Data Protection

Processing and transfer of personal data in Kvaerner

Binding corporate rules
Public version

Table of contents

1 Introduction

1.1 Scope

The Data Protection Procedure contains a set of legally binding rules within Kvaerner which provide principles for processing of personal data and applies to Kværner ASA and its subsidiaries (including partly owned subsidiaries where Kværner ASA directly or indirectly controls more than 50 percent of the voting interest). For the purpose of this procedure, the term “Kvaerner” refers to the whole company group or each of the legal entities as the case may be.

The Data Protection Procedure applies to all Kvaerner personnel. In addition, third parties such as customers, contractors and others shall benefit from the rights granted to them herein. The Data Protection Procedure has two main purposes:

- Establishing a legal basis for transfer of personal data from legal entities established within the EEA to legal entities established outside the EEA (third countries, as defined below).
- Establishing consistent and uniform principles and procedures for the processing of all personal data in Kvaerner in accordance with applicable EU/EEA data protection law.

The Data Protection Procedure provides a legal basis (binding corporate rules) for transfer of personal data from legal entities within the EEA to legal entities in third countries. Legal entities in third countries are bound by this procedure by their signing of an agreement regarding bindingness.

1.2 Data protection

Data protection is about providing individuals with the right to control the use of any information concerning them.

The Data Protection Procedure is based on applicable EU/EEA data protection law, including the EU General Data Protection Regulation 2016/679 (GDPR). While conducting its day-to-day business Kvaerner processes personal data about its employees, customers, business contacts and others.

Applicable EU/EEA data protection law does not allow for the transfer of personal data to third countries which do not ensure an adequate level of data protection unless there is a legal basis for such transfer. Kvaerner has legal entities in third countries, and the local law of these countries may not ensure an adequate level of data protection. The purpose of the Data Protection Procedure is to ensure adequate safeguards to provide a legal basis for such transfers.

Kvaerner’s Data Protection Procedure is based on the following data protection principles:

- The processing of personal data shall take place in a fair, lawful and transparent way.
- The collection of personal data shall only be made for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes
- The collection of personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose of the intended processing
- Personal data shall be kept accurate and where necessary, up to date
- Personal data shall not be stored longer than is necessary for the purposes for which the data were collected or for which they are further processed
- Personal data shall be kept confidential and stored in a secure way
- Personal data shall not be shared with third parties except when necessary in order for them to provide services upon agreement. In such cases personal data shall be protected with appropriate safeguards, see sections 4.10, 4.11 and 4.12
- Data subjects shall have the right of access to, rectification, erasure, restriction and objection to processing of own personal data

1.3 Definitions

The following definitions shall have the same meaning as the relevant definitions set out in the General Data Protection Regulation (EU) 2016/679 (GDPR).

1.3.1 Binding corporate rules (BCR)

BCR means personal data protection policies which are adhered to by Kvaerner legal entities established on the territory of the European Economic Area (EEA) for transfers or a set of transfers of personal data to any (Kvaerner) legal entity located in one or more third countries. Kvaerner's BCR is set out in the Data Protection Procedure.

1.3.2 Consent

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

1.3.3 Controller

The Controller means the natural or legal person, e.g. Kværner ASA and/or a legal entity, which alone or jointly with others determines the purpose and means of the processing of personal data.

1.3.4 Data subject

A data subject is an identified or identifiable individual to whom the personal data being processed relates to, for example an employee of Kvaerner, a person applying for a job at Kvaerner by entering information on Kvaerner's website or a representative of a Kvaerner business partner. An identifiable individual is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

1.3.5 EEA

The European economic area, meaning the EU member states together with the EFTA countries (Liechtenstein, Iceland and Norway).

1.3.6 Kvaerner

For the purpose of this standard Kvaerner shall mean Kværner ASA and its subsidiaries (including partly owned subsidiaries where Kværner ASA directly or indirectly owns at least 50 percent and which is governed by Kvaerner's Corporate Governance Policies). Further, for the purpose of this procedure, the term "Kvaerner" refers to the whole company group or each of the subsidiaries as the case may be.

1.3.7 Legal entity

Legal entity shall mean a subsidiary in which Kværner ASA directly or indirectly owns at least 50 percent of the voting interest.

1.3.8 Personal data

Personal data includes all types of information that directly or indirectly may be related or linked to the data subject.

