EXTERNAL VERSION

BINDING CORPORATE RULES FOR PROCESSING AND TRANSFER OF PERSONAL DATA WITHIN THE PGS GROUP

1. INTRODUCTION AND BACKGROUND

1.1 External Version

This document is an external version of the Binding Corporate Rules that are adopted by the PGS Group (defined below). This external version is made open to the public and data subjects that are external to PGS (defined below). This external version contains certain redactions compared with the internal Binding Corporate Rules which are solicited for approval by the relevant supervisory authorities. These redactions are primarily about removing references to appendices, yet are predominantly in line with the approved official version.

1.2 The PGS Group – an overview

Petroleum Geo-Services ASA, org. no 916 235 291 and its subsidiaries (according to the Norwegian Public Limited Liability Companies Act 1997 Section 1-3) are involved in marine seismic data acquisition, licensing, imaging, vessel- and technology ownership, and related services and businesses. ("**PGS**" or the "**PGS Group**"). The PGS Group is headquartered in Oslo where its ultimate parent company Petroleum Geo-Services ASA is listed on the Oslo Stock Exchange (OSE: PGS).

The main operational offices of the PGS Group are located in:

- Norway (Oslo);
- UK (Weybridge);
- USA (Houston); and
- Malaysia (Kuala Lumpur).

In addition, the PGS Group operates vessels for offshore seismic acquisition worldwide.

The PGS Group also has sales offices and data processing centers in the following locations:

- Norway (Stavanger)
- Australia (Perth)
- Malaysia (Kuala Lumpur)
- China (Beijing)
- Japan (Tokyo)
- Egypt (Cairo)
- Brazil (Rio de Janeiro)
- Angola (Luanda)
- Nigeria (Lagos)
- Mexico City (Mexico)
- Ghana (Accra)

1.3 Binding Corporate Rules – legal basis and purpose

These Binding Corporate Rules (the "**BCR's**") are set up in compliance with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 Article 47 (hereinafter the "**GDPR**"). The main purposes of the BCR's are to:

(i) establish appropriate safeguards and legal basis for transfer of or making available Personal Data from PGS Group companies located in the European Union ("**EU**") and the European Economic Area (the "**EEA**") to PGS Group companies located in countries that are not considered to provide an adequate level of protection for Personal Data and to international organizations ("**Third Countries**"), and

(ii) implement appropriate technical and organizational measures in the PGS Group to ensure and to be able to demonstrate that Processing of Personal Data is performed in accordance with the GDPR, and which apply for the processing of Personal Data by the PGS Group.

As these BCR's govern PGS Group's processing of personal data, certain key terms are defined:

"**Data Subject**" means an identified or identifiable natural person.

"**Personal Data**" means any information relating to a Data Subject by reference to an identifier, such as name, address, telephone number, identification number, location data, IP addresses, email addresses, post addresses, date of birth, online identifier, or ton one or more factors specific to the physical,

physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data includes all types of information that are directly or indirectly (used in conjunction with other data) referable to the data subject).

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated 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.

The BCR's contain legally binding rules for the PGS Group companies regarding the Processing of Personal Data and give:

- obligations to all entities within the PGS Group involved in the Processing of Personal Data, both in their capacity as Controllers and as Processors;
- obligations to all employees in the PGS Group which are involved in Processing of Personal Data;
- obligations to external third party companies Processing Personal Data on behalf of the PGS Controller;
- rights to all Data Subjects, such as PGS Group employees, candidates applying for work in the PGS Group, customer representatives, other business partner representatives, visitors on www.pgs.com, and others that leave their Personal Data with the PGS Group.

The BCR's are part of the PGS Personal Data Protection Policy (the "**Policy**"). According to the governing management system in the PGS Group, the Policy and the BCR's are binding for all the companies and entities in the PGS Group.

Other defined terms used but not defined herein shall have the same meaning as the defined term in the Policy or in the Laws defined therein.

2. THE PGS GROUP

2.1 The PGS Group – legal structure and main operational offices

The legal structure of the PGS Group is updated on a routinely basis according to the PGS governance policies, and is *inter alia* available in the latest edition of the PGS Annual Report. For a more recent update, please contact the PGS Legal Department. The Global Data Protection Officer have access to a fully updated list of the PGS Group companies which have employees, at all times.

The PGS Group companies involved in Processing of Personal Data are listed below.

The PGS Group is headquartered in Oslo, and the PGS Group's ultimate parent company is PGS. PGS is listed on the Oslo Stock Exchange (OSE: PGS).

The main operational company within each region, as further set out in Section 4, is also the company determining the purposes and means of the Processing of Personal Data within each region (each a "**Controller**").

PGS Geophysical AS, org. no. 960 563 085 ("**PGS Geophysical**") is acting as the main Controller for the PGS Group as a whole (the "**Main Controller**").

The main operational offices identified in Section 1 above have the following contact details:

PGS Geophysical AS, Lilleakerveien 4C, 0283 Oslo, NORWAY, attn. Daphne Bjerke, phone +47 67 51 43 65

PGS Exploration (UK) Ltd, 4 The Heights, Brooklands, Weybridge, Surrey, KT13 0NY, the UNITED KINGDOM, c/o PGS Geophysical AS, Lilleakerveien 4C, 0283 Oslo, NORWAY attn. Daphne Bjerke, phone +47 67 51 42 87

Petroleum Geo-Services Inc., West Memorial Place I, 15375 Memorial Drive, Suite 100, Houston, TX 77079, USA, attn.: Silvia Martins, phone: +1 281 509 8158

PGS Data Processing & Technology Sdn Bhd., Ground Level (Right Wing), Quill Building 3, 3501 Jalan Teknokrat 5, 63000 Cyberjaya, Selangor, MALAYSIA, attn. Evelyn Seow, phone: +603 2175 3741

