Personal Data Protection Manual - Binding Corporate Rules

This Personal Data Protection Manual and Binding Corporate Rules (“BCRs”) is part of PGS ASA and its subsidiaries (“PGS”) overall compliance program for managing and protecting Personal Data processed in relation to its operations. These BCRs were approved by the relevant data protection authorities on [•].

Table of Contents

1. DEFINTIONS

"Adequate Third Countries" means any EU, EEA country or other Third Country that is determined as offering adequate protection for Personal Data pursuant to applicable data protection law. As of March 2023, the EU Commission has so far recognised Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom and Uruguay as providing adequate protection.

"Audit Committee" means the audit committee of the Board of Directors of the ultimate parent company in the PGS Group, namely PGS ASA.

"BCRs" means the binding corporate rules as set forth in this document.

"Data Controller" means an entity (whether a natural or legal person, public authority, agency or other body) which alone, jointly or in common with others determines the purposes and means in which any item of Personal Data is processed.

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

"DPO" means PGS Global Data Protection Officer.

"DPR" means the regional PGS Global Data Protection Officer.

"DPIA" means a Data Protection Impact Assessment, as further outlined in Section 11.2.

"EEA" means the zone of economic cooperation known as the European Economic Area and those countries which are participants in such zone, collectively.

"External Processor" means an entity (whether a natural or legal person, public authority, agency or any other body) outside of the PGS Group which processes Personal Data on behalf of and upon instructions of PGS, as further set out in Section 10.

"External Data Processing Agreement" is defined in Section 10.

"EU" means the European Union.

"EU Personal Data" means Personal Data which is or has been subject to European Data Protection Laws.

"European Essential Guarantees" means the European Data Protection Board's recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020 found here.

"ICA" means the intercompany agreement entered into between all PGS entities contractually binding them to the BCRs.

"Data Subject" means any identified or identifiable natural person whose information is Processed by or on behalf of PGS; 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; Data Subjects include current and past employees, job applicants, contractors, representatives of customers and other business partners, and consumers.

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

"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 11.1.

"Personal Data" means any information relating to an identified or identifiable natural person; 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" or **"PGS Group"** means PGS ASA and its subsidiaries in which PGS ASA holds directly or indirectly more than 50% of the voting rights or otherwise has control, as well as its and their directors, officers and employees.

"PGS Compliance Hotline" means system which facilitates receipt by PGS of reports of suspected violations of law, regulation, policy or procedure, or ethically questionable conduct.

"PGS C&IA" means PGS Group Compliance & Internal Audit Department.

"PGS EIT" means PGS Group Enterprise IT department.

"PGS General Counsel" means PGS Group General Counsel.

"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.

"Record of Processing Activity" is defined in Section 5.1.

"Supervisory Authority" means the Norwegian Data Protection Authority.

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

"Third Countries" means international organizations and countries that are not considered to provide an adequate level of protection.

"TPA" means a Data Transfer Assessment as further outlined in Section 11.3.

"UniSea" means the governance management system in the PGS Group.

2. INTRODUCTION

2.1 Commitment and Purpose

The purpose of these BCRs is for PGS to:

- comply with the GDPR and other Data Protection Laws;
- establish adequate safeguards for the transfer of Personal Data from countries within the EU and the EEA to 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 Data Protection Laws, and
- establish a set of principles and routines that shall ensure effective internal controls for compliance with the GDPR and other Data Protection Laws regarding the Processing of all Personal Data within the PGS Group.

2.2 Legally Binding BCRs

These BCRs contains legally binding rules for the PGS Group companies regarding the Processing of Personal Data and:

- Impose obligations on all companies within the PGS Group; and
- impose obligations on all System Owners and other employees in the PGS Group who are involved in Processing of Personal Data.

These BCRs are binding upon all companies in the PGS Group, through the execution of the ICA, and as being part of UniSea. Also, each PGS Group company has passed or will pass a board resolution whereby the agree to be bound by the provisions of the BCRs.

All participating PGS entities and employees are bound by the BCRs, irrespective of their geographical location and abide by the same internal rules for Processing of Personal Data. It also means that Data Subjects' rights remain the same no matter where Data Subjects' Personal Data is Processed by PGS.

2.3 Changes to these BCRs

The DPO shall make updates and revisions to these BCRs 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 these BCRs.

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

2.4 Reporting on Deviating Legal Requirements

These BCRs are 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 these BCRs, the higher protection requirements shall prevail.

Upon any PGS Group employee suspecting that applicable legislation prevents the fulfillment of the provisions of these BCRs, or has substantial effect on the guarantees provided by these BCRs, 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 PGS General Counsel take necessary steps to assess whether any changes to these BCRs need to be made, and if there is any doubt the DPO and PGS General Counsel will consult with the Supervisory Authority.

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 these BCRs, 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 PGS to a local authority shall not be massive, disproportionate or non-discriminatory beyond what is necessary in a democratic society.

2.5 Cooperation with the Supervisory Authority

2.5.1 General Cooperating Procedures

All PGS entities have a duty to cooperate with the Supervisory Authority or other competent authority within the EU/EEA for information or inspection. Each PGS entity will comply with their advice on any issues relating to the BCRs (any advice would be subject to legal review to consider any factors which inhibit the entity's ability to comply and where relevant discussions regarding alternative legal remedies with the Supervisory Authority). Each PGS entity shall be willing to be audited by the Supervisory Authority if required or provide audit results and reports if asked to do so. No transfer will be made to a PGS entity under the BCRs until they have signed the ICA and are effectively bound by the BCRs. However, other transfer mechanisms to facilitate transfers may be used until they join the BCRs. Changes to the BCRs' entity list will be reported to all PGS entities signed up to the BCRs and to the relevant supervisory authorities via the Supervisory Authority.

2.5.2 Routine Reporting matters to the Supervisory Authority

PGS will report routine updates to the BCRs along with an updated list of PGS entities being part of the BCRs as part of PGS internal annual update.

2.5.3 Reporting of Changes to these BCRs

Any material changes to these BCRs 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 these BCRs or otherwise significantly affect these BCRs shall be communicated to the Supervisory Authority promptly and without undue delay.

