KONGSBERG

Kongsberg Gruppen ASA

Processing and transfer of personal data in KONGSBERG (Binding Corporate Rules)

Public version

Table of Contents

1. Introduction

1.1 Objective

Kongsberg Gruppen ASA has implemented Binding Corporate Rules for the Processing and transfer of Personal Data within KONGSBERG (the "BCR").

Under European data protection law, transfers of Personal Data to countries outside the EEA that do not provide an adequate level requires a valid legal basis. The objective of KONGSBERG's BCR is to establish such legal basis for transfers of Personal Data from Group Companies established within the EEA to Group Companies established outside the EEA and to establish internal control system containing legally binding principles for the Processing of all Personal Data within KONGSBERG in accordance with the EU Data Protection Directive 95/46/EC, and from 25 May 2018, the EU General Data Protection Regulation 2016/679 (GDPR).

This document is a public excerpt and summary of KONGSBERG's BCR. The document explains the content of KONGSBERG's BCR, in particular which rights Individuals have vis-à-vis KONGSBERG and how to exercise these rights. The BCR do not limit or reduce any rights or remedies that Individuals may have under applicable local law.

The BCR in their entirety, and the list of Members of the BCR, will be made available upon request to the Corporate Privacy Officer, see contact information in Section 24.

1.2 Scope

The BCR apply to Group Companies, i.e. Kongsberg Gruppen ASA and subsidiaries listed in the document "Members of the BCR". For the purpose of the BCR, the term "KONGSBERG" refers to all or each of the Group Companies that are bound by the BCR.

The BCR apply to Processing of Personal Data relating Personnel, Customers, Suppliers and Business Partners (jointly "**Individuals**"), who shall benefit from the rights granted to them therein.

The BCR apply to all Processing of Personal Data by electronic means and in systematically accessible paper-based filing systems carried out within KONGSBERG.

KONGSBERG may supplement the BCR through sub-policies, procedures or notices that are consistent with the BCR. The BCR supersede all KONGSBERG privacy policies, procedures and notices that exist on the Effective Date to the extent they are in contradiction with the BCR.

1.3 Accountability

The BCR are binding on KONGSBERG. The President Business Area is responsible for his or her Group Companies' compliance with the BCR. All Personnel must comply with the BCR. This means that every member of Personnel working for KONGSBERG is bound by the rules of the BCR.

2. Description of Processing regulated by the BCR

KONGSBERG processes the following main categories of Personal Data, concerning Personnel, Customers, Suppliers and Business Partners for the following main purposes:

Data category	**Purpose of Processing**
HR management data (for example general contact information, salary information, CV, education level, performance reviews, recruitment information, union membership, bank account number, details of next of kin etc.)	Administer and manage all aspects of the Personnel relationship (including job applicants, former employees, temporary employees, employees, apprentices, students, contractors, consultants, next of kin and dependants).
IT-administration data (for example electronic logs regarding an Individual's use of IT-resources, user profile/account information etc.)	Support and manage information technology (IT) and information system (IS) administration and information security.
HSE data (for example data relating to HSE incidents and safety certificates)	Support and manage occupational health services and the registration, managing and reporting of health, service and environment (HSE) related information (incidents, issues etc.).
Planning, control data and HR reports (for example registration of hours worked, absences, holiday, overtime, employment history within KONGSBERG, gender, nationality and age)	Scheduling time tables, recording time, conducting surveys, controls and internal audits, statistics and analysis.
Background check, Integrity Due Diligence and security clearance data (for example name, gender, age, roles in companies, information available in public available sources)	Due diligence against anti-corruption laws and export controls, Integrity Due Diligence of business partners (including self-assessment and background check), processing of security clearance applications (for complying with legal obligations under the Security Act) and process requests for visits (visitors).
Video surveillance / activity logs (for example CCTV recordings and access logs)	Support and manage safeguarding against illegal or unauthorized entry into areas, buildings or rooms or to support the control of equipment and/or production processes.
Business-related data (for example business relations, business interest and security data)	Support and manage customer, supplier or partner relationships (internal/external), processing of personal data as part of provision of products and services to third parties, business operation and protection of business interests and security (e.g. information security, logging, conduction of audits and controls, surveys, analysis, reports and managing of daily operations and transactions/possible transactions involving KONGSBERG).
Complaints (for example name and contact information of complainant and contents of complaint)	Follow-up on complaints and concerns reported by Personnel to their supervisor or the Corporate Compliance Officer.

