BINDING CORPORATE RULES

PUBLIC VERSION

TABLE OF CONTENTS

INTRODUCTION

Jotun A/S and its Group Companies (Jotun) have committed themselves to the protection of Personal Data of Jotun Employees and the protection of Personal Data of Jotun Customers and Suppliers (Data Subjects).

These Data Protection Binding Corporate Rules (BCR) have 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 to a Group Company located outside of the European Economic Area (EEA).

Jotun will supplement these rules through sub-policies that are consistent with this BCR, typically through internal policies and operational procedures.

1. SCOPE, APPLICABILITY AND IMPLEMENTATION

1.1. Scope

This 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. Data Processors that handle Personal Data on behalf of Jotun shall be subject to the same rules that apply to Jotun.

This 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

This 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

Employees and Data Subjects keep any rights and remedies they may have under applicable local law. This BCR shall apply only where it provides supplemental protection. Where applicable local law provides more protection than this BCR, local law shall apply. Where this BCR provides more protection than applicable local law or provides additional safeguards, rights or remedies, this BCR shall apply.

1.4. Accountability and binding nature

The Controller shall be accountable for compliance with this BCR.

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

Group Companies shall ensure adherence to this BCR via necessary actions that are required by the statutory local law and the respective corporate governance regulations.

1.5. Records of Processing activities

All members of the BCR shall maintain an electronic record of Processing activities under its responsibility. The record shall contain the following information:

i. Controller name and contact details
ii. Purposes of the Processing

iii. Categories of Employee and Data Subjects and categories of Personal Data
iv. Categories of recipients
v. Transfers of data to External Parties
vi. Retention policy for the different categories of Personal Data
vii. Information regarding ISMS and this BCR

The record shows the nature and categories of processed Personal Data. The records of processing activities shall be made available to the Supervisory Authority on request.

1.6. Effective date and access

This BCR has been adopted by Jotun and shall enter into force when approved (Effective Date).

The BCR will be available on JOIN for the Employees at all times. Other Data Subjects than Employees, including Suppliers and Customers, will have access to parts of the BCR on which information to the data subjects is mandatory in accordance with Art. 47.2.g GDPR and this will be published on the Jotun webpages and in other suitable interfaces. On the Jotun webpages and in other suitable interfaces all Data Subjects benefitting from the third party beneficiary rights will be provided with the information as required by Articles 13 and 14 GDPR, information on their third party beneficiary rights with regards to the processing of their Personal Data and on the means to exercises those rights, the clause relating to the liability and the clauses relating to the data protection principles.

1.7. Data protection principles

Jotun acknowledge the data protection principles in the GDPR and shall through the implementation of and by compliance with this BCR adhere to these principles. In particular;

i. the purpose limitation principle (BCR art.2.1.1),
ii. the accuracy and data minimisation principle, processing of special categories of personal data and limited storage periods (BCR art. 2.4, 2.7.2, 2.6 and 2.7.1),
iii. data protection by design and default principle (BCR art.4.1),
iv. the principle of lawfulness, fairness and transparency (BCR 2.1, 2.9 and 5),
v. measures to ensure data security (BCR art. 4.3), and
vi. the requirements for onward transfers to bodies not bound by the BCR, hereunder the principles for integrity and confidentiality (BCR art.4.6 and 4.9).

1.8. Third party beneficiary rights

Employees and Data Subjects whose personal data is transferred from an EU/EEA Jotun entity to a Jotun entity outside the EU/EEA and processed there, shall be able to enforce the rights listed below as third party beneficiaries, and obtain compensation in case of any breach of one of the enforceable elements. Such employees and Data Subjects have the right to lodge a complaint with a supervisory authority and the right to an effective judicial remedy when the rights conferred to them under this BCR have been infringed as a result of Processing of their Personal Data in non-compliance with this BCR. The enforceable rights for Employees and Data Subjects under this BCR include the right;

i. to have Personal Data Processed according to the data protection principles (BCR Art. 1.9) and in a transparent matter with easy access to this BCR (BCR art. 1.6, 2.9 and art. 5 GDPR);
ii. to access to and rectification of Personal Data (BCR art. 4.2);
iii. to have Personal Data deleted and restricted or object to Processing (BCR art. 2.9, 2.7.2 and 3.5, 3.6, 4.2.1 and 4.2.4), right not to be subject to decisions based solely on automated processing, including profiling (BCR art. 4.6);
iv. to enforce liability and jurisdiction provisions (art. 47.2.e and f GDPR), to obtain judicial remedies and redress and, where appropriate, the right to obtain compensation in case of any breach of one of the enforceable elements, and to lodge a complaint internally in Jotun as well as with a competent supervisory

authority (choice before the authority in the Member State of complainants habitual residence, place of work or place of the alleged infringement, pursuant to art. 77-82 GDPR) or the courts according to BCR art. 4.14 (choice for the data subject to act before the courts where the controller or processor has an establishment or where the data subject has his or her habitual residence pursuant to art. 79 GDPR)

Data subjects shall furthermore be able to enforce the following elements of the BCR:

i. National legislation preventing respect of BCRs (Art. 47.2.m GDPR, see BCR art 4.15);

v. Right to complain through the internal complaint mechanism of the companies (Art. 47.2.j GDPR, see BCR art. 4.13)

vi. Cooperation duties with Data Protection Authority (Art. 47.2.k and l GDPR, see BCR art. 4.14.7 and 4.13)

