# BINDING CORPORATE RULES

## PUBLIC VERSION

Last updated: 2 September 2025

TABLE OF CONTENTS

## INTRODUCTION

Jotun A/S and its Group Companies (Jotun) have committed themselves to the protection of Personal Data of Data Subjects by implementing Binding Corporate Rules (BCR) for Processing of Personal Data. A list of entities bound by the BCR with contact details is available on https://www.jotun.com/no-en/about-jotun/contact.

The BCR has been created to establish Jotun's approach to compliance with European data protection law and specifically to all Transfers of Personal Data between the Group Companies, with the primary aim of ensuring an adequate level of protection when Personal data is Transferred from a Group Company inside the European Economic Area (EEA) to a Group Company located outside the EEA.

This public version of the BCR contains a summary of the BCR and is designed to explain the content of the BCR and help ensure that Data Subjects are able to exercise their rights following from the BCR.

Jotun will supplement the BCR through sub-policies that are consistent with the BCR, typically through internal policies and operational procedures. For the sake of clarity, such sub-policies are not considered part of the BCR.

## 1 SCOPE, APPLICABILITY AND IMPLEMENTATION

### 1.1 Scope

The BCR addresses all Processing of Personal Data within Jotun; of Jotun Employees, Customers, employees of Customers, Suppliers and employees of Suppliers, where Jotun will be legally defined as Controller of Personal Data, and where Personal data is Processed by Jotun.

The BCR shall also be applied where a Group Company Processes Personal Data on behalf of another Group Company.

### 1.2 Electronic and paper-based Processing

The BCR applies to all Processing of Personal Data by electronic means and in systematically accessible paper-based filing systems.

### 1.3 Applicability of local law and BCR

Data Subjects keep any rights and remedies they may have under applicable local law. Nothing in the BCR shall be construed as taking away any rights or remedies that Data Subjects may have under applicable local law. The BCR provides supplementary rights and remedies to Data Subjects only.

In the event of any inconsistency or conflict between the BCR and other Jotun privacy documents, the BCR shall take precedence to the extent they address the same issues.

### 1.4 Accountability and binding nature

Every Group Company acting as Controller shall be responsible for and be able to demonstrate compliance with the BCR.

All Group Companies and Employees are bound by and obliged to respect and abide by the provisions of the BCR.

### 1.5 Records of Processing activities

All members of the BCR shall, in order to demonstrate compliance, maintain an electronic record of Processing activities under its responsibility.

When a Group Company acts as a Controller, the record shall contain the following information:

i. the name and contact details of the Controller and, where applicable, the joint Controller, the Controller's representative and the data protection officer;
ii. the purposes of the Processing;
iii. a description of the categories of Data Subjects and of the categories of Personal Data;
iv. the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organizations;
v. where applicable, Transfers of Personal Data to a third country or an international organization, including the identification of that third country or international organization and, in the case of Transfers referred to in the second subparagraph of Article 49(1) GDPR, the documentation of suitable safeguards;
vi. where possible, the envisaged time limits for erasure of the different categories of Personal Data;
vii. where possible, a general description of the technical and organizational security measures referred to in Article 32(1) GDPR.

When a Group Company acts as a Processor, the record shall contain the following information:

i. the name and contact details of the Processor or Processors and of each Controller on behalf of which the Processor is acting, and, where applicable, of the Controller's or the Processor's representative, and the data protection officer;
ii. the categories of Processing carried out on behalf of each Controller;
iii. where applicable, Transfers of Personal Data to a third country or an international organization, including the identification of that third country or international organization and, in the case of Transfers referred to in the second subparagraph of Article 49(1) GDPR, the documentation of suitable safeguards;
iv. where possible, a general description of the technical and organizational security measures referred to in Article 32(1) GDPR.

The records of processing activities shall be made available to the Competent Supervisory Authority on request.

### 1.6 Effective date

The BCR has been adopted by Jotun and shall enter into force when approved on 18 August 2020 (Effective Date) and was last updated 5 August 2025.

### 1.7 Implementation

The BCR shall be implemented in Jotun at the time when approved by the Data Protection Authorities.

### 1.8 Data Subjects' access to the BCR

This public version of the BCR and the list of entities bound by the BCR shall be made available for all Data Subjects on Jotun's website (https://www.jotun.com).

The full version of the BCR will be available on JOIN for the Employees at all times.

### 1.9 Third party beneficiary rights

Data Subjects shall be able to enforce the rights listed below as third party beneficiaries. The enforceable rights for Data Subjects under the BCR include:

i. Data protection principles, lawfulness of Processing, security and Personal Data Breach notification and Onward Transfer, including
    a. Data protection principles in Article 2;
    b. Data protection by design and default in Article 4.1;
    c. Security and confidentiality requirements in Article 4.2;
    d. Notification of Personal Data Breaches to Data Subjects in Article 4.3.3;
    e. Transfer and Onward Transfer to external Controllers or Processors in Article 4.7
ii. Transparency and easy access to the BCR, including
    a. Data Subject's access to the BCR in Article 1.8;
    b. Information to be provided to the Data Subjects in Article 3.1;
iii. Data Subjects' rights in Article 3;
iv. Obligations related to conflict between the BCR and applicable law and in case of government access requests in Articles 6.5 and 6.6;
v. The right to complain in accordance with Article 5.4;
vi. Obligations concerning cooperation with Data Protection Authorities in Article 6.3;
vii. Obligations with regard to applicable law and available remedies, limitation of damages and burden of proof regarding damages in Articles 6.1 and 6.2;
viii. The right to information about any update of the BCR and of the list of Group Companies in Article 7.1 first paragraph, cf. Article 1.8; and
ix. This Article 1.9 on third party beneficiary rights.

For the avoidance of doubt, the rights referred to in this Section 1.9 do not extend to those elements of the BCR pertaining to internal mechanisms implemented within the Group Companies, such as detail of training, audit programmes, compliance network and procedures for updating the BCR.

## 2 DATA PROTECTION PRINCIPLES

### 2.1 General principle

Personal Data shall be processed lawfully, fairly and in a transparent manner in accordance with the principles of the BCR. This means that the Personal Data shall be Processed in accordance with Applicable Law, and that the legitimate interests of the Data Subject should be taken into account when Processing Personal Data.

### 2.2 Lawfulness of Processing

#### 2.2.1 *Legal basis for Processing of Personal Data*

Jotun shall ensure that all Processing of Personal Data only takes place for legitimate purposes and has a legal basis. Jotun may Process Personal Data for legitimate purposes if at least one of the following legal bases applies:

i. the Data Subject has given his or her unambiguous Consent. In order to rely on Consent, Jotun must follow the procedure set forth in Article 2.2.4;
ii. the Processing is necessary for the performance of an agreement between the Data Subject and a Group Company, or in order to take steps at the request of the Data Subject prior to entering into such an agreement;
iii. the Processing is necessary for compliance with a legal obligation to which Jotun is subject;

iv. the Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
v. the 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 Group Company; or
vi. the Processing is necessary for legitimate purposes pursued by a Group Company or by a third party to whom the Personal Data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject.