Whistleblowing, complaints and investigation information (for example the identity of notifying person, details on potential misconduct, information on alleged person(s) involved and information revealed as part of the investigation)	Whistleblowing hotline (available for Personnel and third parties) for raising concerns, managing investigations of incidents and concerns (e.g. related to employee's potential violation of terms of employment or incidents or concerns that may have an adverse effect on the business).
Data necessary to comply with legal obligations (for example tax and accounting information and information relating to legal proceedings)	Comply with legal obligations to which KONGSBERG is subject and/or protect a legal position of KONGSBERG.

3. Fair and lawful Processing

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

4. Requirements regarding purposes for Processing Personal Data

4.1 Purpose specification

Personal Data shall only be collected, used or otherwise Processed for specified, explicit and legitimate purposes objectively justified by the activities of KONGSBERG and not further Processed in a way incompatible with those purposes, cf. Section 2.

KONGSBERG's Processing of Personal Data includes, but is not limited to, Processing for the purposes specified in Section 2.

4.2 Generally permitted purposes for further Processing (secondary purposes)

Processing of Personal Data further to collection can only take place if such Processing is not incompatible with the purposes that are originally specified for the Processing. The following purposes will as a main rule not be incompatible with the purposes stated in Section 2 above:

a) audits, business controls, due diligence and investigations;
b) dispute resolution;
c) legal and business affairs;
d) research; and
e) insurance and pension.

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

a) limiting access to the Personal Data;
b) imposing additional confidentiality requirements and security measures;
c) informing the Individuals about the purposes of the further Processing; or
d) obtaining Consent from the Individuals.

4.3 Consultation

In case of doubt, the Business Area Privacy Officer shall be consulted before any Processing starts, to decide whether the Personal Data and Sensitive Personal Data in particular may be Processed on the basis of the provisions in Section 4.1 or 4.2, including whether implementation of possible additional measures is required. The Business Area Privacy Officer shall in case of doubt, consult the Corporate Privacy Officer.

5. Criteria for making data Processing lawful

5.1 Processing of Personal Data

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

a) the Individual has given his or her unambiguous Consent. In order to rely on Consent, KONGSBERG must follow the procedure set forth in 5.4 below;
b) the Processing is necessary for the performance of an agreement between the Individual and KONGSBERG, or in order to take steps at the request of the Individual prior to entering into such an agreement;
c) the Processing is necessary for compliance with a legal obligation to which KONGSBERG is subject;
d) the Processing is necessary in order to protect the vital interests of the Individual or of another natural person;
e) the Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in KONGSBERG; or
f) the Processing is necessary for legitimate purposes pursued by KONGSBERG or by a Third Party to whom the Personal Data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the Individual.

5.2 Processing of special categories of data (Sensitive Data)

KONGSBERG may only Process Sensitive Personal Data for legitimate purposes if at least one of the following legal basis applies:

a) the Individual has given his or her explicit Consent. In order to rely on Consent, KONGSBERG must follow the procedure set forth in Section 5.4 below;
b) the Processing is necessary for the purposes of carrying out the obligations and specific rights of KONGSBERG in the field of employment, social security and social protection law in so far as it is authorized by applicable law providing for adequate safeguards;
c) the Processing is necessary to protect the vital interests of the Individual or of another person;
d) the Processing relates to Sensitive Personal Data which are manifestly made public by the Individual;
e) the Processing is necessary for the establishment, exercise or defence of legal claims (including for dispute resolution) or Processing is necessary for compliance with a legal obligation to which KONGSBERG is subject;
f) the Processing is necessary for the performance of a task for reasons of substantial public interest;
g) the Processing is required for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the Individual, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services, and the Sensitive Personal Data are Processed by a health professional subject to applicable law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy;

h) the Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health;
i) the Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

5.3 Processing of Personal Data relating to criminal convictions and offences

KONGSBERG shall establish internal procedures for the Processing of Personal Data relating to criminal convictions and offences in compliance with applicable law.

5.4 Consent

If Consent is allowed or required under applicable law for Processing Personal Data or Sensitive Personal Data, the following conditions apply:

a) When seeking Consent, KONGSBERG must inform the Individual of;
    i. the identity and contact details of the Group Company being the Controller of the Processing;
    ii. the purposes for which his or her Personal Data will be Processed;
    iii. the categories of Third Parties to which the Personal Data will be disclosed (if any);
    iv. other relevant information provided in Section 7.1, if necessary to ensure that the Individual's Consent is informed.
b) KONGSBERG must be able to demonstrate that the Individual has consented to Processing of his or her Personal Data. Where Processing is undertaken at the request of an Individual (e.g. he or she subscribes to a service or seeks a benefit), he or she is deemed to have provided Consent to the Processing.
c) If the Individual's Consent is given in the context of a written declaration which also concerns other matters, the request for Consent shall, if applicable law so requires, be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.
d) Consent cannot be used as a legal basis for Processing Personal Data relating to Personnel if it has foreseeable adverse consequences for the Individual. This means that Consent will as a main rule not be applicable as a legal basis relating to Processing Personal Data relating to Personnel.