2. ON PERSONAL DATA OF EMPLOYEES

2.1. General rules for collecting and Processing Employee Personal Data

2.1.1. Legitimate Business Purposes (Purpose limitation)

Employee Personal Data shall be collected, used or otherwise Processed for one or more of the following Business Purposes:

i. *Human resources and personnel management purposes*
This includes Processing that is necessary for the performance of an employment contract, or other contract with an Employee (or to take necessary steps at the request of an Employee prior to entering into a contract), and for administrating the employment or the employment-at-will relationship. e.g. management and administration of recruiting and outplacement, compensation and benefits, payments, tax issues, career and talent development, performance evaluations, disciplinary actions, training, travel and expenses and Employee communications.

ii. *Business process execution and internal management purposes*
This includes activities such as scheduling of work, recording time, managing company assets, for efficiency purposes, conducting internal audits and investigations, implementing business controls and managing and using Employee directories, transaction history.

iii. *Health, safety and security purposes*
This includes activities such as those involving occupationally safety and health, the protection of companies' and Employee assets and the authentication of Employee status and access rights, including the issuing of access cards with photo id.

iv. *Organizational analysis and development and management reporting purposes*
This includes activities such as conducting Employee surveys, managing mergers, acquisitions, divestitures and Processing Employee Personal data for management reporting and analysis.

v. *Compliance with legal obligations*
This includes the Processing of Employee Personal data as necessary for compliance with Jotun's legal obligations. Such as tax reporting and book-keeping obligations.

vi. *Protecting the vital interests of Employees or Data Subjects*
This includes Processing which is necessary to protect the vital interests of an Employee or Data Subject.

If there is doubt of whether the Processing of Employee Personal Data can be based on a Business Purpose listed above, the advice of the Global Data Protection Officer shall be sought before the Processing takes place.

2.2. Employee Consent

In general, Employee Consent cannot be used as legal grounds for Processing Employee Personal Data. Thus, Employee Personal Data cannot be Processed unless Jotun has a

legitimate interest related to a specific Business Purpose. If applicable local law so requires, Jotun shall seek Employee Consent for the Processing, in addition to having a Business Purpose for the relevant Processing. If none of the Business Purposes applies, Jotun may request Employee Consent for Processing Employee Personal Data, but only if the Processing has no foreseeable adverse consequences for the Employee.

A request for Employee Consent requires the authorization of the Global Data Protection Officer prior to seeking Consent.

2.2.1. Denial or withdrawal of Employee Consent

The Employee may both deny Consent and withdraw Consent at any time without consequence to his/her employment relationship. Where Processing is undertaken at the Employee's request (e.g. he/she subscribes to a service or seeks a benefit), he/she is deemed to have provided Consent to the Processing.

When seeking Employee Consent, Jotun shall at the same time inform the Employee;

i. of the purposes of the Processing for which Consent is requested;
ii. of the possible consequences for the Employee of the Processing; and
iii. that the Consent is freely given, and that he/she is free to refuse and withdraw Consent at any time without any kind of consequence.

2.3. Limitations on Processing Data of Dependants of Employees

Jotun will Process Personal Data of Dependants of an Employee if;

i. the Personal Data were provided with the Consent of the Employee or the Dependant; or
ii. Processing of the Personal Data is necessary for the performance of a contract with the Employee or for managing the employment-at-will relationship; or
iii. the Processing is required by mandatory applicable local law; or
iv. The Processing is permitted by applicable local law and not prohibited by this BCR.

Should this Personal Data pertain a child belonging to the household of an employee, particular care shall be taken in processing such information.

2.4. Data minimisation

Jotun shall restrict the Processing of Employee Personal Data to Personal Data that are adequate, relevant and limited to what is necessary in relation to the applicable Business Purposes for which they are Processed. Jotun shall take every reasonable step to delete Employee Personal Data that are not required for the applicable Business Purpose.

2.5. Use of Employee Personal Data for Secondary Purposes

2.5.1. Use of Employee Personal Data for Secondary Purposes

Generally, Employee Personal Data shall be used only for the Business Purposes for which they were originally collected (Original Purpose). Employee Personal Data may be Processed for a legitimate Business Purpose of Jotun different from the Original Purpose (Secondary Purpose) only if the Original Purpose and Secondary Purpose are compatible. In all such cases an assessment of compatibility shall be undertaken and documented and the Employee shall be informed of the processing prior to its commencement.

Depending on the sensitivity of the relevant Employee Personal Data and whether use of the Data for the Secondary Purpose has potential negative consequences for the Employee, the secondary and compatible use may require 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 Employee Consent in accordance with Article 2.2.

Typical use that may, according to a closer documented assessment of compatibility, constitute permitted secondary use in accordance with Article 2.5.1 are;

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.

2.6. Purposes for Processing Special Categories Personal Data of Employees

2.6.1. Specific purposes for Processing

Jotun shall Process Special Categories Personal Data of Employees only to the extent necessary to serve the applicable Business Purpose.