Personal data may include:

- Names and dates of birth
- Contact details such as addresses, e-mail addresses and telephone numbers
- Indirect information such as IP address, laptop name
- Expressions of opinions on living individuals
- Information concerning salary
- Client/customer information (if linked to an individual)

For example, an IP address is deemed as personal data as long as the IP address in conjunction with additional information (such as an internet provider's billing information) can identify the individual using the IP address. Encrypted information is also deemed to be personal data if the information can be made readable and linked to an identifiable individual.

1.3.9 Personal data breach

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

1.3.10 Processing

Processing means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaption or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The definition is technology-neutral and includes the processing of personal data that is wholly or partly performed with the aid of computers or similar equipment that is capable of automatically processing personal data. The definition also includes manual registers or filing systems if the personal data is included in, or is intended to form part of, a structured collection making the personal data available for searching or compilation according to specific criteria.

1.3.11 Processor

A processor is any natural or legal person public authority, agency or other body which processes personal data on behalf of the controller, for example an outsourcing partner or service provider of a legal entity.

1.3.12 Special categories of data (sensitive data)

Sensitive data is defined as Personal data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a data subject
- data concerning health
- data concerning a data subject's sex life or sexual orientation

1.3.13 Third countries

Third country or third countries shall mean countries outside the EEA.

1.3.14 Attachments

Internal policy documents, guidelines, instructions routines or procedures applicable to Kvaerner and related to the Data Protection Procedure.

1.3.15 Transfer

Any personal data disclosure, copy or move via a network, or any personal data disclosure, copy or move from one medium to another irrespective of type of medium within the EEA to a recipient outside the EEA. The legal entity who transfers the personal data will be the data exporter, and the receiving party will be the data importer.

1.3.16 Responsibility

This Data Protection Procedure is part of Kvaerner's People Policy, and is under the responsibility of the Human Resources & Organisational Development department (HR & Org. Dev.). SVP HR & Org. Dev is responsible for ensuring that the Data Protection Procedure is applied in all legal entities. The local data privacy contact is responsible for the implementation of the Data Protection Procedure in its legal entity/region. The local data privacy contact is the country manager or general manager of the relevant subsidiary. All employees are responsible for adhering to this standard.

Kværner ASA and every legal entity acting as controller shall be responsible for and be able to demonstrate compliance with this Data Protection Procedure.

2 Description of processing regulated by the Data Protection Procedure

2.1 Material and geographical scope

The Data Protection Procedure applies to all processing of personal data in Kvaerner, and shall apply to legal entities as described in section 1.1. The official list of Kvaerner legal entities and their location can be obtained by contacting Kvaerner, please see section 6 for contact details.

2.2 Categories of personal data and purpose of the data processing

The following main categories of personal data, concerning employees and their next of kin, clients, subcontractors, press release subscribers, tenants, visitors, joint ventures, partners and third parties for the following main purposes for the following main purposes:

- General contact information: (e.g. name, address, email address, phone number, picture, date of birth etc.)
- Employee management-information (HR management):
  - Salary information, CV, education level, performance reviews, recruitment information, union membership, bank account number, details of next of kin etc.)
  - Registration of hours worked, absences, holiday, overtime
  - Records of compulsory training, e-learning, and safety certificates
  - Employment history within Kvaerner: e.g. start date, company and corporate seniority, job grade, position, organizational unit (department), immediate superior, contract details, employee type, job location, leaving date etc.
- Other employee data for statistical purposes: (e.g. gender, nationality, age)Travel related information
- Access control data and CCTV footage
- Customer information (e.g. name, address, email address, phone number, picture etc.)
- Subcontractor's information (e.g. name, address, email address, phone number, picture etc.)
- IT-related information (electronic logs regarding a person's use of IT-resources, user profile/account information etc.)

The corporate health care services will process medical data, etc.

The processing has the following main purposes:

- Contact information
- Employee administration
- Customer administration
- Subcontractors administration
- IT administration and information security administration
- Authentication and authorisation
- Physical security
- Administer IT-costs per employee, and internal CRM-information
- Register and report on HSE related information (e.g. incidents, issues etc.)
- Support the recruitment process (e.g. registering applications and CVs etc.)
- Collaboration tool for internal projects and organisational teams and activities (e.g. document and content management)
- Provide input to the organisation regarding trends and reasons for leaving the company (e.g. exit interview)

2.3 Records of processing activities

Kvaerner acting as controller shall maintain a record of processing activities under its responsibilities in accordance with GDPR Article 30. The records shall be made available to the competent data protection authority upon request.

2.4 Kvaerner's use of processors

When Kvaerner (controller) contracts with service providers as processors for the delivery of services involving processing of personal data on behalf of Kvaerner, a data processing agreement shall be entered into.