2.5.4 Conflicts between local laws and the BCRs

PGS has a duty to inform the Supervisory Authority of any conflict between local law requirements and the BCRs where this conflict would have a substantial adverse effect on the guarantees provided under

the BCRs. PGS entities have a duty to report such conflicts to the DPO as soon as they become aware. This includes any legally binding requests for disclosure of personal data to a law enforcement or other security agency as explained directly below.

2.5.5 Disclosure and transfer requests

All PGS entities agree that transfers of Personal Data to any public authority or body cannot be massive, disproportionate and indiscriminate. All PGS entities must report any such disclosure requests to the DPO. The DPO will then inform the Supervisory Authority about the request, the identity of the requesting party and the legal basis for the request, unless such entity is prohibited or temporarily prevented from doing so under criminal law provisions specifying confidentiality during the course of a law enforcement investigation. All PGS entities must endeavor to have the prohibition on notification waived as soon as possible to provide the Supervisory Authority with as much information as possible to be able to evidence their efforts to do so. All PGS entities must keep a record of these disclosure requests it receives. These records should include details about the disclosure, the categories of data requested, the identity of the requestor unless prohibited by law to retain this information and any other relevant information. The PGS entities must provide the Supervisory Authority with an annual update of these records.

2.6 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.

2.7 Sanctions upon breach

Violations by any PGS employee of the provisions laid out in these BCRs and any confidentiality obligations may result in disciplinary measures and even termination of employment. While PGS retains the discretion as to how to respond to any violation of the BCRs, any disciplinary process will be undertaken in accordance with all applicable local laws, legal requirements and PGS policy and procedure. PGS employees who have concerns about any issue that they believe (or suspect) may violate any law or violate the BCRs or any other PGS policy or procedure have a right to speak up and PGS encourages them to use the PGS Compliance Hotline referred to in Section 14.2.

3. OVERVIEW OF THE PGS GROUP

3.1 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), the United Kingdom (London), and the United States of America (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).

3.2 Legal Structure and Contact Details

The PGS Group encompasses a number of companies in various locations around the world, all of which are subject to these BCRs. The overview of the legal structure of the PGS Group is updated routinely 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.

3.3 Applicability and Scope

3.3.1 Applicability

The BCRs apply to all Personal Data Processed by any entity within the PGS Group as a Data Controller for our own purposes, such as recruitment, employment or marketing. The PGS Group processes

Personal Data for a range of Data Subjects, including potential recruits, employees, prospective and existing clients and contacts, more fully set out in Schedule 2.

The BCR commitments are to:

- Require all PGS entities and employees who collect, use and store personal data to understand the rules and their responsibilities when processing personal data;
- require all PGS employees to understand how to respect and manage individual rights in relation to their data; and
- govern the circumstances in which one PGS entity Processes Personal Data on behalf of another PGS entity.

In the event that any entity within the PGS Group is removed from the PGS Group and is therefore not bound by the provisions of these BCRs, such entity will immediately stop processing all Personal Data in accordance with these BCRs and will either delete or return all Personal Data to PGS, upon PGS' written request to do so.

3.3.2 Scope

These BCRs do not apply to PGS as data processor for services it provides to its clients. For client provided Personal Data, PGS has a separate privacy policy and procedure to implement data privacy requirements applicable to client-owned data.

This document is without prejudice and does not override any applicable national data privacy laws and regulations in countries where PGS operates.

3.3.3 PGS Group entities

PGS has offices and operations throughout the world. Personal Data may be transferred or accessible throughout PGS' global business and between its entities. For a full list of the PGS entities which are signed up to the BCRs and their location see Schedule 1.

3.3.4 Categories of individuals, categories of personal data and processing, purposes, recipients, countries

The table in Schedule 2 sets out information about (i) the categories of Data Subjects, (ii) the categories of Personal Data PGS may Process about them; and (iii) a description of the purposes for which PGS Processes Personal Data. The PGS data privacy notices and data privacy statements are where we provide specific information to Data Subjects, for example the PGS privacy statement located here on the www.pgs.com.

4. RESPONSIBILITIES

4.1 Global Personal Data Protection Officer

The PGS Group has appointed a DPO. The DPO is: Daphne Bjerke, c/o PGS Geophysical AS, Lilleakerveien 4C, 0283 Oslo, Norway. The DPO shall report on Personal Data matters to the PGS General Counsel and to 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 these BCRs, 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 employee of the PGS Group;
- **Monitoring**: monitoring compliance by PGS of the GDPR and these BCRs in concert with the PGS C&IA 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 PGS EIT 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 these BCRs;
- **Notification Forms and DPIAs**: in concert with the PGS C&IA 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 PGS C&IA 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 these BCRs 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.

4.2 Regional Personal Data Protection Representatives

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

- **For Norway and the Middle East**: Iselin Askvik, 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 United Kingdom, Africa Asia-Pacific**: 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 these BCRs as regards Processing within their own geographical region, and act as the regional contact point on Personal Data matters towards the DPO.

4.3 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 C&IA during the self-assessments and certifications and in investigations of violations of the GDPR or these BCRs.

4.4 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 legally bound to comply with these BCRs through their employment agreements and governance structure.

4.5 Accountability

Everyone who works for PGS is:

- Responsible and accountable for Processing Personal Data ethically and lawfully;
- expected to comply with PGS' policies and data privacy guidance when Processing Personal Data;
- expected to understand the data privacy requirements which have relevance to the Personal Data they process on behalf of PGS, using its policies, procedures and training material.

PGS also has processes and procedures in place to manage and monitor our compliance with data privacy requirements. PGS has appropriate technical and organizational measures to meet these requirements. Everyone at PGS is expected to follow our processes and comply with out procedures and measures.

5. THE NATURE OF THE PERSONAL DATA AND PROCESSING

5.1 The Record of Processing Activities

According to the GDPR Article 30, PGS shall maintain a Record of Processing Activities under its responsibility. PGS has prepared a Record of Processing Activities and documented this in an excel file showing the mapping results available on the PGS Group intranet site 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;
- 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.

5.2 Personal Data Flow out of the EU/EEA

According to the PGS Group's organizational structure, routines and practice, PGS transfer to or makes Personal Data available in Third Countries internally in the PGS Group. PGS 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 these BCRs for Personal Data protection and transfers, cf. GDPR Article 47 and the Recommendation 1/2022.

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.

