EQUINOR

BINDING CORPORATE RULES

- PUBLIC DOCUMENT

Effective date: From the data the new personal data act implementing GDPR comes into effect in Norway

The purpose of this Equinor Binding Corporate Rules Public Document is to explain the content of the Binding Corporate Rules (BCR) and help ensure that Data Subjects are able to exercise their rights following from the BCRs.

Equinor binding corporate rules for personnel, business partners and other external parties

1 INTRODUCTION

Equinor has implemented Equinor Binding Corporate Rules ("BCRs") for the Processing of Personal Data within the Group. The purpose of the BCRs is to provide an adequate level of protection for Processing of Personal Data within the Group.

European data protection law restricts transfer of personal data to countries outside the EU/EEA that do not ensure an adequate level of data protection. Several of the countries in which the Group operates are not regarded as providing an adequate level of data protection. Binding corporate rules are developed to allow multinational corporations, such as Equinor, to make intra-group transfers of personal data across borders in compliance with European data protection laws.

The BCRs are approved by the Norwegian and other European Data Protection Authorities and are binding on Equinor ASA and other entities in the Group. An updated list of the members of the BCRs is available on request to the Data Protection Officer. The Group is under a legal duty to respect and comply with the BCRs.

The BCRs apply to Personal Data relating to Personnel, Business Partners and other External Parties of Equinor to the extent these data are protected by applicable European data protection law, and for which the BCRs are required in order to transfer the relevant data outside of EU/EEA to a country that is not recognised by the EU Commission as ensuring an adequate level of protection.

The BCRs do not deprive Data Subjects of any rights or remedies provided to them under applicable data protection law. To the extent that applicable data protection law requires a higher level of protection for Personal Data, such applicable legislation will take precedence over the BCRs.

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

2 DEFINITIONS USED IN THIS DOCUMENT/THE BCRS

ARCHIVE shall mean an archive kept by the Group for historical, scientific, statistical or other general archiving purposes.

BUSINESS PARTNERS shall mean Data Subjects with whom the Group has a business relationship, either directly with the relevant Data Subject or with the relevant Data Subject's employer. Data Subjects that are also covered by the definition of Personnel shall be regarded as Personnel instead of Business Partners.

BCR/BCRs shall mean the documents adopted as the Group's binding corporate rules.

CEC shall mean the corporate executive committee in the Group.

CONTROLLER shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data.

DATA EXPORTER shall mean a Controller established in the EU/EEA who transfers Personal Data to an Importer established outside the EU/EEA.

DATA IMPORTER shall mean a Controller or Processor established outside the EU/EEA who receives Personal Data from an Exporter.

DATA PROTECTION AUTHORITY shall mean the competent data protection authority according to applicable EU/EEA law.

DATA PROTECTION OFFICER shall mean the appointed Data Protection Officer as further detailed in the BCRs.

DATA SUBJECT shall mean an identifiable person who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person. In the BCRs the Data Subjects are Personnel, Business Partners, other External Parties and their Next of Kin.

EFFECTIVE DATE shall mean the date on which the BCRs become effective.

EXTERNAL PARTY shall mean any natural or legal person, public authority, agency or any other body outside of the Group.

FILING SYSTEM shall mean any structured set of Personal Data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

GROUP shall mean the members of the BCRs referred to in Article 1.

LEGITIMATE PURPOSES shall mean purposes that are objectively justified by the activities of the Group as specified in Article 3.6 below.

LINE/LINE MANAGEMENT shall mean the various areas established to be Lines, and the management of such areas, in accordance with the Group's management system at any given time.

LOCAL FUNCTION MANAGERS shall mean the managers of the various local Function Areas in accordance with the Group's management system at any given time.

NEXT OF KIN shall mean the spouse, partner or child of Personnel, Business Partners and other External Parties that are Data Subjects.

PERSONAL DATA shall mean any information relating to an identified or identifiable natural person, Data Subject. The Personal Data comprised by the BCRs shall be Personal Data comprised by applicable EU/EEA data protection legislation.

PERSONAL DATA BREACH shall mean breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

PERSONNEL shall mean employees, candidates and former employees of the Group. The term Personnel also includes present and former consultants and employees of Business Partners providing services to the Group through the Group's information technology systems or from the Group's premises, in the same manner as employees.

PROCESSING/PROCESS shall mean any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

PROCESSOR shall mean a natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of the Controller.

FUNCTION AREAS shall mean the various areas established to be Function Areas in accordance with the Group's management system at any given time.

FUNCTION OWNERS shall mean the persons appointed as Function Owners in accordance with the Group's management system at any given time.