If a Kvaerner entity contracts with a service provider established in a third country, the Kvaerner entity is responsible for ensuring that the legal grounds for the transfer of personal data is in place.

3 Key principles of the Data Protection Procedure

3.1 Data Subjects' rights

3.1.1 Beneficiary rights

All data subjects whose personal data is being processed under this procedure shall benefit from the rights herein.

- The data subject's rights include the right to enforce:
- Fair, lawful and transparent processing
- Purpose limitation
- Data minimisation, accuracy and storage limitation
- Criteria for making the processing lawful
- Transparency and easy access to the Data Protection Procedure
- Rights of access, rectification, erasure and restriction of data
- Right to object to the processing
- Right not to be subject to automated decisions
- Security and confidentiality
- Restrictions on onward transfers outside of the group of companies
- National legislation preventing respect of the Data Protection Procedure
- Right to complain through the internal complaint mechanisms of the companies
- Cooperation duties with data protection authority
- Liability and jurisdiction provisions

Data Subjects' queries and complaints shall be handled in a timely manner by the relevant local data privacy contact.

3.1.2 Information about data subjects' rights

All data subjects who benefit from the Data Protection Procedure shall have easy access to information describing their rights. An electronic version of the Data Protection Procedure is available for Kvaerner's personnel on Kvaerner's intranet and this public version containing an excerpt of the Data Protection Procedure is available on Kvaerner's website.

A privacy statement is available on Kvaerner's website and applies to the online activities of the company. A link is provided from the privacy statement to this public version of the Data Protection Procedure.

A privacy statement for all Kvaerner employees is included in the Personnel Handbook and is also available on Kvaerner's intranet.

3.1.3 Liability

Kværner ASA has appointed Kværner AS to take the responsibility for and agrees to take the necessary action to remedy the acts of legal entities outside of EEA and to pay compensation in accordance with applicable EU/EEA law, cf. section 3.9, for any damages resulting from the violation of this Data Protection Procedure by legal entities outside the EEA.

Any data subject that can demonstrate that he or she has suffered damages due to violation of this Data Protection Procedure, shall be entitled to compensation of damages to the extent provided by applicable EU/EEA law, provided that he or she can establish facts which show that it is plausible that the damage has occurred because of a violation of this Data Protection Procedure. To the extent permitted by applicable law, the compensation shall be limited to direct damages which exclude, without limitation, lost profits or revenue, lost turnover, cost of capital and downtime cost.

It will subsequently be for Kværner AS to prove that the damages suffered by the data subject due to violation of this Data Protection Procedure are not attributable to any legal entity established outside the EEA in order to avoid liability.

3.2 Training and awareness program

Kvaerner shall provide appropriate training on the data protection standard to personnel with permanent or regular access to personal data and to personnel involved in the collection of personal data or in the development of tools used to process personal data.

3.3 Compliance and supervision of compliance

The Data Protection Procedure has several measures to ensure compliance and supervision of compliance, including:

- The establishment of a multidiscipline team responsible for supporting the organisation with follow-up of Kvaerner's processing of personal data
- Establishment of internal control mechanisms - ongoing monitoring
- Review program

Kvaerner has appointed the following positions to oversee and ensure compliance with the rules of this Data Protection Procedure:

- SVP HR & Org. Dev. is the overall responsible for monitoring compliance with the Data Protection Procedure as well as monitoring training and complaint handling
- Multidiscipline data privacy team
- Local data privacy contacts who shall handle local complaints from data subjects

Kvaerner's review program covers all aspects of the Data Protection Procedure including methods of ensuring that corrective actions will take place.

3.4 Complaint mechanisms

All data subjects, i.e. employees and third party beneficiaries, shall have the right to claim that any of Kvaerner's legal entities is not compliant with the Data Protection Procedure, by making a complaint about this.

If the data subject is an employee, he or she may choose to bring the complaint to the local HR representative or to his or her manager, or he or she may choose to contact the local data privacy contact or SVP HR & Org Dev. If the data subject is a third party beneficiary (for example customer), the data subject may take its case to the SVP HR & Org Dev.

Data subjects' queries and complaints shall be handled in a timely manner in accordance with internal procedures, as further detailed in section 4.7 herein.

Data subjects are encouraged to first follow the complaints procedure set forth in this section 3.5 before filing any complaint or claim with competent data protection authorities or the courts.

In case of violation of this Data Protection Procedure, the data subject may, at his or her choice, submit a complaint or a claim to the data protection authority or the courts:

a) in the EEA country at the origin of the personal data transfer, against the legal entity in such country of origin responsible for the relevant transfer;
b) in Norway, against Kværner AS; or
c) in the EEA country where the data subject resides or has its place of work, against the legal entity being the controller of the relevant personal data.