PGS has guidance in place to ensure that appropriate safeguards (including contractual arrangements where needed) are put in place for transfers of Personal Data to Third Countries. This guidance includes information on when to apply the correct safeguards and contractual arrangements before any such cross-border transfers take place. This includes assessments of Third Country laws and practices prior to the transfer taking place in order to determine to what extent the European Essential Guarantees are respected. PGS entity may only use the BCRs as a tool for transfer where this assessment has occurred.

If PGS concludes that an adequate level of protection for personal data cannot be guaranteed in the Third Country concerned, that data exporter in the EU, if needed with the help of a data importer, shall assess and define supplementary measures to ensure a level of protection which is essentially equivalent to the measures applicable in the EU. Where effective supplementary measures could not be put in place, the transfers at stake will be suspended or ended.

PGS has put in place procedures for implementing these safeguards to cover our day-to-day Processing, for example, via these BCR for internal transfers, or procurement contracts that include relevant obligations conferred upon processors or sub-processors as specified in privacy laws or other mechanisms. PGS safeguards include sufficient protections to guard against any onward transfer of data to controllers or processors which are not part of the BCR.

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

6. 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 PGS to comply with the principles hereof. Any questions relating to these principles can be addressed to the DPO.

6.1 Personal Data Processing Principles

As set out in the GDPR Article 5, PGS shall deal with Personal Data 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 6.2 and 6.3 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.

6.2 The Legal Basis for Processing of Personal Data

PGS Processes Personal Data for specified and lawful purposes which are clearly explained to Data Subjects when we process their data. Lawful processing means that PGS will not process Personal Data, unless one of the following conditions apply:

- The Data Subject has given its consent to the Processing of its Personal Data for one or more specific purposes;
- PGS processes the data to:
  - perform, or take steps with a view to enter into, 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;
  - comply with a legal obligation to which PGS is subject too;
  - protect the vital interests of the Data Subject or another natural person;
  - perform a task carried out in the public interest or in the exercise of official authority vested in PGS; or
- necessary for the purposes of the legitimate interests pursued by PGS 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.

PGS will not use Personal Data for new purposes without following its internal procedures to verify that such processing can take place lawfully by taking the following into account:

- Links between the current purposes and further respective Processing purposes;
- the context of the original data collection, with a particular focus on the relationship between PGS and Data Subjects;

- the nature of the Personal Data, in particular, if the data in question is sensitive Personal Data;
- possible consequences for Data Subjects if their Personal Data is Processed further; and
- appropriate safeguards which may include encryption or pseudonymization.

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

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

As set out in the GDPR Article 9, Processing by PGS 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 in respect of either PGS 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.

In relation to Personal Data relating to criminal convictions and offences or related security measures based on Article 6(1) of the GDPR, PGS will only Process such Personal Data under the control of the relevant official authority or when the Processing is authorized by the EU or the relevant member State of the EU providing for appropriate safeguards for the rights and freedoms of Data Subjects. Any register of criminal convictions shall be kept only under the control of the relevant official authority.

7. ORGANIZATIONAL AND TECHNICAL MEASURES

7.1 Lawful, fair, transparent and purpose limitation

PGS 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.

PGS 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.

Where required by applicable law, Personal Data will be Processed for specific and legitimate purposes and not further Processed in a way incompatible with those purposes. Further Processing will not be considered incompatible for example when it is (i.) with the Data Subject's consent or authorization, (ii.) in an emergency situation such as when the Data Subject's life or vital interests are at stake, or (iii.) in order to establish, exercise, or defend a legal claim.

These BCRs set a minimum standard of data privacy protection. Where applicable law requires a higher level of protection for Personal Data than the level of protection set out in the BCRs, PGS will apply such higher level of protection. For example, when Processing is permitted only on the basis of one or more grounds specified by law, PGS will meet such requirements.

Where PGS has reason to believe that a law prevents it from complying with these BCRs, PGS will take a responsible decision on what action to take in consultation with the DPO and consult with the Supervisory Authority if PGS deems necessary.

7.2 Minimization

PGS shall implement measures to ensure that the Processing of Personal Data shall be relevant and limited to what is necessary in relation to the purposes for which they are Processed.

Where required by applicable law, PGS will take measures to minimize Processing of Personal Data, including by privacy by design.

7.3 Access Control

PGS shall implement measures to ensure that any person or Processor who has access to Personal Data shall not Process these except on lawful instruction to do so, 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.

7.4 Confidentiality

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

PGS requires that each employee commits to confidentiality obligations to ensure confidential treatment of sensitive information such as Personal Data.

PGS 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.

7.5 Security, Integrity and Privacy by Design and Default

PGS will take reasonable steps to ensure 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.

In the event of a Personal Data breach, PGS will (i) consult with the DPO, which keeps a record of Personal Data breaches, and (ii) inform the affected Data Subjects about the breach in accordance with applicable law.

Privacy by Design - PGS considers data privacy as an integral component of the design, development, operation and management of new projects, tools, applications, internal services and offerings which Process Personal Data. To this end, there is internal guidance and processes on how to incorporate privacy as an essential part at the beginning of the design and development stages. When PGS engages vendors and partner organizations as part of any design, development and implementation work, PGS has procedures in place to ensure privacy by design is an integral component.

Privacy by Default - PGS will use or adopt privacy as the default setting when designing, developing, operating and implementing new tools, apps and other technology used by PGS and its employees. PGS will request its vendors and partner organizations to do the same.

7.6 Storage Limitation

PGS 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.

7.7 Accuracy

PGS will take reasonable 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.

8. THE RIGHTS OF AND THE INFORMATION TO THE INDIVIDUALS

8.1 Rights of Data Subjects

Where required by applicable law, an individual can submit a request to PGS to exercise the following rights given to individuals under applicable data privacy laws or these BCRs :

- **Withdrawal of consent**: Where the Processing is based on consent, the consent shall be given in a lawful way and PGS shall be able to demonstrate that the Data Subject has consented to Processing of his or her Personal Data. To the extent that PGS 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 PGS without undue delay, and as a general rule no later than one (1) month from PGS' 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 PGS and its representatives, 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, PGS 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 PGS 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 PGS, 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 PGS 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 PGS 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 PGS restrictions of Processing if; (i) the accuracy of Personal Data is contested by the Data Subject, for a period enabling PGS 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) PGS 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 PGS 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 PGS 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 PGS carrying out a task in public interest or being necessary for PGS or a third party pursuing legitimate interests, unless PGS 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 Data Subject 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 PGS 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 PGS 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**: In accordance with the Escalations Options, set out in Section 8.6 below;
- **Right to Compensation**: To be entitled to compensation from PGS 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 PGS; 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 PGS has an establishment or association to promote its rights under the GDPR Articles 77, 78, 79 and 82, cf. the GDPR Article 80.