2.2 The PGS Group – subsidiaries

The PGS Group has a number of subsidiaries placed in various locations around the world, all of which are subject to the BCR's. Please note that the PGS Group is in the process of reorganizing the legal structure. Hence, the list of subsidiaries is correct as of 1 January 2018, but will change throughout the year. The list shall be updated yearly, and can be documented by contacting the PGS Legal Department. The list below only includes only the PGS Group companies that as of 1 January has employees or otherwise are involved in Processing of Personal Data:

Petroleum Geo-Services ASA, Lilleakerveien 4C, 0283 Oslo, NORWAY, attn. Daphne Bjerke, phone +47 67 51 42 87

PGS EM Ltd, C/CMS Cameron McKenna LLP, Saltire Court, 20 Castle Terrace, Edinburgh, EH1 2EN, SCOTLAND, attn. c/o PGS Geophysical AS, Lilleakerveien 4C, 0283 Oslo, NORWAY attn. Daphne Bjerke, phone +47 67 51 42 87

PGS Reservoir Ltd, 4 The Heights, Brooklands, Weybridge, Surrey, KT13 0NY, the UNITED KINGDOM, c/o PGS Geophysical AS, Lilleakerveien 4C, 0283 Oslo, NORWAY attn. Daphne Bjerke, phone +47 67 51 42 87

PGS Pension Trustee Ltd, 4 The Heights, Brooklands, Weybridge, Surrey, KT13 0NY, the UNITED KINGDOM, c/o PGS Geophysical AS, Lilleakerveien 4C, 0283 Oslo, NORWAY attn. Daphne Bjerke, phone +47 67 51 42 87

PGS Geophysical (Angola) Ltd, 4 The Heights, Brooklands, Weybridge, Surrey, KT13 0NY, the UNITED KINGDOM, c/o business address House 29, Rua Maria Antunes, Luanda, ANGOLA, c/o PGS Geophysical AS, Lilleakerveien 4C, 0283 Oslo, NORWAY attn. Daphne Bjerke, phone +47 67 51 42 87

PGS Marine Services (Isle of Man) Ltd., 12-14 Finch Road, Douglas IM1 2PT, ISLE OF MAN, c/o PGS Geophysical AS, Lilleakerveien 4C, 0283 Oslo, NORWAY attn. Daphne Bjerke, phone +47 67 51 42 87

PGS Data Processing Middle East SAE, Block B-1, Road 14, Public Free Zone, Nasr City, Cairo, EGYPT, c/o PGS Geophysical AS, Lilleakerveien 4C, 0283 Oslo, NORWAY attn. Daphne Bjerke, phone +47 67 51 42 87

PGS Egypt for Petroleum Services L.L.C. 39, Road 83 P O Box 114, 11431 Maadi, Cairo, EGYPT, c/o PGS Geophysical AS, Lilleakerveien 4C, 0283 Oslo, NORWAY attn. Daphne Bjerke, phone +47 67 51 42 87

PGS Geophysical Nigeria Limited, 15, Eletu Ogabi Street, Victoria Island, Lagos, NIGERIA, c/o PGS Geophysical AS, Lilleakerveien 4C, 0283 Oslo, NORWAY attn. Daphne Bjerke, phone +47 67 51 42 87

P.G.S Imaging S.A. de C.V, Av. Paseo Tabasco No. 1406 Piso 3, Torre Plaza Atenas, Col. Oropeza C.P. 86030, Villahermosa, Tabasco, MEXICO, Main: +52 (993) 310-3939, Fax: +52 (993) 310-3938, c/o Petroleum Geo-Services Inc., West Memorial Place I, 15375 Memorial Drive, Suite 100, Houston, TX 77079, USA, attn.: Silvia Martins, phone: +1 281 509 8158

PGS Investigacao Petrolifera Ltda, Rua Victor Civita, 77, Bloco 1, Edifício. 6.2, 4º andar, Rio Office Park – Jacarepagua, 22775-044 Rio de Janeiro – RJ, BRAZIL, c/o Petroleum Geo-Services Inc, c/o Petroleum Geo-Services Inc., West Memorial Place I, 15375 Memorial Drive, Suite 100, Houston, TX 77079, USA, attn.: Silvia Martins, phone: +1 281 509 8158

PGS Suporte Logístico e Serviços Ltda, Rua Victor Civita, 77, Bloco 1, Edifício. 6.2, 4º andar, Rio Office Park – Jacarepagua, 22775-044 Rio de Janeiro – RJ, BRAZIL, c/o Petroleum Geo-Services Inc., West Memorial Place I, 15375 Memorial Drive, Suite 100, Houston, TX 77079, USA, attn.: Silvia Martins, phone: +1 281 509 8158

Petroleum Geo-Services Exploration (M) Sdn. Bhd , Menara Dion, Level 11, 27 Jalan Sultan Ismail
50250 Kuala Lumpur, MALAYSIA, c/o PGS Data Processing & Technology Sdn Bhd., Ground Level (Right Wing), Quill Building 3, 3501 Jalan Teknokrat 5, 63000 Cyberjaya, Selangor, MALAYSIA, attn. Evelyn Seow, phone: +603 2175 3741

Petroleum Geo-Services Asia Pacific Pte Ltd., Fusionopolis Place, #03-20, Galaxis (West Lobby)
SINGAPORE 138522, c/o PGS Data Processing & Technology Sdn Bhd., Ground Level (Right Wing), Quill Building 3, 3501 Jalan Teknokrat 5, 63000 Cyberjaya, Selangor, MALAYSIA, attn. Evelyn Seow, phone: +603 2175 3741

PGS Australia Pty Ltd, Level 4, IBM Centre, 1060 Hay Street, West Perth 6005, AUSTRALIA, c/o PGS Data Processing & Technology Sdn Bhd., Ground Level (Right Wing), Quill Building 3, 3501 Jalan Teknokrat 5, 63000 Cyberjaya, Selangor, MALAYSIA, attn. Evelyn Seow, phone: +603 2175 3741

PGS Japan K.K., 5th Floor, UD Hibiya Building, 1-1-2 Uchisaiwaicho, Chiyoda-ku, Tokyo 100-0011
JAPAN, c/o PGS Data Processing & Technology Sdn Bhd., Ground Level (Right Wing), Quill Building 3, 3501 Jalan Teknokrat 5, 63000 Cyberjaya, Selangor, MALAYSIA, attn. Evelyn Seow, phone: +603 2175 3741

As stated in the Policy, each PGS Group company has an obligation to conduct its operations and Processing of Personal Data in accordance with the BCR's, see Section 4 below.

