The purpose of this Statoil 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. The content of this Statoil Binding Corporate Rules Public Document is protected by copyright law. Copyright in this document is vested with Statoil. The Statoil Binding Corporate Rules Public Document is supplied on the expressed condition that the content must not be used for purposes other than that for which it has been supplied, or reproduced, wholly or in part without the prior written permission of Statoil.

Security Classification: Open
Status: Final

Page 1 of 16
STATOIL BINDING CORPORATE RULES FOR PERSONNEL, BUSINESS PARTNERS AND OTHER EXTERNAL PARTIES

1 INTRODUCTION ................................................................. 3
2 DEFINITIONS USED IN THIS DOCUMENT/THE BCRS .................................................. 4
3 SUMMARY OF THE BCRS ........................................................................ 6
  3.1 Legal basis for Processing of Personal Data ................................................................. 6
  3.2 Legal basis for Processing of Sensitive Personal Data ................................................. 6
  3.3 Requirements regarding purposes for processing of personal data – purpose limitations ........................................................................ 7
  3.4 Legitimate Purposes for Processing further to collection (secondary purposes) .......... 8
  3.5 Data quality and proportionality ............................................................................... 8
  3.6 Transparency and information rights ...................................................................... 9
    3.6.1 Availability of the BCRs ................................................................................... 9
    3.6.2 Information requirements ............................................................................... 9
  3.7 Individual rights of access, rectification and objection to processing of personal data ... 9
  3.8 Automated individual decisions ............................................................................. 10
  3.9 Data security and confidentiality ........................................................................... 10
  3.10 Transfer of personal data .................................................................................... 11
    3.10.1 Transfer to internal Processors (within the Group) ............................................... 11
    3.10.2 Transfer to external Processors (outside the Group) ........................................... 11
    3.10.3 Transfer to Controllers .................................................................................. 12
  3.11 Training program ................................................................................................. 12
  3.12 Audit, monitoring program and mitigation ............................................................... 12
  3.13 Complaint mechanism ......................................................................................... 12
  3.14 Third Party beneficiary rights .............................................................................. 13
  3.15 Mutual assistance and cooperation with data protection authorities ..................... 13
  3.16 Conflict between national legislation and the BCRs and/or other overriding interests ... 13
  3.17 Liability ............................................................................................................. 15
  3.18 Sanctions ........................................................................................................... 15
  3.19 Changes of the BCRs – applicable version .......................................................... 15
  3.20 Legal issues: Governing law, jurisdiction and competence of the Norwegian Data Protection Authority .............................................................................. 15
4 CONTACT .......................................................................................... 16
1 INTRODUCTION

Statoil has implemented Statoil 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 Statoil, 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 Statoil ASA and other entities in the Group. 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 or other External Parties of Statoil 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 identification number or to one or more factors specific to his physical, physiological, 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.

LEGITIMATE PURPOSES shall mean purposes that are objectively justified by the activities of the Group as specified in Article 3.3 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 PROCESS MANAGERS** shall mean the managers of the various local Process 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.

**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, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, 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.

**PROCESS AREAS** shall mean the various areas established to be Process Areas in accordance with the Group’s management system at any given time.

**PROCESS OWNERS** shall mean the persons appointed as Process Owners in accordance with the Group’s management system at any given time.

**SENSITIVE PERSONAL DATA** shall mean Personal Data about racial or ethnic origin, or political opinions, philosophical or religious beliefs, the fact that a Data Subject has been suspected of, charged with, indicted for or convicted of a criminal act, health, sex life and trade-union membership.

**THE DATA SUBJET’S CONSENT/CONSENT** shall mean any freely given specific and informed indication of wishes by which the Data Subject signifies his/her agreement to Personal Data, relating to him/her being Processed.

**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 an agreement between the Data Subject and the Group, or in order to take steps prior to entering into such an agreement;

(ii) The Processing is necessary for Legitimate Purposes pursued by the Group or by a Third Party to whom the Personal Data is disclosed, 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;

(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

(vi) The Processing is necessary for the performance of a task carried out in the public interest.

