WILHELMSEN
BINDING CORPORATE RULES

Contents

1 INTRODUCTION 5

2 DESCRIPTION OF THE DATA FLOWS IN THE GROUP - SCOPE AND APPLICABILITY OF THE BCRS 5

2.1 Scope and applicability of the BCRs 5

2.2 Description of the data flows within the Group 6

2.3 Overview of BCR Appendices and sub-policies 6

3 DEFINITIONS 6

4 LEGAL BASIS FOR PROCESSING OF PERSONAL DATA 9

4.1 Introduction 9

4.2 Legal basis for Processing of Personal Data 9

4.3 Legal basis for Processing of Special Categories of Personal Data 10

4.4 Processing of Personal Data relating to criminal convictions and offences 11

4.5 Consultation 11

4.6 Data protection in HR applications 11

5 REQUIREMENTS REGARDING PURPOSES FOR PROCESSING PERSONAL DATA – PURPOSE LIMITATION AND DATA MINIMIZATION 11

5.1 Legitimate Purposes and data minimization 11

5.2 Consultation 12

6 RECORDS OF PROCESSING ACTIVITIES 12

7 DATA MINIMIZATION, DATA ACCURACY AND STORAGE LIMITATION 13

7.1 Data minimization and accuracy 13

7.2 Storage limitation 13

7.3 Day to day responsibility 15

8 TRANSPARENCY AND INFORMATION RIGHTS 15

8.1 General transparency and communication requirements 15

8.2 Information requirements 16

8.3 Access to the BCRs 18

8.4 Consultation 19

9 PROCEDURE FOR HANDLING DATA SUBJECT'S REQUESTS FOR ACCESS TO PERSONAL DATA 19

9.1 Purpose 19

9.2 Right of access by the Data Subject 19

10 RIGHT TO RECTIFICATION OF PERSONAL DATA 20

10.1 Purpose 20

10.2 Data Subject's right to rectification 20

11 PROCEDURE FOR HANDLING THE RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN) 20

11.1 Purpose 20

11.2 Right to erasure (right to be forgotten) 21

12 PROCEDURE RELATING TO THE DATA SUBJECT'S RIGHT TO RESTRICTION OF PROCESSING 22

12.1 Purpose 22
12.2 Right to restriction of Processing 22
13 NOTIFICATION OBLIGATIONS RELATING TO RECTIFICATION, ERASURE OR RESTRICTION 22
14 PROCEDURE FOR DATA PORTABILITY 22
14.1 Purpose 22
14.2 Right to data portability 22
15 RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION-MAKING 23
16 SECURITY OF PROCESSING AND CONFIDENTIALITY 23
16.1 Introduction 23
16.2 High level security measures 24
17 DATA PROTECTION BY DESIGN AND BY DEFAULT 25
17.1 Data protection by design 25
17.2 Data protection by default 25
18 PERSONAL DATA BREACH 25
18.1 General obligations related to Personal Data Breaches 25
18.2 Notification of a Personal Data Breach to the Supervisory Authority 26
18.3 Communication of a Personal Data Breach to the Data Subject 27
19 DATA PROTECTION IMPACT ASSESSMENT 27
19.1 Data Protection Impact Assessment 27
19.2 Responsibility and governance 28
19.3 Consultation 29
20 PRIOR CONSULTATION 29
21 ENGAGING INTERNAL PROCESSORS (WITHIN THE GROUP) 29
22 SHARING PERSONAL DATA WITH EXTERNAL PROCESSORS AND CONTROLLERS (OUTSIDE THE GROUP) 30
22.1 External Processors located in the EU/EEA or a country recognised by the EU Commission as ensuring an adequate level of protection 30
22.2 External Processors located outside of EU/EEA and in a country that is not recognised by the EU Commission as ensuring an adequate level of protection 31
22.3 International organisations and Controllers located outside of EU/EEA in a country that is not recognised by the EU Commission as ensuring an adequate level of protection 32
23 SUPERVISION OF COMPLIANCE 32
23.1 The Data Protection Officer's tasks and responsibilities 32
23.2 The Position of the Data Protection Officer 33
23.3 DPO and PDPA management 33
23.4 Training program 33
24 AUDIT AND MONITORING PROGRAM 34
24.1 Monitoring and internal audit 34
24.2 Audits by the Norwegian Data Protection Authority 35
24.3 Corrective Actions 36