2.2.2 *Processing of Special Categories of Personal Data*

Processing of Special Categories of Personal Data is prohibited. Group Companies may nevertheless Process Special Categories of Personal Data for legitimate purposes if at least one of the following legal bases applies:

i. the Data Subject has given his or her explicit Consent. In order to rely on Consent, the Group Company must follow the procedure set forth in Article 2.2.4;
ii. the Processing is necessary for the purposes of carrying out the obligations and specific rights of the Group Company in the field of employment, social security and social protection law in so far as it is authorized by Applicable Law in an EEA country providing for adequate safeguards for the fundamental rights and the interests of the Data Subjectl;
iii. the Processing is necessary to protect the vital interests of the Data Subject or of another person where the person is physically or legally incapable of giving Consent;
iv. the Processing relates to Special Categories of Personal Data which are manifestly made public by the Data Subject;
v. the Processing is necessary for the establishment, exercise or defence of legal claims (including for dispute resolution);
vi. the Processing is necessary for the performance of a task for reasons of substantial public interest on the basis of Applicable Law in an EEA country which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
vii. the Processing is required for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the Data Subject, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services, on the basis of Applicable Law in an EEA country and the Special Categories of Personal Data are Processed by a health professional subject to Applicable Law in an EEA country or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy;
viii. the Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health, on the basis of Applicable Law in an EEA country which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy;
*ix.* the Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on Applicable Law in an EEA country which is proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

2.2.3 *Processing of Personal Data relating to criminal convictions and offences*

Jotun shall ensure that there are internal procedures concerning the Processing of Personal Data relating to criminal convictions and offences in compliance with Applicable Law.

2.2.4 *Consent*

If Consent is allowed or required under Applicable Law for Processing Personal Data or Special Categories of Personal Data, the following conditions apply:

i. When seeking Consent, the Group Company must inform the Data Subject of;
    a. the identity and contact details of the Group Company being the Controller of the Processing;
    b. the purposes for which his or her Personal Data will be Processed;
    c. the categories of Third Parties to which the Personal Data will be disclosed (if any);
    d. other relevant information provided in Article 3.1, if necessary to ensure that the Data Subjects' Consent is informed.
ii. Group Companies must be able to demonstrate that the Individual has consented to Processing of his or her Personal Data.
iii. If the Data Subject's Consent is given in the context of a written declaration which also concerns other matters, the request for Consent shall, if Applicable Law so requires, be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.
iv. Consent cannot be used as a legal basis for Processing Personal Data relating to Data Subjects if it has foreseeable adverse consequences for the Data Subjects. Consent will as a main rule not be applicable as a legal basis for Processing Personal Data relating to Employees. Where Processing is undertaken at the request of a Data Subject (e.g. he/she subscribes to a service or seeks a benefit), he/she is deemed to have provided Consent to the Processing.

2.2.5 *Withdrawal of Consent*

The Data Subject may withdraw Consent at any time without adverse consequences to his or her relationship with the Group Company. The withdrawal of Consent shall not affect the lawfulness of the Processing based on such Consent before its withdrawal.
Prior to giving Consent, the Data Subject shall, where Applicable Law so requires, be informed of his or her right to withdraw his or her Consent without adverse consequences. It shall be as easy to withdraw as to give Consent.

## 2.3 Purpose specification

2.3.1 *Purpose specification*

Personal Data shall only be collected, used or otherwise Processed for specified, explicit and legitimate purposes objectively justified by the Group Companies and not further Processed in a way incompatible with those purposes. The Group Companies' Processing of Personal Data includes, but is not limited to, Processing for the purposes set out in Appendix 1 (Business Purposes).

2.3.2 *Generally permitted purposes for further Processing*

Processing of Personal Data further to collection can only take place if such Processing is not incompatible with the purposes that are originally specified for the Processing.

The following purposes will as a main rule not be incompatible with the purposes stated in Article 2.3.1:

i. internal audits or investigations;
ii. implementation of business controls;
iii. statistical, historical or scientific research
iv. preparing for or engaging in dispute resolutions;
v. legal or business consulting; or
vi. insurance purposes.

Depending on the sensitivity of the Personal Data that are Processed, and whether use of the Personal Data has potential negative consequences for the Data Subjects, Processing further to collection may require the implementation of additional measures, such as:

i. limiting access to the Personal Data;
ii. imposing additional confidentiality requirements;
iii. taking additional security measures;
iv. providing an opt-out opportunity; or
v. obtaining Consent in accordance with Article 2.2.4.

## 2.4 Data minimization, quality, and deletion

Personal Data shall be:

i. adequate, relevant and limited to what is necessary in relation to the Business Purposes for which they are collected and/or further Processed;
ii. accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data which are inaccurate or incomplete, having regard to the Business Purposes for which they were collected or for which they are further Processed, are erased or rectified; and
iii. kept in a form which permits identification of Individuals for no longer than what is necessary for the Busines Purposes for which the data were collected or for which they are further Processed, unless necessary to comply with an applicable legal requirement or as advisable in light of an applicable statute of limitations.

Jotun may specify (e.g. in a sub-policy, notice or records retention schedule) a time period for which certain categories of Personal Data may be kept.

Promptly after the applicable storage period has ended, the Local Data Protection Coordinator shall ensure that the Personal Data is:

i. securely deleted or destroyed; or
ii. anonymized/de-identified.

# 3 DATA SUBJECT RIGHTS

## 3.1 Information to be provided to the Data Subjects

### 3.1.1 *Where the Personal Data is collected from the Data Subject*

Where Personal Data relating to a Data Subject is collected from the Data Subject, the Controller shall, at the time when Personal Data are obtained, provide the Data Subject with all of the following information:

i. the identity and the contact details of the Controller and, where applicable, of the Controller's representative;
ii. the contact details of the data protection officer, where applicable;

iii. the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;
iv. where the Processing is based on point (f) of Article 6(1) GDPR, the legitimate interests pursued by the Controller or by a third party;
v. the recipients or categories of recipients of the Personal Data, if any;
vi. where applicable, the fact that the Controller intends to Transfer Personal Data to a Third Country or international organisation and the existence or absence of an adequacy decision by the EU Commission, or in the case of Transfers referred to in Article 46 or 47 GDPR, or the second subparagraph of Article 49(1) GDPR, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

In addition to the information referred to above, the Controller shall, at the time when Personal Data are obtained, provide the Data Subject with the following further information necessary to ensure fair and transparent Processing:

i. the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
ii. the existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability;
iii. where the Processing is based on point (a) of Article 6(1) GDPR or point (a) of Article 9(2) GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;
iv. the right to lodge a complaint with a Supervisory Authority;
v. whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;
vi. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

Where the Controller intends to further process the Personal Data for a purpose other than that for which the Personal Data was collected, the Controller shall provide the Data Subject prior to that further Processing with information on that other purpose and with any relevant further information as referred to above.

The paragraphs above shall not apply where and insofar as the Data Subject already has the information.