SENSITIVE PERSONAL DATA shall mean Personal Data revealing racial or ethnic origin, political opinions, philosophical or religious beliefs, trade union membership, 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 DATA SUBJET'S CONSENT/CONSENT shall mean any freely given specific, informed and unambiguous indication of the Data Subject's whishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

THIRD PARTY shall mean any natural or legal person, public authority, agency or any other body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to Process Personal Data.

3 SUMMARY OF THE BCRS

3.1 Legal basis for Processing of Personal Data

Personal Data may be processed by the Group for Legitimate Purposes on the following legal basis:

(i) The Processing is necessary for the performance of a contract between the Data Subject and the Group, or in order to take steps prior to entering into such a contract;

(ii) The Processing is necessary for Legitimate Purposes pursued by the Group or by a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject;

(iii) The Data Subject has given his/her Consent to the Processing of his/her Personal Data for one or more specific purposes;

(iv) The Processing is necessary for compliance with a legal obligation to which the Group is subject;

(v) The Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person; or

(vi) The Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Group.

3.2 Legal basis for Processing of Sensitive Personal Data

As a starting point Processing of Sensitive Personal Data is prohibited. The Group can, however, provided that Legitimate Purposes are documented, Process Sensitive Personal Data on the following legal basis:

(i) The Processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the Group or of the Data Subject in the field of employment and social security and social protection law, in so far as it is authorized by national law or a collective agreement pursuant to national law providing for adequate safeguards;

(ii) The 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 Consent;

(iii) The Processing relates to Sensitive Personal Data which is manifestly made public by the Data Subject;

(iv) The Processing of Sensitive Personal Data is necessary for the establishment, exercise or defence of legal claims;

(v) The Data Subject has given his explicit Consent;

In order to rely on Consent, the Group must follow the procedure set out in Article 3.3 below.

(vi) The Processing of Personal Data is required for the purposes of preventive medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of care or treatment or the management of health-care services, and the 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;

(vii) The Processing is necessary for reasons of substantial public interest, on the basis of applicable EU/EEA law in accordance with GDPR Article 9(2)(g);

(viii) The Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of applicable EU/EEA law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

(ix) The Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with GDPR Article 9(2)(j).

3.3 Consent

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

(i) The Group must inform the Data Subject in accordance with the provisions set forth in Articles 3.9.2 and 3.9.3;

(ii) The Group 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;

(iii) If the Data Subject's Consent is given in the context of a written declaration which also concerns other matters, the request for Consent shall, if applicable law so requires, be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language; and

(iv) The Data Subject may withdraw his/her Consent at any time. The withdrawal of Consent shall not affect the lawfulness of the Processing based on such Consent before its withdrawal. Prior to giving Consent, the Data Subject shall, where applicable law so requires, be informed of his/her right to withdraw the Consent. It shall be as easy to withdraw as to give Consent.

3.4 Processing of Personal Data relating to criminal convictions and offences

Processing of Personal Data relating to criminal convictions and offences or related security measures based on Article 6 (1) of the GDPR shall be carried out in compliance with applicable law.

3.5 Processing which does not require identification

If the purposes for which the Group Processes Personal Data for do not or no longer require the identification of a Data Subject, the Group shall not be obliged to maintain, acquire or Process additional information in order to identify the Data Subject for the sole purpose of complying with applicable EU/EEA law. This applies for example where the Personal Data have been anonymized.

Where the Group is able to demonstrate that it is not in a position to identify the Data Subject, Articles 3.10.1-3.10.6 shall not apply except where the Data Subject, for the purpose of exercising his/her rights under those Articles, provides additional information enabling his/her identification. In such cases, the Controller shall inform the Data Subject accordingly, if possible.

3.6 Requirements regarding purposes for processing of personal data – purpose limitations

Personal Data shall only be Processed by the Group for purposes that are objectively justified by the activities of the Group; Legitimate Purposes. The Group shall make sure that Legitimate Purposes exist for Processing at the time of collection of Personal Data.

Sensitive Personal Data shall be provided with additional safeguards in accordance with applicable law and EU/EEA law.

The Group's Processing of Personal Data includes, but is not limited to, Processing for the following specific Legitimate Purposes:

(i) Human resources and management of Personnel;

This purpose includes Processing that is necessary for the performance of an employment/contractor contract or a prospective employment/contractor contract, including but not limited to Processing related to recruitment and deployment, performance and development, reward, employee/contractor relations and change management and continuous improvement. The purpose may i.a. include the Processing of the following categories of Personal Data: contact information, management and administration of compensation and benefits, payments, tax issues, career planning, evaluations, training, travel and expenses, recruiting, outplacement and communication with Personnel.