25 INTERNAL COMPLAINT MECHANISM 36
25.1 Complaints to the Data Protection Officer 36
25.2 Time limits 36
25.3 Information regarding the internal complaint mechanism 36
26 THIRD PARTY BENEFICIARY RIGHTS 37
27 MUTUAL ASSISTANCE AND DUTY TO COOPERATE WITH THE SUPERVISORY AUTHORITIES 38
28 THIRD COUNTRY LAWS AND PRACTICES, THIRD COUNTRY GOVERNMENT ACCESS REQUESTS 39
28.1 Third Country laws and practices which may affect these BCRs 39
28.2 Obligations in the event of Third Country government access requests 41
29 NON-COMPLIANCE WITH THESE BCRS 43
29.1 General requirements 43
29.2 Consequences of non-compliance with these BCRs 43
30 TERMINATION OF BCR MEMBERSHIP 43
31 LIABILITY AND BURDEN OF PROOF 44
31.1 Liability 44
31.2 Burden of proof 44
32 SANCTIONS 44
33 RIGHT TO LODGE A COMPLAINT 44
34 MECHANISM FOR REPORTING AND RECORDING CHANGES OF THE BCRS 45
35 APPLICABLE VERSION OF THE BCRS 46
36 GOVERNING LAW 46
APPENDIX 1: MEMBERS OF THE BCRS .....
APPENDIX 2: MATERIAL SCOPE OF THE BCRS .....
APPENDIX 3: PERSONAL DATA PROTECTION IN GLOBAL HR APPLICATIONS PROCEDURE .....
SUB-APPENDIX 3-1: MINIMUM DATA REQUIREMENTS FOR GLOBAL HR APPLICATIONS .....
APPENDIX 4: *[INTENTIONALLY DELETED]* .....
APPENDIX 5: CYBER SECURITY POLICY .....
APPENDIX 6: PERSONAL DATA PROTECTION MANAGEMENT IN THE WILHELMSEN GROUP .....
SUB-APPENDIX 6-1: THE GROUP-, GLOBAL-, AND LOCAL PERSONAL DATA PROTECTION ADMINISTRATORS .....
APPENDIX 7: INTRAGROUP BCR AGREEMENT .....
APPENDIX 8: TEMPLATE COMPLAINT FORM .....

1 Introduction

These Binding Corporate Rules for controllers ("**BCRs**") constitute a data protection and privacy compliance framework with general rules for the Processing of Personal Data within the Wilh. Wilhelmsen Group (the "**Group**"). The purpose of the BCRs is to provide:

(i) Appropriate safeguards and an adequate level of protection for the transfers and Processing of Personal Data within the Group; and

(ii) Enforceable Data Subject rights and effective legal remedies for Data Subjects affected by the Processing of Personal Data within the Group.

The approval of the BCRs by the Norwegian Data Protection Authority (the "**NDPA**") in accordance with the applicable consistency mechanism set out in the General Data Protection Regulation (the "**GDPR**") allows transfer of Personal Data across borders within the Group in compliance with the GDPR.

The BCRs have been adopted by the Data Protection Officer of the Group, who also has the responsibility to monitor the Group's compliance with the BCRs and to advice the Group on how to comply with the BCRs. The board of Wilh. Wilhelmsen Holding ASA and the GMT has committed to these BCRs.

All BCR Members, including their employees and representatives, are legally bound by-, and shall comply with and respect the BCRs. It is noted, for the sake of completeness, that the BCRs are made legally binding on the BCRs Members through the execution of the Intra-Group BCR Agreement.