#### 3.1.2 *Where the Personal Data has not been obtained from the Data Subject*

Where Personal Data have not been obtained from the Data Subject, the Controller shall provide the Data Subject with the following information:

i. the identity and the contact details of the Controller and, where applicable, of the Controller's representative;
ii. the contact details of the data protection officer, where applicable;
iii. the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;
iv. the categories of Personal Data concerned;
v. the recipients or categories of recipients of the Personal Data, if any;

vi. where applicable, that the Controller intends to Transfer Personal Data to a recipient in a Third Country or international organisation and the existence or absence of an adequacy decision by the EU Commission, or in the case of Transfers referred to in Article 46 or 47 GDPR, or the second subparagraph of Article 49(1) GDPR, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

In addition to the information referred to above, the Controller shall provide the Data Subject with the following information necessary to ensure fair and transparent Processing in respect of the Data Subject:

i. the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
ii. where the Processing is based on point (f) of Article 6(1) GDPR, the legitimate interests pursued by the Controller or by a third party;
iii. the existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject and to object to Processing as well as the right to data portability;
iv. where Processing is based on point (a) of Article 6(1) GDPR or point (a) of Article 9(2) GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;
v. the right to lodge a complaint with a Supervisory Authority;
vi. from which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources;
vii. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

The Controller shall provide the information referred to in the paragraphs above:

i. within a reasonable period after obtaining the Personal Data, but at the latest within one month, having regard to the specific circumstances in which the Personal Data are Processed;
ii. if the Personal Data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject; or
iii. if a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed.

Where the Controller intends to further Process the Personal Data for a purpose other than that for which the Personal Data were obtained, the Controller shall provide the Data Subject prior to that further Processing with information on that other purpose and with any relevant further information as referred to in the second paragraph.

The paragraphs above shall not apply where and insofar as:

i. the Data Subject already has the information;
ii. the provision of such information proves impossible or would involve a disproportionate effort, in particular for Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) GDPR or in so far as the obligation referred to in the first paragraph of this Article is likely to render impossible or seriously impair the achievement of the objectives of that Processing. In such cases the Controller shall take appropriate measures to

protect the Data Subject's rights and freedoms and legitimate interests, including making the information publicly available;

iii. obtaining or disclosure is expressly laid down by EU/EEA law to which the Controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests; or

iv. where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by EU/EEA law, including a statutory obligation of secrecy.

### 3.2 Right of access

All Data Subjects have the right to obtain from the Controller parts of the BCR on which information to the Data Subjects is mandatory (ref Article 1.8) as well as a confirmation as to whether Personal Data are being Processed, and may request a copy of their Personal Data Processed by or on behalf of Jotun.

The Controller shall provide a copy of the Personal Data undergoing Processing. For any further copies requested by the Data Subject, the Controller may charge a reasonable fee based on administrative costs. Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic form. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

Where Personal Data are being Processed, the Data Subject shall also have the right to information about:

i. the Purposes of the Processing;
ii. the categories of Personal Data concerned;
iii. the recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in Third Countries or international organisations;
iv. where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
v. the existence of the right to request from the Controller rectification or erasure of Personal Data or restriction of Processing of Personal Data concerning the Data Subject or to object to such Processing;
vi. the right to lodge a complaint with a Supervisory Authority;
vii. where the Personal Data are not collected from the Data Subject, any available information as to their source;
viii. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

Where Personal Data are Transferred to a Third Country or to an international organisation, the Data Subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 GDPR relating to the Transfer.

### 3.3 Right of rectification

If the Personal Data is incorrect or incomplete, the Data Subject has the right to have the Personal Data concerning them rectified or completed (as appropriate).

### 3.4 Right to erasure

The Data Subject shall have the right to obtain from the Controller the erasure of Personal Data concerning him or her without undue delay and the Controller shall have

the obligation to erase Personal Data without undue delay where one of the following grounds applies:

i. the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise Processed;
ii. the Data Subject withdraws consent on which the Processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2) GDPR, and where there is no other legal ground for the Processing;
iii. the Data Subject objects to the Processing pursuant to Article 21(1) GDPR and there are no overriding legitimate grounds for the Processing, or the Data Subject objects to the Processing pursuant to Article 21(2) GDPR;
iv. the Personal Data have been unlawfully Processed;
v. the Personal Data have to be erased for compliance with a legal obligation in EU/EEA law to which the Controller is subject;
vi. the Personal Data has been collected in relation to the offer of information society services referred to in Article 8(1) GDPR.

Where the Controller has made the Personal Data public and is obliged pursuant to the paragraph above to erase the Personal Data, the Controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other Controllers which are Processing the Personal Data that the Data Subject has requested the erasure by such Controllers of any links to, or copy or replication of, those Personal Data.

The paragraphs above shall not apply to the extent that Processing is necessary:

i. for exercising the right of freedom of expression and information;
ii. for compliance with a legal obligation which requires Processing by EU/EEA law to which the Controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
iii. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) GDPR as well as Article 9(3) GDPR;
iv. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR in so far as the right referred to in the first paragraph is likely to render impossible or seriously impair the achievement of the objectives of that Processing; or
v. for the establishment, exercise or defence of legal claims.

### 3.5 Right to restriction of Processing

The Data Subject shall have the right to obtain from the Controller restriction of Processing where one of the following applies:

i. the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the Controller to verify the accuracy of the Personal Data;
ii. the Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
iii. the Controller no longer needs the Personal Data for the purposes of the Processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;
iv. the Data Subject has objected to Processing pursuant to Article 21(1) GDPR pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

Where Processing has been restricted under the first paragraph, such Personal Data shall, with the exception of storage, only be Processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or an EU/EEA Member State.

A Data Subject who has obtained restriction of Processing pursuant to the first paragraph shall be informed by the Controller before the restriction of Processing is lifted.

### 3.6 Notification obligation regarding rectification, erasure or restriction

The Controller shall communicate any rectification or erasure of Personal Data or restriction of Processing carried out in accordance with Articles 3.3, 3.4 and 3.5 to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. The Controller shall inform the Data Subject about those recipients if the Data Subject requests it.

### 3.7 Right to object

The Data Subject shall have the right to object, on grounds relating to his or her particular situation, at any time to Processing of Personal Data concerning him or her which is based on point (e) or (f) of Article 6(1) GDPR, including profiling based on those provisions. The Controller shall no longer Process the Personal Data unless the Controller demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

Where Personal Data are Processed for direct marketing purposes, the Data Subject shall have the right to object at any time to Processing of Personal Data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the Data Subject objects to Processing for direct marketing purposes, the Personal Data shall no longer be Processed for such purposes.

At the latest at the time of the first communication with the Data Subject, the right referred to in the paragraphs above shall be explicitly brought to the attention of the Data Subject and shall be presented clearly and separately from any other information.

In the context of the use of information society services the Data Subject may exercise his or her right to object by automated means using technical specifications.

Where Personal Data are Processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1) GDPR, the Data Subject, on grounds relating to his or her particular situation, shall have the right to object to Processing of Personal Data concerning him or her, unless the Processing is necessary for the performance of a task carried out for reasons of public interest.

### 3.8 Automated individual decision-making, including profiling

Automated tools or profiling may be used to make decisions about Data Subjects, but the Data Subject shall have the right not to be subject to a decision based solely on automated Processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The first paragraph shall not apply if the decision:

i. is necessary for entering into, or performance of, a contract between the Data Subject and a Controller;
ii. is authorised by EU/EEA law to which the Controller is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests; or
iii. is based on the Data Subject's explicit consent.

In the cases referred to in points (i) and (iii) of the second paragraph, the Controller shall implement suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the Controller, to express his or her point of view and to contest the decision.