An Data Subject can exercise his/her rights regardless of whether he/she makes a complaint to PGS or the Supervisory Authority or any other competent supervisory authority. To exercise these rights or to raise a concern or complaint that PGS is not complying with these BCRs, Data Subjects can contact the DPO to obtain more information on the procedure it will apply in order to handle the complaint:

By email to: gdpr@pgs.com

Or in writing to: The Data Privacy Officer, c/o PGS Geophysical AS

P.O. Box 251 Lilleaker

0216, Oslo,

Norway

8.2 Specific Rights in relation to European Personal Data

If EU Personal Data is transferred to a PGS entity outside of EU, PGS will afford a level of protection to EU Personal Data which does not undermine the level of protection granted under the GDPR. PGS will do so, even if such protection is not afforded by the applicable law in the countries of the PGS entities outside of the EU where the EU Personal Data is received.

This means in particular in relation to the data privacy practices described in Section 8.1 respectively, that PGS will:

- Not Process EU Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, genetic data, or biometric data for the purpose of uniquely identifying an

Data Subject, unless such Processing is permitted in accordance with Article 9.2 of the GDPR;

- carry out an assessment of the impact of high risk Processing operations, in accordance with Article 35 of the GDPR, and if risks remain high after implementing mitigating measures identified by the assessment, consult with the competent data protection authority, in accordance with Article 36 of the GDPR;
- Process EU Personal Data for specific and legitimate business purposes;
- Process EU Personal Data which is adequate, relevant and limited to what is necessary in relation to the legitimate business purposes;
- apply privacy by design and privacy by default as appropriate;
- keep a register of Processing activities;
- give notice and transparency to Data Subjects about the use and purpose of the Processing of EU Personal Data in accordance with Articles 13 and 14 of the GDPR; and
- apply the same level of security measures to protect EU Personal Data as provided in the GDPR.

8.3 Breach of EU Personal Data

In the event of a breach of EU Personal Data, each relevant PGS company will:

- Consult with the DPO, which will document the breach in a register and make the relevant documentation available to the competent data protection authority upon request;
- notify without undue delay PGS Geophysical AS who, if the breach is likely to result in a risk to the Data Subject's rights and freedoms, will in turn notify the Supervisory Authority without undue delay and, where feasible, not later than 72 hours after having become aware of the breach;
- inform Data Subjects without undue delay if the breach is likely to result in a high risk to the Data Subject's rights and freedoms;
- respond to requests and complaints of Data Subjects in relation to the Processing of EU Personal Data in accordance with Section 8.7;
- allow Data Subjects to object to a decision based solely on automated Processing which produces legal effects concerning the Data Subject or similarly significantly affects the Data Subject, unless the decision is permitted under Article 22 of the GDPR; and
- transfer EU Personal Data to third parties outside of the EU when adequate protection is provided in accordance with Article 28.3 and Articles 45 to 48 or a derogation under Article 49 of the GDPR.

The Supervisory Authority may verify compliance with these BCRs, including by carrying out audits of PGS in accordance with audit rights conferred under applicable laws.

PGS entities outside of the EU/EEA will cooperate with PGS Geophysical AS as needed to respond to requests by data protection authorities in the EU/EEA to provide relevant audit results in relation to these BCRs.

PGS will communicate to the DPO the audit results in relation to EU Personal Data transferred under the BCRs to PGS entities outside of the EU.

PGS will comply with the advice of the competent data protection authority in the EU with respect to EU Personal Data, subject to the exhaustion of any legal remedies when deemed appropriate by PGS.

8.4 Data Subjects right of Enforcement

The Data Subject whose EU Personal Data is transferred directly or indirectly to a PGS entity outside of the EU derives third party beneficiary rights from, and may directly enforce its rights by:

- contacting the DPO in accordance with Section 8.1, or
- lodging a complaint with a national data protection authority of competent jurisdiction in the country in the EU/EEA where (i) the Data Subject has his or her habitual residence or place of work, or (ii) the alleged infringement of the BCRs took place, or
- bringing a proceeding against the relevant PGS company established in the EU/EEA before a competent court therein, or
- bringing a proceeding against PGS Geophysical AS with registered office at Lilleakerveien 4C 0283, Oslo, Norway before the Norwegian Data Protection Authority or the Norwegian courts or other competent courts referred in Article 79(2) GDPR.

If a valid claim or complaint is brought above, PGS Geophysical AS accepts responsibility for any violation of these BCRs by a PGS entity established outside of the EU/EEA and agrees to take the necessary action to remedy the violation and, where appropriate, to pay compensation for damages resulting from such violation, in accordance with a final decision of a court or Supervisory Authority not subject to further appeal.

If a claim, complaint, or proceeding is brought above, the Data Subject does not have to prove an actual violation of the BCRs by a PGS affiliate outside of the EU; it suffices that the Data Subject demonstrates that it has suffered damage and that such damage has likely occurred as a result of a violation of these BCRs by a PGS affiliate established outside of the EU. The burden of proof is then on PGS Geophysical AS to demonstrate that the PGS affiliate established outside the EU did not violate these BCRs. If PGS Geophysical AS can prove that the PGS affiliate established outside the EU is not liable for the violation, PGS Geophysical AS may discharge itself from any responsibility.

PGS will respond to complaints regarding EU Personal Data without undue delay and in any event within one month of receipt of the request or complaint, which may be extended by two further months where necessary.

Complaints can be submitted by a Data Subject to PGS by email or in writing in accordance with Section 8.6 of these BCRs.

In case PGS considers the complaint as justified, it will inform the Data Subject how it will remedy the issue which gave rise to the complaint. If the complaint is rejected or if the Data Subject is not satisfied with PGS's response, the Data Subject can lodge a complaint or initiate proceedings in accordance with Sections 8.6 of these BCRs. Furthermore if the complaint pertains to Processing of EU Personal Data by PGS entities established outside of the EU/EEA, the Data Subject can also lodge a complaint or initiate proceedings in accordance with Section 8.6 .

