Personal Data Protection Manual - Binding Corporate Rules

This Personal Data Protection Manual and Binding Corporate Rules is part of PGS ASA and its subsidiaries ("PGS") overall compliance program for managing and protecting Personal Data processed in relation to its operations.

Table of Contents

1. INTRODUCTION

1.1 Commitment and Purpose

The purpose of this Personal Data Protection Manual and Binding Corporate Rules (the "Manual") is for PGS Group to:

- comply with the General Data Protection Regulation (GDPR) and Laws related to protection of Personal Data;
- establish adequate safeguards for the transfer of Personal Data from countries within the European Union ("EU") and the European Economic Area (the "EEA") to international organizations and countries that are not considered to provide an adequate level of protection ("Third Countries");
- help ensure the implementation of appropriate technical and organizational measures in PGS Group and be able to demonstrate that Processing of Personal Data within the PGS Group is performed in accordance with the Laws, and
- establish a set of principles and routines that shall ensure effective internal controls for compliance with the Laws regarding the Processing of all Personal Data within the PGS Group.

This Manual is mandated by the Personal Data Protection Standard.

1.2 Legally Binding Manual

This Manual 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 in their capacity as Controllers and Processors;
- obligations to all System Owners and other employees in the PGS Group who are involved in Processing of Personal Data; and
- subject to Sections 7 and 15 below, only give rights to Data Subjects in the EU/EEA whose Personal Data is processed by a PGS Group company within the scope of the GDPR including transferred to a PGS Group company outside of the EU/EEA. These rights do not extend to elements of the Manual relating to internal implementation mechanisms within the PGS Group.

This Manual is binding upon all companies and entities in the PGS Group, including its Controllers and the Processors, through the execution of a binding contract between them, and as being part of the governing management system in the PGS Group ("UniSea").

1.3 Changes to this Manual

The DPO may make updates and revisions to this Manual 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 in UniSea. The DPO will together with the PGS General Counsel keep an updated list of the changes having been made to the Manual.

No transfer of Personal Data to Third Countries based on this Manual shall be made by the exporter until any new importer is effectively bound by the Manual. Any changes to the Manual and the PGS Group companies involved shall be recorded by the DPO and approved by the General Counsel.

Any material changes to the Manual shall be reported to the supervisory authority on an annual basis with a brief explanation of the reasons justifying the update. Changes that affect the level of protection offered by this Manual or otherwise significantly affect the Manual shall be promptly communicated to the supervisory authority.

1.4 Reporting on Deviating Legal Requirements

This Manual is based on the GDPR where the main purpose is to ensure compliance therewith. If any local laws and regulations require higher protection than what follows from this Manual, the higher protection requirements shall prevail.

Upon any PGS Group employee, Controller or Processor suspecting that applicable legislation prevents the fulfillment of the provisions of this Manual, or has substantial effect on the guarantees provided by this Manual, they shall communicate such to the DPO. This obligation of communicating to the DPO shall not apply if prohibited by a law enforcement authority. The DPO will in cooperation with the General Counsel take necessary steps to assess whether any changes to this Manual need 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 in this Manual, including any legally binding request for disclosure of the Personal Data by a local authority, this will be notified to the supervisory authority. This obligation to notify does not apply if prohibited by the relevant local authority. However, the wholly owned PGS-entity – *PGS Geophysical AS* – shall demonstrably make its best efforts to obtain a waiver from this prohibition. If it is not possible to obtain a waiver, PGS Geophysical AS shall annually provide the supervisory authority with general information on the requests it receives from the local authority. Any transfer of Personal Data by a Controller to a local authority shall not be massive, disproportionate or non-discriminatory beyond what is necessary in a democratic society.

1.5 Cooperation with the Supervisory Authority

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

1.6 Contact with media

All contact with press and media is handled through the appropriate person appointed within the PGS Group to handle press, and no other person shall make any statements of behalf of PGS Group, cf. PGS' Corporate Communications Manual.

1.7 Sanctions upon breach

Violations by any PGS Group employee of the provisions laid out in this Manual and any confidentiality obligations may result in disciplinary measures.

2. OVERVIEW OF THE PGS GROUP

2.1 Overview

PGS Group is involved in marine seismic data acquisition, licensing, imaging, vessel- and technology ownership, and related services and businesses. The PGS Group is headquartered in Oslo where its ultimate parent company PGS ASA is listed on the Oslo Stock Exchange under ticker: OSE:PGS.

The main operational offices in the PGS Group are located in Norway (Oslo); UK (Weybridge); and USA (Houston). In addition, the PGS Group operates vessels for offshore seismic acquisition worldwide.

The PGS Group also has sales and operational offices and data processing centers in the following locations: Norway (Stavanger), Malaysia (Kuala Lumpur), Australia (Perth), Japan (Tokyo), Egypt (Cairo), Brazil (Rio de Janeiro), Angola (Luanda), Nigeria (Lagos), and Ghana (Accra).

