

Fourthline

Privacy Statement

QES Services

1. About this Privacy Statement

Fourthline Trust Services AB ("**Fourthline Trust Services**", "**we**", "**our**" "**us**", "**Controller**"), belonging to the Fourthline group, provides this privacy statement ("**Privacy Statement**") for the processing of personal data of natural persons ("**you**", "**your**", "**Data Subject**") in connection with the provision and operation of Qualified Electronic Signature services ("**QES Services**"), including qualified electronic certificate issuance and management.

We act as a Qualified Trust Service Provider ("**QTSP**") within the meaning of Regulation (EU) No 910/2014, as updated by Regulation (EU) 2024/1183 ("**eIDAS**").

Our role is limited to:

- issuing and managing qualified electronic certificates;
- enabling the creation and validation of Qualified Electronic Signatures;
- maintaining the security, integrity, and legal validity of the trust service.

Identity verification required for the issuance of a qualified electronic certificate may be carried out by another Fourthline group entity, acting either:

- as an independent data controller, or
- as a data processor of companies who use the Fourthline group services ("**Business Partners**"),

in each case under its own privacy statement and data protection arrangements.

This Privacy Statement applies only to the processing of personal data carried out by us as a Controller in our capacity as QTSP.

This Privacy Statement is given pursuant to Article 13 of Regulation (EU) 2016/679 ("**GDPR**") and applicable data protection laws.

2. Categories of personal data

Personal data refers to any information that tells us something about you or that we can link to you. In the context of providing QES Services, we may process the following (personal) data:



- Identification data, such as name, date of birth, biometric data, identity document details, and other attributes obtained as part of the identity verification process (which may be carried out by another Fourthline group entity) required under eIDAS for certificate issuance;
- Certificate identifiers (e.g. public key, validity period)
- Certificate status information (issued, suspended, revoked, expired)
- References or identifiers linking the verification result to the certificate
- Electronic signatures created using the QES Services
- Signature creation events and timestamps
- Hashes of signed documents
- IP addresses and device/browser data
- System logs and audit trails related to QES operations

We may receive your personal data either directly from you, through a Fourthline group entity and/or Business Partner with whom you want to enter into a business relationship.

3. Purpose and legal grounds for processing

We process personal data for the following purposes and on the following legal grounds:

Provision of QES Services

To issue, manage, maintain, suspend, or revoke qualified electronic certificates and enable Qualified Electronic Signatures.

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

Compliance with legal and regulatory obligations

To comply with obligations under eIDAS, applicable national trust service laws, and supervisory authority requirements.

Our legal ground for such processing is compliance with a legal obligation.

Evidence retention and dispute handling

To retain records and logs necessary to demonstrate compliance, support audits, and handle disputes or legal claims.

Our legal ground for such processing is compliance with a legal obligation and, where applicable, legitimate interest in establishing, exercising, or defending legal claims and ensuring the integrity of the QES Services.



4. 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 4.

Fourthline group 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 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 our legal and regulatory obligations, we may disclose personal data to competent supervisory authorities, conformity assessment bodies, and other public or professional bodies where required by law, including judicial or investigative authorities (such as the police, public prosecutors, courts, and arbitration or mediation bodies), as well as lawyers, trustees, 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



Cryptomathic A/S	Any personal data included in the qualified certificate, including data subject name or alias and any attribute of data subject specified in the certificate policy. Data required to perform the signature creation service and the authentication and authorisation service, including proof of authentication delivered in the format of a JWT token.	Providing trust services in accordance with eIDAS, including issuing digital certificates and generating electronic signatures.	Luxembourg France
------------------	---	---	-------------------

Business transfers

The Fourthline group may buy or sell business units or affiliates. In such circumstances, we may transfer your 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. Your rights and how we respect them

We respect your rights as a Data Subject 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 4.

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.

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.

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 Swedish Authority for Privacy Protection's (IMY).

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 QTSP 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. 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 secure

Although we always do our utmost best to protect your personal data, we cannot guarantee the security of such data transmitted to our websites or applications; 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

We store and process your personal data only for as long as necessary for the purposes described in this Privacy Statement and in accordance with applicable legal and regulatory requirements.

In particular, pursuant to the eIDAS Regulation, a qualified trust service provider is required to record and keep accessible, for an appropriate period of time (including after the activities of the qualified trust service provider have ceased), all relevant information concerning data issued and received by the qualified trust service provider. For these purposes, we retain the relevant records and evidence, including related personal data, for a period of at least ten (10) years from the date of issuance of the qualified electronic certificate in accordance with the requirements of the applicable trust service legislation.

Where personal data is no longer required to be retained under applicable law, such data will be securely deleted or anonymised in accordance with our internal retention policies.

10. Contact us

If you want to know more about our 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.