5.5 Withdrawal of Consent

The Individual may withdraw Consent at any time without adverse consequences to his or her relationship with KONGSBERG. The withdrawal of Consent shall not affect the lawfulness of the Processing based on such Consent before its withdrawal.

Prior to giving Consent, the Individual shall, where applicable law so requires, be informed of his or her right to withdraw his or her Consent without adverse consequences. It shall be as easy to withdraw as to give Consent.

5.6 National identification numbers

National identification numbers and social security numbers shall be processed in accordance with applicable local law.

6. Data quality, proportionality and deletion

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;
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; and
c) kept in a form which permits identification of Individuals for no longer than what is necessary for the purposes for which the data were collected or for which they are further processed, unless necessary to comply with an applicable legal requirement or as advisable in light of an applicable statute of limitations.

KONGSBERG may specify (e.g. in a sub-policy, notice or records retention schedule) a time period for which certain categories of Personal Data may be kept. Promptly after the applicable storage period has ended, the Personal Data shall be:

a) securely deleted or destroyed; or
b) anonymized.

7. Individual's rights

7.1 Transparency and information rights

7.1.1 Availability of the BCR

A full version of the BCR shall be made available for Personnel on KONGSBERG's corporate intranet. In addition, this public version (excerpt and summary) of the BCR shall be made available for all Individuals on KONGSBERG's website (https://kongsberg.com/). The BCR in their entirety and the list of Members of the BCR will be made available upon request to the Corporate Privacy Officer, see contact information in Section 24.

7.1.2 Information in cases of collection of data from the Individual

At the time when Personal Data are collected from the Individual, KONGSBERG shall inform the Individuals, e.g. through a published data privacy policy or by other means, about:

a) the identity and the contact details of the Group Company being the Controller of the Processing;
b) the contact details of the appropriate Business Area Privacy Officer;
c) the purposes for which their Personal Data will be Processed and the legal basis for the Processing;
d) which legitimate purposes are pursued when the Processing is based on Section 5.1 f);
e) the categories of Third Parties to which the Personal Data will be disclosed (if any); and
f) whether any Personal Data is transferred 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 applicable transfer mechanism shall be provided, cf. Section 10.2.2.

In addition, when required by applicable law and if necessary to ensure fair and transparent Processing, KONGSBERG shall provide the Individual 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) the existence of the right to request access to, correction, deletion or restriction of Processing concerning the Individual (cf. Sections 7.2.1 and 7.2.2) or to object to Processing (cf. Section 7.2.3) as well as the right to data portability;
c) where the Processing is based on Individual's Consent, the existence of the right to withdraw Consent at any time as described in Section 5.5, without affecting the lawfulness of Processing Consent before its withdrawal;

d) the right to lodge a complaint with a Data Protection Authority;
e) whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and whether the Individual 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 7.3 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 Individual.

Where KONGSBERG intends to further Process the Personal Data for a secondary purpose, KONGSBERG shall, if applicable law so requires, provide the Individual prior to the further Processing with information on the secondary purpose and any relevant further information as set out above.

The requirements of this Section 7.1.2 may be set aside where and insofar the Individual already has the information.

7.1.3 Information where the data have not been obtained from the Individual

If applicable local law so requires, where Personal Data have not been obtained directly from the Individual, KONGSBERG shall within the timeframes set out below provide the Individual with the following information:

a) the identity and the contact details of the Group Company being the Controller of the Processing;
b) the contact details of the appropriate Business Area Privacy 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 categories of Third Parties to which the Personal Data will be disclosed (if any); and
f) whether any Personal Data is transferred 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 applicable transfer mechanism shall be provided, cf. Section 10.2.2.

In addition, when required by applicable law and if necessary to ensure fair and transparent Processing, KONGSBERG shall provide the Individual 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) which legitimate purposes are pursued when the Processing is based on Section 5.1 f);
c) the existence of the right to request access to, correction, deletion or restriction of Processing concerning the Individual (cf. Sections 7.2.1 and 7.2.2) or to object to Processing (cf. Section 7.2.3) as well as the right to data portability;
d) where the Processing is based on the Individual's Consent, the existence of the right to withdraw Consent at any time as described in Section 5.5, without effecting the lawfulness of the 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 7.3 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 Individual.

The information mentioned above shall be provided:

a) within a reasonable time after obtaining the Personal Data, but at the latest within one month from obtaining the Personal Data, having regard to the specific circumstances in which the Personal Data are Processed;

b) if the Personal Data are to be used for communication with the Individual, at the latest at the time of the first communication to the Individual; or
c) if a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed.