The following categories of Special Categories Personal Data of Employees may be collected, used, or otherwise Processed only for one or more of the Business Purposes specified below:

i. Racial or ethnic data:
   a. In some countries, photos and video images of Employees qualify as racial or ethnical data. Jotun may nevertheless Process photo and video images for the protection of Jotun and Employee assets, site access, security reasons and for inclusion in the Employee directories
   b. providing preferential status to persons from particular ethnic or cultural minorities Jotun can Process these categories of Personal Data to remove or reduce inequality or to ensure diversity in staffing, provided that the use of the relevant Special Categories of Personal Data allows for an objective determination that an Employee belongs to a minority group and that the Employee has not filed a written objection to the relevant Processing.

ii. *Physical or mental health data*
   Physical or mental health data includes any opinion of physical or mental health and data relating to disabilities and absence due to illness or pregnancy. This Personal Data can be Processed in order for Jotun to:
   a. Provide health services to an Employee provided that the relevant health data are Processed by or under the supervision of a health professional who is subject to professional confidentiality requirements;
   b. administer pensions, health and welfare benefit plans, maternity, paternity or family leave programs, or collective agreements (or similar arrangements) that create rights depending on the state of health of the Employee;
   c. reintegrate or provide support for Employees entitled to benefits in connection with illness or work incapacity;
   d. asses and make decisions on (continued) eligibility for positions, projects or scope of responsibilities, or to
   e. provide facilities in the workplace to accommodate health problems or disabilities.

iii. *Criminal data*
Criminal data includes data relating to criminal behaviour, criminal records or proceedings regarding criminal or unlawful behaviour. This Personal Data can be Processed by Jotun in order to:
   a. Asses an application by an Employee to make a decision about the Employee or provide a service to the Employee; or
   b. to protect the interest of Jotun with respect to criminal offences that have been or, given the relevant circumstances are suspected to have been, committed against Jotun or its Employees.

iv. *Sexual preference*
The information on sexual preference can be inferred from data relating to partners of Employees. This Personal Data can be Processed by Jotun in order to:
   a. Administer Employee pensions and benefits programs; and
   b. administering Employee memberships.

v. *Religious or philosophical beliefs*
Information relating to religious or philosophical beliefs can be Processed in order for Jotun to:
   a. Accommodate for religious or philosophical practices, dietary requirements or religious holidays.

vi. *Trade-union membership*
Information regarding trade-union membership can be Processed in order for Jotun to:
   a. Facilitate and register any Employee' tax rebates in connection with costs related to memberships in trade-unions.

vii. *Biometric data*
Biometric data may include fingerprints, face recognition software solutions and iris scans, and may be Processed for the purpose of information security and for the protection of Jotun' and Employee assets, site access and security reasons.

2.6.2. General purposes for Processing of Special Categories Personal Data of Employees

In addition to Purposes mentioned in 2.6.1, all categories of Special Categories Personal Data of Employees may be Processed if it is;

i. required by or allowed under applicable EU/EEA;
ii. to establish, exercise, or defend a legal claim;
iii. to protect a vital interest of the Employee, but only where it is impossible to obtain the Employee's Consent first; and
iv. to the extent necessary to comply with an obligation of international public law (e.g. treaties); or
v. where the Special Categories Personal Data of Employees have manifestly been made public by the Employee.

2.6.3. Employee Consent for Processing Special Categories Personal Data of Employees

Employee Consent generally cannot be used as legal basis for Processing Special Categories Personal Data of Employees. One of the grounds listed in Article 2.6.1 or 2.6.2 shall exist for any Processing of Special Categories of Personal Data.

If applicable local law so requires, in addition to having one of the grounds listed in Article 2.6.1 or 2.6.2 for the relevant Processing, Jotun shall also seek Employee Consent for the Processing. If none of the grounds listed in Article 2.6.1 or 2.6.2 applies, Jotun may request Employee Consent for Processing Special Categories Personal Data of Employees, but only if the Processing has no foreseeable adverse consequences for

the Employee (e.g. Employee diversity programs or networks, research, product development, selection of candidates in hiring or management development processes). Article 2.2 applies to the granting, denial or withdrawal of Employee Consent.

2.6.4. Prior authorization of Global Data Protection Officer

Where Special Categories Personal Data of Employees is Processed based on legal requirements other than the local law applicable to the Processing, or based on the Consent of the Employee, the Processing requires the prior authorization of the Global Data Protection Officer.

2.6.5. Use of Special Categories of Personal Data for Secondary Purposes

Special Categories of Personal Data of Employees or Dependents may be Processed for Secondary Purposes in accordance with this Article 2.6 and Article 2.5.

2.7. Data quality

2.7.1. Storage period

Jotun generally shall retain Employee Personal Data only for the period required to serve the applicable Business Purpose, to the extent 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 record retention schedule) a time period for which certain categories of Employee 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.

2.7.2. Quality of Personal Data

Employee Personal Data shall be accurate, complete and kept up-to-date.

2.8. "Self-service"

Where Jotun requires an Employee to update his/her own Employee Personal Data, Jotun shall remind him/her at least once a year to do so.

2.9. Employee information requirements

2.9.1. When obtaining Personal Data from the Employee

Jotun shall, at the time when the Personal Data is obtained or earlier, inform Employees through a published privacy policy or notice about:

i. The Business Purpose and legal basis for which the Data are Processed and where legal basis is legitimate interest, information on what legitimate interests are pursued;
ii. which Group Company is responsible for the Processing;
iii. The contact information of the Local Data Protection Coordinator and Global Data Protection Officer
iv. How long the Personal Data will be stored;
v. The right to lodge a complaint with their local supervisory authority;
vi. The existence of the right to access their Personal Data and receive a copy
vii. The right to request that their Personal Data is rectified if the Personal Data is not correct and to have it erased or demand restricted Processing under certain conditions.

viii. The right to object to Processing and to data portability, thus having Jotun transfer their data to a new Processor;
ix. The obligation to provide Jotun with certain Personal Data
x. The categories of External Parties to which the Personal Data are disclosed (if any)
xi. Where applicable, if the Personal Data will be transferred to a third country and the applicable safeguards taken,
xii. How Employees can exercise their rights.