2 Description of the data flows in the group - scope and applicability of the BCRs

2.1 Scope and applicability of the BCRs

As mentioned in Section 1, the BCRs shall be binding upon all BCR Members, including their employees and representatives. The list of BCR Members, including their contact details, is set out in Appendix 1 (Members of the BCRs) of the BCRs. Appendix 1 (Members of the BCRs) also sets out the structure of the Group.

These BCRs applies to the Processing of Personal Data wholly or partly by automated means and to the Processing other than by automated means of Personal Data which form part of a Filing System or are intended to form part of a Filing System. The BCRs are required in order to transfer (including by way of onward transfers) the Personal Data outside of EU/EEA, to a country that is not recognised by the EU Commission as ensuring an adequate level of protection, as well as to Process such transferred Personal Data.

These BCRs do not, and shall not, deprive Data Subjects of any rights or remedies provided to them under applicable data protection law or the GDPR.

These BCRs supersede all other privacy policies and guidelines that exist on the Effective Date within the Group to the extent such privacy policies and guidelines address the same issues as these BCRs.

The Group may implement sub-policies that are consistent with these BCRs. An overview of the Group's sub-policies, including other documents that form a part of these BCRs, are set out in Section 2.3. For the avoidance of doubt, in the event of a conflict between the main body of the BCRs and such documents, the main Body of the BCRs shall prevail.

2.2 Description of the data flows within the Group

The categories of Data Subjects affected by the Group's Processing may be divided into two broad categories:

(i) Personnel; and

(ii) Business Partners and other External Partners.

The material scope of the BCRs (i.e., data transfers, categories of Personal Data, the type of Processing and its purposes, and the types of Data Subjects affected) are further described in Appendix 2.

The Group operates internationally, and Personal Data will be transferred and in other ways Processed in order for the Group to operate its business.

Most transfers of Personal Data will take place from Norway, where the Group's head, Wilh. Wilhelmsen Holding ASA, is located. The above Personal Data transferred under these BCRs will be transferred to and from, respectively, importers and exporters both in the EU/EEA and outside of the EU/EEA (i.e., to all BCR Members) in accordance with these BCRs.

2.3 Overview of BCR Appendices and sub-policies

The following Appendices shall form an integral part of the BCRs:

Appendix #	Appendix name
Appendix 1	Members of the BCRs
Appendix 2	Material Scope of the BCRs

3 Definitions

BCR/BCRs shall mean the documents adopted as the Group's binding corporate rules.

Business Partners shall mean Data Subjects with whom the Group has a business relationship, either directly with the relevant Data Subject or with the relevant Data Subject's employer. Data Subjects that are also covered by the definition of Personnel shall be regarded as Personnel instead of Business Partners.

Competent Supervisory Authority means the Supervisory Authority competent for the Exporting BCR Member.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Law, the controller or the specific criteria for its nomination may be provided for by Law.

Data Protection Officer or DPO shall mean the Group's appointed Data Protection Officer as further detailed in Section 23 of these BCRs.

Data Subject means 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.

The EDPB shall mean the European Data Protection Board.

Effective Date shall mean the date on which these BCRs 12 January 2026.

Exporting BCR Member shall mean the BCR Member established in the EU/EEA, that is directly or indirectly transferring the relevant Personal Data to a BCR Member established in a Third Country (i.e. the "**Importing BCR Member**").

External Party shall mean any natural or legal person, public authority, agency or any other body outside of the Group.

EU/EEA shall mean the European Union and the European Economic Area.

EU/EEA Member State shall mean the Member States of the European Union and the Member States of the European Economic Area.

Filing System means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

General Data Protection Regulation or GDPR shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Group shall mean all of the entities included in Appendix 1.

Group Management Team or **GMT** means the group management team appointed by the Group and consisting of top executives from Wilhelmsen, inter alia the Group chief executive officer, and the Group chief financial officer.