In the event of a conflict between the BCRs and a legal requirement in a country outside of the EU as described in Section 3.3, PGS will notify the competent data protection authority in the EU if such legal requirement, including a legally binding request for disclosure of EU Personal Data by a law enforcement authority or a state security body of a country outside the EU, is likely to have a substantial adverse effect on the guarantees provided in the BCRs with regard to EU Personal Data.

In addressing this obligation, PGS undertakes to conduct an assessment which takes due account of: (i) the specific circumstances of the transfers; (ii) the laws and practices of the third countries of destination (relevant in light of the specific circumstances of the transfers, and the applicable limitations and safeguards); and (iii) the relevant contractual, technical and organizational security measures put in place under the BCRs. Affiliates outside of the EU receiving European Personal Data will make best efforts to provide relevant information to assist with this assessment, which PGS will document and make available to the competent data protection authority upon request. If PGS becomes aware that a PGS affiliate outside of the EU can no longer fulfil its obligations under the BCRs, PGS will promptly identify appropriate supplementary measures to be adopted by the relevant PGS affiliate(s) to address the situation. The relevant PGS affiliate(s) will suspend the transfer if PGS considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent data protection authority to do so.

If notification to the competent data protection authority in the EU is prohibited, PGS will use its best efforts, as reasonably practical, to obtain the right to waive this prohibition, and will document

that it did so. If in spite of its best efforts, as reasonably practical, PGS cannot notify the competent data protection authority in the EU about the requests it receives, it will annually provide general information on the requests.

PGS will assess the legality of a request for disclosure as described above – in particular, whether it is within the powers granted to the requesting public authority – and challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and/or principles of international comity. PGS will, under the same conditions, pursue possibilities of appeal. When challenging a request, PGS will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. PGS will document its legal assessment and any challenge to the request for disclosure, and to the extent permissible under the laws of the country of destination, make the documentation available to the competent data protection authority on request. PGS will not disclose the Personal Data requested until required to do so under the applicable procedural rules, and shall provide the minimum amount of information permissible when responding, based on a reasonable interpretation of the request.

PGS will take measures to prevent any transfers of EU Personal Data to any public authority (as well as any direct access by such authorities to Personal Data transferred under the BCRs) that are massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

8.5 Publication

These BCRs are made available via www.pgs.com to external parties and internally via the PGS internal portal and Unisea. Where PGS is required to publish these BCRs in a local language, we will do so. Upon request, PGS will also email an electronic PDF version of the BCRs to an Data Subject.

8.6 Escalation Options

- **Making a complaint to PGS:** Data Subjects have the right to come directly to PGS for resolution of complaints concerning non-compliance with these BCRs or PGS' Privacy Policy. These will be dealt with in accordance with PGS' internal processes and guidance. PGS welcomes individuals to come to PGS first to seek resolution of any complaint and PGS proposes that they make use of the PGS Compliance Hotline, referred to in Section 14.2.
- **Making a complaint to a supervisory authority:** Data Subjects also have the right to register a complaint directly with the Supervisory Authority or any other competent supervisory authority. In some complex situations, PGS may have already consulted with a competent supervisory authority before reaching its decision. If this is the case, PGS will make the individual aware of this. This could be the supervisory authority where the individual lives or works or where the alleged data privacy infringement occurred. It is up to the individual to decide which supervisory authority they wish to deal with.
- **Making a claim:** Data Subjects can also make a claim against PGS via a competent court subject to local laws. PGS has the right to object where it has such rights. The competent court is recognized as being in the member state of the EU where the individually (habitually) resides or where the relevant PGS controller has an establishment. It is up to the individual to decide which competent court they would look to register a claim with.

9. CROSS BORDER TRANSFER OF PERSONAL DATA

PGS affiliates will not transfer EU Personal Data under the BCRs to other PGS affiliates unless the latter are bound by these BCRs.

Data privacy laws place restrictions on transfers of Personal Data across borders for any type of Processing. These restrictions also apply to internal transfers of Personal Data within PGS across the countries where we operate, and to transfers of Personal Data to vendors, suppliers, partners or other third parties located in different countries.

PGS has guidance in place to ensure that appropriate safeguards (including contractual arrangements where needed) are put in place for transfers of Personal Data to Third Countries. This guidance includes information on when to apply the correct safeguards and contractual arrangements before any such cross-border transfers take place. This includes assessments of third country laws and practices prior to the transfer taking place (including data in transit) in order to determine to what extent European Essential Guarantees are respected. The BCR participating entities may only use the BCRs as a tool for transfer where this assessment has occurred.

If PGS concludes that an adequate level of protection for Personal Data cannot be guaranteed in the Third Country concerned, the data exporter in a Member State, if needed with the help of the data importer, shall assess and define supplementary measures to ensure a level of protection which is essentially equivalent to that in the EU. Where effective supplementary measures could not be put in place, the transfers at stake will be suspended or ended.

PGS has a uniform approach towards the handling of personal data requests that are massive, disproportionate and indiscriminate from public authorities directed to any PGS entity by any public authority or body, whether such personal data relates to PGS employees, contractors, service providers, PGS clients or their customers, for example according to local surveillance laws or regulations.

PGS has put in place procedures for implementing these safeguards to cover our day-to-day processing, for example, via these BCR for internal transfers, or procurement contracts that include the relevant obligations conferred upon processors or sub-processors as specified in privacy laws and other mechanisms. Our safeguards include sufficient protections to guard against any onward transfer of data to controllers or processors which are not part of the BCR.

10. EXTERNAL PROCESSORS

PGS 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 PGS involving the handling of Personal Data on behalf of PGS 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 PGS;
- 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 PGS;
- assist PGS in 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 PGS 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.

11. NOTIFICATION FORM AND DATA PROTECTION IMPACT ASSESSMENT

11.1 Notification Forms

PGS has 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.