(ii) Management and administration of business relationships;

This purpose includes Processing of Personal Data that is necessary with regards to a business relationship with Business Partners or other External Parties. The purpose may i.a. include the Processing of the following categories of Personal Data: management and administration of contact information, compensation, payments, tax issues, evaluations, training, travel and expenses, recruiting and other circumstances related to business relationships as well as communication with relevant Data Subjects with regards to business relationships.

(iii) Health, safety and environment;

This purpose includes Processing that is necessary to provide health services and protect health, safety and environment related to Personnel, Business Partners, other External Parties, their Next of Kin or the public. The Processing may i.a. include Processing of the following categories of Personal Data: health data, data related to preventing and following up drug or alcohol abuse, certificates, incident reports, access control logs etc.

(iv) Planning and control measures;

This purpose includes Processing related to activities such as planning, scheduling time tables, recording time, conducting surveys, controls, internal audits and investigations. The Processing may i.a. include the following categories of Personal Data: time registration of hours worked, absences and leaves, training, certificates, records of work-related training, rates and cost information, etc.

(v) Business operation and protection of business interests and security; and

This purpose includes Processing in relation to business operation and protection of business interests and security; e.g. information security, access control, security check, CCTV, logging, conduction of controls, surveys, analysis, reports, managing of daily operations and transactions/possible transactions involving the Group, screening, background check and integrity due diligence. The

Processing may i.a. involve the following categories of Personal Data: name, gender, age, biometric data, activity logs, complaints, roles in companies, details on potential misconduct, etc.

(vi) Compliance with legal obligations and protection of legal position.

This purpose includes Processing of Personal Data that is necessary in order to ensure compliance with legal obligations and/or to protect a legal position of the Group, e.g. tax and accounting information and information relating to legal proceedings.

3.7 Legitimate Purposes for Processing further to collection (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 Legitimate Purposes are examples of purposes that are not incompatible with the Legitimate Purposes stated above:

(i) Audits, business controls and investigations;

(ii) Dispute resolution;

(iii) Legal and business affairs;

(iv) Research;

(v) Transfer of Personal Data to an Archive; and

(vi) Insurance.

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

(i) Limiting access to the Personal Data;

(ii) Imposing additional confidentiality requirements and security measures;

(iii) Informing the Data Subjects about the Legitimate Purposes; or

(iv) Obtaining Consent from the Data Subjects.

3.8 Data quality and proportionality

Personal Data shall at any time be accurate, complete and kept up-to-date as reasonably required, to meet Legitimate Purposes.

The Group shall only Process Personal Data that are adequate for, relevant and not excessive to the Legitimate Purposes.

The Group shall only retain Personal Data for the period that is required to serve the Legitimate Purposes, to comply with applicable law or as advisable due to applicable statute of limitations.

When retention is no longer necessary in accordance with these requirements, Personal Data shall be:

(i) Securely deleted or destroyed;

(ii) Anonymized;

(iii) To the extent permitted under applicable EU/EEA law, restricted; or

(iv) Transferred to an Archive, to the extent such transfer is permitted by applicable law.

3.9 Transparency and information rights

3.9.1 Availability of the BCRs

This public version of the BCRs (a summary version) shall be available for all Data Subjects on the Group's website, Equinor.com.

The BCRs in its entirety, as well as the list of members of the BCRs, will be made available to the Data Subjects upon request to the Data Protection Officer. Please see contact information in Article 4 below.

3.9.2 Information in cases of collection of data from the Data Subject

Before Personal Data is Processed, the Group shall make sure that the Data Subjects receive information about:

(i) The identity and contact details of the Controller;

(ii) The contact details of the Data Protection Officer, where applicable;

(iii) The purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;

(iv) Where the Processing is based on Article 3.1(ii), the legitimate interests pursued by the Controller or Third Parties;

(v) The recipients or categories of recipients of the Personal Data, if any; and

(vi) Where applicable, the fact that the Controller intends to transfer Personal Data to a country outside of EU/EEA or an international organization and the existence or absence of an adequacy decision by the EU Commission or reference to the appropriate safeguards, e.g. the Group's BCR or applicable legal basis mentioned in Article 3.13.3, and the means on how to obtain a copy of them or where they have been made available.