Importing BCR Member is defined above, i.e. in the definition of the term "Exporting BCR Member".

International Organisation means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Intra-Group BCR Agreement means the intra-group agreement, set out in Appendix 7 to the BCRs, which the BCR Members have entered into for the purpose of ensuring that the BCRs are made legally binding on the Members.

Law shall mean EU/EEA law or the law of a EU/EEA Member state of the relevant BCR Member that Processes Personal Data.

Legitimate Purposes shall have the meaning as specified in Section 5.

Member(s) or BCR Member(s) shall mean an entity listed in Appendix 1.

Next of Kin shall mean the spouse, partner or child of Personnel.

NDPA shall mean the Norwegian Data Protection Authority.

Personal Data means any information relating to an identified or identifiable natural person (i.e. a Data Subject).

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

Personal Data Protection Administrators or **PDPAs** shall mean the Group's appointed Personal Data Protection Administrators as further detailed in Appendix 6 (Personal Data Protection Management in the Wilhelmsen Group), and inter alia consisting of the Group PDPA, including the Global and Local PDPAs.

Personnel shall mean employees, candidates and former employees of the Group. The term Personnel also includes present and former consultants and employees of Business Partners providing services to the Group through the Group's information technology systems or from the Group's premises, in the same manner as employees.

Processing/Process 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Special Categories of Personal Data shall mean personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Supervisory Authority means an independent public authority established by a Member State for the purpose of being responsible for monitoring the application of the GDPR, in order to protect the fundamental

rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU/EEA.

Supervisory Authority concerned means a Supervisory Authority which is concerned by the processing of personal data because:

a) The Controller or processor is established on the territory of the Member State of that Supervisory Authority;

b) Data subjects residing in the Member State of that Supervisory Authority are substantially affected or likely to be substantially affected by the processing; or

c) A complaint has been lodged with that Supervisory Authority.

Supplementary Measure shall have the meaning ascribed to such term in Section 28 of the BCRs.

Third Country means a country outside the EU/EEA.

Third Party means a natural or legal person, public authority, agency or body other than the Data Subject, the Controller, the processor and persons who, under the direct authority of the Controller or processor, are authorised to Process Personal Data.

Transfer Impact Assessment or TIA shall mean the assessment described in Section 28 of the BCRs.

WWH shall mean Wilh. Wilhelmsen Holding ASA.

4 Legal basis for Processing of Personal Data

4.1 Introduction

The Group shall make sure that all Processing of Personal Data only takes place for Legitimate Purposes, has a legal basis, and is Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

4.2 Legal basis for Processing of Personal Data

Personal Data relating to Personnel, Business Partners and other External Parties are Processed by the Group for Legitimate Purposes on the following legal basis:

(i) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;

(ii) Processing is necessary for Legitimate Purpose pursued by the Group or by 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, in particular where the Data Subject is a child;

(iii) The Data Subject has given consent to the Processing of his or her Personal Data for one or more specific purposes;

(iv) Processing is necessary for compliance with a legal obligation, based on EU/EEA or EU/EEA Member State law to which the relevant Controller is subject.

(v) Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person; or

(vi) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller. The basis for this processing must be laid down by EU/EEA or EU/EEA Member State law to which the Controller is subject.

The following requirements will apply when the Group's Processing is based on consent (cf. item (iii) above):

(i) The consent must be a freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her;

(ii) The relevant Controller shall be able to demonstrate that the Data Subject has consented to Processing of his or her Personal Data;

(iii) If the Data Subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of these BCRs shall not be binding.

(iv) The Data Subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of Processing based on consent before its withdrawal. Prior to giving consent, the Data Subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

(v) When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the Processing of Personal Data that is not necessary for the performance of that contract.