2.9.2. When obtaining Personal Data from other sources

If obtaining information on an Employee from other sources than the Employee, Jotun shall inform the Employee as set out in item 2.9.1 above, and in addition:

i. From which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

Such information shall be given

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 Employee, at the latest at the time of the first communication to that Employee; or
iii. if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

2.9.3. Exemptions

The duty to inform does not apply when, according to a documented assessment:

1. the Employee already has the information.

3. ON PERSONAL DATA OF DATA SUBJECTS

3.1. Purposes for Processing Personal Data of Data Subjects

3.1.1. Legitimate Business Purposes

Personal Data of Data Subjects, shall be collected, used or otherwise Processed for the following Business Purposes, for which legal basis shall be documented. Global Data Protection Officer shall be consulted before processing is based on an assessment of legitimate interest and in all situations where there is uncertainty on the legal basis. Relevant purposes and legal basis are:

i. Based on that the processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
ii. Based on the conclusion and execution of agreements with Customers, Suppliers and Business Partners Personal data may be used for the purpose to record and financially settle delivered services, products and materials to and from Jotun.

iii. In order to comply with legal obligations, Jotun may process Personal Data for purposes such as managing company assets, conducting internal audits and investigations, finance, tax and accounting.

iv. Based on documented assessments of legitimate interest, typical purposes may be:

- Implementation of business controls, provision of central processing facilities for efficiency purposes, managing mergers, acquisitions and divestitures, and Processing Personal Data for management reporting and analysis.
- Development and improvement of products and/or services purposes, including Processing that is necessary for the development and improvement of Jotun products and/or services, research and development.
- Relationship management and marketing purposes, including activities such as maintaining and promoting contact with Customers, Suppliers and Business Partners, account management, customer service, recalls and the development, execution, and analysis of market surveys and marketing strategies.
- Business process execution, internal management, and management reporting purposes, including activities such as Health, safety and security purposes as well as
- activities relating to the protection of Jotun and Employee assets, and the authentication of Customer, Supplier or Business Partner status and access rights.

Processing in order to protect vital interests of Employees or Data Subjects, including processing that is necessary to protect the vital interests of an Employee or Data Subject.

3.2. Consent of the Data Subject

If a legal basis does not exist or if applicable local law so requires, Jotun shall seek Consent from the Data Subject for the Processing.

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.

When seeking Consent or when Consent is otherwise obtained, Jotun shall inform the Data Subject:

i. Of the Purposes and legal basis of the Processing for which Consent is required;
ii. that Consent can be withdrawn at any time;
iii. the consequences of the Consent being withdrawn;
iv. the contact information of the Local Data Protection Coordinator;
v. how long the Personal Data will be stored;
vi. the right to lodge a complaint with their local supervisory authority;
vii. the existence of the right to access, rectification, erasure, restriction, objection and data portability;
viii. the categories of External Parties to which the Personal Data is disclosed (if any), and
ix. how Data Subjects can exercise their rights.

3.2.1. Denial or withdrawal of Consent

The Data Subject may both deny Consent and withdraw Consent at any time.

3.3. Use of Subject Personal Data for Secondary Purposes

Generally, Personal Data shall be used only for the Business Purposes for which they were originally collected (*Original Purpose)*.

Personal Data may be Processed for a legitimate Business Purpose of Jotun different from the Original Purpose (Secondary Purpose) only if the Original Purpose and the Secondary Purpose are compatible. Depending on the sensitivity of the relevant Personal Data and whether use of the Data for the Secondary Purpose has potential negative consequences for the Data Subject, the Secondary use may require additional measures such as:

i. Limiting access to the Personal Data;
ii. imposing additional confidentiality measurements;
iii. taking additional security measures;
iv. informing the Data Subject about the Secondary Purpose;
v. providing an opt-out opportunity; or
vi. obtaining Data Subject Consent in accordance with Article 3.2.

Typical use that may, according to a closer documented assessment of compatibility, constitute permitted secondary use in accordance with Article 2.5.1 are:

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.

3.4. Purposes for Processing Special Categories of Personal Data on Data Subject

This Article sets forth specific rules for Processing Special Categories of Personal Data. Jotun shall Process Special Categories of Personal Data only to extent necessary to serve the applicable Business Purpose. The following categories of Special Categories of Personal Data may only be collected, used, or otherwise Processed for one or more of the purposes specified below:

i. Racial or ethnic data: In some countries photos and video images of Data Subjects qualify as racial or ethnic data. Jotun may Process photos or video images for the protection of Jotun and Employee assets, site access, and security reasons, and the authentication of Customer, Supplier or Business Partner status and access right.
ii. Criminal data (including data relating to criminal behaviour, criminal records, or proceedings regarding criminal or unlawful behaviour) can be Processed for the purpose of protecting the interests of Jotun with respect to criminal offences that have been or, given the relevant circumstances are suspected to have been, committed against Jotun or its Employees.