11.2 Data Protection Impact Assessments

Privacy reviews and Data Protection Impact Assessments ("**DPIA**") are assessment tools used by PGS to assess privacy and security risks as part of our risk mitigation procedures. PGS has a process to initiate privacy reviews to assess our own practices, service offerings, technology to mitigate risks and allow for privacy integration through measures such as privacy by design or adopting privacy as the default setting. The privacy review may also identify the need for a DPIA. Not all processing requires a DPIA. We use DPIAs where this is a mandatory requirement for certain types of processing which carry a high risk or have greater implications for rights and freedoms of individuals. The outcome of a DPIA is to identify the necessary measures to minimize risk and comply with the GDPR. PGS will consult with the Competent Supervisory Authority prior to processing taking place, when required to do so. PGS has internal processes in place to manage privacy reviews and DPIAs. All PGS entities are required to act on the outcome of a DPIA or review to help mitigate any privacy risks, including implementing additional measures to mitigate those risks.

11.3 Transfer Impact Assessments

When PGS acts as a data exporter of Personal Data from the EEA, Switzerland and the UK to another country that was not found to be adequate, PGS performs a Transfer Impact Assessments ("**TIA**") to identify any risk associated with the transfer (including the possibility of access requests by public authorities) and to define supplementary measures to safeguard the data, if necessary. Where effective supplementary measures could not be put in place the transfers at stake will be suspended or ended.

The completion of the TIA is the responsibility of the DPO. There is no need to repeat the assessment every time there is the same transfer of a specific type of EEA/UK/Swiss personal data to the same Third Country.

The TIA and, where needed, the decision on what supplementary measures to implement are documented and centrally stored within PGS and internally accessible. These are made available to the Supervisory Authority on request.

12. PERSONAL DATA RETENTION

12.1 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.

12.2 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 this 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 Record of Processing Activity. Other Personal Data categories not specified in the Record of Processing Activity 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.

12.3 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).

13. MONITORING, AUDIT AND VERIFICATION OF COMPLIANCE

13.1 Mapping of Personal Data

PGS shall implement routines for mapping Personal Data to ensure that PGS is, at any given time, in compliance with the requirements of these BCRs and the Laws. Such routines shall be subject to annual review in accordance with these BCRs, 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 PGS shall maintain a system that facilitates compliance with these BCRs.

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

13.2 Monitoring and Self-Assessments/Certification

PGS 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 these BCRs 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. PGS 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.

13.3 Audits

PGS has a privacy compliance audit program. The purpose of the audits is to assess PGS’ compliance with its internal procedures and practices, applicable data privacy laws and these BCRs.

Different aspects of its auditing program address data privacy compliance. Audits will generally be carried out at regular intervals but also by exception, where there is a particular need to conduct an audit outside of the regular schedule. Audits are conducted internally by the PGS C&IA, working to together with the DPO, or an external organization, specializing in audits.

PGS conducts regular reviews and regular risk assessments for data privacy. PGS has developed a series of audit controls against which to monitor its data privacy compliance. These controls cover compliance with the commitments it makes in these BCRs, its data privacy policies, procedures and processes and compliance with data privacy laws.

All entities within the PGS Group agree to be audited by the Supervisory Authority if required to do so. During the audit, each PGS entity shall cooperate with the auditor[s] and shall disclose to the auditors any and all information or documents as may be required for the accomplishment of the auditor's objectives, subject to compliance with local laws and regulations.

The results of all the audits relating to the processing of personal data shall be made available to the PGS DPO and any other relevant PGS function and market leadership. Upon request, the results will be made available to supervisory authorities.

Audit follow up procedures will include a corrective action plan based on the audit findings and procedures for ensuring the corrective action is implemented.

14. NOTIFICATION OF PERSONAL DATA BREACH – THE COMPLAINT PROCEDURE

14.1 Introduction

PGS 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 Supervisory Authority within 72 hours from PGS becoming 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.

PGS 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.

14.2 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 www.pgs.com.

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.

14.3 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 an external business partner. 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.

15. TRAINING

PGS maintains a data privacy training program for all of its employees. All PGS employees who regularly Process Personal Data will be given appropriate and timely data privacy training. If required to do so, PGS will provide the Supervisory Authority or other relevant supervisory authorities with examples of our training program.

All PGS employees are required to undergo data privacy on an annual basis and covers, amongst others, the handling and international transfer of Personal Data, keeping Personal Data secure, the various data protection principles, and reporting a data breach.

16. LIABILITY

Each PGS affiliate 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 any affiliate within the PGS Group established outside of the EU/EEA that are bound by these BCRs 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 these BCRs is required in order to protect their Personal Data in a transfer to a Third Country. Where a Data Subject demonstrates that they have suffered damage and establish facts which show it is likely that such damage has occurred because of a breach of the BCRs, the burden lies with PGS Geophysical AS to prove that the BCR member outside of the EEA was not responsible for such breach or that no such breach took place.

17. 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.

Schedule 1: List of PGS Entities and their location

Entity	Location
PGS Holding I Ltd	England
PGS Holding II Ltd	England
PT Petroprima Geo-Servis Nusantara	Malaysia
Petroleum Geo-Services AS	Norway
PGS Geophysical AS	Norway
Petroleum Geo-Services Inc	United States
PGS Suporte Logistico e Servicos Ltda	Brazil
Petroleum Geo-Services (UK) Ltd	England
PGS Geophysical Nigeria Ltd	Nigeria
Multiklient Invest AS	Norway
PGS Titan AS	Norway
Petroleum Geo-Services Asia Pacific Pte.Ltd	Malaysia
PGS Finance Inc	United States
PGS Japan K.K.	Japan
PGS Falcon AS	Norway
PGS Imaging S.A. de C.V.	Mexico
Seahouse Insurance Ltd	Bermuda
PGS Data Processing Middle East SAE	Egypt
PGS Australia Pty Ltd	Australia
NCS Subsea Inc	United States
PGS Egypt for Petroleum Services LLC	Egypt
Petroleum Geo-Services Asia Pacific Labuan Ltd	Labuan
PGS Shipowner AS	Norway
Petroleum Geo-Services Inc	United States
Petroleum Geo-Services Exploration (M) Sdn Bhd	Malaysia
PGS Data Processing and Technology Sdn Bhd	Malaysia
PGS Seismic Services Ltd	United Kingdom
Natuna Ventures Pts Ltd	Singapore
PGS Arabia Ltd	Saudi Arabia
Baro Industrieiendom AS	Norway
Ulmatec Baro AS	Norway
Ocean Floor Geophysics Inc	Canada
Ocean Geo-Frontier Co. Ltd	Japan
Azimuth I Ltd	Bermuda
Azimuth II Ltd	Bermuda

Azimuth III Ltd	Bermuda
Versal AS	Norway
PGS Ghana Ltd	Ghana
PT Petroprima Geo-Servis Nusantara	Indonesia
PGS Exploration (UK) Ltd	England
PGS Geophysical (Angola) Ltd	England
Panoceanic Energy Ltd	England
PGS Pension Trustee Ltd	England

Schedule 2: Categories of individuals, categories of personal data and processing, purposes, recipients, countries

This table sets out the types of individuals we **may** process personal data about, the categories of personal data we may process about them, and the purposes for which we process personal information. This table is intended to be a generic summary. It does **NOT** mean we process this data about all these types of individuals.