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 specific rights of the Group in the field of employment law, in so far as it is authorized by national law providing for adequate safeguards;

The Group processes certain health information about Personnel in order to adapt the working place as required by law on this legal basis.

Further, also on this legal basis, the Group Processes information about the fact that a Data Subject has been suspected of, charged with, indicted for or convicted of a criminal act in relation to various schemes, such as whistle blowing schemes, in accordance with applicable law requirements.

(ii) The Processing is necessary to protect the vital interests of the Data Subject or of another person;

(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 or to comply with applicable law obligations;

On this legal basis the Group Processes information about the fact that a Data Subject has been suspected of, charged with, indicted for or convicted of a criminal act in relation to various schemes, such as whistle blowing schemes, in accordance with applicable law requirements.
(v) The Data Subject has given his Consent; or

(vi) Processing of Personal Data is required for the purposes of preventive medicine, 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.

3.3 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. This purpose i.a. includes 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 that is necessary with regards to a business relationship with Business Partners or other External Parties. This purpose i.a. includes 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 security;

This purpose includes Processing that is necessary to provide health services, protect health, safety and security related to Data Subjects or the public.

(iv) Planning and control measures;

This purpose includes Processing related to activities such as scheduling time tables, recording time, conducting surveys, controls, internal audits and investigations.

(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, logging, conduction of controls, surveys, analysis, reports and managing of daily operations and transactions/possible transactions involving the Group.

(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.

3.4 **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.

3.5 **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, blocked; or

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

3.6 **Transparency and information rights**

3.6.1 *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 Statoil.com.

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

3.6.2 *Information requirements*

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

(i) The identity of the Controller;

(ii) The purposes of the Processing; and

(iii) Any further information such as

- the recipients or categories of recipients of the Personal Data; and
- the existence of the right of access to, and rectifying of Personal Data.

The Group is only required to give the stated information if this is necessary having regard to the specific circumstances in which Personal Data are collected, to guarantee fair Processing in respect of the Data Subjects.

Further, where Personal Data have not been obtained from the Data Subjects, the obligation to inform the Data Subjects does not apply if it proves impossible or would involve a disproportionate effort to give information, or if recording or disclosure is expressly laid down by law.

3.7 **Individual rights of access, rectification and objection to processing of personal data**

Data Subjects have the right to obtain without expense:

(i) Confirmation as to whether or not Personal Data relating to him/her are being Processed and information as to the purposes of the Processing, the categories of Personal Data concerned, and the recipients or categories of recipients to whom the Personal Data are disclosed;

(ii) Information about the Personal Data that are Processed by the Group and of available information about the source of such Personal Data; and

(iii) Information regarding the logic involved in the automatic processing of Personal Data concerning him/her in the case of the automated decisions as described in Article 3.8 below.
The Data Subjects may require rectification, erasure or blocking of Personal Data if the Processing does not comply with the provisions of the BCRs, and in particular if Personal Data are incomplete or inaccurate.

Further, the Data Subjects may object to the Group’s Processing of Personal Data based on compelling legitimate grounds relating to their particular situation and based on non-compliance with the BCRs and/or applicable law. In the event that an objection is justified, the Group shall cease or adjust the Processing of Personal Data as required without undue delay.

The Group shall give notification to recipients of Personal Data of any rectification, erasure or blocking carried out in accordance with these provisions, unless this proves impossible or involves a disproportionate effort for the Group.

Requests should be filed in writing to the relevant Process Owner. The Data Protection Officer shall provide information about the identity of the relevant Process Owner if required. Please see contact information in Article 4 below.

The relevant Process Owner shall respond to requests in writing no later than four (4) weeks from receipt of a request.

If special circumstances should make it impossible to reply within the time limit, implementation may be postponed until it is possible to reply. In such case, a provisional reply shall be given stating the reason for the delay and when the reply is likely to be given.