In addition, where required by applicable law and if necessary to ensure fair and transparent Processing, the Group shall provide the Data Subject with the following further information:

(vii) The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

(viii) The existence of the right to request access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or the right to object to Processing as well as the right to data portability, cf. Article 3.10;

(ix) Where the Processing is based on a Data Subject's Consent, the existence of the right to withdraw Consent at any time as described in Article 3.3, without affecting the lawfulness of Processing based on Consent before its withdrawal;

(x) The right to lodge a complaint with a Data Protection Authority;

(xi) Whether the provision of Personal Data is a statutory or a 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;

(xii) The existence of automated decision-making, including profiling, referred to in Article 3.11 below and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

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

The requirements of this Article 3.9.2 may be set aside where and insofar the Data Subject already has the information.

3.9.3 Information where Personal Data have not been obtained from the Data Subject

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

(i) The identity and contact details of the Controller;

(ii) The contact details of the Data Protection Officer, where applicable;

(iii) The purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;

(iv) The categories of Personal Data concerned;

(v) The recipients or categories of recipients of the Personal Data, if any; and

(vi) Where applicable, the fact that the Controller intends to transfer Personal Data to a country outside of EU/EEA or an international organization and the existence or absence of an adequacy decision by the EU Commission or reference to the appropriate safeguards, e.g. the Group's BCR or applicable legal basis mentioned in Article 3.13.3, and the means 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 Group shall provide the Data Subject with the following further information:

(i) The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

(ii) Where the Processing is based on Article 3.1(ii), the legitimate interests pursued by the Controller or Third Parties;

(iii) The existence of the right to request access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or the right to object to Processing as well as the right to data portability, cf. Article 3.10;

(iv) Where the Processing is based on a Data Subject's Consent, the existence of the right to withdraw Consent at any time as described in Article 3.3, without affecting the lawfulness of Processing based on Consent before its withdrawal;

(v) The right to lodge a complaint with a Data Protection Authority;

(vi) From which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources;

(vii) The existence of automated decision-making, including profiling, referred to in Article **Error! R eference source not found.** below 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:

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

(ii) If the Personal Data are used for communication with the Data Subject, at the latest at the time of the first communication with the Data Subject; or

(iii) If a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed.

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

The requirements of this Article 3.9.3 may be set aside where and insofar:

(iv) The Data Subject already has the information;

(v) 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 Group shall take appropriate measures to protect the Data Subject's rights and freedoms and legitimate interests, including making the information publicly available;

(vi) Obtaining or disclosure is expressly laid down in applicable EU/EEA law to which the Controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests; or

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.

3.10 Data Subjects' rights of access, rectification, erasure, restriction and objection to Processing of Personal Data

3.10.1 Data Subject's right of access

Data Subjects have the right to obtain the following information:

(i) Confirmation as to whether or not Personal Data relating to him/her is being Processed and where that is the case, access to the Personal Data processed by the Group;

(ii) The purposes of the Processing, the categories of Personal Data concerned, and the recipients or categories of recipients to whom the Personal Data is disclosed, in particular recipients located outside of EU/EEA in a country that is not recognised by the EU Commission as ensuring an adequate level of protection. In the cases of such transfers, the Data Subject shall have the right to be informed of the appropriate safeguards pursuant to Article 3.13.3 relating to the transfer;

(iii) Where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;

(iv) The existence of the right to request from the Group rectification or erasure of Personal Data or restriction of the Processing of Personal Data concerning the Data Subject or to object to such Processing;

(v) The right to lodge a complaint with a Data Protection Authority;

(vi) Where the Personal Data have not been collected from the Data Subject, any available information about the source of such Personal Data; and

(vii) Information about the existence of automated decisions, including profiling, referred to in Article 3.11 below 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 Group shall provide a copy of the Personal Data undergoing Processing. The right to obtain a copy shall not adversely affect the rights and freedoms of others. For any further copies requested by the Data Subject, the Group may charge a reasonable fee based on administrative costs.

When the Data Subject makes the request by electronic means, the response shall be provided by electronic means where possible, unless otherwise requested by the Data Subject.

3.10.2 Data Subject's right to rectification

The Data Subject shall have the right to obtain from the Group without undue delay, the rectification of inaccurate Personal Data concerning him/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 providing a supplementary statement.

3.10.3 Data Subject's right to erasure

Where required by applicable law, the Data Subject shall have the right to obtain from the Group the erasure of Personal Data concerning him/her without undue delay. The Group shall have the obligation to erase Personal Data without undue delay when one of the following grounds applies:

(i) The Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise Processed;

(ii) The Data Subject withdraws his/her Consent to the Processing and where there is no other legal basis for the Processing;

(iii) The Data Subject objects to the Processing pursuant to Article 3.10.6 first and second paragraph and there are no overriding legitimate grounds for the Processing, or the Data Subject objects to the Processing pursuant to Article 3.10.6 third paragraph;

(iv) The Personal Data have been unlawfully Processed;

(v) The Personal Data have to be erased for compliance with a legal obligation in applicable EU/EEA law to which the Group is subject.