2.2 Legal Structure and Contact Details

The PGS Group has a number of subsidiaries placed in various locations around the world, all of which are subject to this Manual. An overview of the PGS Group companies that has employees or otherwise are involved in Processing of Personal Data is set forth in Section 18.

The overview of legal structure of the PGS Group is updated on a routinely basis according to the PGS Group governance policies, and is inter alia available in the latest edition of the PGS Annual Report. For a more recent update the DPO may be contacted.

2.3 The Controllers and Processors within the PGS Group

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, Weybridge (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, however such that the office in Oslo is responsible for Processing in Weybridge. This implies that the main operational company within each region is a Controller for its region, as set forth below: The Controllers shall be responsible for the Processing conducted by itself and the Processors within its region as set forth below:

Region:	**Europe, Africa and the Middle East**	**North and South America**	**Asia-Pacific**	**Offshore**
Controllers:	**PGS Geophysical AS**	**Petroleum Geo-Services. Inc.**	**Petroleum Geo-Services Exploration (M) Sdn. Bhd**	**PGS Geophysical AS**
Processors:	Itself (Oslo based activities) PGS ASA PGS Exploration (UK) Ltd PGS Geophysical Nigeria Limited PGS Ghana Ltd PGS Pension Trustee Ltd PGS Geophysical (Angola) Ltd PGS Data Processing Middle East SAE PGS Egypt for Petroleum Services	Itself (Houston based activities) PGS Suporte Logístico e Serviços Ltda PGS Geophysical AS	Itself (Kuala Lumpur based activities) PGS Data Processing & Technology Sdn Bhd Petroleum Geo-Services Asia Pacific Pte Ltd PGS Japan K.K. PGS Australia Pty Ltd PGS Geophysical AS	Itself (Offshore based activities) Petroleum Geo-Services. Inc. Petroleum Geo-Services Asia Pacific Pte Ltd

2.4 The impact of Brexit

The Brexit transition period ended on 31 December 2020. As part of the new trade deal, the EU has agreed to delay transfer restrictions for up to 6 months (the “bridge”). On 19 February 2021 the European Commission published its draft decisions on the UK’s adequacy under the GDPR and Law Enforcement Directive (LED). If the adequacy decisions are not adopted at the end of the bridge, transfers from the EU/EEA to the UK will need to comply with GDPR transfer restrictions. From a practical perspective for the PGS Group, this will mean that transfers of Personal Data from the EU/EEA to PGS Group entities in the UK will, as per this Manual, be treated as a transfer to a PGS Group Processor located in a Third Country.

3. RESPONSIBILITIES

3.1 Controllers

The entities and organizations that determine the purpose and means of the Processing of Personal Data are Controllers pursuant to the GDPR. Section 2.3 outlines which entitles within the PGS Group that are controllers (the “Controllers”). Each Controller shall have the overall responsibility for the implementation of the Manual, and shall ensure that Processing is done in compliance with the Laws and this Manual by itself and its Processors outlined in the table in Section 2.3 above. Moreover, each Controller shall be responsible for the Processing conducted by itself and its Processors within its region

as set forth above in Section 2.3 and the implementing the principles laid down in Section 5 below for such Processing.

3.2 Processors and Main Processor

The entities and organizations that are responsible for Processing the Personal Data on behalf of the Controllers are Processors pursuant to the GDPR. Section 2.3 above outlines which entitles within the PGS Group that are the Processors (the "Processors"). The Norwegian main operational entity within the PGS Group – PGS Geophysical AS – is authorized to operate and deliver certain IT services, HR and administration services to the other Controllers and Processors worldwide under intra group service provision agreements. As such, this entity is the main Processor within the PGS Group (the "Main Processor"). The service provision rendered by the Main Processor and the Processing done by any other Processor is governed by this Manual.

3.3 PGS Senior Management

The PGS Senior Management is the overall responsible and accountable for procuring compliance with this Manual, including implementing proper governance structures, internal controls and routines for information security and monitoring compliance with the Laws within PGS Group. The PGS Senior Management are associated with or employed by the Controllers.

3.4 Global Personal Data Protection Officer

The PGS Group has appointed a Global Personal Data Protection Officer (or the "DPO"). The DPO is: Daphne Bjerke, c/o PGS Geophysical AS, Lilleakerveien 4C, 0283 Oslo, Norway. The Global Data Protection Officer shall report on Personal Data matters to the General Counsel and to the Audit Committee of the Board of PGS ASA (the "Audit Committee").