Decisions referred to in the second paragraph shall not be based on special categories of Personal Data referred to in Article 9(1) GDPR, unless point (a) or (g) of Article 9(2) GDPR applies and suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests are in place.

## 3.9 Data Subject rights procedure

### 3.9.1 *Request Procedure*

The Data Subject should send his/her request to the Global Data Privacy Officer. Prior to fulfilling the request, Jotun may request the Data Subject to;

i. show proof of his/her identity;
ii. specify the type of Personal Data to which he/she is seeking access
iii. specify the Personal Data system in which the Personal Data is likely to be stored;
iv. specify the circumstances in which Jotun obtained the Personal Data; and
v. in the case of a request for rectification, deletion or blockage specify the reasons why the Personal Data is incorrect, incomplete or not Processed in accordance with applicable law or the BCR.

However, Jotun is not relieved from evaluating a request should item ii-iv above not be given.

### 3.9.2 *Response period*

Without undue delay, and no later than one month after receiving the request, the Global Data Privacy Officer shall inform the Employee or Data Subject in writing of Jotun's position with regards to the request and any action Jotun has taken or will take in response. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. The Controller shall inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Where the Data Subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the Data Subject.

### 3.9.3 *Complaint*

A Data Subject may file a complaint in accordance with Article 5.4.1 if:

i. The response to the request is unsatisfactory to the Data Subject (e.g. the request is denied); or

ii. the Data Subject has not received a response as required by Article 3.9.2.

3.9.4 *Denial of Requests*

Jotun may deny a request if:

i. The identity of the relevant Data Subject cannot be established by reasonable means; or
ii. the request is made within an unreasonable time interval of a prior request or otherwise constitutes an abuse of rights.

If the request constitutes an abuse of rights in accordance with ii) above, Jotun may, instead of denying the request, charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested.

# 4 DATA PROTECTION OBLIGATIONS

## 4.1 Data protection by design and default

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the Processing, the Controller shall, both at the time of the determination of the means for Processing and at the time of the Processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the Processing in order to meet the requirements of the GDPR and protect the rights of Data Subjects.

The Controller shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are Processed. That obligation applies to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default Personal Data are not made accessible without the individual's intervention to an indefinite number of natural persons.

## 4.2 Security and confidentiality requirements

4.2.1 *Data Security*

Jotun has developed an Information Security Management System (ISMS). This system is based on business risk assessments to establish, implement, manage, maintain and improve information security. Jotun's ISMS is also developed to comply with Data security requirements to protect Personal Data.

The Group Companies shall ensure that appropriate technical and organisational measures have been implemented to ensure a level of security appropriate to the risks related to the Processing for the rights and freedoms of natural persons, including from misuse or accidental, unlawful or unauthorized destruction, loss alternation, disclosure, acquisition or access and to ensure a level of security appropriate to the risk, including inter alia as appropriate:

i. the pseudonymisation and encryption of Personal Data;
ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

iii. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

The corresponding policies and internal instructions will be continuously updated and improved.

4.2.2 *Access to Personal Data*

Employees shall be authorized to access Personal Data only to the extent necessary to serve the applicable Business Purpose and to perform their job.

4.2.3 *Confidentiality obligations*

Employees who access Personal Data shall comply with confidentiality obligations and sign a non-disclosure agreement.

## 4.3 Breach notification duties

4.3.1 *Notification to Supervisory Authority*

In the case of a Personal Data Breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Personal Data Breach to the Competent Supervisory Authority unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of the Data Subjects. Where the notification to the Supervisory Authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The Controller shall document all Personal Data Breaches, comprising the facts relating to the Personal Data Breach, including its effects and the remedial action taken. The documentation shall be made available for the Competent Supervisory Authority upon request.

The notification shall include information pertaining to;

i. the nature of the Personal Data Breach including where possible, the categories and approximate number of Employees or Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
ii. the name and contact details of the Global Data Privacy Officer or other contact point where more information can be obtained;
iii. the likely consequences of the Personal Data Breach; and
iv. the measures taken or proposed to be taken by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Personal Data Breach shall also be communicated without undue delay to Jotun A/S (i.e. the Liable BCR member) and Global Data Privacy Officer.

4.3.2 *Notification from Processor to Controller*

A Group Company acting as Processor shall notify the Controller without undue delay after becoming aware of a Personal Data Breach.

4.3.3 *Notification to the Data Subject*

If a Personal Data Breach has occurred, the Controller shall, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of the Data Subjects, communicate the Personal Data Breach to the Data Subjects without undue delay.

## 4.4 Data Protection Impact Assessment (DPIA) and prior consultation

Where a type of Processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the Processing, is likely to result in a high risk to the rights and freedoms of Data Subjects, the Controller shall, prior to the Processing, carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data.

The Controller shall seek the advice of the Global Data Privacy Officer when carrying out a Data Protection Impact Assessment. Where appropriate, the Controller shall seek the views of Data Subjects or their representatives on the intended Processing, without prejudice to the protection of commercial or public interests or the security of Processing operations.

The Data Protection Impact Assessment shall at least contain:

i. a systematic description of the envisaged Processing operations and the purposes of the Processing, including, where applicable, the legitimate interest pursued by the Controller;
ii. an assessment of the necessity and proportionality of the Processing operations in relation to the purposes;
iii. an assessment of the risks to the rights and freedoms of Data Subjects; and
iv. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of Data Subjects and other persons concerned.

Where necessary, the Controller shall carry out a review to assess if Processing is performed in accordance with the Data Protection Impact Assessment at least when there is a change of the risk represented by Processing operations.

## 4.5 Use of Processors

A Group Company shall only use Processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of the GDPR and ensure the protection of the rights of the Data Subject.

The Processing by a Processor shall be governed by a contract that, as a minimum, sets out the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of the Data Subjects and the obligations and rights of the Controller (a data processing agreement). The contract shall stipulate, in particular that the Processor:

i. Processes the Personal Data only on documented instructions from the Controller, including with regard to Transfers of Personal Data to a Third Country or an international organization, unless required to do so by EU/EEA law to which the Processor is subject; in such a case, the Processor shall inform the Controller

of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

ii. Ensures that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

iii. Takes all measures required by law related to the security of Processing;

iv. Respects the conditions referred to below related to engagement of another Processor;

v. Taking into account the nature of the Processing, assists the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights under Applicable EU/EEA Data Protection Law;

vi. Assists the Controller in ensuring compliance with the legal obligations related to security of Processing and consultation with the Data Protection Authorities taking into account the nature of Processing and the information available to the Processor;

vii. At the choice of the Controller, deletes or returns all the Personal Data to the Controller after the end of the provision of services relating to Processing, and deletes existing copies unless Applicable EU/EEA Law requires storage of the Personal Data; and

viii. Makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the BCR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

The Processor shall not engage another Processor without prior specific or general written authorisation of the Controller. In the case of general written authorisation, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other Processors, thereby giving the Controller the opportunity to object to such changes.

Where a Processor engages another Processor for carrying out specific Processing activities on behalf of the Controller, the same data protection obligations as set out in the contract between the Controller and the Processor as referred to above shall be imposed on that other Processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of the GDPR. Where that other Processor fails to fulfil its data protection obligations, the initial Processor shall remain fully liable to the Controller for the performance of that other Processor's obligations.