3. DATA PROTECTION OFFICER AND REPRESENTATIVES

3.1 Global Data Protection Officer and the GDPR working group

The Global Data Protection Officer is the overall responsible for coordinating the PGS Group's Processing of Personal Data. The Global Data Protection Officer for the Main Controller is:

Mrs. Daphne Bjerke
c/o PGS Geophysical AS
Lilleakerveien 4C, 0283 Oslo
Norway

In addition to Mrs. Daphne Bjerke, the PGS Group also has appointed four Regional/Operations Data Protection Representatives as further set out in Section 3.2 below.

The Global Data Protection Officer shall have the responsibility to:

(a) have expert knowledge of the GDPR and Personal Data practices;
(b) inform and advise each Controller, Processor and employee who carry out Processing of their obligations under the GDPR, the Policy and the BCR's and all employees to whom the PGS Group is processing Personal Data;
(c) monitor compliance by each Controller and Processor of the GDPR, the Policy and the BCR's together with the PGS Compliance group;
(d) assign responsibilities in relation hereto;
(e) have a complete overview of the Processing of Personal Data in the PGS Group and to set up protocols of all Processing activities, and shall keep an updated list of External Processors and related Data Processing Agreements;
(f) procure the awareness-raising and training of the PGS Group staff involved in Processing of Personal Data;
(g) maintain an overview of all Personal Data and governing documents in the PGS Group related thereto;
(h) conduct self-assessments and certify compliance for the PGS Group with the GDPR, the Policy and the BCR's;
(i) provide advice for and conduct with the PGS Compliance group the Data Protection Impact Assessment and monitor its performance;
(j) cooperate with the supervisory authority and act as the PGS Group's contact point thereto;
(k) be a contact point for all questions concerning the PGS Group's Processing of Personal Data and be the advisor for any complaints by the Data Subjects to the PGS Compliance Hotline; and
(l) keep an updated register of detected or reported deviations from the Policy containing the date of deviation, description of the deviation, the source of the reporting, department/system, seriousness, status of the incident and responsible person for following up within time limits for implementing any corrective measures; and
(m) oversee regular supply chain reviews and audits of External Processors and to monitor their compliance with the provisions of the GDPR and the terms of the Data Processing Agreements.

3.2 Regional/Operations Data Protection Representatives

The PGS Group has also appointed a Regional/Operations Data Protection Representative. These are:

North and South America Silvia Martins c/o Petroleum Geo-Services, Inc. West Memorial Place I, 15375 Memorial Drive, Suite 100, Houston, TX 77079 USA	**Asia and the Pacific** Evelyn Seow c/o Petroleum Geo-Services Exploration (M) Sdn. Bhd. Menara Dion, Level 11, 27 Jalan Sultan Ismail, 50250 Kuala Lumpur, MALAYSIA

Europe, Africa and the Middle East Stein Erik Steira c/o PGS Geophysical AS Lilleakervn. 4C 0283 Oslo, Norway	**Operations (Offshore)** Mark Jack Smith c/o PGS Geophysical AS Lilleakervn. 4C 0283 Oslo, Norway

The main tasks of the Regional Data Protection Representatives are to coordinate, supervise and monitor compliance with the GDPR, the Policy and the BCR's for Processing within their own region and operation and act as the regional contact point to the Global Data Protection Officer.

4. THE CONTROLLERS

According to the organizational and operational structure of the PGS Group, its operations are divided globally between four regional operational main offices located in Oslo, London, Kuala Lumpur and Houston, as well as worldwide offshore, respectively. As such, the main operational company within each region is also the company determining the purposes and means of the Processing of Personal Data within each region. This implies that the main operational company within each region is a Controller for its region. The Controllers shall comply with the provisions of the Policy and the BCR's. The Controllers shall be responsible for the Processing conducted by itself and the various processors set out below (each a "**Processor**").

Region:	**Europe, Africa and the Middle East**	**North and South America**	**Asia and the Pacific**	**Offshore**
Controllers:	**PGS Geophysical AS**	**Petroleum Geo-Services. Inc.**	**PGS Data Processing & Technology Sdn Bhd**	**PGS Geophysical AS**
Determining the purpose and measures for Processing done by:	Itself (Oslo activities)	Itself (Houston activities)	Itself (Kuala Lumpur activities)	Itself (Offshore activities)
	Petroleum Geo-Services ASA	P.G.S Imaging S.A. de C.V	Petroleum Geo-Services Exploration (M) Sdn. Bhd	PGS Marine Services (Isle of Man) Ltd
	PGS Exploration (UK) Ltd	PGS Investigacao Petrolifera Ltda	Petroleum Geo-Services Asia Pacific Pte Ltd	Petroleum Geo-Services. Inc.
	PGS Geophysical Nigeria Limited	PGS Suporte Logístico e Serviços Ltda	PGS Japan K.K.	Petroleum Geo-Services Asia Pacific Pte Ltd
	PGS EM Ltd		PGS Australia Pty Ltd	
	PGS Reservoir Ltd			

	PGS Pension Trustee Ltd			
	PGS Geophysical (Angola) Ltd			
	PGS Marine Services (Isle of Man) Ltd			
	PGS Data Processing Middle East SAE			
	PGS Egypt for Petroleum Services L.L.C.			

