

Fearnley Offshore AS

Privacy Policy

Effective: 1st July 2018
Revised: 15th June 2020

Contents

Privacy Policy	3
What personal data we process?	4
When is our Privacy Policy published and effective?.....	4
Who is responsible for processing your personal data?	4
From which source do we collect your personal data?	4
What are our legal grounds for processing your personal data?	4
In which situations do we process your personal data?.....	4
Do we perform automated decision-making and automated profiling?	5
Processing purposes.....	5
How long do we keep your personal data?	5
Do we share your personal data?.....	5
Do we transfer your personal data outside the EU or EEA?.....	5
Are your personal data secure?.....	5
Are we certified and do we follow a code of conduct?	6
What are your rights?.....	6
How can you exercise your rights?	7
Do you have a right to complain?.....	7
Can you choose your privacy settings?.....	8
Will you be informed about our privacy policy changes?	8
Explanation of words and expressions in this Privacy Policy.....	8

Privacy Policy

Protecting your privacy is of great importance to Fearnley Offshore. Accordingly, Fearnley Offshore attaches great care to the protection of the data you give us, and to process it correctly and in compliance with applicable rules defined in the General Data Protection Regulation ("GDPR"). GDPR stipulates rules as to how Fearnley Offshore can process personal data. Based on the GDPR, Fearnley Offshore has prepared additional privacy rules. These rules supplement the current terms of agreement that Fearnley Offshore has entered into with its customers and applies to all services, both present and future.

The Privacy Policy, powered by the Signatu GDPR platform, describes how Fearnley Offshore treats, processes and stores personal data collected from our customers and users of our services and/or our website. You should familiarize yourself with this Privacy Policy. By using the services of Fearnley Offshore, you provide your consent to us for processing personal data in accordance with this Policy and in compliance with the legislation applicable at any time.

Please contact h.bakkeatfearnleys.no if you have any questions concerning Fearnley Offshores' data processing or this Privacy Policy.

For Fearnley Offshore,

Knut Frøystad
Managing Director

What personal data we process?

- We use your email address to send you our research and market reports.
- We use your email address to communicate about business opportunities and transactions.
- We use phone numbers to get in touch with you to discuss business opportunities and transactions.

When is our Privacy Policy effective?

Our privacy policy is:

- effective as of: 01.07.2018

Who is responsible for processing your personal data?

Responsibility and role

We decide why and how your personal data is processed. We are responsible for processing your personal data.

Contact

We have a contact person for handling GDPR requests:

Contact details: Hege Bakke, h.bakke@fearnleys.no

From which source do we collect your personal data?

We collect your personal data from the following sources:

- a publicly accessible source: public available websites
- directly from you: email address and phone numbers
- from a third party: company websites - Name, email address and phone number

What are our legal grounds for processing your personal data?

According to consent, legitimate reason and/or statutory obligations we will process your personal data.

In which situations do we process your personal data?

We collect personal data:

- of customers and/or clients.
- of contractors.
- visitors to our website www.fearnleyoffshore.com.
- potential customers and/or clients.
- job applicants.

Our role

We are:

- a recipient of your personal data.
- an enterprise.
- an enterprise that controls an undertaking or we are a member of an undertaking.

Sector

We process your personal data in the private sector.

Situation

We process your personal data in a situation that concerns:

- an activity that is professional or commercial.
- the offering of goods or services.
- an online activity.

- a contract or that concerns an entry into a contract.

Do we perform automated decision-making and automated profiling?

- We do not use your personal data to automatically evaluate aspects of your personality.
- We do not use your personal data to make automated decisions about you.

Processing purposes

We process your personal data for the purposes that are described in Section 3.

Our processing purposes are:

- real,
- present, and
- legitimate.

New purposes

We do not process your personal data for secondary purposes that are inconsistent with the primary purposes for which your personal data is collected initially,

- without your prior consent,
- without a legitimate interest, and
- without legal ground.

How long do we keep your personal data?

- We limit the duration we store your personal data to what is necessary for our processing purposes.
- We continuously review the necessity of our continued storage of your personal data:
- We delete your personal data according to routines and statutory obligations for such deletion.
- If the further retention of your personal data is necessary for the purposes that are specified by law, we can further retain your personal data.

Do we share your personal data?

We disclose your personal data to the following recipients:

- HubSpot to monitor website activity.
- Microsoft to host and facilitate our information services, including business documents, mail and CRM systems.
- Astrup Fearnley AS ICT department to host and facilitate parts of our information services.
- Astrup Fearnley AS Accounting department for accounting processing.
- Superoffice as CRM system.

Do we transfer your personal data outside the EU or EEA?

We transfer your personal data to countries outside the EU and EEA, or an international organization. The personal data are transferred to:

- USA to HubSpot
- Non-EU local offices

Are your personal data secure?

Security

We secure your personal data:

- with appropriate technical measures,
- with appropriate organisational measures,
- with an appropriate level of security,
- against unauthorised processing,

- against unlawful processing,
- against accidental or unlawful loss,
- against accidental or unlawful destruction, and
- against accidental or unlawful damage.

Actions when security breach is discovered

If we have a reasonable degree of certainty of a breach of the security of the processing of your personal data, then we will:

- report the security breach to the management.
- assign a person with responsibility to
 - assess whether the security breach can have unfavourable effects for you,
 - inform relevant persons in our organisation,
 - determine the level of security breach and proper required actions thereof and,
 - determine whether it is necessary to notify the Supervisory Authority (Data Protection Authority) of the security breach.