Type	Explanation
Categories of individuals	1. PGS employees (past and present) - includes permanent and contracting staff [temporary or casual workers, freelancers, contractors, trainees]. 2. Non-employee workers including volunteers, assignees, advisors, consultants, agents and other professional experts, secondees, apprentices, interns, alumni, other third parties. 3. Individuals identified by the aforementioned data subjects as dependents and beneficiaries, including insured spouses and partners, children, guardians and parents, family members and contact persons for emergencies. 4. Job applicants, candidates and pre-hires. 5. Client contacts, current and past contacts and prospects - including employees, officers, agents, consultants and other professional experts. 6. Vendor, supplier contacts. 7. Members of the press and other organizations (including charities, educational institutions, Regulators, business intermediaries, etc.). 8. Website users and complainants, correspondents and enquirers. 9. Individuals attending our events. 10. Shareholders. 11. Alumni. 12. Other third parties.
Categories of personal data and processing	**Personal details [employment context**] - Name, preferred pronoun, all types of contact details (such as e-mail, phone numbers, physical home and place of work address), gender, date of birth, place of birth, national identification number, social security number and health insurance number, insurance information, internal company employee or id numbers, marital/civil partnership status, domestic partners, dependents, disability status, emergency contact information, ethnic origin, minority flag, biometric data (such as facial images, voice recognition/patterns, iris patterns or fingerprints), photograph, and images/footage captured on CCTV or other video systems, footage/voice recordings captured during events/sessions (including recording of virtual or live workshops or similar events), smart building controls and metric systems used for data analytics, driver license number, car details and other necessary data for use of company cars (including clearing, damage events, insurances), government-issued ID number; emergency contact details; information obtained through the use of surveys; investigations, complaints and grievances data including as part of the business ethics line; mergers and acquisitions data, work anniversary. **Personal details [clients & prospects]** - Name, all types of contact details (such as salutation, job title, e-mail, phone numbers, physical home and place of work address), contact preferences, preferred language for communications, marketing preferences, data relating to goods and services provided or obtained, relationship with PGS

	[prospect, client, alumni now client]; data related to events [invitations, attendance, relevant costs]. **Personal details [vendors, service providers, suppliers, payees and intermediaries, legal services data]** – Name, all types of contact details (such as salutation, job title, e-mail, phone numbers, physical home and place of work address); preferred language for communications; data related to invitations for business trips or other business events (e.g., itinerary, costs); entity tax identification number and commercial registry registration number; entity nationality; entity bank details and payment related information, bill to and ship addresses, billing currency; VAT (or equivalent) number; customer/vendor/supplier number or other unique identifier; country registration number, where applicable; information derived from the deployment and use of information systems and tools including from third parties; records related to the provision and management of products orders or returns, provision of services, accounts and internal administration and accounting; curriculum vitae; time and expense records concerning the provision of services; operational data; details of relationship with PGS. **Other individuals [alumni, corporate citizenship/outreach, website visitors]** - Name, all types of contact details (such as salutation, job title, e-mail, phone numbers, physical home and place of work address), contact preferences, preferred language for communications, marketing preferences, data relating to interaction or relationship with PGS - enquiry, complaint, site visit, application for award, grant, educational initiative, competition. **Documentation required under immigration laws** - Citizenship, passport data, professional work visa, details of residency or work permit (a physical copy and/or an electronic copy). **Compensation and payroll** - Remuneration details (including historic pay, base pay and bonus or incentive pay, salary banding, frequency of payments), pay deductions, tax codes, insurance codes and statutory and voluntary contributions, benefits, loans, overtime and shift work, compensation type, pay frequency, salary reviews and performance appraisals, banking details including credit card details [both company and personal where the employee has used this], working time records (including vacation and other absence records, leave status, hours worked and department standard hours), pay data and termination date, compensation details, offers, reductions/reimbursements, employee/capital-forming investments, expense descriptions, amounts claimed, cost type, approval and pre-approvals, data required to support expenses claims including bills, receipts, documents, interests in businesses and equity holdings. **Leaves of absence** - Vacation, statutory leaves and voluntary leaves (including maternity and paternity leaves, sabbaticals), justification for paid absences (including education, family events, social activities, children and other dependents' care). Data relating to administration or leave (including start date, end date, temporary suspension), illness including accidents at work and occupational health (in accordance with local law). Dates (beginning, end and duration).