Where the Controller has made the Personal Data public and is obliged pursuant to the first paragraph of this Article 3.10.3 to erase the Personal Data, the Controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other Controllers which are processing the Personal Data that the Data Subject has requested the erasure by such Controllers of any links to, or copy or replication of, those Personal Data.

The Data Subject's right to erasure in the first and second paragraphs of this Article 3.10.3 shall not apply to the extent that the Processing is necessary for:

(vi) Exercising the right of freedom of expression and information;

(vii) 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 Group;

(viii) Reasons of public interest in the area of public health in accordance with points (h) and (i) of GDPR Article 9(2) as well as Article 9(3);

(ix) Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with GDPR Article 89(1) in so far as the right to erasure referred to in the first paragraph of this Article 3.10.3 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(x) The establishment, exercise or defence of legal claims.

3.10.4 Data Subject's right of restriction of Processing

Where required by applicable law, the Data Subject shall have the right to obtain from the Group restriction of Processing where one of the following applies:

(i) The accuracy of the Personal Data is contested by the Data Subject, for a period enabling the Controller to verify the accuracy of the Personal Data;

(ii) The Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;

(iii) The Group no longer needs the Personal Data for the purposes of the Processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;

(iv) The Data Subject has objected to the Processing under Article 3.10.6 pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

Where Processing has been restricted under the first paragraph, such Personal Data shall, with the exception of storage, only be Processed:

(v) with the Data Subject's Consent;

(vi) for the establishment, exercise or defence of legal claims;

(vii) for the protection of the rights of another natural or legal person; or

(viii) for reasons of important public interest of the EU/EEA or of a country in the EU/EEA.

The Group shall inform the Data Subject who has obtained restriction of Processing, before the restriction of Processing is lifted.

3.10.5 Notification obligation regarding rectification, erasure or restriction of Processing

Where required by applicable law, the Group shall give notification to recipients of Personal Data of any rectification, erasure or restriction carried out in accordance with Articles 3.10.2 to 3.10.4, unless this proves impossible or involves a disproportionate effort for the Group. The Group shall inform the Data Subject about those recipients if the Data Subject requests it.

3.10.6 Data Subject's right to object

The Data Subject shall have the right to object, on grounds relating to his/her particular situation, at any time to the Group's Processing of Personal Data concerning him/her if the Processing is based on Articles 3.1(ii) or (vi). This includes profiling based on those provisions.

It a Data Subject objects to the Processing, the Group shall no longer Process the Personal Data unless:

(i) The Group demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or

(ii) For the establishment, exercise or defence of legal claims.

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

The Data Subject's 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 the first communication with the Data Subject.

3.10.7 Procedure for handling requests relating to Data Subjects' rights

Requests in accordance with Article 3.10 should be filed in writing to the relevant Owner. The Data Protection Officer shall provide information about the identity of the relevant Function Owner if required.

The relevant Function Owner shall respond to requests in accordance with this Article 3.10 in writing without undue delay and in any event no later than one month from receipt of a request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Data Subject shall be informed of any such extension within one month of receipt of the request, together with the reasons for the delay.

When the Data Subject makes the request by electronic means, the response shall be provided by electronic means where possible, unless otherwise requested by the Data Subject.

If Data Subjects are not satisfied with the response to their requests, Data Subjects may file a complaint in accordance with Article 3.16.

3.11 Automated individual decisions

The Data Subject shall have the right not to be subject to a decision based solely on automated Processing of Personal Data, including profiling, which produces legal effects concerning him/her or similarly significantly affects him/her, unless the decision:

(i) Is necessary for entering into, or performance of, a contract between the Data Subject and the Group;

(ii) Is authorized by applicable EU/EEA law to which the Group is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests; or

(iii) Is based on the Data Subject's explicit Consent.

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

Decisions referred to in the second paragraph shall not be based on Sensitive Personal Data unless Articles 3.2(v) or 3.2(vii) applies and suitable measures to safeguard the Data Subject's rights, freedoms and legitimate interests are in place.

3.12 Data security and confidentiality

The Group has developed and implemented IT policy documents. These policy documents establish routines for evaluation of risks represented by the Processing of Personal Data. Further, the documents establish the technical and organizational measures that are in place to ensure sufficient level of security and to protect Personal Data against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access.

Specific measures are implemented and shall always be in place to protect Personal Data when the Processing involves transmission over a network and against unlawful forms of Processing.

Sensitive Personal Data are Processed with enhanced security measures in accordance with applicable law.