Each Controller shall have the overall responsibility for the implementation of the Policy and the BCR's for and on behalf of itself and the Processors outlined in the above table, and each Controller shall be liable for violation of the GDPR, the Policy and the BCR's, and Personal Data breaches for which the Controller and its Processors are liable.

5. THE MAIN PROCESSOR

PGS Geophysical AS is authorized to operate and deliver certain IT services, HR and administration services to the other Controllers and Processors. Such service provisions are governed by the Policy.

This has the implication that Personal Data is processed and transferred both from PGS Group companies located in the EEA to Third Countries, and from PGS Group companies located in Third Countries to the EEA. An overview of the Personal Data flows follows from Section 7.2.

As such, PGS Geophysical is the main Processor within the PGS Group (the "**Main Processor**"), and has entered into a written data processing agreement (the "**Data Processing Agreement**") with the other PGS Group companies, covering the Processing made by the Main Processor on behalf of such Controllers and/or Processors. All Processing done by the Main Processor shall be done in accordance with the PGS Personal Data Protection Policy. The Main Processor shall comply with the provisions of Section 17 of the BCR's.

6. EXTERNAL PROCESSORS

The Main Processor and the Controllers require from time to time the procurement of services from external suppliers which entail Processing of Personal Data on behalf of the Controllers, the Main Processor or the Processors within the PGS Group ("**External Processors**").

The companies within the PGS Group shall use only External Processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that Processing will meet the requirements of the GDPR and ensure the protection of the rights of the Data Subjects. All Processing done by such External Processors shall always be governed by a written data processing

agreement (the "**External Data Processing Agreement**"). According to the GDPR Article 28, such agreement shall *inter alia* stipulate that the External Processors shall:

a) Process the Personal Data only on instructions from the Controller or the Main Processor;
b) guarantee to have implemented appropriate technical and organizational measures to protect the Personal Data against (i) accidental or unlawful destruction or loss, (ii) alteration, (iii) unauthorized disclosure or access, or (iv) any other form of unlawful Processing;
c) ensure the rights of the Data Subjects;
d) not engage another data processor without the prior written authorization of the Controller or the Main Processor;
e) assist the Controller for the fulfilment under its obligations in the GDPR;
f) delete or return all Personal Data at the expiry or termination of the Data Processing Agreement; and
g) give the Controller and the Main Processor audit rights to inspect the External Processor's compliance with the GDPR and the terms of the Data Processing Agreement.

The Global Data Protection Officers shall keep a list of all External Processors that the PGS Group has engaged, together with the applicable External Data Processing Agreement. The External Processor shall maintain a record of processing activities for the Main Controller, in accordance with the GDPR Article 30.

In the event the Main Processor or a Controller within EU/EEA uses an External Processor placed in a Third Country and involving transfer of Personal Data to a Third Country, the Main Processor or Controller shall ensure that the legal grounds for the transfer of Personal Data is in place. Such a legal ground could for example be an executed version of the EU Standard Clauses for transfer of Personal Data from EU/EEA Controllers to Non-EU/EEA Processors.

The PGS Group has routines for appointing third party vendors and Data Processing Agreements in its governance management system.

7. THE NATURE OF THE PERSONAL DATA AND PROCESSING

7.1 Record of Processing Activities

According to the GDPR Article 30, all Controllers shall maintain a record of processing activities under its responsibility. PGS has an excel file showing the mapping results (the **"Record of Processing Activities**"), and contains an overview of:

a) Personal Data categories and type;
b) the purpose of Processing;
c) type of Data Subjects;
d) Personal Data's origin;

e) the legal basis for Processing within the EEA;
f) the identity of the Controller and any Processor;
g) who has access to the Personal Data;
h) the systems used for Processing;
i) the data flow and transfer to Third Countries; and
j) Retention and storage period.

The PGS Group has also made a notification form that is reflected the Notification of Processing of Personal Data Form (the "**Notification Form**"). The purpose of the Notification form is to assess the data flow and controls within each system that contains Personal Data in PGS Group.

The Record of Processing Activities and Notification Form are reviewed and updated on an annual basis, cf. Appendices 2 and 3.

8. DATA PROTECTION PRINCIPLES

The PGS Group adheres to and complies with the general data protection principles as set forth in the GDPR for Processing of Personal Data. It is the responsibility of each Controller to comply with the principles hereof. Any questions relating to these principles can be addressed to the Global Data Protection Officer or the Regional Data Protection Representatives.

8.1 Personal Data Processing Principles

As set out in the GDPR Article 5 and under the BCR's, Personal Data shall within PGS Group be dealt with in the following way:

a) **Lawfulness, fairness and transparency**: Processed lawfully, fairly, and in a transparent manner in relation to the Data Subject, please see Section 8.2 and 8.3 below;
b) **Purpose limitation**: collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes as set out in the Notification Form where the purposes of the Processing is listed;
c) **Minimization**: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, see Section 9.2 below;
d) **Accuracy**: accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that the Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) **Storage limitation**: kept in a form which permits identification of the Data Subjects for no longer than is necessary for the purpose for which the Personal Data are processed; and

f) **Integrity and confidentiality**: Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful Processing and against accidental loss, destruction or damage using appropriate technical or organizational measures.

8.2 The Legal Basis for Processing of Personal Data

As set out in the GDPR Article 6, Processing of Personal Data by the PGS Group shall only be done if:

a) The Data Subject has given its consent to the Processing of its Personal Data for one or more specific purposes;
b) it is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;
c) it is necessary for compliance with a legal obligation to which the Controller is subject too;
d) necessary in order to protect the vital interests of the Data Subject or another natural person;
e) necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; or
f) necessary for the purposes of the legitimate interests pursued by the Controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data.