In addition to the specific purposes listed above, all categories of Special Categories of Personal Data may be Processed under one or more of the following circumstances:

i. The Data Subject has given the explicit Consent to the Processing thereof;
ii. as required by or allowed under applicable local law;
iii. for the establishment, exercise, or defence of a legal claim;
iv. to protect a vital interest of an Data Subject, but only where it is impossible to obtain the Data Subject`s Consent first;
v. to the extent necessary to comply with an obligation of international public law (e.g. treaties); or

vi. if the Special Categories of Personal Data have manifestly been made public by the Data Subject.

The information requirements apply to the granting, denial, or withdrawal of Consent.

Where Special Categories of Personal Data is Processed based on a requirement of law other than the local law applicable to the Processing, the Processing requires the prior authorization of the Global Data Protection Officer.

Special Categories of Personal Data of Data Subjects may be Processed for Secondary Purposes in accordance with Article 3.3.

3.5. Quantity and quality of Data

Jotun shall restrict the Processing of Personal Data to Data that are adequate for and relevant to the applicable Business Purpose. Jotun shall take every reasonable step to delete Personal Data that are not required for the applicable Business Purpose.

Jotun generally shall retain Personal Data only for the period required to fulfil the applicable Business Purpose, to the extent it is reasonably necessary to comply with an applicable legal requirement or advisable in light of an applicable statute of limitations. Jotun shall specify (e.g., in a sub-policy, notice, or retention schedule) a time period for which certain categories of Personal Data may be kept. Promptly after the applicable storage period has ended, the Global Data Protection Officer shall ensure that the Data is:

i. Securely deleted or destroyed; or
ii. anonymized or de-identified.

Personal Data shall be accurate, complete, and kept up-to-date.

3.6. Data Subject information requirements

3.6.1. When obtaining Personal Data from the Data Subject

In line with the requirements set forth in GDPR and specifically as set out in Article 13 and 14, Jotun shall at the time when the Personal Data is obtained or earlier, inform Data Subjects through a privacy policy or notice about:

iii. The Business Purpose and legal basis for which the Data are Processed and where legal basis is legitimate interest, information on what legitimate interests are pursued;
iv. which Group Company is responsible for the Processing;
v. The contact information of the Local Data Protection Coordinator and Global Data Protection Officer;
vi. How long the Personal Data will be stored;
vii. The right to lodge a complaint with their local supervisory authority;
viii. The existence of the right to access their Personal Data and receive a copy;
ix. The right to request that their Personal Data is rectified if the Personal Data is not correct and to have it erased or demand restricted Processing under certain conditions;
x. The right to object to Processing and to data portability, thus having Jotun transfer their data to a new Processor;
xi. The categories of External Parties to which the Personal Data are disclosed (if any);
xii. Where applicable, if the Personal Data will be transferred to a third country and the applicable safeguards taken,

xiii. How Data Subjects can exercise their rights.

3.6.2. When obtaining Personal Data from other sources

If obtaining information on a Data Subject from other sources than the Data Subject, Jotun shall inform the Data Subject as set out in item 3.6.1 above, and in addition:

ii. From which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

Such information shall be given

iv. 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;
v. 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
vi. if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

3.6.3. Exemptions

The duty to inform does not apply when, according to a documented assessment:

1. the Data Subject already has the information;

When the information originates from another source that the Data Subject, the duty to inform does not apply when, according to a documented assessment:

1. 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 GDPR Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases Jotun shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

2. obtaining or disclosure is expressly laid down by Union or Member State law to which Jotun is subject and which provides appropriate measures to protect the Data Subject's legitimate interests; or

3. where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

4. REGULATION PERTAINING TO PERSONAL DATA OF EMPLOYEES AND DATA SUBJECTS

4.1. Data Protection by design and default

Only Personal Data which are necessary for each specific Business Purpose of the processing shall be Processed by Jotun. 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, Jotun shall ensure that by default, Personal Data are not made accessible to an indefinite number of natural persons without the specific and deliberate action of a person, and to implement necessary safeguards designed to

meet the requirements of GDPR and protect the rights of the Employees and the Data Subjects.

4.2. Rights of Access and Rectification

4.2.1. Right of Access

All Employees and Data Subjects have the right to obtain from the Controller parts of the BCR on which information to the data subjects is mandatory (ref Section 1.6) 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. Where applicable, the Employees and Data Subjects shall receive information regarding the source, type, purpose and categories of recipients of the relevant Personal Data as well as how long the Personal Data will be stored, the rights of rectification, erasure and the right to complain to their local supervisory authority.

If the Personal Data is incorrect, incomplete, or not Processed in compliance with applicable law or this BCR, the Employees or Data Subjects have the right to have the Personal Data rectified, deleted or blocked (as appropriate). In addition, they have the right to object to the Processing of Personal Data and demand restricted Processing.

4.2.2. Request Procedure

The Employee or Data Subject should send his/her request to the Global Data Protection Officer. Prior to fulfilling the request, Jotun may request the Employee or 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
v. and
vi. 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.

4.2.3. Response period

As soon as possible, and no later than one month after receiving the request, the Global Data Protection Officer shall inform the Employee or Data Subject in writing:

i. Of Jotun's position with regards to the request and any action Jotun has taken or will take in response, hereunder handing out the required information; or
ii. in case that several Employees or Data Subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of Jotun, the ultimate date on which he/she will be informed of Jotun's position, which date shall be no later than one month thereafter.