The data protection authorities and courts shall apply their own substantive and procedural laws to the dispute. Any choice made by the data subject will not prejudice the substantive or procedural rights he or she may have under applicable law.

3.5 Mutual assistance and cooperation with data protection authorities

Kvaerner undertakes to cooperate with the data protection authorities, particularly by applying recommendations and advice from the authorities, and also by responding to requests from the authority regarding the Data Protection Procedure.

The data protection authorities may conduct audits in order to ascertain compliance with the Data Protection Procedure.

SVP HR & Org. Dev. shall be the main contact point between relevant data protection authorities and Kvaerner on any matter arising out of the Data Protection Procedure or processing of personal data in general. The local data privacy contact shall be the local point of contact.

3.6 Relationship between national laws and the Data Protection Procedure

Nothing in this Data Protection Procedure shall be construed as a limitation of rights or remedies that individuals may have under applicable local law. This Data Protection Procedure provides supplemental rights and remedies to individuals only.

3.7 Procedure for updating the Data Protection Procedure

Kvaerner may make amendments to the Data Protection Procedure, e.g. due to modifications of relevant legislation or changes to Kvaerner legal structure.

Updates of the Data Protection Procedure are possible without having to re-apply for authorisation by the data protection authorities, provided that:

a) The SVP HR & Org Dev. keeps a fully updated list of members and keep track of and record of any updates to the rules and provide the necessary information to the data subjects or data protection authorities upon request
b) No transfer of personal data is made to a new member until the exporter of the data has made sure that the new member is effectively bound by this Data Protection Procedure, and can demonstrate compliance
c) Any substantial changes to the Data Protection Procedure or to the list of members are reported once a year to the data protection authorities granting the authorisations with a brief explanation of the reason justifying the update

The current version of the Data Protection Procedure shall always be available for all legal entities and employees.

Kvaerner shall communicate any substantial modifications to the rules to the data subjects by making the necessary changes to all relevant documents, including this public version of the Data Protection Procedure.

3.8 Governing law

This Data Protection Procedure shall be governed by and interpreted in accordance with Norwegian law.

4 General privacy principles observed by Kvaerner

The following general principles are based on the GDPR and applicable EU/EEA data protection law. Kvaerner has by implementing this Data Protection Procedure established a basis for internal control and procedures that ensures compliance with these principles when Processing Personal Data. It is the responsibility of each legal entity as a controller to apply such internal control and procedures.

4.1 Fair, lawful and transparent processing

Personal data shall be processed fairly, lawfully, in a transparent manner and pursuant to the principles stipulated in the Data Protection Procedure. This means that the personal data shall be processed in accordance with law, and that the legitimate interests of the data subject should be taken into account when processing personal data.

4.2 Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.3 Data minimisation, accuracy and storage limitation

Personal data shall be:

a) adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and/or further processed ("data minimisation");
b) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified ("accuracy"); and
c) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed ("storage limitation").

4.4 Criteria for making data processing lawful

4.4.1 Processing of personal data

Personal data may be processed only if at least one of the following legal bases applies:

a) the data subject has given his consent to the processing of his personal data for one or more specific purposes. In order to rely on consent, the conditions in section 4.4.4 must be fulfilled;
b) 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;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another individual;
e) 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 controller; or
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection of personal data.

4.4.2 Processing of special categories of data (sensitive data)

It is prohibited to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and to process 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.

The special categories of data mentioned above may only be processed if at least one of the following legal bases applies:

a) the data subject has given his explicit consent to the processing of those data for one or more specific purposes, except where the local laws applicable to the legal entity provide that the prohibition above may not be lifted by the data subject’s giving his/her consent. In order to rely on consent, the conditions in section 4.4.4 must be fulfilled;
b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment and social security and social protection law in so far

as it is authorized by local law providing for adequate safeguards for the fundamental rights and the interests of the data subject;

c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent;
d) the processing relates to data which are manifestly made public by the data subject;
e) the processing is necessary for the establishment, exercise or defence of legal claims; or
f) the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, 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 or pursuant to contract with a health professional that is subject to the obligation of professional secrecy or another person subject to an equivalent obligation of secrecy
g) allowed according to other national rules than a)-f) above that have been established in accordance with the GDPR

4.4.3 Processing of personal data relating to criminal convictions and offences

Processing of data relating to criminal convictions, offences or related security measures may only be carried out in accordance with applicable law.

