Policy: Data Protection Policy

Document number: LEG16p1

Scope: Global

Date	Revision	Description	Owner	Approver
08 Jun 2018	0	Renumbered from HR20p1, Rev 01, 15 Mar 2018. No changes to content	Senior Legal Advisor	CFO
05 July 2018	01	Full update to reflect GDPR	Senior Legal Advisor	CFO
10 Sep 2018	02	Amendment to DPO details at Clause 2	Senior Legal Advisor	CFO

Table of Contents

1 Introduction

This policy sets out how Sparrows Offshore Group Limited (“Sparrows Group”) and all subsidiary companies (”we”, “our”, “us”, “the Company”) handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

This policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This policy applies to all Company Personnel (”you”, “your”). You must read, understand and comply with this policy when Processing Personal Data on our behalf and attend training on its requirements, if required.

This policy sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

Where you have a specific responsibility in connection with processing such as capturing Consent, reporting a Personal Data Breach, conducting a Data Protection Impact Assessment (DPIA) as referenced in this policy or otherwise then you must comply with all related policies and privacy guidelines.

2 Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

All directors, individual business areas, managers and supervisors are responsible for ensuring all Company Personnel comply with this policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

Our Senior Legal Advisor will assume the responsibilities of the data protection officer (“DPO”). All correspondence should be addressed to DPO@sparrowsgroup.com

Please contact the DPO with any questions about the operation of this policy or GDPR, or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to Process Personal Data (including the legitimate interests used by the Company);
(b) if you need to rely on Consent and/or need to capture explicit Consent;
(c) if you need to draft privacy notices;
(d) if you are unsure about the retention period for the Personal Data being processed;
(e) if you are unsure about what security or other measures you need to implement to protect Personal Data;
(f) if there has been a Personal Data Breach;
(g) if you are unsure on what basis to transfer Personal Data outside the EEA;
(h) if you need any assistance dealing with any rights invoked by a Data Subject;
(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes others than what it was collected for;

(j) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making;
(k) If you need help complying with applicable law when carrying out direct marketing activities; or
(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).

3 Definitions

Throughout this Policy, the terms “we”, “Sparrows”, the “Company”, “Sparrows Group”, “Group” and “us” refers to Sparrows Offshore Group Limited and/or any of its subsidiaries and/or affiliated companies, including Alpha Offshore Service A/S.

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject’s wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: means Personal Data relating to criminal convictions and offences.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of

an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

4 Personal Data Protection Principles

The GDPR contains eight data protection principles, which must be followed in the holding and Processing of Personal Data. Personal Data must:

- Be Processed lawfully, fairly and in a transparent manner.
- Be collected only for specified, explicit and legitimate purposed.
- Be adequate, relevant and limited to what is necessary in relation to the purpose for which it is Processed.
- Be accurate and where necessary kept up to date.
- Not be kept in a form which permits identification of the Data Subjects for longer than is necessary for the purpose for which the data is being Processed.
- Be Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage.
- Not be transferred to another country without appropriate safeguards being in place.
- Be made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data.

5 Lawfulness, fairness, transparency

5.1 Lawfulness and fairness

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows processing for specific purposes, some of which are set out below:

(a) The data subject has given his or her Consent;
(b) The Processing is necessary for the performance of the contract with the Data Subject;
(c) To meet our legal compliance obligations;
(d) To protect the Data Subject's vital interests; or
(e) To pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purpose for which we Process Personal Data for legitimate interests need to be set out in applicable privacy notices.

5.2 Consent

A Controller must only Process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which includes Consent.

A Data Subject Consents to Processing of their Personal Data if they indicate agreement clearly either by statement or positive action to the Processing.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first Consented.

Unless we can rely on another legal basis of Processing, explicit Consent is usually required for Processing Special Categories of Personal Data and Criminal Convictions Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require explicit Consent) to Process most types of Special Categories of Personal Data and Criminal Convictions Data. Where explicit Consent is required, you must issue a privacy notice to the Data Subject to capture explicit Consent.