4.2.4. Complaint

An Employee or Data Subject may file a complaint in accordance with Article 4.12.1 if:

i. The response to the request is unsatisfactory to the Employee or Data Subject (e.g. the request is denied);
ii. the Employee or Data Subject has not received a response as required by Article 4.2.3; or

iii. the time period provided to the Employee or Data Subject in accordance with Article 4.2.3 is, in light of the relevant circumstances, unreasonably long and the Employee or Data Subject has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response.

4.2.5. Denial of Requests

Jotun may deny a request if:

i. The identity of the relevant Employee or 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.

4.3. Security and Confidentiality Requirements

4.3.1. 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.

4.4. Automated decision making including profiling

Automated tools or profiling may be used to make decisions about Employees or Data Subjects, but decisions may not be based solely on the results provided by the automated tool or profiling. The restriction does not apply if:

i. The use of automated tools is required or authorized by EU or member state law;
ii. the decision is necessary for entering into or performing a contract between Jotun and the Data Subject, such as
    a. where automated tools are used to filter submissions for promotional or contest purposes
    b. managing the employment- relationship, e.g. where automated tools are used to filter job applications.

Such decisions shall not be based on special categories of personal data unless it is based on explicit consent or processing is necessary for reasons of substantial public interest, or on the basis of Union or Member State law which shall be proportionate to the aim pursued, and respect the essence of the right to data protection and provide for suitable and that specific measures to safeguard the fundamental rights and the interests of the data subject are in place.

If using automated decision making including profiling, the Data Subject shall be given meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

If such processing is based on entering into or performing a contract or consent, suitable measures shall be implemented 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.

4.5. Intra-group Processing of Personal Data

4.5.1. Intra-group Processing

Transferring Personal Data between Group Companies which have adhered to this BCR may be done pursuant to the terms herein.

When one Group Company acts as Processor for another Group Company being the Controller, the Processor is obliged to:

i. Delete all information transferred from the Controller once the assignment for the Group Company is terminated.
ii. Establish and maintain sufficient procedures to safeguard the Processed Personal Data according to the Controller's local legislation and this BCR.
iii. Not subcontract the Processing without a written consent from the Controller, either in the form of a specific written confirmation or as set out below in this BCR. Such subcontracting shall only take place by way of a written agreement with the sub-processor which imposes at least the same obligations on the sub-processor as are imposed on the Processor under this BCR.
iv. Notify the Controller immediately upon any breaches of applicable data protection law and this BCR with impact on the Personal Data being Processed.
v. Making available relevant documentation regarding security, risk, quality assurance, IT-systems and registers to its personnel.
vi. Implement the regime for audits and controls set forth in this BCR.
vii. Provide all necessary support to the Controller in regards to the handling of requests from Employees and Data Subjects relating to their rights.

4.5.2. Intra-group transfer (to another Group Company Controller)

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

4.5.3. Consent to sub-processing

As Controllers, the Group Companies bound to this BCR, consent to sub-contracting as set out under 4.5.1, provided that:

i. The Processor provides prior notice to the Controller about the sub-contracting
ii. The Processor has provided sufficient safeguards, as set out in 4.5.1.

4.6. Transfer to External Parties

4.6.1. General

This Article sets forth requirements concerning the transfer of Personal Data from Jotun to an External Party.

4.6.2. External Controllers and External Processors

There are two categories of External Parties:

i. *External Processors:*
These are External Parties that Process Personal Data solely *on behalf of* Jotun, under Jotun's direction (e.g. External Parties that Process salaries on behalf of Jotun).
ii. *External Controllers:*
These are External Parties that Process Personal Data and determine the purpose and means of the Processing. For Employee Personal Data this may be government authorities or service providers that provide services directly to Employees.

4.6.3. Transfer for applicable purposes only

Jotun shall transfer Personal Data to an External Party only to the extent necessary to serve the applicable Business Purpose for which the Personal Data are Processed

(including Secondary Purposes as per Article 2.5, 2.1 or purposes for which the Employee or Data Subject has provided Consent in accordance with Article 2.2).

4.6.4. External Controller contracts

External Controllers (other than government agencies) may Process Personal Data only if they have a written contract with Jotun. In the contract Jotun shall seek to contractually protect the Personal data of Employees or the Data Subjects. All such contracts shall be drafted in consultation with the Global Data Protection Officer.

4.6.5. External Processors contracts

External Processors may Process Personal Data only if they have a written contract with Jotun. The contract with an External Processor shall include the following provisions:

i. The Processor shall Process Personal Data only in accordance with Jotun's instructions and for the purposes authorized by Jotun.
ii. The Processor shall keep the Personal Data confidential.
iii. The Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Data.
iv. The External Processor shall not permit sub-contractors to Process Personal Data in connection with its obligation to Jotun without the prior written Consent of Jotun.
v. Jotun has the right to review the security measures taken by the External Processor and the External Processor shall submit its relevant data processing facilities to audits and inspections by Jotun or other relevant government authority.
vi. The External Processor shall promptly inform Jotun of any actual or suspected security breach involving Personal Data.
vii. The External Processor shall take adequate remedial measures as soon as possible and shall promptly provide Jotun with all relevant information and assistance as requested by Jotun regarding the security breach.
viii. The External Processor shall provide all necessary support to the Controller in regards to the handling of requests from Employees or Data Subjects relating to their rights.

More details on the process are described in applicable Jotun internal policies.