### 4.6 Intra-group Transfer (to another Group Company Controller or Processor)

Personal Data may be Transferred to a Jotun Group Company located in a Third Country subject to the provisions of the BCR.

### 4.7 Transfer and Onward Transfer to external Controllers or Processors

In addition to the other requirements set out in the BCR, any Transfer or Onward Transfer of Personal Data to an external Controller or Processor, i.e. a Controller or Processor not bound by the BCR, that is established in a Third Country must have a legal basis in accordance with Chapter V GDPR, including, but not limited to:

i. An adequacy decision by the EU Commission in accordance with Article 45 GDPR;

ii. Appropriate safeguards pursuant to Article 46 GDPR, such as standard data protection clauses adopted by the EU Commission; or
iii. A derogation for specific situations under Article 49 GDPR.

A disclosure of Personal Data that does not constitute a Transfer or Onward Transfer is subject to Article 4.5 if the recipient is a Processor.

# 5 SUPERVISION, TRAINING, AUDITS AND COMPLAINTS

## 5.1 Supervision and compliance

### 5.1.1 *Global Data Privacy Officer*

Jotun shall appoint a Global Data Privacy Officer who is responsible for supervising the general Group level compliance with the BCR.

### 5.1.2 *Regional Data Protection Coordinators*

The Regional Data Protection Coordinator shall implement the Personal Data management process, systems and tools in its region.

### 5.1.3 *Local Data Protection Coordinator*

The Local Data Protection Coordinator shall assist the GM/MD to ensure overall Personal Data protection management compliance within the company.

### 5.1.4 *Process owners*

Process owners are responsible for the Processing of Personal Data in his or her unit.

## 5.2 Training

Jotun shall provide appropriate and up-to-date training on the BCR and related confidentiality obligations to Employees and other personnel. Training will be tailored to the needs and tasks of the Employee and other personnel.

## 5.3 Monitoring and auditing compliance

### 5.3.1 *Audits*

Jotun shall regularly perform audits in accordance with the BCR and internal policies.

## 5.4 Complaints procedure

### 5.4.1 *Complaints from Data Subjects*

Data Subjects may file a complaint, preferably in writing, regarding any Group Company's compliance with the BCR or violations of their rights under applicable local law and;

i. send it to dataprotection@jotun.com; or
ii. file it with the Global Data Privacy Officer, see contact information in Article 8;

While the Data Subjects are encouraged to use the points of contact above, this is not mandatory.

In addition, the Data Subject may file a complaint regarding any Group Company's compliance with the BCR by;

i. lodging a complaint at a Supervisory Authority in the EU/EEA member state where the Data Subject has his/her habitual residence, place of work or the place where the alleged infringement took place; or
ii. lodging a complaint before the competent court where the Controller or Processor has an establishment or where the Data Subject has his/her habitual residence.

When the Global Data Privacy Officer is informed of the complaint, he/she shall;

i. notify the Regional and Local Data Protection Coordinator;
ii. initiate an investigation; and
iii. when necessary, advise the business on the appropriate measures for compliance and monitor, through to completion, the steps designed to achieve compliance.

The Global Data Privacy Officer may consult with any government authority having jurisdiction over a particular matter about the measures taken.

5.4.2 *Reply to the Data Subject*

Without undue delay and in any case within one month of Jotun receipt of a complaint, the Global Data Privacy Officer shall inform the Data Subject in writing either;

i. of Jotun`s position with regard to the complaint and any action Jotun has taken or will take in response; or
ii. when he/she will be informed of Jotun`s position, which normally shall be no later than one month after receiving the complaint, but may in particular cases be extended with two further months taking into consideration the complexity and number of requests.

The Global Data Privacy Officer shall send a copy of the complaint and his/her written reply to the Regional and Local Data Protection Coordinator.

5.4.3 *Complaints to Head of Compliance*

Data Subjects may file a complaint with the Head of Compliance if:

i. the handling of the complaint by the Global Data Privacy Officer is unsatisfactory to the Data Subject (e.g. the complaint is rejected);
ii. the Data Subject has not received a response as required by Article 5.4.2;
iii. the time period provided to the Data Subject pursuant to Article 5.4.2 is, in light of the relevant circumstances, unreasonably long and the Data Subject has rejected but has not been provided with a shorter, more reasonable time period in which he/she will receive a response.

The procedure described in Article 5.4 shall apply to complaints filed with the Head of Compliance.

If the Data Subject is not satisfied by the reply, the Data Subject has the right to lodge a claim before the competent court and a complaint before a Supervisory Authority, in accordance with Article 6.2. For the sake of clarity, the right to lodge a claim or a complaint is not dependent on the Data Subject having used the complaint handling process beforehand.

# 6 JURISDICTION, REMEDIES, NON-COMPLIANCE, CONFLICT WITH LOCAL LAWS AND GOVERNMENT ACCESS REQUESTS

## 6.1 Relation to applicable law

### 6.1.1 *Local Law and jurisdiction*

Any Processing by Jotun of Personal Data shall be governed by applicable local law. Employees and Data Subjects keep their own rights and remedies as available in their local jurisdiction. Local government authorities having jurisdiction over the relevant matters shall maintain their authority.

### 6.1.2 *Law applicable to BCR; BCR has supplemental character*

The BCR shall be governed by Norwegian law. Its terms and definitions shall be interpreted in line with the GDPR. Where applicable local law provides more protection than the BCR, local law shall apply. Where the BCR provides more protection than applicable local law or provides additional safeguards, rights or remedies for Employees, the BCR shall apply.

All Group Companies shall promptly inform Jotun A/S of legal requirements preventing the Group Company from fulfilling its obligations under the BCR.

### 6.1.3 *Supervision of compliance and lead authority*

Compliance with the BCR may be supervised by any competent Data Protection Authority. The Norwegian Data Protection Authority, Datatilsynet, is the lead authority regarding the BCR.

## 6.2 Available remedies, limitation of damages and burden of proof regarding damages

Jotun's liability and responsibility pursuant to this section is subject to the limitations in Article 1.9 (Third party beneficiary rights).

Jotun A/S with Head Office in Sandefjord, Norway, is responsible for and agrees to take the necessary action to remedy the acts of Group Companies established outside the EEA and to pay compensation in accordance with applicable EU/EEA law for any material or non-material damages suffered by a Data Subject resulting from a violation of the BCR by Group Companies established outside the EEA.

Where a Data Subject can demonstrate that it has suffered damage and establish facts which show it is likely that the damage has occurred because of a violation of the BCR, it will be for Jotun A/S to prove that the damages suffered due to a violation of the BCR are not attributable to the relevant Group Company established outside the EEA or that no such violation took place in order to avoid liability.

The Group Companies accept that Data Subjects may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) GDPR.

If a Group Company established outside the EEA violates the BCR, the courts or other judicial authorities in the EEA will have jurisdiction and the Data Subjects have the rights and remedies against Jotun A/S as if the violation had been caused by Jotun A/S in Norway, instead of the Group Company outside the EEA.

## 6.3 Mutual assistance and cooperation with Data Protection Authorities

All Group Companies undertake to cooperate with, to accept to be audited and to be inspected, including where necessary, on-site, by the competent EEA Data Protection Authorities to take into account their advice, and to abide by decisions of these Data Protection Authorities on any issue related to the BCR, particularly by applying recommendations and advice from the authorities, and also by responding to requests from the authorities regarding the BCR.