If Data Subjects are not satisfied with the response to their requests, Data Subjects may file a complaint in accordance with the complaint mechanism described in Article 3.13.

### 3.8 Automated individual decisions

No evaluation of or decision about the Data Subjects, which significantly affects them, can be based solely on automated Processing of Personal Data unless:

(i) The use of automated tools is required or permitted by applicable law; and

(ii) Suitable measures are taken to safeguard the interests of the Data Subjects, e.g. the use of automated tools has been discussed with employee representatives or other representatives of the relevant Data Subjects.

### 3.9 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.

3.10 Transfer of personal data

Transfer to a Processor or a Controller must always be in line with the Legitimate Purposes set forth in Article 3.4 above.

3.10.1 Transfer to internal Processors (within the Group)

When Personal Data are transferred to 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 measures shall satisfy a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data in question, having regard to the state of the art and the cost of implementation of the relevant measures. To the extent this is required under applicable law, the Controller shall instruct the Processor by written agreement.

3.10.2 Transfer to external Processors (outside the Group)

If the Group engages external Processors (outside the Group) a written agreement as described in Article 3.10.1 must be entered into.

The Group shall ensure that the European rules on transborder data flows are complied with when Personal Data are transferred to external Processors (outside of the Group) located outside of EU/EEA or 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:

(i) The transfer of Personal Data is necessary for the performance of a contract between a Data Subject and the Group;

(ii) 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;

(iii) The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;

(iv) The transfer is necessary in order to protect the vital interests of the Data Subject;

(v) A contract has been entered into between the Group and the relevant Third Party, which adduces adequate safeguards with respect to the Personal Data, in accordance with the Directive 95/46/EC Article 26(2), e.g. EU Standard Contractual Clauses;

(vi) The Third Party has been certified under a program that is considered providing an adequate level of protection according to an adequacy decision by the EU Commission pursuant to the Directive 95/46/EC Article 25(6);
(vii) The Third Party has implemented binding corporate rules or other accepted transfer mechanisms which provide adequate level of data protection under EU data protection law; or

(viii) The Data Subject has unambiguously given his/her Consent, and transfer based on Consent is in compliance with applicable law.

3.10.3 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.

If Personal Data are transferred to external Controllers (outside the Group) which are located outside of EU/EEA, or located in a country that is not recognised as ensuring an adequate level of protection, the requirements following from European rules on transborder data flows as described in 3.10.2 must be complied with.

3.11 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.

3.12 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 system bi-annually. 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.

3.13 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 3.14 below.

### 3.14 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 3.14. The Data Subjects’ rights cover judicial remedies for breaches of the rights following from the BCRs, including right to obtain a copy of the BCRs upon request, rights with respect to transparency and information as described in Article 3.6, rights regarding access, rectification and objection as described in Article 3.7, rights to complain as described in Article 3.13 and right to receive compensation as described in Article 3.17.

Data Subjects can choose to lodge claims based on the BCRs before:

(i) The court in the jurisdiction of Statoil ASA; Stavanger tingrett, Stavanger, Norway;

(ii) The Norwegian Data Protection Authority; or

(iii) The jurisdiction of the Data Exporter.

Data Subjects are encouraged to first follow the complaints procedure set forth in Article 3.13 above before filing any complaint with the Data Protection Authority or court.

### 3.15 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.

### 3.16 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 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 3.4 Legitimate Purposes for Processing further to collection (secondary purposes);
(ii) Article 3.6.2 Information to the Data Subjects;
(iii) Article 3.7 Individual rights of access, rectification and objection to processing of personal data;
(iv) Article 3.9 Data security and confidentiality; and
(v) Article 3.10 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.
3.17 Liability
Statoil 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, Statoil 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.

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

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

3.19 Changes of the BCRs – applicable version
All material changes to 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 on the Group’s website Statoil.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.

3.20 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 3.16 apply.

If a Data Protection Authority of one of the 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 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 3.14 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@statoil.com