4.7. Transfer of Personal Data to a Third Country

This Article sets forth additional rules for the transfers of Personal Data to an External Party located in a country that is not considered to provide an "adequate" level of protection for Personal Data (Third Country).

Personal Data may be transferred to an External Party located in a Third Country only if:

i. The transfer is necessary for

a. the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request, e. g. the performance of a contract with the Employee or Data Subject, for managing the employment-at-will relationship, or managing a contract with the Employee or Data Subject or to take necessary steps at the request of the Employee or Data Subject prior to entering into a contract or an employment-at-will relationship, e.g. for processing job applications or orders; or

b. the conclusion of performance of a contract concluded in the interest of the Employee or Data Subject between Jotun and an External Party (e.g. in case of the booking of an airline ticket);

AND

ii.

a. a contract has been concluded between Jotun and the relevant External Party that provides for safeguards at a similar level of protection as that provided by this BCR. The contract shall conform to any model contract requirement under applicable law (if any), the EU Standard Contractual Clauses shall be used wherever possible; or External Party has been certified under any applicable arrangement approved by the European Commission that is recognized as providing "adequate" level of data protection; or

OR

iii. the transfer on an exceptional basis

a. is necessary to protect a vital interest of the Employee or Data Subject, where the Employee or Data Subject is physically or legally incapable of giving consent;
b. is necessary for the establishment, exercise or defence of a legal claim;
c. is necessary to satisfy a pressing need to protect the public interests of a democratic society;

4.8. Employee Consent for transfer

Jotun generally shall not seek Employee Consent for a transfer of Employee Personal Data to an External Party located in a Third Country. One of the grounds for transfer listed in Article 4.7 shall exist. If applicable local law so requires, in addition to having one of the grounds listed in Article 4.7 Jotun shall also seek Employee Consent for the relevant transfer. If none of the grounds listed in Article 4.7 exists Jotun may request Employee Explicit Consent for a transfer to an External Party located in Third Country, but only if;

i. the transfer has no foreseeable adverse consequences for the Employee; or
ii. the Consent is requested prior to the participation of the Employee in specific projects, assignments or tasks that require the transfer of the Personal Data.

Requesting Employee Explicit Consent for a transfer requires the prior approval of the Global Data Protection Officer. Prior to requesting Employee Explicit Consent, the Employee shall be provided with the following information:

i. the purpose of the transfer;
ii. the identity of the transferring Group Company;
iii. the identity or categories of External Parties to which the Personal data will be transferred;
iv. the categories of Personal Data that will be transferred;
v. the country to which the Personal Data will be transferred; and
vi. the fact that the Personal Data will be transferred to a Third Country, where the Personal Data may be processed by a controller who is not bound by the BCR.

Article 2.6.3 and 2.2.1 applies to denial or withdrawal of Consent.

4.9. Supervision and compliance

4.9.1. Global Data Protection Officer

Controller shall appoint a Global Data Protection Officer who is responsible for supervising the general Group level compliance with this BCR.

4.9.2. Regional Data Protection Coordinators

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

4.9.3. Process owners

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

Local Data Protection Coordinator shall;

Assist the GM/MD to ensure overall Personal Data protection management compliance within the company.

4.10. Training

4.10.1. Employee Training

Jotun shall provide training in this BCR and related confidentiality obligations to Employees. Training will be tailored to the needs and tasks of the Employee.

4.11. Monitoring and auditing compliance

4.11.1. Audits

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

4.12. Complaints procedure

4.12.1. Complaints from Employees or Data Subjects

Employees and Data Subjects may file a complaint, preferably in writing, regarding compliance with this BCR or violations of their rights under applicable local law and;

i. send it to dataprotection@jotun.com;
ii. file it with the Global Data Protection Officer;
iii. lodge a complaint at their local supervisory authority in the EU/EEA member state where the Employee or Data Subject has his/her habitual residence, place of work or the place where the alleged infringement took place; or
iv. lodge a complaint before the competent court where the Controller or Processor has an establishment or where the Employee or Data Subject has his/her habitual residence.

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

4.12.2. Reply to Employee or Data Subject

Within one month of Jotun receipt of a complaint, the Global Data Protection Officer shall inform the Employee or 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 Protection Officer shall send a copy of the complaint and his/her written reply to the Regional and Local Data Protection Coordinator.

4.12.3. Complaints to Head of Compliance

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

i. the handling of the complaint by the Global Data Protection Officer is unsatisfactory to the Employee or Data Subject (e.g. the complaint is rejected);
ii. the Employee or Data Subject has not received a response as required by Article 4.12.2;
iii. the time period provided to the Employee or Data Subject pursuant to Article 4.12.2 is, in light of the relevant circumstances, unreasonably long and the Employee or 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 4.12 shall apply to complaints filed with the Head of Compliance.

4.13. Relation to applicable law

4.13.1. 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.

4.13.2. Law applicable to BCR; BCR has supplemental character

This 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 this BCR, local law shall apply. Where this BCR provides more protection than applicable local law or provides additional safeguards, rights or remedies for Employees, this 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.

4.13.3. Supervision of compliance and lead authority

Compliance with this BCR may be supervised by any competent Data Protection Authority. The Norwegian Data Protection Authority, Datatilsynet, is the lead authority regarding the BCR pursuant to WP263 rev.01.

4.13.4. Exclusive jurisdiction under BCR

Jotun A/S agrees, to the extent set out in Article 4.13.5, to take necessary action to remedy the acts of other Group Companies outside of the EEA bound by the BCRs and

to pay compensation for any material or non-material damages resulting from the violation of the BCRs by such Group Company.