The DPO is responsible for:

- **Knowledge**: having expert knowledge of the GDPR and Personal Data practices;
- **Overview**: having an overview of the Processing of Personal Data in the PGS Group, and maintain an overview of all Personal Data and governing documents in UniSea;
- **Review and update**: reviewing and updating annually this Manual, the Record of Processing Activities, the Data Protection site on PGS intranet, and all other governing documents related to Personal Data protection in UniSea;
- **Training**: facilitating training and awareness-raising of each Controller, Processor, System Owner and other employees of the PGS Group who carry out Processing of Personal Data their of their obligations under the GDPR and this Manual;
- **Monitoring**: monitoring compliance by each Controller and Processor of the GDPR and the Manual in concert with the PGS Compliance Department as set out in Section 12.3, and that the System Owners set up protocols of all Processing activities
- **External Processors**: keeping an updated list of External Processors and related External Data Processing Agreements (defined in Section 9 below), and facilitate supply chain reviews and audits of External Processors and monitor their compliance with the provisions of the GDPR and the terms of the External Data Processing Agreements
- **Self-assessments and certifications**: following up with Global IT Department and System Owners that they conduct annual self-assessments and certifications as set out in Section 12.4, and based on this certify compliance for the PGS Group with the GDPR and the Manual;
- **Notification Forms and DPIAs**: in concert with the Compliance Department reviewing and providing advice on corrective actions in Notification Forms (defined in Section 10 below) and assess the need for and conduct a DPIA (defined in Section 10 below);

- **Cooperate**: cooperating with the supervisory authority and act as the PGS Group's contact point thereto;
- **Contact point**: being a contact point for all questions concerning the PGS Group's Processing of Personal Data, follow up with the DPRs (defined in Section 3.5 below)
- **Complaints**: in concert with the Compliance Department advising on and handle complaints made by the Data Subjects and others in the PGS Compliance Hotline set forth in Section 13; and
- **Register**: keeping an updated register of detected or reported deviations from the Manual 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

3.5 Regional Personal Data Protection Representatives

In addition to the DPO, the PGS Group also has appointed five Regional/Operations Data Protection Representatives (each a "DPR"):

- **For Norway and the Middle East**: Stein Erik Steira, c/o PGS Geophysical AS, Lilleakervn. 4C, 0283 Oslo, Norway.
- **For North and South America**: Kimberly Adams, c/o Petroleum Geo-Services, Inc. West Memorial Place I, 15375 Memorial Drive, Suite 100, Houston, TX 77079, USA
- **For Asia-Pacific**: Evelyn Seow, c/o Petroleum Geo-Services Exploration (M) Sdn. Bhd., Menara Dion, Level 11, 27 Jalan Sultan, 50250 Kuala Lumpur, Malaysia
- **For the United Kingdom and Africa**: Gareth Jones, c/o PGS Exploration (UK) Ltd, 4 The Heights Brooklands, Weybridge KT13 ONY, United Kingdom.
- **For Offshore Vessel Operations**: Anna Landquist, c/o PGS Geophysical AS, Lilleakervn. 4C, 0283 Oslo, Norway

The DPRs are responsible for coordinating compliance with the Manual as regards Processing within their own geographical region, and act as the regional contact point on Personal Data matters towards the DPO.

3.6 System Owners

Each System Owner shall ensure to:

- complete and keep up-to-date the Notification Form (see Section 10),
- when applicable, complete and keep up-to-date the DPIA (see Section 10) the for the Personal Data flows which he/she is responsible,
- implement and uphold the controls deemed necessary to meet the rights of the Data Subject,
- communicate without delay any known or suspected data breaches, and
- assist the DPO and the PGS Compliance department during the self-assessments and certifications and in investigations of violations of the GDPR or the Manual.

3.7 Employees

All other employees within PGS Group involved in the Processing of Personal Data shall familiarize themselves and comply with the requirements set forth herein. All employees involved in Processing are bound to compliance with this Manual through its employment agreements and governance structure.

4. THE NATURE OF THE PERSONAL DATA AND PROCESSING

4.1 The Record of Processing Activities

According to the GDPR Article 30, all Controllers shall maintain a record of Processing activities under its responsibility (the "Record of Processing Activities"). The Controllers have jointly prepared a Record of Processing Activities and documented this in an excel file showing the mapping results available on the Data Protection site on the PGS Group intranet and contains an overview of:

- Personal Data categories and type;
- the purpose of Processing;
- type of Data Subjects;
- Personal Data's origin;
- the legal basis for Processing within the EU/EEA;
- the identity of the Controller and any Processor;
- who has access to the Personal Data;
- the systems used for Processing; and
- the data flow and transfer to Third Countries.

The Record of Processing Activities is reviewed and updated by the DPO on an annual basis.

4.2 Personal Data Flow out of the EU/EEA

According to the PGS Group's organizational structure, routines and practice, PGS transfers to or makes Personal Data available in Third Countries internally in the PGS Group. PGS is only permitted to transfer Personal Data to Third Countries if in compliance with the GDPR Chapter V. A permissible ground for transfer is that PGS has taken appropriate safeguards. As such safeguard, the PGS Group has implemented Binding Corporate Rules for Personal Data protection and transfers as contained in this Manual, cf. GDPR Article 47 and the WP 256.

The main purposes for such transfers are: Vessel operation and crew management (visa, medical and travel), and data disaster recovery. The supporting purposes for such transfers are: Accounting, business controls, communication, finance, compliance and audit, insurance, IT services, legal services, HR administration, performance management, settlement and invoicing, tax and treasury.

The below illustrations show the Personal Data flow in the PGS Group companies out of the EU/EEA:

5. 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 DPO.