4.3 Legal basis for Processing of Special Categories of Personal Data

As a starting point, the Processing of Special Categories of Personal Data is prohibited. The Group can, however, provided that Legitimate Purposes are documented, Process Special Categories of Personal Data on the following legal basis:

(i) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Group or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorized by Law or a collective agreement pursuant to Law providing for appropriate safeguards;

(ii) Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;

(iii) Processing relates to Personal Data which are manifestly made public by the Data Subject;

(iv) Processing is necessary for the establishment, exercise or defence of legal claims;

(v) The Data Subject has given explicit consent to the Processing of those Personal Data for one or more specified purposes, except where the Group cannot rely upon the Data Subject's consent under Law;

(vi) Processing is 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 Law or pursuant to contract with a health professional and subject to following conditions and safeguards:

a) The aforementioned Personal Data may only be Processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Law or rules established by national competent bodies or by another person also subject to an obligation of secrecy Law or rules established by national competent bodies.

4.4 Processing of Personal Data relating to criminal convictions and offences

Processing of Personal Data relating to criminal convictions and offences or related security measures based on Section 16 of the BCRs shall be carried out by the Group only when the processing is authorised by Law providing for appropriate safeguards for the rights and freedoms of Data Subjects.

4.5 Consultation

If it is doubtful whether Processing has legal basis in accordance with this Section 4, and in any event if the Group intends to Process Personal Data on the basis of Consent, the Data Protection Officer shall be consulted before any Processing starts.

4.6 Data protection in HR applications

This Section 4 and the main body of the BCRs is supplemented by Appendix 3 of the BCRs (Personal data protection in global HR applications procedure).

Appendix 3 applies to Personal Data processed in the Group's global HR application, currently Workday.

5 Requirements regarding purposes for Processing Personal Data – purpose limitation and data minimization

5.1 Legitimate Purposes and data minimization

The Group shall comply with the principle of purpose limitation. Personal Data shall therefore be collected for specified, explicit and Legitimate Purposes and not further Processed in a manner that is incompatible with those purposes.

The Group Processes Personal Data about Personnel, Business Partners and other External Partners. for the following specific Legitimate Purposes:

(i) Human resources and management of Personnel.

This purpose includes Processing that is necessary for the performance of an employment/contractor contract or a prospective employment/contractor contract, including but not limited to Processing related to recruitment and deployment, performance and development, management and administration of payments, compensations, benefits and rewards, tax issues, career planning, evaluations, training, travel and expenses, outplacement, communication with personnel, employee/contractor relations, change management and continuous improvement.

(ii) Health, safety, and security.
This purpose includes Processing that is necessary to protect health, provide safety and security related to Personnel and their next of kin or the public.

(iii) Planning and control measures.
This purpose includes Processing related to activities such as scheduling timetables, recording time, conducting surveys, controls, internal audits and investigations.

(iv) Business operation and protection of business interests and security.
This purpose includes Processing in relation to business operation and protection of business interests and security; e.g. information security, logging, conduction of controls, surveys, analysis, reports and managing of daily operations and transactions/possible transactions involving the Group.

(v) Compliance with legal obligations and protection of legal position.
This purpose includes Processing of Personal Data that is necessary in order to ensure compliance with legal obligations and/or to protect a legal position of the Group.

(vi) Management and administration of business relationships.
This purpose includes Processing of Personal Data that is necessary with regard to relationships with business partners and other Third Parties. The purpose includes management and administration of contact information, compensation, payments, tax issues, evaluations, training, travel and expenses, recruiting and other circumstances related to business relationships.

5.2 Consultation

In case of doubt, the Data Protection Officer shall be consulted before any Processing starts, to decide whether Personal Data, and in particular, Special Categories of Personal Data, may be Processed on the basis of the provisions in Section 5.1.

6 Records of processing activities

The Group shall maintain records regarding all categories of Processing activities under the Group's responsibility. These records shall be maintained in writing, including in electronic form, and shall be made available to the Supervisory Authority on request.