Where KONGSBERG intends to further Process the Personal Data for a secondary purpose, KONGSBERG shall, if applicable law so requires, provide the Individual prior to the further Processing with information on the secondary purpose and any relevant further information as set out above. The requirements of this Section 7.1.3 may be set aside where and insofar:

a) the Individual already has the information;
b) it is impossible or would involve a disproportionate effort to provide the information to Individuals or providing the information would be likely to render impossible or seriously impair the achievement of the objectives of the Processing. In such cases, KONGSBERG shall take appropriate measures to protect the Individual's rights and freedoms and legitimate interests, 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 Individual'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.

7.2 The Individual's rights of access, correction, deletion, restriction and objection

7.2.1 Individual's right of access

Every Individual shall have the right to information on the following without excessive delay or expense:

a) if Personal Data relating to him or her are being Processed;
b) the purposes of the Processing;
c) the categories of Personal Data concerned;
d) the recipients or categories of recipients to whom the Personal Data are disclosed;
e) where possible, the period for which the Personal Data is planned to be stored or the criteria used to determine that period;
f) information on the source of personal data where they are not collected from the Individual; and
g) information regarding the logic involved in the automated Processing of Personal Data concerning him or her in the case of automated decisions referred to in Section 7.3.

7.2.2 Individual's right to correction, deletion or restriction of Processing

Individuals may require correction, deletion or restriction of Processing if the Processing does not comply with the BCR, and in particular if Personal Data are incomplete or inaccurate.

KONGSBERG shall give notification to recipients of Personal Data of any correction, deletion or restriction of Personal Data carried out in accordance with this section, unless this proves impossible or involves a disproportionate effort for KONGSBERG.

7.2.3 Individual's right to object

The Individual shall have the right to object, on grounds relating to his or her particular situation, at any time of Processing of Personal Data concerning him or her if the Processing is based on point e) or f) of Section 5.1. This includes profiling based on those provisions.

If an Individual objects to the Processing, the Group Company shall no longer Process the Personal Data unless:

a) it demonstrates compelling legitimate grounds for the processing which override the interests and rights of the Individual; or
b) the Processing is necessary for the establishment, exercise or defence of legal claims.

If the Personal Data are Processed for direct marketing purposes, the Individual shall, at any time, have the right to object to Processing of his or her Personal Data for such marketing. This includes profiling to the extent that it is related to such direct marketing. Where the Individual 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 Individual's attention in a clear way and separately from any other information, at the latest at the time of first communication with the Individual.

7.2.4 Procedure

Requests in accordance with this Section 7.2.1, 7.2.2 and 7.2.3 should be filed in writing to the relevant Privacy Officer. Prior to fulfilling the Individual's request, KONGSBERG may, where appropriate, request the Individual to:

a) in the case of an access request, specify the categories of Personal Data to which he or she wants to access;
b) specify the IT system in which the Personal Data are likely to be stored;
c) specify the circumstances in which KONGSBERG obtained the Personal Data;
d) show proof of his or her identity; and
e) in the case of a request for correction, deletion or blockage, specify the reasons why the Personal Data are incorrect, incomplete or not Processed in accordance with applicable law or the BCR;
f) in the case of an objection to processing, specify the processing operation to which the objection relates.

The Privacy Officer shall respond to requests in accordance with this Section 7.2.1, 7.2.2 and 7.2.3 in writing no later than four (4) weeks from receiving a request. In the case of an objection, the Privacy Officer 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 special circumstances should make it impossible to respond within the time limit, the response may be postponed until it is possible to respond. In such a case, a temporary response shall be given stating the reasons for the delay and when the response may be expected.

If Individuals are not satisfied with the response to their requests, Individuals may file a complaint in accordance with Section 14.

7.3 Automated individual decisions

The Individual shall have the right not to be subject to a decision based solely on automated processing, including profiling which produces legal effects concerning him or her or similarly significantly affects him or her, unless the decision:

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

In the cases referred to in a) and c) above, the Group Company shall implement suitable measures to safeguard the Individual's rights, freedoms and legitimate interests, and at least the right to obtain human intervention on the part of the Group Company, to express his or her point of view and to contest the decisions.

The automated decisions referred to in this Section shall not be based on Sensitive Personal Data unless point a) or g) of Section 5.2 applies and suitable measures to safeguard Individual's rights, freedoms and legitimate interests are in place.

8. Security of Processing

KONGSBERG shall implement appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of Personal 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.