4.4.4 Conditions for consent

If consent is allowed or required under applicable law for the processing of personal data or processing of sensitive data, the following conditions apply:

a) Kvaerner must be able to demonstrate that the data subject has consented to the processing of his/her personal data. Where processing is undertaken at the request of the data subject, he or she is deemed to have provided consent to the processing;
b) Kvaerner must inform the data subject in accordance with the provisions set forth in section 4.5.1 below;
c) 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, where 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; and
d) where the data subject is an employee of Kvaerner or other circumstances where there is an employment relationship between Kvaerner and the data subject, consent may not be used as a legal basis for processing personal data relating to such data subjects if the processing has foreseeable adverse consequences for the data subject.

The data subject may withdraw his/her consent at any time and the data subject shall, where applicable law so requires, be informed of his or her right to withdraw the consent. The withdrawal of consent shall not affect the lawfulness of the processing based on such consent before its withdrawal. It shall be as easy to withdraw as to give consent.

4.4.5 National identification numbers

National identification numbers shall be processed in accordance with the relevant provisions in local legislation in the controller's country.

4.5 Information to be given to the data subject

4.5.1 Information in cases of collection of data from the data subject

Where personal data are collected from the data subject the controller must, when the personal data are obtained, provide the data subject with the following information:

a) the identity and the contact details of the legal entity being the controller and of his representative, if any;
b) the contact details of the SVP HR & Org Dev. or the relevant local data privacy contact;
c) the purposes of the processing and the legal basis for the processing;
d) where the processing is based on section 4.4.1(f), the legitimate interests pursued by the controller or by a third party;
e) the recipients or categories of the personal data (if any); and

f) whether the controller intends to transfer any personal data to a third country and whether that country is recognised by the EU Commission as ensuring an adequate level of protection. If the country is not recognised as ensuring an adequate level of protection, a reference to the appropriate safeguards mentioned in Section 4.11.2 and 4.12.2 shall be provided together with information on how to obtain a copy of them where they have been made available.

In addition, where required by applicable law and if necessary to ensure fair and transparent processing, the controller shall provide the data subject with the following further information:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
b) 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 the processing as well as the right to data portability;
c) where the processing is based on data subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
d) the right to lodge a complaint with a supervisory authority;
e) 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;
f) the existence of automated decision-making, including profiling, referred to in section 4.7.2 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 a controller intends to further process the personal data for a secondary purpose, the controller shall, if applicable law so requires, provide the data subject prior to the further processing with information about the secondary purpose and any relevant information as set out in paragraph 2 of this Article 4.5.1.

It is not necessary to provide the information mentioned above to the Data Subject if he/her already has it.

4.5.2 Information where the personal data have not been obtained from the data subject

If applicable local law so requires where the personal data have not been obtained from the data subject, the controller shall within the timeframes set out below provide the data subject with the following information:

a) the identity and the contact details of the legal entity being the controller of the processing;
b) the contact details of the relevant data protection officer;
c) the purposes for which their personal data will be processed and the legal basis for the processing;
d) the categories of personal data concerned;
e) the recipients or categories of the personal data (if any); and
f) whether the controller intends to transfer any personal data to a country outside the EEA and whether that country is recognised by the EU Commission as ensuring an adequate level of protection. If the country is not recognised as ensuring an adequate level of protection, a reference to the appropriate safeguards mentioned in section 4.11.2 and 4.12.2 shall be provided together with information on how to obtain a copy of them where they have been made available.

In addition, when required by applicable law and if necessary to ensure fair and transparent processing, the controller shall provide the data subject with the following further information:

a) the period for which the personal data will be stored, or the criteria used to determine that period;
b) where the processing is based on section 4.4.1(f), the legitimate interests pursued by the controller or by a third party;
c) 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 the processing as well as the right to data portability;

d) where the processing is based on data subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
e) the right to lodge a complaint with a data protection authority;
f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
g) the existence of automated decision-making, including profiling, referred to in section 4.7.2 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 information mentioned above shall be provided:

a) within a reasonable time after obtaining the personal data, at the latest within one month from obtaining the personal data;
b) if the personal data are used for communication with the data subject, at the latest at the time of the first communication with the data subject;
c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

Where a controller intends to further process the personal data for a secondary purpose, the controller shall, if applicable law so requires, provide the data subject prior to the further processing with information about the secondary purpose and any relevant information as set out in paragraph 2 of this Article 4.5.2.