Where the Group and/or a BCR Member acts as a Controller, the relevant records shall include the following information:

(i) The name and contact details of the Controller and, where applicable, the joint Controller, the Controller's representative and the data protection officer;

(ii) The purposes of the Processing;

(iii) A description of the categories of Data Subjects and of the categories of Personal Data;

(iv) The categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organizations;

(v) Where applicable, transfers of Personal Data to a third country or an international organization, including the identification of that third country or international organization the documentation of suitable safeguards;

(vi) Where possible, the envisaged time limits for erasure of the different categories of data; and

(vii) Where possible general description of the technical and organizational security measures implemented by the Member.

Where the Group and/or a BCR Member acts as a Processor, the relevant records shall include the following information:

(i) The name and contact details of the Processor or Processors and of each Controller on behalf of which the Processor is acting, and, where applicable, of the Controller's or the Processor's representative, and the data protection officer;

(ii) The categories of Processing carried out on behalf of each Controller;

(iii) Where applicable, transfers of Personal Data to a third country or an international organization, including the identification of that third country or international organization the documentation of suitable safeguards;

(iv) Where possible, a general description of the technical and organizational security measures implemented (cf. inter alia Section 16 below).

7 Data minimization, data accuracy and storage limitation

7.1 Data minimization and accuracy

Personal data shall at any time be adequate, relevant and limited to what is necessary in relation to the Legitimate Purposes for which they are processed (data minimization).

The Group shall also ensure that Personal Data is accurate and, where necessary, kept up to date (accuracy). The Group shall therefore take every reasonable step to ensure that Personal Data which are inaccurate, are erased or rectified without undue delay.

If the Group sees that it is necessary that the Data Subjects update their own Personal Data in order to ensure that the Personal Data are accurate and kept up to date, a request shall be sent to the Data Subject on a regular basis.

7.2 Storage limitation

The Group shall only Process Personal Data that is adequate for, relevant and not excessive to the Legitimate Purposes.

When retention is no longer necessary in accordance with this Section 7.1 and Section 7.2, Personal Data shall be:

(i) Securely deleted or destroyed; or

(ii) Anonymized.

With respect to Personal Data of the Group's Personnel, the Group will observe the following general deletion routines:

(i) Unnecessary information and Personal Data shall be removed from reports or similar documentation after the completion of appraisal/ conversations on absence due to sickness;

(ii) Unnecessary information and Personal Data shall be deleted upon termination of the employment;

(iii) Annual assessment on the need for continued storage of Personal Data shall be carried out after termination of employment;

(iv) No Personal Data which are not relevant for the administration of the employment shall be stored;

(v) Information that an employee is suspected of criminal offences (e.g. allegations of fraud) shall be deleted immediately if it turns out that the suspicion was not correct. Otherwise, such information shall be deleted when the Legitimate Purpose of the Processing (typically conducting necessary sanctions under labour law) is achieved;

(vi) The Group's IT-department shall expedite deletion of data in accordance with this BCR and established sub-policies.

With respect to the Personal Data of Business Partners and External Parties, the Group will observe the following deletion routines:

(i) Unnecessary Personal Data shall be removed continuously and upon termination of the relationship with the relevant Business Partner and/or External Party;

(ii) Annual assessment on the need for continued storage shall be carried out after the assessment upon termination of the relationship with the relevant Business Partner and/or External Party;

(iii) The Group's IT-department shall expedite deletion of data in accordance with this BCR and established sub-policies.

Where appropriate, the Group's information systems shall be set for automatic deletion before the Group's deletion routines set out in sub-policies.

As mentioned above, anonymization of Personal Data may be an alternative to deletion. Personal Data is regarded as anonymized when it is no longer possible to retrieve the link between the Data Subject and the relevant data.

The foregoing provisions shall not apply where the retention of Personal Data is required under applicable Law or Third Country law (i.e., where the Personal Data has been transferred and is subsequently Processed by an Importing BCR Member). For clarity, the latter described scenario is without prejudice to Section 28 of these BCRs, in particular the requirement for the Importing BCR Member to notify the Exporting BCR Member, throughout the duration of Importing BCR Member's BCR membership, if it has reason to believe that it is or has become subject to Third Country laws or practices not in line with the requirements under Section 28 of the BCRs.