5.1 Personal Data Processing Principles

As set out in the GDPR Article 5, Personal Data shall by each Controller and Processor be dealt with in the following way:

- **Lawfulness, fairness and transparency**: Processed lawfully, fairly, and in a transparent manner in relation to the Data Subject, see also Sections 5.2 and 5.3 below;
- **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 or otherwise;
- **Minimization**: adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed, see also Section 6.2 below;
- **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;
- **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, see also Section 11. PGS also has elaborated a Retention Schedule; and
- **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, see also the PGS Information Security Policy.

5.2 The Legal Basis for Processing of Personal Data

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

- The Data Subject has given its consent to the Processing of its Personal Data for one or more specific purposes;
- 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;
- it is necessary for compliance with a legal obligation to which the Controller is subject too;
- necessary in order to protect the vital interests of the Data Subject or another natural person;
- 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

- 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 Sections 4.1 and 10.1, each Controller has set out the legal basis for Processing in the Record of Processing Activities and Notification Form.

5.3 The Legal Basis for Processing of Special Categories of Personal Data

As set out in the GDPR Article 9, Processing by the Controllers and Processors 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:

- The Data Subject has given its explicit consent to the Processing of its Sensitive Personal Data for one or more specified purposes;
- 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;
- 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;
- 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;
- it relates to Personal Data which are manifestly made public by the Data Subject;
- is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- 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;
- 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 GDPR Article 8(3);
- 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

- is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with 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.

6. ORGANIZATIONAL AND TECHNICAL MEASURES

6.1 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 7 hereto.

Each Controller is responsible for procuring that each System Owner shall for each system in which Personal Data is Processed fill in the Notification Form and send this to the DPO for review and follow up. Each System Owner is responsible for complying with the requirements set forth by the DPO. The DPO will monitor the System Owner's compliance with the requirements set up in each Notification Form.

6.2 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.

6.3 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.

6.4 Confidentiality

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

Each Controller require that a Statement of Confidentiality is signed for all of its employees to ensure confidential treatment of sensitive information, such as Personal Data.

Each Controller shall procure that External Processors are bound by an External Data Processing Agreement (defined in Section 9 below) which shall contain sections concerning confidentiality for all personnel within the External Processors.

6.5 Security, Integrity and Privacy by Design and Default

Each Controller shall procure that Personal Data is processed in a manner that ensures risk based and appropriate security for 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. See also the PGS Information Security Policy. 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 also implemented a routine for a DPIA (defined in Section 10.2 below) to be made according to GDPR Article 35.

As a security measure, all Controllers and Processors shall notify PGS Geophysical AS and the DPO of any data breaches.

Each Controller shall, in taking a risk based approach, ensure to implement privacy by design and default in the systems that is Processing Personal Data. See also the PGS Information Security Policy.

6.6 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 as set out in Section 11 and the Retention Schedule.

6.7 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.

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

7.1 The Rights of the Data Subjects

Subject to Section 15 below, all Data Subjects in the EU/EEA whose Personal Data is processed by a PGS Group company within the scope of the GDPR including transferred to a PGS Group company outside of the EU/EEA have the following rights (these rights do not extend to elements of this Manual relating to internal implementation mechanisms within the PGS Group):

- **Withdrawal of consent**: Where the Processing 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 the Controller's Processing of Personal Data at any time, cf. the GDPR Article 7.3;
- **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;
- **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 DPO, (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;

- **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;
- **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;
- **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;
- **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;

- **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;
- **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;
- **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;
- **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 DPO; (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;
- **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 or where the Data Subject has his or her habitual residence. The Data Subject may also lodge a complaint to the PGS Compliance Hotline, see also Section 13 below;
- **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
- **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.

7.2 Information

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

- The Manual is made available to all PGS Group employees through the PGS intranet and available in UniSea;
- The Data Subjects general rights are outlined on the PGS intranet; and
- Information articles will be published on the PGS intranet.

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

- The Manual is made available to all external Data Subjects on www.pgs.com, and
- The Data Privacy Statement and the PGS Code of Conduct is available on www.pgs.com.

8. TRANSFER OF PERSONAL DATA

As shown in Section 4.2 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:

8.1 Transfer to Controllers and Processors within the PGS Group

8.1.1 From Controller to Controller

Transfers of Personal Data between Controllers that are bound by this Manual may take place, provided that the provisions in Sections 5-7 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.

8.1.2 From Controller to Processor

Transfers of Personal Data from a Controller to a Processor that are bound by this Manual 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 6; and (ii) the Processor shall act only on the instructions from the Controller. It is hereby required that any Processing done by a Processor shall be in compliance with the instructions given by the Controller, cf. Section 2.3.

8.2 Transfer to Controllers outside of the PGS Group

8.2.1 Transfer to a Controller within the EU/EEA

Transfer of Personal Data from a Controller established in the EU/EEA to another receiving controller outside of the PGS Group and established within the EU/EEA may take place provided that the Controller complies with the Sections 5-7 hereof and the receiving controller complies with the principles laid down in Section 5-7 as reflected in the GDPR, and that the requirements contained in Section 6 on appropriate security measures are implemented to protect the Personal Data during transfer and further Processing by the receiving controller.