All Group Companies must provide the competent Data Protection Authorities, upon request, with any information about the Processing operations covered by the BCR.

Any dispute related to the competent Data Protection Authority's exercise of supervision of compliance with the BCR will be resolved by the courts of the EU or EEA Member State of that Data Protection Authority, in accordance with that Member State's procedural law. The Group Companies shall submit themselves to the jurisdiction of these courts.

The Group Company that is responsible for the Processing to which the request, complaint or claim relates, shall bear all costs and loss involved and reimburse Jotun A/S.

## 6.4 Non-compliance

### 6.4.1 *Sanctions for non-compliance*

Non-compliance of Employees with the BCR may result in disciplinary action up to and including termination of employment.

### 6.4.2 *Non-compliance*

No Transfer shall be made to a Group Company unless the Group Company is effectively bound by the BCR and can deliver compliance.

The Data Importer shall promptly inform the Data Exporter if it is unable to comply with the BCR, for whatever reason, including the situations further described under Article 6.5.

Where the Data Importer is in breach of the BCR or unable to comply with them, the Data Exporter should suspend the Transfer.

The Data Importer should, at the choice of the Data Exporter, immediately return or delete the Personal Data that has been Transferred under the BCR in its entirety, where:

i. the Data Exporter has suspended the Transfer, and compliance with the BCR is not restored within a reasonable time, and in any event within one month of suspension; or
ii. the Data Importer is in substantial or persistent breach of the BCR; or
iii. the Data Importer fails to comply with a binding decision of a competent court or Competent Supervisory Authority regarding its obligations under the BCR.

The same commitments shall apply to any copies of the data. The Data Importer shall certify the deletion of the data to the Data Exporter.

Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with the BCR.

In case of local laws applicable to the Data Importer that prohibit the return or deletion of the Transferred Personal Data, the Data Importer shall warrant that it will continue to ensure compliance with the BCR, and will only process the data to the extent and for as long as required under that local law.

For cases where applicable local law and/or practices affect compliance with the BCR, Article 6.5 applies.

## 6.5 Conflict between the BCR and applicable local law

6.5.1 *Obligations to assess local law and practices*

The Group Companies commit that they will use the BCR as a tool for Transfers only where they have assessed that the law and practices in the third country of destination applicable to the Processing of the Personal Data by the Group Company acting as Data Importer, including any requirements to disclose Personal Data or measures authorising access by public authorities, do not prevent it from fulfilling its obligations under the BCR.

For the sake of clarity, laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the BCR.

6.5.2 *Assessment of local laws and practices when Transferring Personal Data to third countries*

In assessing the laws and practices of the third country which may affect the respect of the commitments contained in the BCR, the Group Companies have taken due account, in particular, of the following elements:

i. The specific circumstances of the Transfers or set of Transfers, and of any envisaged Onward Transfers within the same third country or to another third country, including:
    a. purposes for which the data are Transferred and Processed (e.g. marketing, HR, storage, IT support, clinical trials);
    b. types of entities involved in the Processing (the Data Importer and any further recipient of any Onward Transfer);
    c. economic sector in which the Transfer or set of Transfers occur;
    d. categories and format of the Personal Data Transferred;
    e. location of the Processing, including storage; and
    f. transmission channels used.
ii. The laws and practices of the third country of destination relevant in light of the circumstances of the Transfer, including those requiring to disclose data to public authorities or authorising access by such authorities and those providing for access to these data during the transit between the country of the Data Exporter and the country of the Data Importer, as well as the applicable limitations and safeguards.
iii. Any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the BCR, including measures applied during the transmission and to the Processing of the Personal Data in the country of destination.

6.5.3 *Consultation*

The BCR should also contain a commitment that where any safeguards in addition to those envisaged under the BCR should be put in place, the Liable Group Company, and the relevant Privacy officer or Function will be informed and involved in such assessment.

6.5.4 *Obligation to document the assessment*

The Group Companies must document appropriately such assessment, as well as the supplementary measures selected and implemented. They should make such documentation available to the competent Supervisory Authorities upon request.

6.5.5 *Notification to the Data Exporter and supplementary measures*

Any Group Company acting as Data Importer to promptly notify the Data Exporter if, when using these BCR as a tool for Transfers, and for the duration of the BCR membership, it has reasons to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the BCR, including following a change in the laws in the third country or a measure (such as a disclosure request). This information should also be provided to the Liable Group Company.

Upon verification of such notification, the Group Company acting as Data Exporter, along with the Liable Group Company and the relevant Privacy officer or Function, shall commit to promptly identify supplementary measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the Group Company acting as Data Exporter and/or Data Importer, in order to enable them to fulfil their obligations under the BCR. The same applies if a Group Company acting as Data Exporter has reasons to believe that a BCR member acting as its Data Importer can no longer fulfil its obligations under the BCR.

6.5.6 *Suspension of Transfers*

Where the Group Company acting as Data Exporter, along with the Liable Group Company and the relevant Privacy officer or Function, assesses that the BCR – even if accompanied by supplementary measures – cannot be complied with for a Transfer or set of Transfers, or if instructed by the Competent Supervisory Authorities, it commits to suspend the Transfer or set of Transfers at stake, as well as all Transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the Transfer is ended.

Following such a suspension, the Group Company acting as Data Exporter has to end the Transfer or set of Transfers if the BCR cannot be complied with and compliance with the BCR is not restored within one month of suspension. In this case, Personal Data that have been Transferred prior to the suspension, and any copies thereof, should, at the choice of the Group Company acting as Data Exporter, be returned to it or destroyed in their entirety.

6.5.7 *Notification to all Group Companies*

The Liable Group Company and the relevant Privacy officer or Function shall inform all other Group Companies of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of Transfers is carried out by any other Group Companies or, where effective supplementary measures could not be put in place, the Transfers at stake are suspended or ended.

6.5.8 *Obligation to monitor developments*

The Data Exporters shall monitor, on an ongoing basis, and where appropriate in collaboration with Data Importers, developments in the third countries to which the Data Exporters have Transferred Personal Data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such Transfers.

## 6.6 Obligations of the Data Importer in case of government access requests

6.6.1 *Notification of government access requests*

Without prejudice to the obligation of the Group Company acting as Data Importer to inform the Data Exporter of its inability to comply with the commitments contained in the BCR:

The Group Company acting as Data Importer will promptly notify the Data Exporter and, where possible, the Data Subject (if necessary with the help of the Data Exporter) if it:

i. receives a legally binding request by a public authority under the laws of the country of destination, or of another third country, for disclosure of Personal Data Transferred pursuant to the BCR; such notification will include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided;
ii. becomes aware of any direct access by public authorities to Personal Data Transferred pursuant to the BCR in accordance with the laws of the country of destination; such notification will include all information available to the Data Importer.

6.6.2 *Demonstration of best effort to waive prohibition to notify*

If prohibited from notifying the Data Exporter and / or the Data Subject, the Data Importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the Data Exporter.

6.6.3 *Information regarding the request*

The Data Importer will provide the Group Company acting as Data Exporter, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the Data Importer is or becomes partially or completely prohibited from providing the Data Exporter with the aforementioned information, it will, without undue delay, inform the Data Exporter accordingly.