9. Transfer to Controllers and Processors bound by the BCR (internal transfer)

9.1 Disclosure from Controller to Controller

Disclosure of Personal Data between Controllers that are bound by the BCR may take place, provided that:

a) it takes place for legitimate purposes and is not incompatible with the purpose for which the Personal Data originally were collected, cf. Section 4;
b) it is in accordance with the principle of data quality and proportionality, cf. Section 6;
c) the criteria for making the Processing legitimate is fulfilled, cf. Section 5;
d) if applicable, information is given to the Individual in accordance with Section 7.1; and
e) appropriate security measures protect the Personal Data during transfer and further Processing by the receiving Controller, cf. Section 8.

9.2 Transfer from Controller to Processor

Transfer of Personal Data from a Controller to a Processor, both bound by the BCR, may take place, provided that that the Processor provides sufficient guarantees in respect of the technical and organisational security measures. These security measures shall satisfy a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data in question, as described in Section 8.

If required under applicable law, the Controller shall instruct the Processor through a written agreement in accordance with the requirements set out in Section 10.2.1 below.

10. Transfer to external Controllers and Processors not bound by the BCR (external transfer)

10.1 Disclosure and transfer to external Controllers

10.1.1 Disclosure to external Controllers established within the EEA or a country recognised by the EU Commission as ensuring an adequate level of protection

Disclosure of Personal Data from a Controller established in the EEA to another Controller established in the EEA or a country recognised by the EU Commission as ensuring an adequate level of protection may take place, provided that:

a) it takes place for legitimate purposes and is not incompatible with the purpose for which the Personal Data were collected, cf. Section 4;

b) it is in accordance with the principle of data quality and proportionality; cf. Section 6;
c) the criteria for making data Processing legitimate is fulfilled, cf. Section 5;
d) if applicable, information is given to the Individual in accordance with Section 7.1; and
e) appropriate security measures protect the data during transfer and further Processing by the receiving Controller, cf. Section 8.

10.1.2 Disclosure and transfer to external Controllers established in a country outside the EEA that is not recognised by the EU Commission as ensuring an adequate level of protection

Disclosure to an external Controller established in a country outside the EEA that is not recognised by the EU Commission as ensuring an adequate level of protection may take place provided that the conditions in 10.1.1 are fulfilled, and there is a legal basis for the transfer as described in Section 10.2.2.

10.2 Transfer to external Processors not bound by the BCR

10.2.1 Transfer to external Processors established within the EEA or a country recognised by the EU Commission as ensuring an adequate level of protection

Transfer of Personal Data from a Controller established in the EEA to a Processor established in the EEA may take place, provided that the Processor's Processing on behalf of the Controller is governed by a contract ("**Data Processing Agreement**") which stipulates the following:

a) the Processor shall Process Personal Data only in accordance with the Controller's instructions and for the purposes authorized by the Controller;
b) the Processor shall keep the Personal Data confidential;
c) the Processor shall take appropriate technical, physical and organisational security measures to protect the Personal Data;
d) the Processor shall not permit sub-processors to Process Personal Data in connection with its obligations to the Controller without the Controller's prior written consent;
e) the Controller has the right to review the security measures taken by the Processor
    i. by an obligation of the Processor to submit its relevant data processing facilities to audits and inspections by the Group Company; or
    ii. by means of a statement issued by a qualified independent third party assessor on behalf of the Processor, certifying that the data processing facilities of the Processor used for the Processing of the Personal Data comply with the requirements of the Data Processing Agreement;
f) the Processor shall promptly inform the Controller of any actual or suspected Personal Data Breach involving Personal Data; and
g) the Processor shall take adequate remedial measures as soon as possible and shall promptly provide the Controller with all relevant information and assistance as requested by the Controller regarding the Personal Data Breach.

10.2.2 Transfer to external Processors established in a country outside the EEA that is not recognised by the EU Commission as ensuring an adequate level or protection

Transfer of Personal Data from a Controller established within the EEA to a Processor established in a country outside the EEA that is not recognised by the EU Commission as ensuring an adequate level of protection may only take place if the requirements of Section 10.2.1 are fulfilled and one of the following applies:

a) the Processor has implemented Binding Corporate Rules or a similar transfer mechanism that provides appropriate safeguards under applicable law;

b) the Controller and the Processor have provided appropriate safeguards by entering into EU Standard Contractual Clauses (model contract);
c) the Controller and the Processor have provided appropriate safeguards by entering into Standard Data Protection Clauses adopted by the EU Commission or a DPA;
d) the Processor 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; or
e) an approved code of conduct or an approved certification mechanism pursuant to Section 46(1)(e) and (f) of the General Data Protection Regulation is provided for.

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

f) the transfer is necessary for the performance of a contract between the Controller and the Individual or for taking necessary steps at the request of the Individual prior to entering into a contract;
g) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Individual between the Controller and the Processor;
h) the transfer is necessary for important reasons of public interest;
i) the transfer is necessary for the establishment, exercise or defence of a legal claim;
j) the transfer is necessary to protect a vital interest of the Individual; or
k) the transfer is required by any law to which the relevant Controller is subject.