As set out in Section 7.1, the PGS Group has set out the legal basis for Processing in the Record of Processing Activities and Notification Form.

8.3 The Legal Basis for Processing of Special Categories of Personal Data (Sensitive Personal Data)

As set out in the GDPR Article 8, Processing by the PGS Group of special categories of Personal Data revealing racial, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data, biometric data, data concerning health or sex life or sexual orientation, and data relating to criminal convictions and offences ("**Sensitive Personal Data**") shall only be done if:

a) The Data Subject has given its explicit consent to the Processing of its Sensitive Personal Data for one or more specified purposes;
b) it is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or the Data Subject in the field of employment, social security and social protection laws in so far as it is authorized by the EU or EU/EEA Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and interests of the Data Subject;

c) it is necessary in order to protect the vital interests of the Data Subject or another natural person where the Data Subject is physically or legally incapable of giving consent;
d) if carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for profit body with a political, philosophical, religious or trade union aim and on condition that the Processing relates solely to the members or former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside of that body without the consent of the Data Subject;
e) it relates to Personal Data which are manifestly made public by the Data Subject;
f) is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
g) necessary for reasons of substantial public interest, on the basis of EU or EU/EEA Member State Law which shall be proportionate to the aim pursued, respect the essence of the right to the data protection and provide suitable and specific measures to safeguard the fundamental rights and interests of the Data Subject;
h) necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or EU/EEA Member State Law or pursuant to a contract with a health professional and subject to the conditions and safeguards referred to in the GDPR Article 8 paragraph 3;
i) 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 services on the basis of EU or EU/EEA Member State Law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy; or
j) is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the GDPR Article 89 (1) based on EU or EU/EEA Member State Law which shall be proportionate to the aim pursued, respect the essence of the right to Data Protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the Data Subject.

9. ORGANIZATIONAL AND TECHNICAL MEASURES

9.1 Lawful, fair, transparent and purpose limitation

Each Controller shall procure the implementation of measures to ensure that the Personal Data is Processed lawfully, fairly, and in a transparent manner in relation to the Data Subject, and is collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. The Data Subjects' rights are outlined in Section 10 hereto.

9.2 Minimization

Each Controller shall procure the implementation of measures so that Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

9.3 Access Control

Each Controller shall procure the implementation of measures to ensure that any person or Processor who has access to Personal Data shall not Process these except on instructions from the Controller, unless required to do so by applicable laws. PGS has in its PGS Information Security Policy set out the routines for granting access to systems and Personal Data.

9.4 Confidentiality

Each Controller shall procure the implementation of measures to ensure that all PGS personnel having access to Personal Data shall treat these confidential.

PGS has a Statement of Confidentiality to be used when treating confidential information that sets up confidentiality obligations for PGS Group employees. The PGS Standard Data Processing Agreement Template for External Processors, contains sections concerning confidentiality for all personnel at the External Processors.

9.5 Security and Integrity

Each Controller shall procure that Personal Data is processed in a manner that ensures appropriate security of the Personal Data by using appropriate technical or organizational measures, including protection against unauthorized or unlawful Processing and against accidental loss, alteration, unauthorized disclosure or access, destruction or damage.

Having regard to state of the art measures and their cost of implementing, such measures shall ensure a level of security appropriate to the risks represented by the Processing and the nature of the data to be protected.

PGS has implemented a routine for the Data Protection Impact Assessments to be made according to the GDPR article 35.

9.6 Storage Limitation

Each Controller shall procure the implementation of measures to ensure that Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than it is necessary for the purpose for which the Personal Data are processed.

9.7 Accuracy

Each Controller shall procure the implementation of measures to ensure that Personal Data being Processes is accurate and, where necessary, kept up to date, and shall take every reasonable step to ensure that Personal Data being inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

10. THE RIGHTS OF AND THE INFORMATION TO THE DATA SUBJECTS

10.1 The Rights of the Data Subjects

All Data Subjects over which the PGS Group Processes Personal Data have the following rights, and we also refer to the Policy for further information:

(a) **Withdrawal of consent**: Where the Processing in the PGS Group is based on consent, the consent shall be given in a lawful way and the Controller shall be able to demonstrate that the Data Subject has consented to Processing of his or her Personal Data. To the extent the Controller relies on a consent given by the Data Subject for Processing, the Data Subjects shall have the right to withdraw any such consent given for PGS' processing of Personal Data at any time, cf. the GDPR Article 7.3;

(b) **Concise, transparent, intelligible and easy accessible information**: To be provided with any information relating to its Personal Data in a concise, transparent, intelligible and easy accessible manner, see (c) below. Any requested information shall be given by the Controller without undue delay, and as a general rule no later than one (1) month from the Controller's receipt of the request. cf. the GDPR Article 12;

(c) **Information about Data collected and to be collected**: To receive information about (a) the identity and contact details of the Controller and its representative, as well as contact details to the Global Data Protection Officer, (b), the purposes of Processing of the Personal Data and its legal basis; (c) the recipients or categories of recipients of the Personal Data; and (d) any intentions about transferring Personal Data to a Third Country and the appropriate safeguards and the means by which to obtain a copy of them or where they have been made available, cf. the GDPR Article 13.1.

Information shall also be given about; (a) the period for which the Personal Data will be stored; (b) the right to request access and rectify errors, and to the extent of consent being, given the right to erase, restrict, and transfer Personal Data and withdraw consent; (c) the right to lodge a complaint with the supervisory authority; (d) whether the Personal Data is collected under a statutory or

contractual requirement, or as a requirement to entering 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, cf. the GDPR Article 13.2.