8.2.2 Transfer to a Controller outside of the EU/EEA

Transfer of Personal Data from a Controller established in the EU/EEA to another receiving controller outside of the PGS Group and not established within the EU/EEA is prohibited, unless:

- 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 of the receiving controller is compliant with the principles set forth in Sections 5-7 hereof; or
- 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, Articles 45 and 46; or (ii) a supervisory authority and approved by the EU Commission pursuant to the GDPR Articles 45 and 46; or
- one of the derogations in the GDPR Article 49 applies, and the Processing is compliant with the principles set forth in Sections 5-7 hereof.

8.3 Transfer to External Processors

8.3.1 To External Processors established within the EEA

Transfer of Personal Data to an External Processor (defined in Section 9 below) established within the EU/EEA may take place provided that;

- the principles set forth in Sections 5-7 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
- the Processing is governed by an External Data Processing Agreement (defined in Section 9 below).

8.3.2 To External Processors established outside of the EEA

Transfer of Personal Data to an External Processor (defined in Section 9 below) not established within the EU/EEA is prohibited, unless:

- 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 the principles set forth in Sections 5-7 hereof, and the Processing is governed by an External Data Processing Agreement (defined in Section 9 below); and/or
- 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, Articles 45 and 46; or (ii) a supervisory authority and approved by the EU Commission pursuant to the GDPR Articles 45 and 46; and the Processing is governed by an External Data Processing Agreement; or
- one of the derogations in the GDPR Article 49 applies and the Processing is compliant with the principles set forth in Sections 5-7 hereof.

9. EXTERNAL PROCESSORS

Controllers or Processors within the PGS Group may from time to time order services from an external service provider or data processor (the "External Processors") that may involve Processing of Personal Data.

All such services procured by any Controller or Main Processor involving the handling of Personal Data on behalf of such Controller from, 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:

- Process the Personal Data only on instructions from the Controller or the Main Processor;
- 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;
- ensure the rights of the Data Subjects;
- not engage another data processor without the prior written authorization of the Controller or the Main Processor;
- assist the Controller for the fulfilment under its obligations in the GDPR;
- delete or return all Personal Data at the expiry or termination of the External Data Processing Agreement; and
- give the Controller and the Main Processor audit rights to inspect the External Processor's compliance with the GDPR and the terms of the External Data Processing Agreement.

The template for the External Data Processing Agreement is available on the PGS intranet. The DPO shall keep a list of all External Processors that the PGS Group has engaged, together with the applicable External Data Processing Agreement. The External Processors shall maintain a record of processing activities in accordance with the GDPR Article 30.

In the event a Controller or Main Processor established within EU/EEA uses an External Processor placed in a Third Country that involve transfer of Personal Data to a Third Country, the Controller or Main Processor 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.

10. NOTIFICATION FORM AND DATA PROTECTION IMPACT ASSESSMENT

10.1 Notification Forms

The Controllers have implemented a structure for each System Owner to report to the DPO of any system in PGS Group in which Personal Data is Processed. The structure involves that each System Owner shall fill in and submit to the DPO a written notification of Processing of Personal Data in a system (the "Notification Form").

All System Owners shall complete the Notification Form and submit it to the DPO for review. The review by the DPO may reveal the need for corrective action(s) in order to bring the system or process in

compliance with the requirements under the GDPR. The Notification Form template is available on PGS intranet.

The purpose of filling in and submitting the Notification Form is to assess the data flow and controls within each system that contains Personal Data in PGS Group, and document the Personal Data flows and conditions for Processing and measures that ensure that the Processing complies with the GDPR.

The filled in and submitted Notification Form shall be updated by each System Owner when there are changes affecting the Processing of Personal Data and reviewed annually to confirm that it is up-to-date.

10.2 Data Protection Impact Assessment

In some instances, the Notification Form may reveal a need for a more detailed Data Protection Impact Assessment (or a "DPIA"), in which case, the DPO will contact with the System Owner and procure the completion of a DPIA on the basis of the DPIA forms. The DPIA template is available on PGS intranet.

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 in consultation with the DPO carry out a DPIA. Such assessment shall in particular be required in the case of:

- 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;
- Processing on large scale of Sensitive Personal Data; and
- A systematic monitoring of a publicly accessible area on large scale.

11. PERSONAL DATA RETENTION

11.1 Introduction

The GDPR requires that no Personal Data is retained for any longer than is necessary for the purpose it was obtained for. The purpose of this Section 11 is therefore to provide guidance (i) to System Owners and other employees Processing Personal Data so that all such records, in electronic and hard copy format, are retained for no longer than what is necessary for the purpose its was obtained it for, and (ii) so that records are securely disposed at the end of the retention period. Each System Owner and each employee that processes Personal Data's is obliged to apply the appropriate retention period as specified in this work instruction or in applicable local legal requirements, whichever is the strictest.