The requirements of this Section 4.5.2 may be set aside where and insofar:

a) the data subject already has the information;
b) it is impossible or would involve a disproportionate effort to provide the information to data subjects or providing the information would be likely to render impossible or seriously impair the achievement of the objectives of the processing. In such cases, the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interest, including making the information publicly available;
c) obtaining or disclosure is expressly laid down by applicable EU/EEA law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by applicable EU/EEA law, including a statutory obligation of secrecy.

4.6 The data subject’s rights

4.6.1 Data subject's right of access

Every data subject shall have the right to obtain from the controller:

a) confirmation as to whether or not data relating to him are being processed and where that is the case, access to the personal data processed by the controller;
b) information about the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the data are disclosed, in particular recipients located in a third country that is not recognised by the EU Commission as ensuring an adequate level of protection or international organisations. In the cases of such transfers, the data subject shall have the right to be informed of the appropriate safeguards pursuant to sections 4.11.2 and 4.12.2;
c) where possible, information about the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
d) information about the existence of the right to request from the controller rectification or erasure of personal data or restriction of the processing of personal data concerning the data subject or to object to such processing;
e) information about the right to lodge a complaint with a data protection authority;
f) where the Personal Data have not been collected from the Data Subject, any available information as to their source; and
g) the existence of automated decision-making, including profiling, referred to in the Data Protection Procedure section 4.7.2 and, at least in those cases, meaningful information about the logic involved in any automatic processing as well as the significance and the envisaged consequences of such processing for the data subject.

4.6.2 Data subject's right of rectification

Where required by applicable law, the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of a supplementary statement.

4.6.3 Right of erasure

Where required by applicable law, 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:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws his/her consent to the Pprocessing and where there is no other legal basis for the processing;
c) the data subject objects to the processing pursuant to section 4.6.6 (a) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to section 4.6.6 (b);
d) the personal data have been unlawfully processed;
e) the personal have to be erased for compliance with a legal obligation in applicable EU/EEA law to which the controller is subject.

Where the controller has made the personal data public and is obliged pursuant to paragraph 1 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 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 data subject's right to erasure described in paragraph 1 and 2 above shall not apply to the extent that the processing is necessary for:

a) exercising the right of freedom of expression and information;
b) compliance with a legal obligation which requires processing by applicable 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;
c) the establishment, exercise or defence of legal claims.

4.6.4 Right to restriction of processing

Where required by applicable law, the data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

a) 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;
b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) 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;
d) the data subject has objected to processing pursuant to section 4.6.5 pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted under paragraph 1, 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/EEA or of a EU/EEA country where the Legal Entity is established.

A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

4.6.5 Notification obligation regarding rectification or erasure of personal data or restriction of processing

Where required by applicable law, the controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Section 4.6.2 to 4.6.4 above to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

Where required by applicable law, the controller shall inform the data subject about those recipients if the data subject requests it.

4.6.6 Right of data portability

Where required by applicable law, the data subject shall have the right to data portability, being the right to receive the personal data concerning him or her, which he or she has provided to the controller, in a structured, commonly used and machine readable form and have the right to transmit those data to another controller without hindrance.

4.6.7 The data subject's right to object to the processing

The data subject has the right to object at any time, on grounds relating to his or her particular situation, to processing of personal data concerning him or her in the cases referred to in section 4.4.1 e) and f). This includes profiling based on those provisions.

If a data subject objects to the processing, the controller shall no longer process the personal data unless:

a) The controller demonstrates compelling legitimate grounds for the processing which override the interests and rights of the data subject; or
b) the processing is necessary for the establishment, exercise or defence of legal claims.

The data subject shall, where personal data are processed for direct marketing purposes, have the right to object at any time to processing of personal data concerning him/her for such marketing. This 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.

The right to object shall be explicitly brought to the data subject's attention in a clear way and separately from any other information, at the latest at the time of first communication with the data subject.

4.6.8 Automated individual decisions

The data subject has the right not to be subject to a decision which produces legal effects concerning him or her, or significantly affects him or her and which is based solely on automated processing of personal data, unless the decision:

a) is necessary for entering into or performance of a contract between the data subject and the controller;
b) is authorised by applicable law which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or
c) is based on the data subject's explicit consent.

In the cases referred to in a) and c) above, the controller shall implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, and 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 decisions.

The automated decisions referred to in this section 4.6.7 shall not be based on the processing of sensitive personal data unless point a) or g) of section 4.4.2 applies and suitable measures to safeguard the data subject's rights, freedoms and legitimate interests are in place.