Before any Processing of personal data is taken, as far as practicable, it shall be considered whether there are statutory requirements determining how long Personal Data are to be stored and how long it is necessary to keep the Personal Data in order to fulfil the relevant purpose. Unless otherwise specified, the deletion deadline is determined based on what the Group considers as the required storage time.

7.3 Day to day responsibility

The Group's Personal Data Protection Administrator shall ensure that Personal Data is deleted continuously in accordance with this Section 7 and any applicable sub-policies. The DPO shall monitor the compliance with the deletion routines. The DPO shall annually request confirmation from the Global and Local Personal Data Protection Administrators that Personal Data has been deleted in accordance with this Section 7 and any applicable sub-policies.

8 Transparency and information rights

8.1 General transparency and communication requirements

The Group shall take appropriate measures to provide any information referred to in this Section 8 and communication under Sections 9 to 15 below to Data Subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

The Group shall facilitate the exercise of Data Subject rights under Sections 9 to 15 below.

The Group shall provide information on action taken on a request under Sections 9 to 15 below to the Data Subject without undue delay, and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Group shall inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the Data Subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the Data Subject.

If the Group does not take action on the request of the Data Subject, the Group shall inform the Data Subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a Supervisory Authority and seeking a judicial remedy.

Information provided under this Section 8 and any communication and any actions taken under Sections 9 to 15 and Section 18.3 of these BCRs shall be provided free of charge. Where requests from a Data Subject

are manifestly unfounded or excessive, in particular because of their repetitive character, the Group may either:

(i) Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(ii) Refuse to act on the request.

The Group shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. Where the Group has reasonable doubts concerning the identity of the natural person making the request referred to in Sections 9 to 15 below, the Group may request the provision of additional information necessary to confirm the identity of the Data Subject.

8.2 Information requirements

8.2.1 Information to be provided where Personal Data are collected from the Data Subject

When collecting Personal Data from the Data Subject, the Group shall first inform the Data Subject of the following:

- Name and address of the Controller and his / her representative;
    - The term "Controller" in this bullet point means the legal entity in the Group which is responsible for the relevant Processing of Personal Data.
- Contact information of the Group's Data Protection Office.
- Purpose of the Processing.
- Legal basis for the Processing.
    - Where the processing is based on the legitimate interest test (cf. Section 4.2(ii) above), the legitimate interest pursued must be described.
- The recipients or categories of recipients of the Personal Data (if any).
- If possible, how long the Personal Data will be stored or, if this is not possible, the criteria used to determine storage time.
- Where relevant, the fact that the Group will transfer Personal Data to a Third Country or an International Organization and whether the EU Commission has made a decision on the adequacy of the level of protection or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
- The right to request access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability.
- The right to lodge a complaint with the Supervisory Authority.

- The right to withdraw a consent at any time, if the Processing is based on the consent of the Data Subject.

- Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter 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.

- The existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

- Subject to Sections 4, 5 7 of these BCRs, if the Group is to Process Personal Data for a purpose other than originally collected, the Group shall provide the Data Subject with information about the new purpose, as well the information listed in the bullet points above, before the new processing takes place.

The above listed information requirements do not apply if the Data Subject already has the information.

8.2.2 Information to be provided where Personal Data have not been obtained from the Data Subject

If the Group has not obtained the Personal Data from the Data Subject, the Group shall provide the Data Subject with the information set out in Section 8.2.1. The Group shall in addition provide the following information to the Data Subject:

- The categories of Personal Data which will be Processed.

- Where Personal Data was obtained and, if relevant, whether the information is collected from publicly available sources.

The information requirements set forth in this Section 8.2.2 shall not apply insofar as:

- The Data Subject already has the information.