If a Group Company located outside the EU violates the BCRs, the courts or other competent authorities in the EU have jurisdiction and the data subject will have the rights and remedies against the Group Company that has accepted responsibility and liability, as if the violation had been caused in the relevant Member State.

4.13.5. Available remedies, limitation of damages, burden of proof regarding damages

Jotun´s liability and responsibility pursuant to this section is subject to the limitations in section 1.10.

Employees or Data Subjects shall be entitled to any effective judicial remedies available to Employees or Data Subjects. Jotun A/S with Head Office in Sandefjord shall be liable for any material or non-material damages suffered by an Employee or Data Subject resulting from a violation of this BCR. Where an Employee or 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.

4.13.6. Cooperation with the relevant Data Protection Authority

All Group Companies accept to cooperate with and be audited by the relevant European data protection authorities and comply with their legally binding orders. BCR members outside EEA will through adhering to this BCR commit to comply with legally binding orders issued by supervisory authorities in the EEA.

4.14. Conflict between the BCR and applicable local law

4.14.1. Conflict of law when transferring data

Where a legal requirement to transfer Personal Data conflicts with the laws of the Member States of the EEA, the transfer requires the prior approval of the Global Data Protection Officer. The Global Data Protection Officer shall seek the advice of the Norwegian Data Protection Authority or another competent government authority.

Where any legal requirement a Group Company is subject to in a third country is likely to have a substantial adverse effect on the guarantees provided by the BCR, the problem shall be reported to the relevant supervisory authority. The supervisory authority should be clearly informed about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure, unless otherwise prohibited.

If in specific cases, notification is prohibited, the Group Company will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so. If, in the above cases, despite having used its best efforts, the Group Company is not in a position to notify the competent supervisory authority, the Group Company must annually provide general information on the received requests to the competent supervisory authorities (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).

In any event, 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.

4.14.2. Conflict between BCR and law

In all other cases, where there is a conflict between applicable local law and the BCR, the relevant Local Data Protection Coordinator shall promptly inform Jotun AS (being

the EU/EEA headquarters) or the EU BCR member with delegated data protection responsibilities and consult with the Global Data Protection Officer to determine how to comply with this BCR and resolve the conflict to the extent reasonably practicable to the relevant Group Company.

4.14.3. New conflicting legal requirements

The relevant Local Data Protection Coordinator shall promptly inform the Global Data Protection Officer of any new legal requirement that may interfere with Jotun's ability to comply with this BCR.

4.15. Changes to the BCR

4.15.1. Prior approval

Any changes to this BCR require the prior approval of Head of Compliance, which shall keep a fully updated list of the Group Companies and keep track of and record any updates to the rules. Significant changes or modifications that affects the level of the protection offered by the BCR shall be promptly notified by Jotun to all BCR members and to the relevant Supervisory Authority together with an explanation of the reasons justifying the update. 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.

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

4.15.2. No Consent

This 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.

4.15.3. Entry into force

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

4.15.4. Relevant BCR

Any request, complaint or claim of an Employee or Data Subject involving this 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.

4.15.5. Applicability for new Group Companies

Transfers involving companies that enter the Jotun Group after the Effective date of this 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.

5. PUBLICATION

The BCR document will be published on JOIN and other interfaces as set out in this BCR article 1.6.

6. CONTACT DETAILS

The Global Data Protection Officer may be contacted at:

dataprotection@jotun.com

Postal address:

Jotun A/S
Att; Group Legal and Compliance
Hystadveien 167,
Pb 2021
3202 Sandefjord
Norway

DEFINITIONS

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 2.1.1or for Processing Special Categories of Personal Data as specified in Article 2.6..
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 Subject	Data Subject shall mean an identifiable, living natural person that is either a Customer, an employee of a Customer, a Supplier or an employee of a Supplier, to whom Personal Data relates.
Data Protection Team	Data Protection Team shall mean the team referred to in Article 0.
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; i. a sale of shares as a result whereof the Group Company so divested no longer qualifies as a Group Company; and/or 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 this 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 EU that transfers Personal Data to Group Company located outside of the EU.
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 company or legal entity of which Jotun A/S, directly or indirectly owns more than 50 per cent of the issued shared capital, has 50 per cent or more of the voting power at general meetings of shareholders, has the power to appoint a majority of the directors, or otherwise directs the activities of such other legal entity; however, any such company or legal entity shall be deemed a Group Company only as long as a liaison and/or relationship exists, and that it is covered by the BCR.
Global Data Protection Officer	Global Data Protection Officer shall mean the officer as referred to in Article 4.9.1.
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 located outside of EU that receives Personal Data from a Group Company located in the EU.
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 4.11.6. and other relevant articles in the BCR.
MD	MD shall mean the Managing Director of a Group Company.
Third Country	THIRD COUNTRY shall mean a country that is outside the European Union or EEA, ref. chapter 5 of the GDPR.
Original Purpose	ORIGINAL PURPOSE shall mean the purpose for which Personal Data was originally collected.
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.
Secondary Purpose	SECONDARY PURPOSE shall mean any purpose other than the Original Purpose for which Employee Data is further Processed.
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.
Supplier	A company providing services or products to Jotun.

INTERPRETATIONS

Interpretation principles of this 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 this 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 this BCR) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by this BCR or that other document.

***