, Finland, Singapore, Taiwan
Governikus GmbH & Co. KG	Data from electronic identity documents including: Name, Surname, Gender, Date of Birth, Place of Birth, Nationality, Address, ID document information	Performing authentication via the German eID function and transmitting identity data to support identity verification	Germany
IPinfo Inc.	IP addresses and location data	Extraction of location information of IP addresses and validation of IP addresses	United States
Microsoft Ireland Operations, Ltd	All personal data processed by Fourthline	Office collaboration, SharePoint	Ireland, the Netherlands
Tink AB	Identity information of end clients such as: Surname, Name and IBAN	Payment initiation Services	Ireland, Netherlands, Belgium
Zoom Video Communications, Inc.	All personal data processed by Fourthline	Zoom's platform is occasionally used to provide remote training to Genpact's training team of KYC analysts in a controlled-to-controlled environment	Netherlands Germany Sweden

Additionally, we may share personal data with service providers required for a particular task or service we involve them in, who act as independent data controllers. These parties independently determine the purposes and means of their further processing of personal data. This includes the following list of controllers.

Controller	Purpose	Location of processing	More info
InfoCert S.p.A.	Issues qualified electronic certificates as required for a Qualified Electronic Signature (QES)	EEA	Made available in the onboarding flow, to the extent applicable
Latvijas Banka	Instant verification service as required for IBAN verification	EEA	https://www.bank.lv/en/about-us/useful/processing-of-personal-data#purposes-of-and-lawfulness-of-personal-data-processing
Namirial GmbH	Issues qualified electronic certificates as required for a Qualified Electronic Signature (QES)	EEA	Made available in the onboarding flow, to the extent applicable

Business transfers

The Fourthline Group may buy or sell business units or affiliates. In such circumstances, we may transfer Client data 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 data may be disclosed to our new Business Partners or owners.

With your permission

We may use your data 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 Group's Websites (and some emails) use "cookies" and similar technologies, which store small amounts of information on your computer or device to collect certain data from your web browser and enhance your user experience. Cookies are widely used on the internet and allow websites/portals to recognize a user's device, without uniquely identifying the individual person using that device. This makes it easier for you to sign in to and use our Websites and collects certain information for us, for example which parts of the website you visit.

When you first visit our Websites, you are presented with a cookie banner that allows you to accept or reject non-essential cookies or manage your preferences. Strictly necessary cookies are used without consent as they are required for the operation of the Websites.

Our policy on cookies, including how you can see which cookies have been stored and how to manage, block, and/or delete them, is set out in this section 4.

Which cookies do we use and what do they do?

Our Websites use the following types of cookies:

Functional cookies

Functional cookies may store your browser name, the type of device you are using, and technical information about your means of connection to our Websites, such as the operating system and the internet service provider (ISP). This information is used to technically facilitate the navigation and use of our Websites. In addition, functional cookies may be used to store personal settings, such as language, or to remember your data for future visits if so requested.

Analytics and Performance cookies

We use analytics cookies and real user monitoring (RUM) tracking technologies to understand how visitors interact with our Websites. These cookies collect information about your browsing behavior, page performance, loading times, and user interactions to help us improve our Services and website functionality. The data collected includes page views, session duration, click patterns, device information, and performance metrics. This information is processed in aggregate form and helps us optimize your user experience.

Third-party and social-media cookies

Our Websites contain cookies from third-party websites, mainly social media websites. When stored on your device, they automatically activate useful functionalities, for example, a Facebook "like" button or an X post button. These cookies inform our Websites whether you are signed in to such social media and they also enable you to share parts of our website on social media. When visiting our websites, the Fourthline Group asks for your consent to use these cookies.

Do you object to cookies?

Cookies generally collect your IP address, but they do not save your personal data such as email address or phone number. If you do not want to have cookies stored on your device 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. Please note that disabling certain cookies may affect the functionality and performance of our website.

5. Your rights and how we respect them

The Fourthline Group respects your rights as a Client to determine how your personal data is used.

How you can exercise your rights depends on the type of personal data we are processing. We aim to respond to your request to exercise a right as quickly as possible. In certain cases, we may deny such request and inform you of the reason within a reasonable timeframe, if legally permitted. If you want to exercise your rights or submit a complaint, you can send an email to dpo@fourthline.com.

Your privacy rights are set out below in this section 5.

Right of access

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 have shared data about you with a third party that is later corrected, we will also notify that party.

Right to object

You can object to us using your personal data for our own legitimate interests. We will consider your objection and whether processing your data has any undue impact on you that requires us to stop doing so.

You can also object to receiving personalized 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 personalized commercial messages.

To submit an objection, you can send an email to dpo@fourthline.com.

Rights related to automated decision-making

We sometimes use systems to make automated decisions based on your personal data 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;
- You gave us consent to do so.

You have the right to obtain human intervention by a Fourthline Group analyst and to express your opinion on and/or contest such automated decisions. You can do so by sending an email to dpo@fourthline.com.

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;
- We no longer need 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 do so.

Right to erasure

You have the right to 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 it for our own legitimate interests or for personalized commercial messages;
- We process it unlawfully;
- A law of the European Union (EU) or an EU member state requires us to erase your personal data.

Right to lodge a complaint

If you are unhappy with the way we treat your personal data for any reason, you can file a complaint with our Data Protection Officer by sending an email to dpo@fourthline.com. You can also contact the data protection authority in your country or our lead supervisory authority, which is the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*).

6. Your duty to provide data

There is certain information that Fourthline Payments 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 data that we are legally obliged to collect. Without this data, we may not be able to enter into an agreement with you.

7. How we protect your personal data

The Fourthline Group applies an internal framework of policies, procedures, and standards to keep your data safe. These policies and standards are periodically updated to comply with regulations and respond to market developments. More specifically and in accordance with the law, we take appropriate technical and organizational measures (such as policies and procedures, and IT security) to ensure the confidentiality and integrity of your personal data and the way it is processed. This includes clean-room policies and access restrictions. In addition, our employees are subject to confidentiality agreements and may not disclose your personal data unlawfully or unnecessarily.

8. How you can help us keep your data safe

Although we always do our utmost best to protect your personal data, we cannot guarantee the security of such data transmitted to our Websites; any such transmission is at your own risk. Once we have received your data, we follow strict procedures and implement security controls to prevent unauthorized access as far as possible.

There are certain things you can do to help protect your personal data:

- Using up-to-date endpoint protection software (such as antivirus) and network protection services (such as firewalls), or similar protections;
- Choosing strong authentication methods, including multifactor authentication, and strong passwords where possible, and keeping them confidential;
- Safeguarding your electronic devices, identity documents, payment methods, and other similar physical items;
- Staying alert while using online services or electronic communications where unusual or fraudulent activity or attempts against your data may occur.

9. How long we keep your personal data

The Fourthline Group stores and processes 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 such data. Fourthline Payments is legally required to store your personal data pertaining to your onboarding as a Client for five years after termination of our business relationship with you, or five years after execution of a transaction pursuant to the Dutch Prevention of Money Laundering and Terrorism Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme)*. There may be circumstances (such as fraud, anti-money laundering requirements, law enforcement investigation, or exercise of legal claims) whereby we are obliged to store your personal data even longer. In cases of fraud, we may store your personal data relating to an offence for up to eight years.

10. Contact us

If you want to know more about the Fourthline Group's data policies or how we use your personal data, or if you want to receive a copy of the international transfer safeguards, you can send us an email to dpo@fourthline.com. Please note the DPO e-mail address may only be used for inquiries related to data privacy. All other e-mails will not be read by the Fourthline Group.