The measures in place shall always ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected, having regard to the state of the art and the cost of implementation of the relevant measures.

Personnel with technical access to Personal Data are only authorized to access Personal Data to the extent that this is necessary, in order for them to perform their job, and otherwise in accordance with the BCRs and applicable law.

Personnel who access Personal Data must meet their confidentiality obligations.

3.13 Transfer of personal data

Transfer to a Processor or a Controller must always be in line with the Legitimate Purposes set forth in Article 3.6 above.

3.13.1 Use of internal Processors (within the Group)

If the Group engages an internal Processor (within the Group), the Controller shall ensure that the Processor provides sufficient technical, security and organizational measures, and shall ensure compliance with those measures. The Processing of Personal Data by a Processor on behalf of a Controller shall be governed by Equinor's Group Data Processing Agreement, cf. Intercompany Agreement Regarding Bindingness of Equinor's Binding Corporate Rules section 4. The description of the Processing shall be set out in the relevant Privacy Standard.

3.13.2 Written contract with external Processors (outside the Group)

If the Group engages external Processors (outside the Group), a written contract must be entered into, stipulating that the Processor shall be responsible for the implementation of adequate security and confidentiality measures. The contract shall set out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Controller. The contract shall be in accordance with applicable EU/EEA law requirements and, to the extent required, stipulate that the Processor:

(i) Shall only Process Personal Data on documented instructions from the Controller, hereunder with regard to transfers of Personal Data to a recipient located outside of EU/EEA in a country that is not recognized by the EU Commission as ensuring an adequate level of protection or an international organisation. The Processor shall inform the Controller of any legal requirement that hinders the Processor from following the Controller's instructions, unless that law prohibits such information on important grounds of public interests;

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

(iii) Takes all measures required according to GDPR Article 32;

(iv) Shall not engage another Processor without prior specific or general written authorisation of the Controller. In the case of general written authorisation, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other Processors, thereby giving the Controller the opportunity to object to such changes. The same obligations as set out in the contract between the Controller and the Processor shall be imposed on that other Processor by way of contract;

(v) Taking into account the nature of the Processing, assists the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising Data Subjects' rights laid down in GDPR Chapter III;

(vi) Assists the Controller in ensuring compliance with the obligations pursuant to GDPR Articles 32 to 36 taking into account the nature of Processing and the information available to the Processor;

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

(viii) Makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in applicable EU/EEA law and allow for and contribute to audits, including

inspections, conducted by the Controller or a third party auditor mandated by the Controller. The Processor shall immediately inform the Controller if, in its opinion, an instruction pursuant to this provision infringes applicable EU/EEA data protection law.

3.13.3 Transfers to external Processors outside the EU/EEA

The Group shall ensure that the European rules on transborder data flows are complied with when Personal Data is transferred to external Processors (outside of the Group) located outside of EU/EEA, or located in a country that is not recognised by the EU Commission as ensuring an adequate level of protection. This means that transfer can only take place if there is in place appropriate safeguards according to GDPR Article 46, including:

(i) The Third Party is established in the US and has been certified under the EU-US Privacy Shield or any other similar program that is recognized by the EU Commission as ensuring an adequate level of protection;

(ii) The Third Party has implemented binding corporate rules or other accepted transfer mechanisms which provide adequate level of data protection under applicable EU/EEA data protection law;

(iii) A contract has been entered into between the Group and the relevant Third Party which adduces appropriate safeguards with respect to the Personal Data, in accordance with applicable EU/EEA data protection law, e.g. EU Standard Contractual Clauses;

(iv) The Group and the Third Party have provided appropriate safeguards by entering into Standard Data Protection Clauses adopted by the EU Commission or a Data Protection Authority; or

(v) An approved code of conduct or an approved certification mechanism pursuant to applicable EU/EEA data protection law or GDPR are provided for.

In specific situations where a transfer cannot be based on (i) to (v) above, transfer may take place if at least one of the following conditions applies:

(vi) The transfer of Personal Data is necessary for the performance of a contract between a Data Subject and the Group or for taking necessary steps at the request of the Data Subject prior to entering into a contract;

(vii) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Group and a Third Party;

(viii) The transfer is necessary for important reasons of public interest;

(ix) The transfer is necessary for the establishment, exercise or defence of legal claims;

(x) The transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving Consent;

(xi) The transfer is made from a register which according to applicable EU/EEA law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by applicable EU/EEA law for consultation are fulfilled in the particular case; or

(xii) The transfer can be based on GDPR Article 49(1) second paragraph (i.e. compelling legitimate interest pursued by the Controller which are not overridden by the interest of the Data Subject).