11.2 Retention Schedule

All Personal Data should have a clearly defined retention period. The retention periods can differ based on the type of Personal Data Processed, the purpose of Processing, or legal or industry requirements. Where the Retention Schedule differs from applicable local regulations, the stricter of the requirements will apply.

The retention periods for the different categories of Personal Data are specified in the Retention Schedule. Other Personal Data categories not specified in the Retention Schedule shall be documented in the Notification Form by each System Owner.

Deviations from the retention period must be documented in the Notification Form and include the reason for deviating from standard retention, and the proposed retention period.

11.3 Disposal

Personal Data which has reached its termination date must be securely disposed. The method used for disposal of Personal Data shall be documented in the Notification Form. However, each System Owner or any other employee responsible for Processing of the Personal Data shall in consultation with the DPO verify that there is no legal reason to keep the record(s) for a longer period. If there is legal reason to keep the record(s) for longer, the record(s) must be updated with a new termination date (directly in the system or manually in case of physical storage), which adequately addresses the legal requirement, together with a description of the legal reason to keep the record(s) for longer than originally intended.

The records shall primarily be disposed of by (i) shredding or other secure disposal of physical records and (ii) deletion of the electronic records.

In case deletion of the electronic record is not possible due to interdependencies with other technological or legal limitations, the following methods may be considered: (i) Erasure of the unique identifiers which allow the allocation of a data set to a unique person; or (ii) erasure of single pieces of information that identify the data subject (whether alone or in combination with other pieces of information).

12. MONITORING, AUDIT AND VERIFICATION OF COMPLIANCE

12.1 Mapping of Personal Data

Each Controller shall implement routines for mapping Personal Data in order to ensure that each Controller at any given time is in compliance with the requirements of this Manual and the Laws. Such routines shall be subject to annual review in accordance with the Manual, and shall be designed to detect any changes made in the its Processing of Personal Data. The expected results from compliance with the routines are that each Controller shall maintain a system that facilitates compliance with this Manual.

Each Controller shall procure that all System Owners fill in a Notification Form and as required in consultation with the DPO, a DPIA.

12.2 Monitoring and Self-Assessments/Certification

Each Controller shall procure that the below self-assessments and certifications are made on an annual basis. The DPO and each DPR shall facilitate and monitor compliance herewith:

A. Self-assessments and certifications by the DPO
That this Manual and its pubic version is updated
That the Record of Processing Activities is updated
That data protection training has been completed for new employees and that annual reminders have been sent to PGS Senior Management and System Owners concerning key personal data protection principles
That Personal Data processing flows are documented in Notification Forms and, when applicable, in Data Protection Impact Assessment
That Data Processing Agreements are established with the relevant parties where required
That Personal Data requests and complaints have been handled as appropriately, including verifying that the data breach notification hotline is functional and that Personal Data requests and complaints have been appropriately addressed

That corrective actions following from Notification Forms or self-assessments and certifications done by System Owners and Global IT Department have been implemented as recommended and implemented within reasonable time

B. Self-assessments and certifications by System Owners
That the submitted Notification Form and, when relevant, the Data Protection Impact Assessment, has been completed
That changes from the Notification Forms on conditions for Processing Personal Data, data types, suppliers or security settings have been communicated to the DPO
That only authorized personnel has access to Personal Data in its systems
That Personal Data are deleted in line with the Retention Schedule and as described in the Notification Forms

C. Self-assessments and certifications by Global IT Department
Compliance with PGS security framework
Verify and update application and network map
Control of list of IT equipment and storage media
Status on update of antivirus program on each PC/server has been reviewed
That security penetration testing has been performed
That hardening of network units, including check of safety-copy and switch/router configuration is confirmed
hardening of servers
change of admin passwords
Confirm that in house development of systems processing personal data comply with “security by design and by default” principles
Confirm that the organization has in place appropriate disaster recovery for in-house systems

The results of the self-assessment shall be sent to and kept by the DPO for follow up. The results hereof shall also be available upon request to the supervisory authority.

The self-assessments 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. Each Controller shall comply with any corrective actions and the DPO shall monitor that these are being implemented. Corrective action resulting from identified non-compliance with external or internal requirements will be initiated by the DPO and implemented by the System Owner. The DPO shall follow and monitor that the corrective actions are being implemented within a reasonable timeframe.

The results of the self-assessment will be presented to the PGS Senior Management and to the Audit Committee of the Board of PGS ASA, and identified issues of non-compliance with internal or external requirements will be addressed by corrective actions.

12.3 Audits

The PGS Internal Audit Department pertaining to PGS Geophysical AS shall in line with its regular routines and methods audit compliance with all aspects of this Manual globally within the scope of its annual yearly audit plan. In addition, external auditors may perform compliance audits. The audit may cover elements such as applications, IT systems, systems for Processing Personal Data, transfers to Third Countries, and decisions taken as regards mandatory requirements under national laws that conflicts with this Manual.