To the extent Personal Data has not been received from the Data Subjects, the Controller shall give the above information on the latest date of: (a) within a reasonable period and no later than one month from the date of collecting the Data; (b) if the Personal Data is to be used in communication with the Data Subject, the time of the first communication to that Data Subject; and (c) if disclosure to another recipient is envisaged, when the Personal Data are first disclosed, cf. the GDPR Article 14;

(d) **Right of Access**: To receive confirmation from the Controller about (i) whether its Personal Data is Processed; (ii) the purpose of the Processing; (iii) the categories of Personal Data concerned; (iv) the recipient or categories of recipients to whom the Personal Data has been or will be disclosed, in particular in Third Countries; (v) the envisaged period of storage; (vi) the right to rectify errors, and to the extent of consent is given for Processing, given the right to erase, restrict and transfer Personal Data and withdraw any consent; (vii) the right to lodge a complaint to the supervisory authority; (viii) if the Personal Data are not collected from the Data Subject, and any available information as to their source; (ix) upon transfer to Third Countries, the appropriate safeguards taken by the Controller, and (x) the right to free of charge receive a copy of its Personal Data processed, cf. the GDPR Article 15;

(e) **Right of Rectification**: To require without undue delay the rectification of any inaccurate Personal Data or complete incomplete Personal Data pertaining to the data subject, cf. the GDPR Article 16;

(f) **Right of Erasure**: To without undue delay require that the Controller erase Personal Data that; (i) are no longer necessary to Process in relation to the purposes for which they were collected or Processed; (ii) has its consent withdrawn and no other legal grounds for Processing exists; (iii) the Data Subject lawfully objects to the Processing of, cf. item (i) below and there are no overriding legitimate grounds for the Processing, or is used for marketing purposes; (iv) have been unlawfully Processed; (v) must be erased for compliance with a legal obligations in EU or EU/EEA Member State law to the which the Controller is subject, and (vi) have been collected in relation to the offer of information society services to children, cf. the GDPR Article 17;

(g) **Right to Restrictions of Processing**: To obtain from Controller restrictions of Processing if; (i) the accuracy of Personal Data is contested by the Data Subject, for a period enabling the Controller to verify its accuracy; (ii) the Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restrictions of their use instead; (iii) the Controller no longer needs the Personal Data for the purposes of the Processing but they are required by the Data Subject for the establishment of, exercise or defense of legal claims; or (iv) the Data Subject has objected to Processing, cf. item (i) below and there are no overriding legitimate grounds for the Processing, or

is used for marketing purposes pending verification on whether the legitimacy of the ground of the Controller to Process override those of the Data Subject, cf. the GDPR Article 18;

(h) **Right to Personal Data Portability**: To receive its Personal Data in a structured, commonly used and machine-readable format and have the right to transfer this to another controller without hindrance from the Controller where: (i) Personal Data is Processed based on consent or in relation to a contract held with the Data Subject; or (ii) the Processing is carried out by automated means, cf. the GDPR Article 20;

(i) **Right to Object**: To on particular grounds object to Processing if the Personal Data is Processed: (i) on the grounds of Controller carrying out a task in public interest or being necessary for Controller or a third party pursuing legitimate interests, unless Controller demonstrates compelling legitimate ground for Processing which override the rights and freedoms of the Data Subject, or for the establishment, exercise or defense of legal claims; or (ii) for marketing purposes, cf. the GDPR Article 21;

(j) **Rights re Automated Individual Decision-Making and Profiling**: To avoid being the subject to a decision based on automated Processing, including profiling, which produces legal effects for, or similarly significantly affects, the Data Subject, unless: (i) it is necessary for entering into, or performing a contract between Controller and the Data Subject; (ii) is authorized by applicable EU or EEA Member State law; or (iii) it is based on Data Subject's consent, cf. the GDPR Article 22;

(k) **Right to Information of Breach**: As a main rule, without undue delay to be notified by the relevant Controller upon a Personal Data breach that is likely to result in a high risk to the rights and freedoms of the Data Subject. The communication shall describe in clear language the nature of the breach and contain information on: (i) the name of and contact details of the Global Data Protection Officer; (ii) the likely consequences of the Personal Data breach; and (iii) what measures are taken or proposed to address the breach and which appropriate measures are taken to mitigate its possible adverse effects, cf. the GDPR Article 34;

(l) **Right to lodge a Complaint**: To lodge a complaint with the competent supervisory authority and before the competent courts of the EU/EEA Member State for alleged Personal Data breaches or GDPR infringement, cf. the GDPR Articles 77 and 79. The competent supervisory authority is, in particular in the EU/EEA Members States, the authority in which the Data Subject has its habitual residence, place or work or place of the alleged infringement. The competent court is the place where the Controller or Processors has an establishment. The Data Subject may also lodge a complaint to the PGS Compliance Hotline, and will also be referred to the Personal Data Protection site for more information;

(m) **Right to Compensation**: To be entitled to compensation from the relevant Controller for damage caused by its Processing that infringe the GDPR for which it is responsible, or from the Processor if

the Processor has not complied with its obligations under the GDPR or where it has acted outside of contrary to lawful instructions by the Controller; and

(n) **Right to be Represented**: To be represented by a not-for-profit body, organization cf. the GDPR Article 82. The competent court is the place where the Controller or Processors has an establishment or association to promote its rights under the GDPR Articles 77, 78, 79 and 82, cf. the GDPR Article 80.

10.2 Information

The Data Subjects being PGS Group employees are informed of its rights as follows:

a) The Policy and the BCR's are made available to all PGS Group employees through the PGS intranet and available in the PGS governance document handling system GMS;
b) The PGS Employee Handbooks available on the PGS intranet;
c) The Data Subjects general rights are also outlined on the PGS intranet; and
d) Information articles will be published on the PGS intranet.

The Data Subjects being non-PGS employees are informed as follows:

a) The BCR's are made available to all external Data Subjects on www.pgs.com,
b) The Data Privacy Statement for online activities and the PGS Code of Conduct is available on www.pgs.com;
c) The Data Subjects general rights are outlined in our global recruitment system for candidate employees where these Data Subjects leave Personal Data with PGS; and
d) The Data Subject's general rights are outlined by email to the Data Subjects in the Customer Relations Management system.