If none of the conditions listed above applies or Consent is allowed or required under applicable law, the Group must (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. Prior to requesting Consent for transfer, 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 recognized the country in question as ensuring an adequate level of protection.

When requesting Consent for transfer, the conditions in Article 3.3 shall apply.

3.13.4 Transfer to Controllers

All transfers of Personal Data to Controllers presuppose that there is legal basis for this, as described in Article 3.1 and 3.2. This applies both to internal and external Controllers.

All transfers of Personal Data to external Controllers (outside of the Group) located outside the EU/EEA, or located in a country that is not recognised by the EU Commission as ensuring an adequate level of protection must have a legal basis as set out in Article 3.13.3.

3.14 Training program

The Group provides appropriate training on the BCRs 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.

3.15 Audit, monitoring program and mitigation

General monitoring is conducted within the Group to manage risk and drive performance and learning. Such monitoring is done in accordance with the Group's management system. The monitoring comprises these BCRs. Monitoring is performed by internal or external parties.

The Group shall carry out audits related to the BCRs as set forth in the Group's management systembiennial. The results of the audit shall be communicated to the Data Protection Officer. On the basis of the results of the audit, the Data Protection Officer shall produce an annual data protection report for the Chief Compliance Officer regarding the Group's compliance with these BCRs, data protection risks and other relevant issues.

In accordance with the Group's management system, CEC has the overall responsibility to ensure compliance with the BCRs.

The Data Protection Officer shall ensure that all adequate steps are taken by the Group to rectify breaches of these BCRs that are identified in relation to the audit and monitoring program, including steps to minimize the harm of breaches that have already occurred and to prevent future breaches.

3.16 Complaint mechanism

Data Subjects may complain if any part of the Group is non-compliant with the BCRs. Complaints shall be filed to the Data Protection Officer. Please see contact information in Article 4 below.

Upon receipt of a complaint, the Data Protection Officer shall do an assessment, and if required, initiate an investigation and consult with relevant parts of the Group.

Within four (4) weeks after receipt of a complaint, the Data Protection Officer shall revert to the Data Subject in writing to inform him/her 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 Data Protection Officer will inform the Data Subject 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.

If a complaint is considered as justified, the Data Protection Officer shall give advice on what actions to take and consult with the Norwegian Data Protection Authority in case of doubt.

In the response to the Data Subject the Data Protection 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.

If a complaint is rejected, the Data Subject shall receive information about the result and the reason for the result from the Data Protection Officer.

If a Data Subject is not satisfied with the response to the complaint, Data Subject can choose to lodge claims based on the BCRs in accordance with the provisions in Article 3.17 below.

3.17 Third Party beneficiary rights

The BCRs grant rights to Data Subjects to enforce the rules as third party beneficiaries as set out in this Article 3.17. The Data Subjects' rights cover judicial remedies for breaches of the rights following from the BCRs, including the general data protection principles, the right to obtain a copy of the BCRs upon request, rights with respect to transparency and information as described in Article 3.9, rights regarding access, rectification, erasure, restriction and objection as described in Article 3.10, rights to automated decisions, right relating to national legislation preventing respect of BCRs, right to complain as described in Article 3.16 and right to receive compensation as described in Article 3.20.

In case of violation of these BCRs, the Data Subject may, at his or her choice, submit a complaint or a claim to the Data Protection Authority or the courts:

(i) in the EU/EEA country at the origin of the Personal Data transfer, against the member of the BCR in such country of origin responsible for the relevant transfer;

(ii) in Norway, against Equinor ASA; or

(iii) in the EU/EEA country where the Data Subject resides, has its place of work or place of alleged infringement, against the member of the BCR being the Controller of the relevant Personal Data.

Data Subjects are encouraged to first follow the complaints procedure set forth in Article 3.16 above before filing any complaint with the Data Protection Authority or court.

3.18 Mutual assistance and cooperation with data protection authorities

All members of the BCRs shall cooperate and assist each other to handle requests or complaints from Data Subjects or an investigation or inquiry by a Data Protection Authority. All members of the BCRs

shall cooperate with the Data Protection Authority and comply with the Data Protection Authority's advice.

3.19 Conflict between national legislation and the BCRs and/or other overriding interests

If there is reason to believe that applicable national legislation prevents the Group from fulfilling its obligations under the BCRs, the Data Protection Officer shall be notified without undue delay, except where prohibited by a law enforcement authority, e.g. prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

The Data Protection Officer shall inform the competent Data Protection Authority of any legal requirements to which the Group is subject outside the EU/EEA which are likely to have a substantial adverse effect on the guarantees provided by these BCRs.