Transfers based on g) and j) above require the prior approval of the Corporate Privacy Officer.

10.2.3 Individual's Consent for Transfer

If none of the legal basis for transfer listed in Section 10.2.2 exists or Consent is allowed or required under applicable law, KONGSBERG shall (also) seek an explicit Consent from the Individual for the relevant transfer. The Consent must be requested prior to participation of the Individual in specific projects, assignments or tasks that require the transfer of Personal Data.

Consent cannot be used as a legal basis for transfer if it has foreseeable adverse consequences for the Individual. This means that Consent will as a main rule not be applicable as a legal basis for transfers relating to Personnel.

Prior to requesting Consent, the Individual 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 procedure set out in Section 5.4 shall be followed. The requirements set out in Section 5.5 apply to the granting, denial or withdrawal of Consent.

10.3 Transfers from Group Companies established in a country outside the EEA that is not recognised by the EU Commission as ensuring an adequate level of protection

Transfer of Personal Data that were collected in connection with the activities of a Group Company established in a country outside the EEA that is not recognised by the EU Commission as ensuring an adequate level of protection to a Third Party also established in a country outside the EEA that are not recognised by the EU Commission as ensuring an adequate level of protection is permitted if one of the grounds listed in Section 10.2.2 and 10.2.3 apply or if the transfer is:

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

11. Training and awareness program

KONGSBERG provides appropriate training on the BCR 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.

12. Supervision and monitoring of compliance

12.1 Corporate Privacy Officer (CPO)

KONGSBERG shall appoint a Corporate Privacy Officer who, inter alia, shall monitor compliance with the BCR in KONGSBERG, as well as monitoring training and compliant handling. The CPO shall act as main contact to the Norwegian Data Protection Authority. .

12.2 Business Area Privacy Officer (BAPO)

KONGSBERG shall appoint Business Area Privacy Officers who, inter alia, shall monitor compliance with the BCR in the respective Business Area, as well as monitoring training and complaint handling..

12.3 Local Privacy Officer (LPO)

Depending on the complexity and business model of a Business Area, a Local Privacy Officer may be appointed. The LPO shall, inter alia, monitor compliance with the BCR within its area of responsibility, as well as training and compliant handling.

13. Auditing compliance

KONGSBERG shall regularly carry out internal audits related to the BCR as set forth in KONGSBERG's Governance and Management System. KONGSBERG shall ensure that all adequate steps and corrective actions are taken to rectify breaches of the BCR that are identified in relation to the audit.

14. Complaints procedure

14.1 Complaints to KONGSBERG

All Individuals shall have the right to file a complaint regarding compliance with the BCR or violations of their rights under applicable data protection law.

Personnel may file a complaint orally or in written to the relevant HR representative or relevant Privacy Officer.

Customers and Business Partners may file a complaint to the relevant Privacy Officer or through the general contact section of KONGSBERG's company website.

In the response to the Individual, the relevant Privacy Officer shall provide information about measures that have been or will be implemented on the basis of the complaint and the stipulated timing for such measures. In case a complaint is rejected, the relevant Privacy Officer shall provide the Individual with reasons for the rejection. If an Individual is not satisfied with the response to the complaint, the Individual can choose to lodge claims based on the BCR in accordance with section 14.2.

Within four (4) weeks after receipt of a complaint, the relevant Privacy Officer shall revert to the Individual in writing of the result of the complaint handling. If, due to the complexity of the complaint, a response cannot be given within the four (4) weeks period, the relevant Privacy Officer will inform the Individual

accordingly and provide a reasonable estimate for the timescale within which a response will be provided. The time limit shall not exceed three (3) months from receipt of the complaint.

14.2 Complaints to Data Protection Authorities or courts

Individuals are encouraged to first follow the complaints procedure set forth in Section 14.1 of the BCR before filing any complaint or claim with competent Data Protection Authorities or the courts.

In case of violation of the BCR, the Individual 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 Group Company in such country of origin responsible for the relevant transfer;
b) in Norway, against Kongsberg Gruppen ASA; or
c) in the EEA country where the Individual resides or has its place of work, against the Group Company 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 Individual will not prejudice the substantive or procedural rights he or she may have under applicable law.

15. Liability

Kongsberg Gruppen ASA is responsible for and agrees to take the necessary action to remedy the acts of Group Companies established outside the EEA and to pay compensation in accordance with applicable EU/EEA law, cf. Section 18 below, for any damages resulting from the violation of the BCR by Group Companies established outside the EEA.