11. TRANSFERS OF PERSONAL DATA

As shown in Section 7.2 above, the organizational and operational structure of the PGS Group will entail that Personal Data is transferred between entities both located inside of the EU/EEA and outside of the EU/EEA. In addition to applicable local rules for Processing of Personal Data which shall always be considered prior to transfer, the following rules shall apply for transfers:

11.1 Transfer to Controllers and Processors within the PGS Group

11.1.1 From Controller to Controller

Transfers of Personal Data between Controllers that are bound by the Policy and the BCR's may take place, provided that the provisions in Sections 8, 9 and 10 are complied with both by the sending Controller and the receiving Controller, and that appropriate security measures are implemented to protect the Personal Data during transfer and further Processing by the receiving Controller.

11.1.2 From Controller to Processor

Transfers of Personal Data from a Controller to a Processor that are bound by the Policy and the BCR's may take place provided that (i) the Processor provides sufficient guarantees that it has implemented appropriate technical security and organizational measures governing the Processing to be performed as outlined in Section 10; and (ii) the Processing is governed by the Data Processing Agreement inter alias stipulating that the Processor shall act only on the instructions from the Controller.

11.2 Transfer to Controllers outside of the PGS Group

11.2.1 Transfer to a Controller within the EEA

Transfer of Personal Data from a Controller established in the EU/EEA to another Controller established within the EU/EEA may take place provided that the requirements contained in Sections 8 and 9 are fulfilled both on part of the sending Controller and the receiving Controller, and that the requirements contained in Section 10 on appropriate security measures are implemented to protect the Personal Data during transfer and further Processing by the receiving Controller.

11.2.2 Transfer to a Controller outside of the EEA

Transfer of Personal Data from an internal Controller established in the EU/EEA to another external Controller not established within the EU/EEA is prohibited, unless:

a) The receiving Controller is established in a country which the EU Commission has considered having an adequate level of Personal Data protection, and the Processing is compliant with Sections 8, 9 and 10 hereof; or
b) the transfer is governed by the EU standard contractual clauses adopted by (i) the EU Commission for Controller to Controller transfer of Personal Data pursuant to the GDPR, Article 93(2); or (ii) a supervisory authority and approved by the EU Commission pursuant to the GDPR, Article 93(2); or
c) one of the derogations in the GDPR, Article 49 applies, and the Processing is compliant with Sections 8, 9 and 10 hereof.

11.3 Transfer to External Processors

11.3.1 To External Processors established within the EEA

Transfer of Personal Data to an External Processor established within the EU/EEA may take place provided that;

a) the provisions in Sections 8, 9 and 10 are complied with both by the sending Controller and the receiving Processor, and that appropriate security measures are implemented to protect the Personal Data during transfer and further Processing by the receiving Controller; and
b) the Processing is governed by a Data Processing Agreement.

11.3.2 To External Processors established outside of the EEA

Transfer of Personal Data to an External Processor not established within the EU/EEA is prohibited, unless:

a) The External Processor is established in a country which the EU Commission has considered having an adequate level of Personal Data protection, the Processing is compliant with Sections 8, 9 and 10 hereof, and the Processing is governed by an External Processing Agreement; or
b) the transfer is governed by the EU standard contractual clauses adopted by (i) the EU Commission for Controller to Controller transfer of Personal Data pursuant to the GDPR, Article 93(2); or (ii) a supervisory authority and approved by the EU Commission pursuant to the GDPR, Article 93(2); and the Processing is governed by an Data Processing Agreement; or
c) one of the derogations in the GDPR, Article 49 applies, and the Processing is compliant with Sections 8, 9 and 10 hereof.

12. MONITORING, AUDIT AND VERIFICATION OF COMPLIANCE

12.1 Mapping of Personal Data

The Global Data Protection Officer shall on behalf of the Controller implement routines for mapping Personal Data in order to ensure that PGS at any given time is in compliance with the Policy and the BCR's. Such routines shall be subject to annual review in accordance with the PGS Data Protection Policy, and shall be designed to detect any changes made in the PGS Group's Processing of Personal Data. The expected results from compliance with the routines are that PGS shall maintain a system that facilitates compliance with the Policy and the BCR's.

12.2 Mapping of Processing Risks and Data Protection Impact Assessment

The information security risk shall be assessed by using the principles and tools for risk assessments therein.

Each time where a type of Processing is likely to result in a high risk to the rights and freedoms of a Data Subject, each Controller shall prior to the Processing carry out a Data Protection Impact Assessment. Such assessment shall in particular be required in the case of:

(a) A systematic and extensive evaluation of personal aspects relating to Data Subjects which is based on automated processing, including profiling, and on which decisions are based that produce legal effects or similarly significantly affect, the Data Subjects;
(b) Processing on large scale of Sensitive Personal Data; and
(c) A systematic monitoring of a publicly accessible area on large scale.

12.3 Self-Assessments

Each Controller is responsible for monitoring the PGS Group's compliance with the Policy and the BCR's in each region. The Global Data Protection Officer and each Regional Data Protection Officer shall on behalf of the Controllers annually conduct a self-assessment of the Processing activities conducted in its own region. The Global Data Protection Officer is responsible for following up that the planned activities is conducted. The purpose of this self-assessment is to self-certify compliance with the Policy and the BCR's in the Processing activities in each region. This shall be made in accordance with the PGS Self-Assessment Procedure and the Policy. The results of the self-assessment shall be sent to/kept by the Global Data Protection Officer for follow up. The results hereof shall also be available upon request to the supervisory authority.

The self-assessment shall outline any corrective actions proposed to be implemented to protect the rights of the Data Subjects, and a time line for implementing the corrective actions. The Global Data Protection Officer shall follow and monitor that the corrective actions are being implemented.