	Pension records - Monthly pension, yearly pension, capital sums, deferred compensation sums, type of pension plan; other data related to pension fund (including enlistment and discharges, contribution data and insurance period in the statutory Social Security). **Position and contractual information -** Description of current position, job title, corporate status, career level, management category, job code, job function(s), legal employer entity, location, PGS contact(s), employee identification number, terms and conditions of employment or contract, membership of the board of directors, information on extent of shareholding, work history, hire/re- hire and termination date(s) and reason, information from exit interviews/termination documents, length of service, executive management responsibility, trade union membership, retirement eligibility, promotions and disciplinary records, date of transfers, and reporting manager(s) information. **Work location & relocation -** Working address, place of work (including work place office, home office, shared desk, external work), workplace indicator, work location code, branch office, sales office, building, room, locker, relocation information (including international assignment flag, assignment data and dates, current assignment, future assignment, country, hypotax, tax reconciliation, foreign tax); employment permits (including date); visa country, visa expiration date, mobility preferences, termination date and reason code; assignment responsibility, assignment job title, tasks; employee's willingness to travel or relocate. **Talent management information –** Details contained in letters of application and resume/CV or other provided documents (previous employment background, education history, professional qualifications, any technical specialisations or qualifications, trade licenses, language and other relevant skills, certification, certification expiration dates), information of recruitment interviews/check lists, legal prerequisites for employment, information necessary to complete a background check, details on performance decisions and outcomes, performance feedback and warnings, e-learning/training programs, internal and external certifications and membership of professional associations, performance and development reviews (including information you provide when asking for/providing feedback, creating priorities, updating your input in relevant tools, comments from/re. counsellors/counselees), willingness to relocate, driver's license and car ownership information, assessment information and information used to populate employee biographies. **Management records** - Details of any shares of common stock or directorships, stock purchase plans, stock purchase eligibility and contribution, stock options information. **Website, tools, systems, apps** - Information required to access PGS systems, tools and applications such as System ID, LAN ID, e-mail account, instant messaging account, mainframe ID, previous employee ID, previous manager employee ID, system passwords, access logs, access rights, security level, activity logs, office Wi-Fi

	connection logs, office access credential data, employee status reason, branch state, country code, previous company details, aggregated/hashed professional email/calendar/IM meta-data, previous branch details, and previous department details, and electronic content produced using PGS systems, information derived from the deployment and use of information systems and tools including from third parties; tracking data including data from cookies and other technology, visitor logs, IP addresses, individual posts into chat rooms, blogs, circles, comments, systems' recordings such as web meetings, calls and webinars. **Sensitive data -** Certain types of sensitive information when permitted by local law, such as health/medical information (including data required to mitigate health and safety risks – including during a health crisis), trade union membership information, religion, and race or ethnicity, information on criminal convictions and offences. PGS collects this information for specific purposes, such as health/medical information in order to accommodate a disability or illness and to provide benefits; to get access to and/or to use certain tools or premises; background checks (where permissible under local laws); and diversity-related personal data (such as race or ethnicity) in order to comply with legal obligations and internal policies relating to diversity and anti-discrimination. PGS will only use such sensitive information for the purposes provided by law. **Advertising. marketing and public relations** - Promoting and providing products and services to actual and potential customers; advertising, marketing and PR related activities; communications; compliance; business operations; research, complaints and enquiries handling; management of business relationships and other activities; other services. **Accounts and records data, data relating to vendors, service providers, suppliers, payees and intermediaries, legal services data -** Order management, including billing, credit analysis, shipping, account maintenance, and internal administration and accounting for all commercial relationships; managing and analyzing sales and demand; communications; business operations; customer relationship management (e.g., CRM); conducting internal audits and other internal control activities relating to contract; management with customers, suppliers, vendors, subcontractors and business partners; compliance; due diligence for anticorruption and anti-bribery purposes; reporting activities to fulfil finance and accounts requirements; risk management and corporate audits and assessments (e.g., Background Investigations Tool and Gift & Entertainment Hub) Internal investigations (e.g., Business Ethics Helpline); internal investigations; legal filing and reporting; purchase order and payment; computer system security, including ensuring adequate level of protection of the personal data stored therein; other services on an ad-hoc basis. **Data relating to mergers, ventures and acquisitions -** Management and employment information, compensation and payroll data,

	business operations, customer relationship management, compliance; due diligence, reporting activities to fulfil finance and accounts requirements; risk management and corporate audits and assessments; legal filing and reporting; computer system security, including ensuring adequate level of protection of the personal data stored therein.
Purposes for which PGS uses personal information	Scheduling Talent Acquisition / Recruitment Management and administration of employees Facilitating communication (including in case of emergencies) Operating and managing PGS' business operations Employee engagement, performance management and professional development Financial planning, payroll, fund management and accounting Share plan management and operations Business and market development Advertising, marketing and public relations Building and managing external relationships Maintaining relationships with former employees and Alumni relations Planning and delivery of business integration capabilities Research and development Compliance, audit and insurance purposes, including supplier and customer due diligence Internal and external investigations including liaison with law enforcement/other government agencies where required to do so by law Litigation management Client, supplier and business intermediary/partner management Technology infrastructure, security and support (including business continuity), facilities and data management, internal business support services and monitoring use of PGS's systems and other PGS resources as permitted by local law and/or in accordance with PGS's policies Travel management Knowledge management Corporate Citizenship and outreach programs Complying with legal requirements Reporting to data privacy supervisory authorities - routine reporting and breach notification Liaising with regulators/government departments for routine reporting requirements under law – tax, social security, benefits, national ID programs Mergers & Acquisitions - this includes due diligence and information relevant to potential ventures, joint ventures, mergers and acquisitions Social listening - Identifying and assessing what is being said about PGS and our clients on social media (only publicly accessible content)

	Undertaking data analytics, including analysis of our applicant pool in order to better understand who is applying to positions at PGS and how to attract and keep top talent Other purposes not incompatible with the ones listed above or other purposes required and/or permitted by law or regulation
Recipients	**PGS entities -** PGS entities which are signed up to the BCR or other PGS entities/affiliates outside the BCR [using a different transfer mechanism]**.** **Professional advisors -** Accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors in all of the countries in which PGS operates. **Service providers -** Companies that provide products and services to PGS such as payroll, pension scheme, benefits providers, human resources services, performance, training, expense management, IT systems suppliers and support, advertising and marketing, security and performance monitoring, third parties assisting with equity compensation programs, credit card companies, medical or health practitioners, trade bodies and associations, and other service providers. **Public and governmental authorities -** Entities that regulate or have jurisdiction over PGS such as regulatory authorities, law enforcement, public bodies, and judicial bodies. **Corporate / commercial transaction -** A third party in connection with any proposed or actual reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of PGS business, assets or stock (including in connection with any bankruptcy or similar proceedings). A third party in connection with any proposed or actual client project. **Corporate citizenship -** Corporate citizenship partners/organizations where necessary (e.g. to obtain documentation related a gift or a tax statement).

Countries to which transfers may be made	Many of our global systems are operated from Norway, we also have significant operations in United Kingdom, US Japan and Australia. However, as a global group we transfer to many countries worldwide, inside and outside the EEA, Switzerland and the UK. We publish a list of group companies that have signed the BCR intercompany agreements which is available as part of our BCRs.