The results of the audit shall also be reported to the Audit Committee pertaining of the Board of Directors in PGS ASA, and shall be available upon request to the supervisory authority. Each Controller permit that the supervisory authority in the EEA can audit compliance with this Manual.

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.

13. NOTIFICATION OF PERSONAL DATA BREACH – THE COMPLAINT PROCEDURE

13.1 Introduction

Each Controller shall without undue delay, and where feasible no later than 24 hours from having become aware of the breach, report data breaches to *PGS Geophysical AS* and the DPO via the PGS Compliance Hotline or otherwise. The DPO and the PGS Compliance department will, as appropriate, notify the competent supervisory authority within 72 hours from the Controller become aware of the breach. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, PGS must also inform those individuals without undue delay.

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 DPO 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 record and document any Personal Data breaches, comprising the facts relating to the Personal Data breach, its effects and the remedial action taken, and keep such record available for the supervisory authority.

PGS must also keep a record of any Personal Data breaches, regardless of whether the supervisory authority or any Data Subject shall be notified.

13.2 The PGS Compliance Hotline

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 https://report.whistleb.com/en/pgs.

The PGS Compliance Hotline is available for our employees, clients, suppliers, business partners and everybody else, providing an opportunity for anyone to report concerns about any aspect of our business. If you are an employee, we encourage you first to contact your supervisor, or other appropriate PGS representatives within legal, compliance and human resources to voice any concerns.

13.3 Reports will be Handled Appropriately

Reports to the PGS Compliance Hotline can be named or made anonymously. In both cases they will be handled securely and confidentially. The PGS Compliance Hotline service is provided by our external business partner WhistleB. Their whistleblowing system ensures anonymity, confidentiality and professional handling. The reporting and communication channel is encrypted and password-protected. All reports, anonymous or otherwise, will be investigated promptly according to our Compliance Hotline procedure, and will be handled by the PGS Group thoroughly and fairly. The PGS Compliance department will follow up all reports as set out in the PGS *Compliance Hotline Reporting and Investigation Procedure* available on www.pgs.com.

Once a notification of Personal Data breach is received in the PGS Compliance Hotline, the PGS Compliance department will review the notification and ensure that an assessment in accordance with in accordance with the European Commission "Guidelines on Personal data breach notification under Regulation 2016/679". The DPO will be promptly notified.

For accountability and record keeping purposes, the PGS Compliance Hotline will document the relevant information regarding:

- the data breach details
- the risk evaluation decision
- the steps to contain the data breach
- the steps to correct the circumstances leading to the data breach
- the notification to data controllers, if applicable
- the notification to the authorities, if applicable
- the notification to the data subjects, if applicable,
- any other relevant information.

14. TRAINING

The Controllers has prepared an appropriate Personal Data protection training programs for relevant PGS Group employees. The main purposes of these training program is to (i) ensure implementation of an appropriate level of compliance with the Laws and this Manual within the PGS Group, (ii) make the Laws and this Manual well understood for the relevant PGS Group employees with the Laws and this Manual and effectively applied, and (iii) clarify roles and responsibilities.

The training programs includes a Personal Data protection workshop where the main agenda for is: Background for the Laws with particular focus on the GDPR, objective and requirements of the GDPR, and individual responsibilities related thereto.

The PGS Group employees who shall receive training are the following: EXT and PGS Senior Management, the Global Enterprise IT Department, the Global and Regional HR Departments, the local Office Administration Departments, System Owners, and line managers. These will receive regular tailor made training.

15. LIABILITY

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 in Norway accepts responsibility for and agrees to take the necessary action to remedy the acts of Controllers or Processors within the PGS Group established outside of the EU/EEA that are bound by this Manual and have

violated the GDPR. PGS Geophysical AS will pay compensation for any material or non-material damages resulting from violation of the GDPR by PGS Group companies within the scope of the list contained in the table to WP256, its item 1.3, to the extent that affected Data Subjects are protected by the GDPR for which this Manual is required in order to protect their Personal Data in a transfer to a Third Country. Each Controller and PGS Geophysical AS must prove that it is not responsible for the event giving rise to the damage in order to avoid liability.

16. ACCESS TO EMPLOYEE DATA

Under the provisions of the Norwegian Employment Act 2005, an employer needs to comply with certain rules when accessing an employee's Personal Data stored in email accounts, personal folders on servers, data stored on employee PC, and electronically stored material on the employee's server area ("Employee Data"). However, these rules differ significantly from country to country.

Therefore, prior to any access to Employee Data being made the below persons shall approve this and give guidance as follows:

- PGS Head of Legal shall provide guidance on the rules under the applicable laws for the countries relevant for the case
- Head of HR shall providing guidance on aspects regarding HR policies and staff contract details, and
- Head of Global IT Department shall facilitate the technical access to the Employee Data

17. ADDITIONAL DEFINTIONS

"Controller" means the legal entity within PGS Group who determines the purposes and means of the Processing of Personal Data. The Controllers within PGS Group is set forth in Section 2.3.