The Data Importer will preserve the abovementioned information for as long as the Personal Data are subject to the safeguards provided by the BCR, and shall make it available to the Competent Supervisory Authorities s upon request.

6.6.4 *Consideration of the legality of and challenging the request*

The Data Importer will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the

country of destination, applicable obligations under international law, and principles of international comity.

The Data Importer will, under the same conditions, pursue possibilities of appeal. When challenging a request, the Data Importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the Personal Data requested until required to do so under the applicable procedural rules.

#### 6.6.5 *Documentation of assessment and challenge of the request*

The Data Importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter. It will also make it available to the Competent Supervisory Authorities upon request.

#### 6.6.6 *Limitation of disclosure*

The Data Importer will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### 6.6.7 *Prohibition against massive, disproportionate and indiscriminate Transfers*

Transfers of Personal Data by a Group Company to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

## 7 CHANGES TO AND TERMINATION OF THE BCR

### 7.1 Changes to the BCR

#### 7.1.1 *Requirements for change*

The BCR shall be kept up-to-date in order to reflect the current situation, for instance, to take into account modifications of the regulatory environment, recommendations for the European Data Protection Board or changes to the scope of the BCR.

#### 7.1.2 *Prior approval*

Jotun shall keep a fully updated list of the Group Companies and keep track of and record any updates to the rules. Changes to the BCR shall without undue delay be notified by Jotun to all BCR members. The Head of Compliance shall provide the necessary information about changes to Data Subjects and, upon request, to the Norwegian Data Protection Authority.

Any changes to the BCR or to the list of BCR members shall be notified yearly to the Norwegian Data Protection Authority together with an explanation of the reasons justifying the update. The Norwegian Data Protection Authority shall also be notified once a year in instances where no changes have been made. The annual update or notification shall also include the renewal of the confirmation regarding assets.

As lead Supervisory Authority, the Norwegian Data Protection Authority shall inform EEA competent data protection authorities of such changes.

7.1.3 *No Consent*

The BCR may be changed without Employee's or Data Subject's Consent even though an amendment may relate to a benefit conferred on Employees or Data Subjects.

7.1.4 *Entry into force*

Any amendment shall enter into force after it has been approved and published on JOIN.

7.1.5 *Relevant BCR*

Any request, complaint or claim of a Data Subject involving the BCR shall be considered on the basis of the version of the BCR that is in force at the time of the request, complaint or claim is made.

7.1.6 *Applicability for new Group Companies*

Transfers involving companies that enter the Jotun Group after the Effective date of the BCR, and that require the BCR as legal basis, may only take place after the new member of the Jotun Group has formally adhered to the BCR. No Transfer is made to a new Group Company until said Group Company is effectively bound by the BCR and can deliver compliance accordingly.

## 7.2 Termination

A Group Company acting as Data Importer, which ceases to be bound by the BCR, may keep, return, or delete the Personal Data received under the BCR. If the Data Exporter and Data Importer agree that the data may be kept by the Data Importer, protection must be maintained in accordance with Chapter V GDPR.

# 8 PUBLICATION

The BCR document will be published as set out in the BCR Article 1.8.

## CONTACT DETAILS

Jotun A/S
Hystadveien 167,
Pb 2021
3202 Sandefjord
Norway

+47 33457000

**DEFINITIONS**

| | |
|---|---|
| *Applicable Law* | The national and/or local law applicable to the Group Company. 'Applicable EU/EEA Law' only refers to EU, national or local law in the European Economic Area applicable to the Group Company. |
| *BCR* | BCR (Binding Corporate Rules) shall mean the binding corporate data protection rules for Personal Data herein. |
| *Business Purpose* | BUSINESS PURPOSE shall mean a purpose for Processing Personal Data as specified in Article 2.3.1. |
| *Consent* | CONSENT shall mean any freely given specific, informed and explicit indication of wishes by which Employees or Data Subjects, either by a statement or by a clear affirmative action, signify their agreement to Processing of their Personal Data for one or more specific purposes. |
| *Controller* | CONTROLLER or DATA CONTROLLER shall mean 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. |
| *Customer* | CUSTOMER shall mean any organisation buying products and services from Jotun including consumers of Jotun's products and services. |
| *Data Exporter* | The natural or legal person(s), public authority/ies, agency/ies or other body/ies Transferring the Personal Data to a Third Country. |
| *Data Importer* | The natural or legal person(s), public authority/ies, agency/ies or other body/ies in a Third Country receiving the Personal Data from the Data Exporter, directly or indirectly via another entity. |
| *Data Subject* | Data Subject shall mean an identified or identifiable natural person that is either, to whom Personal Data relates. A Data Subject may for example be a Customer, an employee of a Customer, a Supplier or an employee of a Supplier. |
| *Dependant* | DEPENDANT shall mean the spouse, partner or child belonging to the household of the Employee. |
| *Divested Entity* | DIVESTED ENTITY shall mean the divestment by Jotun of a Group Company or business by means of;<br>i. a sale of shares as a result whereof the Group Company so divested no longer qualifies as a Group Company; and/or<br>ii. a demerger, sale of assets or any other manner or form. |
| *DPIA* | (Data Protection Impact Assessment) is a process designed to describe the Processing, assess the necessity and proportionality of a Processing and to help manage the risk resulting from the Processing of Personal Data. |
| *EEA* | EEA or EUROPEAN ECONOMIC AREA shall mean all Member States of the European Union, plus Norway, Iceland and Liechtenstein. |

| | |
|---|---|
| *Effective Date* | EFFECTIVE DATE shall mean the date on which the BCR becomes effective as set forth in Article 1.6. |
| *Employee* | EMPLOYEE shall mean an employee, job applicant or former employee of Jotun as well as people working at Jotun as consultants or employees of External Parties providing services to Jotun. |
| *Employee Personal Data* | EMPLOYEE PERSONAL DATA shall mean Personal Data of Employee |
| *EU* | EU shall mean the European Union. For the purposes of this document EU also shall include the EEA, and Switzerland as applicable. |
| *Exporter* | EXPORTER shall mean the Group Company located in the EEA that Transfers Personal Data to a Group Company or External Party located outside of the EEA. |
| *External Party* | EXTERNAL PARTY shall mean any person, private organization or government body outside Jotun. |
| *External Controller* | EXTERNAL CONTROLLER shall mean an External Party that Processes Personal Data and determines the purpose and means of the Processing. |
| *External Processor* | EXTERNAL PROCESSOR shall mean an External Party that Processes Personal Data on behalf of Jotun that is not under the direct authority of Jotun. |
| *GDPR* | GDPR shall mean the General Data Protection Regulation (EU) 2016/679. |
| *GM* | GM shall mean the General Manager of a Group Company. |
| *Group Company* | GROUP COMPANY shall mean Jotun A/S and any directly or indirectly wholly owned subsidiary of Jotun A/S and other subsidiaries as listed in the document "Members of the Jotun BCR". |
| *Global Data Privacy Officer* | Global Data Privacy Officer shall mean the officer as referred to in Article 5.1.1. |
| *Head of Compliance* | HEAD OF COMPLIANCE shall mean the Compliance Officer of Jotun Group. |
| *HR review* | HR review shall mean Jotun Group and Regional HR' s review of local HR functions. |
| *Importer* | IMPORTER shall mean the Group Company or External Party located outside of EEA that receives Personal Data from a Group Company located in the EEA. |
| *Internal Audit* | Internal Audit shall mean Jotun A/S' Internal Audit department. |
| *ISMS* | ISMS shall mean the Jotun developed Information Security Management System, which is based on business risk assessments to establish, implement, manage, maintain and improve information security. |
| *JGM* | JGM shall mean Jotun Group Management. |
| *JOIN* | JOIN shall mean Jotun's intranet. |