You will need to evidence Consent captured and keep records of all Consents in accordance with related policies and privacy guidelines so that the Company can demonstrate compliance with Consent requirements.

5.3 Transparency (notifying data subjects)

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate privacy notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a privacy notice.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

6 Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

7 Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only Process Personal Data when the duties of your job requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention policy.

8 Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

9 Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is Processed.

We will not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with the Company's policy on data retention.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

10 Security Integrity and Confidentiality

10.1 Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to

third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

10.2 Reporting a personal data breach

The GDPR requires controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

In the unlikely event that a Personal Data Breach should occur, we will implement a procedure for rectification, reporting to the Information Commissioner's Office (ICO) and, where required, to the Data Subject in accordance with the GDPR

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO. You should preserve all evidence relating to the potential Personal Data Breach.

11 Transfer limitation

Sparrows Group are an international employer with employees all over the world and offices in the UK, Europe, USA, Africa and MEICAP region and, as such, the Data we collect may be transferred to, and stored at, a destination outside the European Economic Area ('EEA'). It may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Such staff may be engaged in, among other things, the fulfilment of your order, the data is safely and appropriately transferred.

Compliance will be supported by a review of existing contracts with data controllers and processors and any data export/sharing arrangements.

12 Data Subject's Rights and Requests

Data Subject, have a number of rights. They can:

- Access and obtain a copy of their Personal Data on request;
- Require the Company to change incorrect or incomplete Personal Data;
- Require the Company to delete or stop Processing their Personal Data, for example where the Personal Data is no longer necessary for the purposes of Processing;
- Object to the Processing of their Personal Data where the Company is relying on its legitimate interests as the legal ground for Processing; and
- Ask the Company to stop Processing Personal Data for a period if Personal Data is inaccurate or there is a dispute about whether or not their interests override the Company's legitimate grounds for Processing Personal Data.

You must verify the identity of an individual requesting data under of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the DPO at the following address: DPO@sparrowsgroup.com.

13 Accountability

13.1 Compliance

The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Company must have adequate resources and controls in place to ensure and to document GDPR compliance.

13.2 Record keeping

The GDPR requires us to keep full and accurate records of all our data processing activities.

You must keep and maintain accurate corporate records reflecting our processing including records of Data Subjects' consents and procedures for obtaining consents.

These records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, processing activities, processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

13.3 Training and audit

You shall be provided with adequate training to enable you to comply with data privacy laws.

You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

13.4 Privacy by Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that process Personal Data by taking into account the following:

(a) the state of the art;
(b) the cost of implementation;
(c) the nature, scope, context and purposes of Processing; and
(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.
(e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

Data Controllers must also conduct DPIAs in respect to high risk processing.
A DPIA must include:
(i) a description of the Processing, its purposes and the Controller's legitimate interests if appropriate;
(ii) an assessment of the necessity and proportionality of the processing in relation to its purpose;
(iii) an assessment of the risk to individuals; and
(iv) the risk mitigation measures in place and demonstration of compliance.

13.5 Direct Marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior Consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

13.6 Sharing Personal Data

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our Sparrows Group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the privacy notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

14 Further Information

Further information in relation to the GDPR and the rights given to individuals under it are available at the Information Commissioner's Website on www.ico.org.uk. In addition, further information can be obtained from the DPO.

The Company's policies, privacy notices, operating procedures or processes related to this policy and designed to protect Personal Data are available on our Sparrows Information Management System (https://sparrowsgroup.sharepoint.com/sites/sims/Pages/LEG16-Data-Protection-%26-GDPR.aspx).

Our privacy notices for external parties are available on our web site www.sparrowsgroup.com

15 Changes to this policy

We reserve the right to change this policy at any time so please check back regularly to obtain the latest copy of this policy.

We last revised this policy on 5th July 2018.

This policy does not override any applicable national data privacy laws and regulations in countries where the Company operates. No policy can cover all eventualities.

Questions in relation to this policy or application of the policy should be directed to the DPO.