Any Individual that can demonstrate that he or she has suffered damages due to violation of the BCR, 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 the BCR. 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 Kongsberg Gruppen ASA to prove that the damages suffered by the Individual due to violation of the BCR are not attributable to any Group Company established outside the EEA in order to avoid liability.

16. Sanctions

Non-compliance with the BCR by Personnel may result in disciplinary actions, including termination of employment.

17. Mutual assistance and cooperation with Data Protection Authorities

All Group Companies shall co-operate and assist each other to the extent reasonably possible to handle requests or complaints from Individuals or an investigation or inquiry by competent Data Protection Authorities.

All Group Companies undertake to cooperate with the Data Protection Authorities, particularly by applying recommendations and advice from the authorities, and also by responding to requests from the authorities regarding the BCR.

Except when a Data Protection Authority in one of the EEA countries has jurisdiction under its applicable data protection law, compliance with these rules shall be exclusively supervised by the Norwegian Data Protection Authority.

To the extent the Norwegian Data Protection Authority has discretionary powers for enforcement of applicable data protection law, it shall have similar discretionary powers for enforcement of the BCR. The Norwegian Data Protection Authority may conduct audits in order to ascertain compliance with the BCR.

The relevant Privacy Officer, in collaboration with the Corporate Privacy Officer, shall be the main contact point between relevant Data Protection Authorities and KONGSBERG on any matter arising out of the BCR.

18. Governing law

The BCR shall be governed by and interpreted in accordance with Norwegian law.

19. Conflicts between the BCR and applicable local law

Nothing in the BCR shall be construed as taking away any rights or remedies that Individuals may have under applicable local law. The BCR provide supplemental rights and remedies to Individuals only.

Where an Individual or Group Company of KONGSBERG has reasons to believe that applicable national legislation prevents KONGSBERG from fulfilling its obligations under this BCR, the Corporate Privacy Officer or the Business Area Privacy Officer (who will inform the Corporate Privacy Officer) shall be notified without undue delay.

Where there is a conflict between applicable national law and the obligations under this BCR, the Corporate Privacy Officer shall give advice on what action to take and consult with the competent Data Protection Authorities when in doubt. This applies except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law investigation.

The Business Area Privacy Officer shall promptly inform the BA Compliance Officer and the Corporate Privacy Officer of any new legal requirement that may interfere with KONGSBERG's ability to comply with the BCR.

20. Procedure for updating the BCR

Changes and modifications can be made to the BCR only in accordance with the mechanism set out in this Section 20.

Updates to the BCR are possible without having to re-apply for authorization from the Data Protection Authorities, provided that:

a) the Corporate Privacy Officer maintains and keeps a fully updated list of members of the BCR and keeps track of and record of any updates to the rules and provides the necessary information to the Individuals or Data Protection Authorities upon request;
b) no transfer is made to a new member until the exporter of the data has made sure that the new member is effectively bound by the BCR, and can demonstrate compliance; and
c) The Corporate Privacy Officer reports any substantial changes to the BCR or to the list of members of the BCR once a year to the Data Protection Authorities granting the authorizations with a brief explanation of the reason justifying the update.

KONGSBERG shall communicate any substantial modifications to the rules to the Individuals by publishing it on the KONGSBERG intranet, and/or by making the necessary changes to all relevant documents, including the public version of the BCR, cf. 7.1.1.

21. Transition period

Except as indicated below, there shall be a two-year transition period for compliance with the BCR. During the transition period, any transfer of Personal Data to a Group Company in a Third Country, may only take place to the extent that the Group Company receiving such Personal Data is:

a) compliant with the BCR; or
b) the transfer meets one of the grounds for transfer listed in Section 10.

Any Group Company that becomes a Group Company after the Effective Date shall comply with the BCR within two years of becoming a Group Company.

Where there are existing agreements with Third Parties that are affected by the BCR, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.

Processing of Personal Data that were collected in connection with activities of a Group Company located in a Third Country, shall be brought into compliance with the BCR within three years of the Effective Date.

22. Definitions

Unless otherwise specifically stated, where relevant, the following definitions shall be interpreted in consistency with and have the same meaning as definitions set out in the EU Data Protection Directive 95/46/EC, and from 25 May 2018, the EU General Data Protection Regulation 2016/679.