4.6.9 Procedure for handling requests

Requests in accordance with section 4.6.1 to 4.6.7 should be filed in writing to the SVP HR & Org Dev. or to the relevant local data privacy contact. Prior to fulfilling the data subject's request, the controller may, where appropriate, request the data subject to:

a) specify the IT system in which the personaldData are likely to be stored;

b) specify the circumstances in which the controller obtained the personal data; and
c) show proof of his or her identity.

Further, in the case of an access request, the controller may, where appropriate, request the data subject to specify the categories of personal data to which he or she requests access.

In the case of a request for rectification, erasure or restriction, the controller may, where appropriate, request the data subject to specify the reasons why the personal data are incorrect, incomplete or not processed in accordance with applicable law or the data protection procedure.

In the case of an objection in accordance with section 4.6.7, the controller may, where appropriate, request the data subject to specify the processing operation to which the objection relates.

When a request has been made by electronic form means, the response shall be provided by electronic means where possible, unless otherwise requested by the data subject. The request shall be responded to without undue delay and in any event within one month of receipt of the request. This period may be extended by two more months where necessary, taking into account the complexity and number of the requests. In such cases, the data subject shall be informed of any such extension within one month from receipt of the request, together with the reasons for the delay.

In the case of an objection, the relevant local data privacy contact or to the SVP HR & Org Dev. shall respond by confirming whether or not the particular processing will be stopped. If the processing is not stopped, the communication must be accompanied with the reasons for continuing the processing.

If data subjects are not satisfied with the response to their requests, they may file a complaint in accordance with section 3.5 herein.

4.7 Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

4.8 Security of processing

4.8.1 Appropriate technical and organisational security measures

Kvaerner, as a controller and/or processor, shall implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the particular kind and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

4.8.2 Data protection by design and by default

Kvaerner shall implement data protection by design and by default.

4.8.3 Use of processor

When processing of personal data is carried out on behalf of Kvaerner as a controller, only processors providing sufficient guarantees to implement technical security measures and organizational measures in such manner that the processing will meet the requirements of applicable EU/EEA data protection laws shall be chosen.

The processing by way of a processor must be governed by a contract or legal act binding the processor to the controller ("Data processing agreement").

4.9 Personal data breach notifications

4.9.1 Notification to data protection authorities

If a personal data breach has occurred or is suspected to have occurred, the person who has become aware of or suspects the personal data breach, shall immediately notify the SVP HR & Org. Dev. or appropriate local data privacy contact who shall forward the notification to the SVP HR & Org. Dev.

If required under applicable law, the controller shall notify a competent data protection authority of a personal data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to data subjects' rights. If a notification is not made within 72 hours, it shall be accompanied by reasons for the delay. The notification shall at least:

a) describe the nature of the personal data breach, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) contain the name and contact details of the SVP HR & Org. Dev. or local data privacy contacts where more information can be obtained;
c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including measures to mitigate its possible adverse effects, where appropriate.

Where required by applicable law, the ontroller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall be available to the competent data protection authority upon request.

4.9.2 Notification to data subjects

If required by applicable law, the controller shall notify the concerned data subject(s) of a personal data breach without undue delay following discovery of such breach, if the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject(s). This applies unless one or more of the following conditions are met:

a) the controller has implemented and applied appropriate technical and organisational protection measures to the personal data affected by the personal data breach, in particular measures that render the personal data unintelligible to any person who is not authorised to access it (such as encryption);
b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialise; or
c) notifying the data subject would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby data subjects are informed in an equally effective manner.

The personal data breach notification to the data subjects shall describe in clear and plain language the nature of the personal data breach and shall at least contain the information and measures referred to in section 4.9.4 (b), (c) and (d).

4.10 Transfer to controllers and processors bound by the Data Protection Procedure (internal transfer)

4.10.1 Transfer from controller to controller

Transfer of personal data between controllers that are bound by the data protection procedure may take place, provided that:

a) it is not incompatible with the purpose for which the personal data were collected, cf. section 2.2. and 4.2;
b) it is in accordance with the principle of data minimisation, accuracy and storage limitation cf. 4.3;
c) the criteria for making data processing lawful is fulfilled, cf. 4.4;
d) if applicable, information is given to the data subject in accordance with 4.5;
e) appropriate security measures protect the data during transfer and further processing by the receiving controller, cf. 4.8.
f) Transfer from controller to processor

Transfer of personal data from a controller to a processor, both bound by the data protection procedure, may take place, provided that:

a) Processing by way of a processor is governed by a contract or legal act binding the processor to the controller which fulfils the requirements set out in 4.9.3.