12.4 Audits

The PGS Internal Audit Department shall include compliance with personal data protection principles and the BCR's, when relevant in the scope of the PGS Group's annual yearly audit plan. In addition, our external auditors may perform GDPR compliance audits. The results of the audit shall also be reported to the Audit Committee pertaining of the Board of Directors in Petroleum Geo-Services ASA, and shall be available upon request to the supervisory authority.

The audit report shall outline the corrective actions proposed to be implemented to protect the rights of the Data Subject, and a time line for implementing the corrective actions. The PGS Internal Audit Department shall follow and monitor that the corrective actions are being implemented.

12.5 Annual Certification

Based on the results of the self-assessment and the Compliance Review Report, the Global Data Protection Officer shall annually certify its compliance with the Policy and the BCR's.

13. NOTIFICATION OF PERSONAL DATA BREACH

Each Controller shall without undue delay, no later than 24 hours from having become aware of the breach, report such data breach to PGS Geophysical /the Global Data Protection Officer via the PGS Compliance Hotline or otherwise. The Global Data Protection Officer and the PGS Compliance department will, as appropriate, notify the competent supervisory authority within 72 hours from having become aware of the breach.

The notice to the supervisory authority shall at least contain: (a) a description of the breach, and where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number Personal Data records concerned; (b) the name of and contact details of the Global Data Protection Officer in PGS; (c) the likely consequences of the Personal Data breach; and (d) what measures are taken or proposed to address the breach and which appropriate measures are taken to mitigate its possible adverse effects.

Each Controller shall document any Personal Data breaches, comprising the facts relating to the Personal Data breach, its effects and the remedial action taken.

14. COOPERATION WITH THE SUPERVISORY AUTHORITY

The Global Data Protection Officer is mandated by all Controllers to cooperate with the supervisory authority to ensure compliance with the GDPR, the Policy and the BCR's. Such cooperation shall inter alia be to apply for recommendations and advice from the supervisory authority, and respond to requests from the authority regarding the Policy and the BCR's, and cooperate with the supervisory authority in any audits undertaken by them. The Global Data Protection Officer shall be the main contact point for any supervisory authority. The Global Data Protection Officer will upon request make available to the supervisory authority the results of any monitoring, audit and verifications measures set out in Section 12 above.

15. THE COMPLAINT PROCEDURE

As outlined in Section 10.1 (l) above, any Data Subject over who the PGS Group is Processing its Personal Data can complain about alleged Personal Data breaches by reporting this on the PGS Compliance Hotline as further set out on www.pgs.com.

16. LIABILITY

Any Data Subject will be entitled to the remedies for data breach as set out in the GDPR Chapter VIII. Each Controller is liable under the GDPR for breach of the GDPR occurring within its region and giving rise to damage for which it is responsible. However, PGS Geophysical AS accepts joint and several liability for breaches of the Policy and the BCR's by any other Controller or Processor within the PGS Group not established within the EEA, and shall only be exempt from liability in whole or in part if it proves that such Controller or Processor is not responsible for the event giving rise to the damage. In any case of legal action against any Controller or Processor within the PGS Group, the PGS Group's General Counsel shall be contacted. The rights to compensation and liability as outlined under the GDPR Article 82, shall only apply to Data Subjects placed within the EEA.

17. TRAINING

PGS has prepared a training program for Personal Data protection for relevant PGS Group personnel. The main purposes of this training program is (i) to ensure implementation of an appropriate level of compliance with the personal data protection regulation and the BCR's within the PGS Group, both inside and outside of the EU/EEA. The main purpose of the training program is to familiarize all personnel with the personal data protection regulation and the BCR's, and (ii) make the personal data protection regulation and the BCR's well understood and effectively applied within the PGS Group.

The training program includes:

- A GDPR Workshop/course to familiarize PGS Group personnel with the Personal Data protection regulation and their role and responsibilities. The agenda for the workshop is:
    - Background for the GDPR
    - Objective and requirements of the GDPR
    - Individual responsibilities

The following PGS Group personnel shall receive training:

- EXT and top management
- Global IT Departments
- Global and Regional HR Departments
- Local Office Administration Departments
- System Application Owners

18. REPORTING ON LEGAL REQUIREMENTS IN THIRD COUNTRIES

The Policy and the BCR's are based on the GDPR where their main purpose is to ensure compliance therewith. If any element of the Policy and the BCR's are in conflict with relevant and mandatory local laws and regulations, the latter shall prevail.

Upon any PGS Group employee, Controller or Processor suspecting that the applicable legislation prevents the fulfillment of the provisions of the Policy and the BCR's, they shall communicate such to the Global Data Protection Officer. The Global Data Protection Officer will in cooperation with PGS Legal Department take necessary steps to assess whether any changes to the Policy and the BCR's needs to be made.

Furthermore, in the event PGS detects any legal requirements in Third Countries which are likely to have a substantial adverse effect on the guarantees provided under the BCR's, these will be notified to the supervisory authority.

19. CHANGES TO THE BINDING CORPORATE RULES

PGS may make updates and revisions to the Policy and the BCR's if required due to organizational changes, amendments in applicable legislation, or for other reasons. Any such change shall be reflected in other governing documents within PGS as appropriate. The current and updated version shall always be available for the PGS Group and its employees.

The Global Data Protection Officer will together with the Legal Department keep an updated list of the changes having been made to the Policy and the BCR's. No transfer of Personal Data to Third Countries based on the BCR's shall be made by the exporter until any new importer is effectively bound by the Policy and the principles of the BCR's.

Any changes to the Policy and the BCR's and the PGS Group companies involved shall be recorded by the Global Data Protection Officer. Any substantial changes to the PGS Data Protection Policy, the BCR's and the involved PGS Group companies shall be reported to the supervisory authority on an annual basis. Such report shall include a brief explanation of the reasons for the changes.