Are we certified and do we follow a code of conduct?

- Yes, we follow a code of conduct and are certified through Achilles and Trace.
- We self-assess that the attestations and assertions in this policy are true.

What are your rights?

Promise to fulfil rights

- You have specific legal rights relating to the personal data we collect from you.
- We will respect your individual rights and handle your concerns appropriately.

Right to access

You may ask from us information regarding personal data that we hold about you, including:

- information as to which categories of personal data we have in our possession or control,
- what your personal data are being used for,
- where we collect your personal data, if not from you directly, and
- to whom your personal data have been disclosed, if applicable.

We will provide you with a copy of your personal data upon your request.

Right to rectification

You have the right to obtain from us rectification of your personal data, that are inaccurate or incomplete, in the latter case provided you supply the corrected or supplementary information.

Right to erasure

You have the right to request that we delete the personal data we process about you.

We must comply with this request if we process your personal data, and if:

- the personal data is no longer necessary for the fulfilment of the purposes for which they have been collected;
- you object to the processing based on our legitimate interest or withdraw your consent;
- the personal data has been processed unlawfully;
- the personal data must be deleted in order to observe a legal obligation incumbent on us.

We must not comply with this request if your personal data is necessary:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation that binds us;

- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
- for the establishment, exercise or defence of legal claims.

Right to restriction

You have the right to obtain from us restriction of processing of your personal data, if:

- you contest the accuracy of your personal data, for the period we need to verify the accuracy,
- the processing is unlawful, and you request the restriction of processing rather than erasure of your personal data,
- we no longer need your personal data, but you require them for the establishment, exercise or defence of legal claims, or
- you object to the processing while we verify the legitimate grounds for the processing of your personal data.

Right to object to direct marketing

You have the right to always object to the processing of your personal data for direct marketing that was based on our legitimate interest, regardless of any reason.

If the marketing was based on your consent, you can withdraw consent.

How can you exercise your rights?

Communication about rights available

We invite you to communicate with us about the exercise of your rights concerning the protection of your personal data.

Answer to request

Your request concerning the protection of your personal data will be answered to your email address.

Person to handle request

Your request concerning the protection of your personal data will be handled by our designated GDPR contact.

Handling request

We ensure that your request concerning the protection of your personal data are recognized, and handled within the time-limits of the law. We will respond to your request within a month.

Do you have a right to complain?

Complain to a supervisory authority

You can lodge a complaint to a supervisory authority:

- where you usually live in the EU and the EEA.
- at the place of your work in the EU and the EEA.
- at the place of the alleged infringement in the EU and the EEA.

The Supervisory Authority should within a reasonable period inform you of:

- the progress of the complaint, and
- the outcome of the complaint.

Mandate an organization to complain

You can mandate that an organization lodges a complaint on your behalf with a Supervisory Authority. The Supervisory Authority should within a reasonable period inform you of:

- the progress of the complaint, and
- the outcome of the complaint.

Judicial remedy

You can seek a judicial remedy in the EU and the EEA against:

- a controller,
- a processor, and
- a Supervisory Authority

Mandate an organization to exercise your right

You can mandate that an organization exercises your right:

- to a judicial remedy on your behalf.
- to a compensation for a damage as a result of a breach of the law on the protection of the personal data on your behalf.

Can you choose your privacy settings?

Privacy settings

You can choose why and how we process your personal data in your privacy settings:

- opt out from research reports
- opt out on request by email

Will you be informed about our privacy policy changes?

New Privacy Policy

If we change our privacy policy, we publish a new version on our website.

Explanation of words and expressions in this Privacy Policy

Unless otherwise defined this Privacy Policy, all terms used in this Privacy Policy will have the meanings given to them below:

Personal data

Personal data means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as:

- a name
- an identification number
- location data
- an online identifier
- the physical identity of a natural person
- the physiological identity of a natural person
- the genetic identity of a natural person
- the mental identity of a natural person
- the identity of a natural person
- the economic identity of a natural person
- the cultural identity of a natural person
- the social identity of a natural person

Regular personal data

Regular personal data are - in the GDPR - personal data that are not special categories of personal data. There is no exhaustive list of such personal data.

Processing

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as:

- collection

- recording
- organisation
- structuring
- storage
- adaptation
- alteration
- retrieval
- consultation
- use
- erasure or destruction
- etc.

Processing Purpose

Processing Purpose means the reason why you process personal data.

Controller

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for in Union or Member State law.

Processor

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Recipient

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Supervisory Authority

Supervisory Authority (Data Protection Authority) means an independent public authority which is established by a Member State pursuant to Article 51 GDPR.

Consent

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

EU-U.S. Privacy Shield Framework

The EU-U.S. Privacy Shield Framework was designed by the U.S. Department of Commerce, and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce. On July 12, 2016, the European Commission deemed the EU-U.S. Privacy Shield Framework adequate to enable data transfers under EU law.

Adequacy Decision by the Commission

The European Commission has the power to determine, on the basis of article 45 GDPR, whether a country outside the EU offers an adequate level of data protection, whether by its domestic legislation or of the international commitments it has entered into.

The effect of such a decision is that personal data can flow from the EEA (EU and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary.

The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations - PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate protection.

Personal Data Breach

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Enterprise

Enterprise means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

Group of undertakings

Group of undertakings means a controlling undertaking and its controlled undertakings.