4.11 Transfer to external controllers not bound by the Data Protection Procedure

4.11.1 Transfer to external controllers established within the EEA

Transfer of personal data from a controller established in the EEA to another controller established in the EEA may take place, provided that:

a) it is not incompatible with the purpose for which the personal data were collected, cf. 4.2;
b) it is in accordance with the principle of data minimisation, accuracy and storage limitation cf. 4.3;
c) the criteria for making data processing lawful is fulfilled, cf. 4.4;
d) if applicable, information is given to the data subject in accordance with 4.5;
e) appropriate security measures protect the data during transfer and further processing by the receiving controller, cf. 4.8.

Applicable local law may have additional requirements and should always be considered before making such transfers.

4.11.2 Transfer to external controllers established outside the EEA

Transfer of personal data from a controller established within the EEA to a controller established outside the EEA is prohibited, except when the conditions in section 4.11.1 are fulfilled and one of the conditions in Section 4.12.2 are met.

4.12 Transfer to external processors not bound by the Data Protection Procedure

4.12.1 Transfer to external Processors established within the EEA

Transfer of personal data from a controller established in the EEA to a processor established in the EEA may take place, provided that the controller complies with this Data Protection Procedure and that the processor's processing on behalf of the controller is governed by a contract (data processing agreement) which fulfils the requirements set out in Section 4.9.3.

See sections 2.4 and 4.9.3 regarding Kvaerner's use of processors.

4.12.2 Transfer to external processor established outside the EEA

Transfer of personal data from a controller established within the EEA to a processor established outside the EEA is prohibited, except when the conditions in Section 4.12.1 are fulfilled and one of the legal basis in the GDPR Article 45, 46, 47 or 49 are met, including:

a) the receiving processor is established in a country which the EU Commission has considered having an adequate level of protection, cf. the Commission's decisions on the adequacy of the protection of personal data in third countries provided at: http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm;
b) the processor is established in the US and has been certified under the EU-US Privacy Shield or any other similar program that is recognised by the EU Commission as ensuring an adequate level of protection;
c) the processor has implemented binding corporate rules or a similar transfer mechanism that provides appropriate safeguards under applicable law;
d) the controller and the processor have provided appropriate safeguards by entering into EU Standard Contractual Clauses (model contract);
e) the controller and the processor have provided appropriate safeguards by entering into standard data protection clauses adopted by the EU Commission or a data protection authority; or

f) an approved code of conduct or an approved certification mechanism pursuant to Article 46(1)(e) and (f) of the General Data Protection Regulation are provided for.

In specific situations where a transfer cannot be based on a) to f) above, transfer may take place on one or more of the following conditions:

a) the transfer is necessary for the performance of a contract between the controller and the data subject or for taking necessary steps at the request of the data subject prior to entering into a contract;
b) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural and legal person;
c) the transfer is necessary for important reasons of public interest;
d) the transfer is necessary for the establishment, exercise or defence of a legal claim;
e) the transfer is necessary to protect a vital interest of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
f) the transfer is required by any law to which the relevant controller is subject.

Transfers based on paragraph 2 litra b) and e) above require the prior approval of the SVP HR & Org. Dev.

4.12.3 Data subject's consent for transfer

If none of the conditions listed in section 4.12.2 are met or if consent is required or appropriate as a legal basis for the transfer under applicable law, Kvaerner shall (also) seek an explicit consent from the data subject for the relevant transfer. The consent must be requested prior to participation of the data subject in specific projects, assignments or tasks that require the transfer of personal data.

A transfer cannot be based on a data subject's consent if it has foreseeable adverse consequences for the data subject. This means that consent will as a main rule not be a valid basis for transfers relating to employees.

Prior to requesting consent, the data subject shall be informed of the possible risks of the transfer due to the absence of appropriate safeguards and the fact that the EU Commission has not recognised this country as ensuring an adequate level of protection. When requesting consent, the conditions in section 4.4.4 apply.

4.12.4 Transfers from legal entities in third countries to third parties in third countries

Transfer of personal data collected in connection with the activities of a legal entity established in a third country that is not recognised by the EU Commission as ensuring an adequate level of protection, to a third party also established in such third country, is permitted if one of the grounds in section 4.12.2 applies or if the transfers are:

a) necessary for compliance with a legal obligation to which the relevant legal entity is subject;
b) necessary to serve the public interest; or
c) necessary to satisfy a legitimate purpose of the legal entity.

5 Last updated

This Public version of the Data Protection Procedure (BCR) was last updated 11 July 2018.

6 Contact

privacy@kvaerner.com