"DPO" means PGS Global Data Protection Officer.

"DPIA" means a Data Protection Impact Assessment, as further outlined in Section 10.2.

"General Data Protection Regulation" or **"GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

"Laws" means GDPR, the Norwegian Personal Data Act 2018, as well as any other data protection laws applicable to the PGS Group.

"Notification Form" means a written notification of Processing of Personal Data in a system to be filled by the System Owner and sent to the DPO, as further outlined in Section 10.1.

"Personal Data" means any information relating to an identified or identifiable natural person ("Data Subject"'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"PGS Group" means PGS ASA and its subsidiaries, as well as its and their directors, officers and employees.

"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.

"Processor" means the legal entity within PGS Group which Processes Personal Data on behalf of the Controller. The Processors within PGS Group is set forth in Section 2.3.

"Retention Schedule" means the list of categories of the various Personal Data and the retention period which is applied to each such category, as further outlined in Section 11.

"System Owners" means each employee within the PGS Group being overall responsible for procuring or handling a system in which Personal Data is Processed.

18. CONTACT DETAILS

The below list outlines the PGS Group companies that has employees or otherwise are involved in Processing of Personal Data:

EUROPE

- **PGS Geophysical AS**, Lilleakerveien 4C, 0283 Oslo, NORWAY, attn. Daphne Bjerke, phone +47 67 51 43 65
- **PGS ASA**, Lilleakerveien 4C, 0283 Oslo, NORWAY, attn. Daphne Bjerke, phone +47 67 51 42 87
- **PGS Exploration (UK) Ltd**, 4 The Heights, Brooklands, Weybridge, Surrey, KT13 0NY, the UNITED KINGDOM, attn. Gareth Jones, phone +44 1932 376448
- **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

AFRICA AND MIDDLE EAST

- **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**, No. 10A Fabac Close, Victoria Island, Lagos, NIGERIA, c/o PGS Geophysical AS, Lilleakerveien 4C, 0283 Oslo, NORWAY attn. Daphne Bjerke, phone +47 67 51 42 87
- **PGS Ghana Limited,** Imperial Square Building, Airport Residential Area, 6th Senchi Street, Accra, Greater Accra, Ghana, c/o Geophysical AS, Lilleakerveien 4C, 0283 Oslo, NORWAY attn. Daphne Bjerke, phone +47 67 51 42 87

NORTH AND SOUTH AMERICA

- **Petroleum Geo-Services Inc**., West Memorial Place I, 15375 Memorial Drive, Suite 100, Houston, TX 77079, USA, attn.: Kimberly Adams, phone: +1 281 509 8329

- **PGS Suporte Logístico e Serviços Ltda,** Rua do Passeio, 38, Suite 1602 and 1603, sector 2, Edifico Passeio Corporate, Centro, Zip Code 20021-290, Rio de Janeiro - RJ 22.775-044 Brazil, c/o Petroleum Geo-Services Inc., West Memorial Place I, 15375 Memorial Drive, Suite 100, Houston, TX 77079, USA, attn.: Kimberly Adams, phone: +1 281 509 8329

ASIA-PACIFIC

- **PGS Data Processing & Technology Sdn Bhd**., Level 33, Suite E, Menera Maxis, Kuala Lumpur City Centre, 50088 Kuala Lumpur, W.P. Kuala Lumpur, Malaysia attn. Evelyn Seow, phone: + +6012 311 0726

- **Petroleum Geo-Services Exploration (M) Sdn. Bhd** , Level 33, Suite E, Menera Maxis, Kuala Lumpur City Centre, 50088 Kuala Lumpur, W.P. Kuala Lumpur, Malaysia, , attn. Evelyn Seow, phone: +6012 311 0726

- **Petroleum Geo-Services Asia Pacific Pte Ltd**., 80 Robinson Road, #02-00, Singapore (068898), c/o Petroleum Geo-Services Exploration (M) Sdn. Bhd, Level 33, Suite E, Menera Maxis, Kuala Lumpur City Centre, 50088 Kuala Lumpur, W.P. Kuala Lumpur, Malaysia attn. Evelyn Seow, phone: +6012 311 0726

- **PGS Australia Pty Ltd**, QV 1 Level 28, 250 St Georges terrace, Perth WA 6000, Australia c/o Petroleum Geo-Services Exploration (M) Sdn. Bhd , Level 33, Suite E, Menera Maxis, Kuala Lumpur City Centre, 50088 Kuala Lumpur, W.P. Kuala Lumpur, Malaysia attn. Evelyn Seow, phone: +6012 311 0726

- **PGS Japan K.K.**, 5th Floor, UD Hibiya Building, 1-1-2 Uchisaiwaicho, Chiyoda-ku, Tokyo 100-0011 JAPAN, c/o Petroleum Geo-Services Exploration (M) Sdn. Bhd , Level 33, Suite E, Menera Maxis, Kuala Lumpur City Centre, 50088 Kuala Lumpur, W.P. Kuala Lumpur, Malaysia attn. Evelyn Seow, phone: +6012 311 0726