Binding Corporate Rules (BCR)	Binding Corporate Rules or BCR shall mean a set of data protection rules approved by the EU data protection authorities that is legally binding on and enforced by every member of a group of undertakings, including their employees, and which under the EU General Data Protection Regulation and EU Data Protection Directive provides the adequate level of protection for the Transfer of Personal Data within that group of undertakings.
Business Area (BA)	Business Area shall mean the Business Area established in accordance with KONGSBERG's Governance and Management System at any given time.
Business Area Privacy Officer (BAPO)	Business Area Privacy Officer shall mean appointed Business Area Privacy Officer as further detailed in Section 12.2 of the BCR.
Business Partner	Business Partner shall mean a Third Party with whom KONGSBERG has a business relationship.
Consent	Consent shall mean any freely given, specific, informed and unambiguous indication of the Individual's wishes by which he or she, by statement, or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
Controller	A Controller is a Group Company that determines the purposes and means of the Processing of Personal Data of Individuals irrespective of whether the Processing takes place by and within the Group Company or by an external Processor.
Corporate Privacy Officer	The Corporate Privacy Officer is the person who shall supervise implementation of the BCR and who is responsible for overall monitoring of data protection compliance in KONGSBERG as set out in Section 12.1 of the BCR.
Customer	Customer shall mean any Third Party that purchases, may purchase or has purchased a KONGSBERG product or service.

Data Processing Agreement	A Data Processing Agreement shall mean an agreement that regulates how the Processor may Process Personal Data on behalf of the Controller as referred to in Section 10.2.1 of the BCR.
Data Protection Authority (DPA)	Data Protection Authority shall mean the competent data protection authority of one of the countries of the EEA according to applicable EU/EEA law.
Directive	Directive shall mean KONGSBERG's Binding Corporate Rules.
Effective Date	Effective Date shall mean the date on which the BCR become effective.
European Economic Area (EEA)	EEA means the European Economic Area, meaning the EU member states and the EFTA countries (Liechtenstein, Iceland and Norway).
Group Company	Group Company shall mean Kongsberg Gruppen ASA and all subsidiaries bound by the BCR. This includes any directly or indirectly wholly owned subsidiary of Kongsberg Gruppen ASA and other subsidiaries as listed in the document "Members of the BCR".
Individual	An Individual shall mean an identified or identifiable natural person to whom the Personal Data being Processed relates. An Individual may for example be an employee of KONGSBERG, a person applying for a job at KONGSBERG, an external contractor working for KONGSBERG, or a representative of KONGSBERG's Business Partner or Supplier.
KONGSBERG	KONGSBERG shall mean Kongsberg Gruppen ASA and all subsidiaries bound by the BCR. This includes any directly or indirectly wholly owned subsidiary of Kongsberg Gruppen ASA and other subsidiaries as listed in the document "Members of the BCR".
Local Privacy Officer	Local Privacy Officer shall mean a Local Privacy Officer as referred to in Section 12.3 of the BCR.
Personal Data	Personal Data means any information relating to an identified or identifiable natural person (Individual) 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 natural person.
Personnel	Personnel shall mean employees and third parties, such as contractors and consultants who act in a similar capacity as employees, who Process Personal Data as part of their respective duties or responsibilities as Personnel or individuals under the direct authority of KONGSBERG using KONGSBERG information technology systems or working primarily from KONGSBERG's premises.
Privacy Officer	Privacy Officer shall mean the relevant Local Privacy Officer, Business Area Privacy Officer or Corporate Privacy Officer as referred to in Section 12 of the BCR.
Processing of Personal Data	Processing means any operation or set of operations performed upon or use of Personal Data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaption or alteration, 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 fully or partly Processing of Personal Data with the aid of computers or similar equipment that is capable of automatically and electronically Processing Personal Data. The definition also includes manual registration or filing systems if Personal Data is included.
Processor	A Processor is any natural or legal person, public authority, agency or other body, which Processes Personal Data on behalf of a Controller. Examples of Processors include external IT-service providers or outsourcing partners of KONGSBERG. A KONGSBERG Group Company (such as Kongsberg Gruppen ASA) may act as an internal Processor, which Processes the Personal Data on behalf of another Group Company acting as a Controller.
Sensitive Personal Data	Sensitive Personal Data is any Personal Data revealing an Individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (for uniquely identifying a natural person), health, sex life or sexual orientation.
Supplier	Supplier shall mean any Third Party that provides goods or services to KONGSBERG (e.g. an agent, consultant or vendor).
Third Country	A Third Country shall mean a country outside the EEA, i.e. all countries except the EU member states and the EFTA countries (Liechtenstein, Iceland and Norway).
Third Party	Third Party shall mean any person, private organization, entity or government body outside KONGSBERG.

23. Effective date and last update

The BCR was signed and authorized by KONGSBERG's CEO 24 November 2017 (Effective date) and was approved by the Norwegian Data Protection Authority 1 February 2018.

This public version of the BCR was last updated 2018-05.16.

24. Contact

The Corporate Privacy Officer may be contacted at:

Email: privacy@kongsberg.com

Postal address:
Corporate Privacy Officer

Kongsberg Gruppen ASA

PO Box 1000

NO-3601 Kongsberg