The Data Protection Officer shall give advice on what action to take and consult with the Norwegian Data Protection Authority in case of doubt.

Under specific circumstances other interests may override some of the obligations of the Group or rights of Data Subjects following from the BCRs. In such case, deviations may be made from the BCRs if there is a need to

(i) protect the legitimate business interests of the Group, including:

(a) the health, security or safety of individuals;

(b) the Group's intellectual property rights, trade secrets or reputation;

(c) the continuity of the Group's business operations;

(d) the preservation of confidentiality in a proposed sale, merger or acquisition of a business; or

(e) the involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes

(ii) prevent or investigate suspected or actual violations of

(a) law (including cooperating with law enforcement);

(b) contracts; or

(c) the Group's policies

(iii) otherwise protect or defend the rights or freedoms of the Group, its Personnel or other persons.

Deviations due to overriding interest may only be made to the following provisions:

(i) Article 3.7 Legitimate Purposes for Processing further to collection (secondary purposes);

(ii) Articles 3.9.2 and 3.9.3 regarding information to the Data Subjects;

(iii) Article 3.10 regarding Data Subject's rights of access, rectification, erasure, restriction and objection to processing of personal data;

(iv) Article 3.12 Data security and confidentiality; and

(v) Article 3.13 Transfer of Personal Data to internal Processors (within the Group) and Transfer of Personal Data to external Processors and Controllers (outside the Group).

Application for deviations shall be handled in accordance with the Group's standard procedure.

Before any deviations from the BCRs are made, the Data Protection Officer shall be consulted. The Data Protection Officer shall give advice on what action to take and whether dispensation can be made. The Data Protection Officer will consult the Norwegian Data Protection Authority in case of doubt.

3.20 Liability

Equinor ASA is responsible for and agrees to take the necessary action to remedy the acts of other entities within the Group outside of EU/EEA and to pay compensation in accordance with Norwegian law, as specified in the BCRs, for any damages resulting from the violation of the BCRs by entities within the Group.

If Data Subjects can demonstrate that they have suffered damages and establish facts which show that it is likely that the damage has occurred because of a breach of the BCRs, Equinor ASA has to prove that the damages suffered by Data Subjects due to a violation of the BCRs are not attributable to any part of the Group in order to avoid liability.

Equinor ASA shall be liable only for direct damages suffered by Data Subjects resulting from a violation of the BCRs.

3.21 Sanctions

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

3.22 Changes of the BCRs – applicable version

All material changes to these BCRs or to the list of members bound by these BCRs, shall be communicated to all members to these BCRs and to the Norwegian Data Protection Authority. Such changes will also be communicated to the Data Subjects by publishing the updated public version on the Group's website, Equinor.com.

Any request or complaint involving the BCRs shall be judged against the version of the BCRs that is in force at the time the request or complaint is set forth.

3.23 Legal issues: Governing law, jurisdiction and competence of the Norwegian Data Protection Authority

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

Where applicable law sets forth additional requirements, applicable law shall apply in addition to the BCRs. If applicable law is in defiance of these BCRs, the provisions set forth in Article 3.19 apply.

If a Data Protection Authority of one of the EU/EEA countries has jurisdiction under its applicable data protection law to evaluate data transfers by members of the BCR established in its country, such Data Protection Authority may evaluate these data transfers also against the BCRs. The Norwegian Data

Protection Authority will provide cooperation and assistance when required, including providing audit reports available with the Norwegian Data Protection Authority insofar as relevant to evaluate the aforementioned data transfers against these BCRs.

Except in case of jurisdiction of a Data Protection Authority pursuant to pursuant to paragraph three above, the Norwegian Data Protection Authority shall have the exclusive power to perform audits and supervise compliance with the BCRs and to advice on the application of the BCRs at all times. The Norwegian Data Protection Authority shall have investigative powers based on the Norwegian Data Protection Act. To the extent the Norwegian Data Protection Authority has discretionary powers for enforcement of the Data Protection Act, it shall have similar discretionary powers for enforcement of these BCRs. All members of the BCRs shall cooperate with the Data Protection Authority and comply with the Data Protection Authority's advice.

Except as established in relation to third party beneficiary rights in the BCRs, as described in Article 3.17 above, the Norwegian Data Protection Authority shall have exclusive jurisdiction over all claims based on the BCRs. Legal venue shall be Stavanger tingrett. Claims set before the courts in Stavanger are limited to remedies available under the Norwegian law.

4 CONTACT

The Data Protection Officer may be contacted at:

gm_dataprotection@Equinor.com