| | |
|---|---|
| *Jotun* | Jotun shall mean Jotun A/S and its Group Companies. |
| *Jotun A/S* | Jotun A/S shall mean the parent company having its registered seat in Sandefjord, Norway. |
| *Local Data Protection Coordinator* | LOCAL DATA PROTECTION COORDINATOR shall mean a person assigned to the tasks described in BCR Article 5.1.3. and other relevant Articles in the BCR. |
| *MD* | MD shall mean the Managing Director of a Group Company. |
| *Onward Transfer* | For the purpose of the BCR, ONWARD TRANSFER shall mean the situation where Personal Data have previously been Transferred under the BCR, and a Group Company discloses or otherwise makes the Personal Data available to an external Controller or Processor outside the EEA not bound by the BCR. |
| *Personal Data* | PERSONAL DATA shall mean any information relating to an identified or identifiable person. |
| *Personal Data Breach* | PERSONAL DATA BREACH shall mean 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. |
| *Processor* | PROCESSOR shall mean the specific Jotun entity which Process Personal Data on behalf of a Controller. |
| *Process Owner* | PROCESS OWNER shall mean the responsible person for a specified process or specified processes handling Personal Data. |
| *Processing* | PROCESSING shall mean any operation that is performed on Personal Data, whether or not by automatic means, such as collection, recording, storage, organization, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. |
| *Regional Data Protection Coordinator (RDPC)* | REGIONAL DATA PROTECTION Coordinator shall mean a Data Protection Coordinator appointed by the Controller. |
| *Special Categories of Personal Data* | SPECIAL CATEGORIES OF PERSONAL DATA are Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. |
| *Supervisory Authority* | SUPERVISORY AUTHORITY and COMPETENT SUPERVISORY AUTHORITY shall mean the competent data protection authority of one of the countries of the EEA according to applicable EU/EEA law. |
| *Supplier* | A company providing services or products to Jotun. |
| *Third Country* | THIRD COUNTRY shall mean a country that is outside the European Union or EEA, ref. Chapter 5 of the GDPR. |

| | |
|---|---|
| *Transfer* | For the purpose of the BCR, TRANSFER shall mean the situation where:<br><br>a) A Controller or a Processor (Exporter) is subject to the GDPR for the given Processing;<br><br>b) The Exporter by transmission or otherwise makes Personal Data, subject to this Processing, available to another Controller, joint Controller or Processor (Importer); and<br><br>c) The Importer is in a Third Country, irrespective of whether or not this Importer is subject to the GDPR for the given Processing in accordance with GDPR Article 3 or is an international organisation. |

**INTERPRETATIONS**

Interpretation principles of the BCR:

i. Unless the context requires otherwise, all references to a particular Article or Annex are referred to that Article or Annex in or to this document, as they may be amended from time to time.
ii. Headings are included for convenience only and are not to be used in construing any provisions of the BCR.
iii. If a word or phrase is defined, its other grammatical forms have a corresponding meaning.
iv. The words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa.
v. A reference to a document (including, without limitation, a reference to the BCR) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by the BCR or that other document.

## APPENDIX 1 PROCESSING OF PERSONAL DATA (BUSINESS PURPOSES)

| Activity | Purpose of Processing | Categories of Personal Data | Categories of Data Subjects | Transfers of Personal Data |
|---|---|---|---|---|
| HR | Recruitment | Name, gender, email, phone number, CV, background checks, interviews, offer/rejection letters etc. | Candidates applying for a job at Jotun | Personal Data may be Transferred to all Group Companies outside the EEA as part of global processes |
| | HR management | Contact information, date of birth, personal identification number, passport information, health information, sick leave information, salary, union membership, education, expenses, Employee reviews and Personal Data related to leaves and vacation management, payroll and expense management, insurance and pension overview | Employees (incl. temporary, current and former), apprentices, students, contractors, consultants, next of kin and dependents | Most of the Processing is carried out within the individual Group Companies. However, Personal Data may be Transferred to all Group Companies outside the EEA as part of global processes |
| Operations | Business operations | Personal Data related to planning, scheduling timetables, time recording, logistics, shipping, conducting surveys and controls | Employees, Suppliers, contractors, consultants | Personal Data may be Transferred to all Group Companies outside the EEA as part of global processes |
| HSEQ | HSEQ management | Personal data related to access control logs, CCTV recordings, visitor registration system, overview of training, | Employees, contractors, consultants, next of kin and dependents, representative | Personal Data is, as a general rule, accessible only to the individual Group |

| | | | | |
|---|---|---|---|---|
| | | competency and safety certificates, support and management of occupational health services, chemical exposure control register, registration and management of HSEQ related information (incidents, issues etc.) | s of Suppliers and Customers | Company, but may be Transferred to all Group Companies as part of global processes |
| CRM | Management and administration of business relationships | Name, company name, address, email address, phone number and other Personal Data related to managing business relationships, handling Customer orders, delivery, invoicing, project administration, support and complaint handling | Employees, contractors, consultants, representatives of Suppliers and Customers | Personal Data is, as a general rule, accessible only to the individual Group Company or the Group Companies within the respective country, but it may be Transferred to all Group Companies as part of global processes |
| Marketing | Newsletter subscription | Name and email address | Employees, contractors, consultants, representatives of Suppliers and Customers | Personal Data is, as a general rule, accessible only to the individual Group Company or the Group Companies within the respective country, but it may be Transferred to all Group |
| | Participant lists for campaigns and events | Names, email address, allergies (if relevant) | | |
| | Websites | Cookie information, comments and favorites on websites, name and email address | | |
| | Social media campaigns | Aggregated user data, e.g. number of total clicks on an ad | | |

| | | | | |
|---|---|---|---|---|
| | Paint school/paint and colour academy | Name, email address, job role and phone number | | Companies as part of global processes |
| IT | IT administration, support and security | Personal Data necessary for IT-administration, support and security, such as overview of devices, profile/account information, electronic logs etc. | Employees, contractors, consultants, Suppliers' and Customers' authorized users of IT services provided by Jotun | Personal Data may be Transferred to all Group Companies outside the EEA as part of global processes |
| Compliance | Whistleblowing and investigations | Personal Data related to e.g. the notifying person, details of potential misconduct, information on alleged person(s) involved and information revealed as part of the investigation | Employees, contractors, consultants, representatives of Suppliers and Customers | Personal Data may be Transferred to all Group Companies outside the EEA as part of global processes |
| | Compliance with legal obligations and protection of legal position | Personal Data related to e.g. tax and accounting and information relating to legal proceedings | Employees, contractors, consultants, representatives of Suppliers and Customers | Personal Data may be Transferred to all Group Companies outside the EEA as part of global processes |