- Notifications will be impossible or will require a disproportionate amount of effort, or if notice will make it impossible or seriously impair the fulfilment of the purpose of the Processing. In such cases, the Group shall take appropriate measures to protect the Data Subject's rights and freedoms, as well as legitimate interests, including making the information publicly available.

- The collection or disclosure of Personal Data is expressly provided for in Law and which establishes appropriate measures to protect the legitimate interests of the Data Subject.

- Where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by Law, including a statutory obligation of secrecy.

8.2.3 When should the information be given?

If the Personal Data is collected from the Data Subject, the Group shall provide the information listed in Section 8.2.1 at the time when the Personal Data is collected.

If the Group has not obtained the Personal Data from the Data Subject, the Group shall provide the Data Subject the information listed in Section 8.2.2 within a reasonable period of time and no later than one (1) month after the Personal Data was obtained. If the Personal Data are to be used for communication with the Data Subject, the aforementioned information shall be given no later than the date of the first communication with the Data Subject. If the Personal Data is intended to be communicated to another recipient, the information listed in Section 8.2.2 shall be provided to the Data Subject at the latest when the Personal Data is disclosed for the first time.

8.3 Access to the BCRs

8.3.1 How the BCRs will be provided to Data Subjects

The Group will provide all Data Subjects whose Personal Data is Processed under these BCRs with an abridged/shortened version of the BCRs.

The abridged version of the BCRs will, in this respect, be published and made available to all Personnel on the Group's intranet on the Effective Date. For the avoidance of doubt, the Group's DPO and the PDPAs will, at all times, have access to the full version of the BCR.

The abridged version of the BCRs will also be published and made available for all Data Subjects on the Group's website.

8.3.2 The list of elements that must be included in the abridged version of the BCRs

The abridged version of the BCRs will be kept up-to-date, and presented to Data Subjects in a clear, plain, intelligible and transparent way.[1]

Furthermore, the abridged version of the BCRs will at all times include the full version (i.e. not a summary version) of the elements of the BCRs regarding:

(i) The scope of the BCRs (cf. Sections 2.1-2.2, as well as Appendix 1 (Members of the BCRs) and Appendix 2 (Material Scope of the BCRs));

(ii) The Group's liability under the BCRs (cf. Section 28.2);

(iii) The data protection principles, including without limitation the elements regarding the lawfulness of the Processing, security, data breach notifications and restrictions on onward transfers (cf. Sections 4, 5, 7, 8, 16, 17, 18, 21, and 22);

(iv) The rights of the Data Subjects (cf. Sections 8-15);

(v) Third party beneficiary rights, including the means to exercise those rights (cf. Section 26); and

(vi) The definitions used in the BCRs (cf. Section 3).

[1] For clarity, the full version of the BCRs will also, at all times, use clear and plain language, ensuring that Personnel in charge of applying the BCRs can fully understand them.

8.4 Consultation

In case of doubt as to how the requirements set forth in this Section 8 shall be fulfilled, the Data Protection Officer shall be consulted.

9 Procedure for handling Data Subject's requests for access to Personal Data

9.1 Purpose

The purpose of this Section 9 is to ensure that Data Subjects are given access to Personal Data Processed by the Group, including information about the relevant Processing and information about the Data Subject's rights in relation to the Processing.

9.2 Right of access by the Data Subject

A Data Subject shall have the right to obtain confirmation as to whether or not the Group Processes Personal Data about him/her and, if so, access to the Personal Data in addition to the following information:

- The purpose of Processing;
- The categories of Personal Data Processed;
- Any recipients or categories of recipients to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organisations;
- If possible, how long the Personal Data will be stored or, if this is not possible, the criteria used to determine storage time;
- The existence of the right to request from the Group rectification or erasure of Personal Data or restriction of Processing of Personal Data concerning the Data Subject or to object to such Processing;
- The right to lodge a complaint with a Supervisory Authority;
- Any available information about where Personal Data is obtained from if the Personal Data is not collected from the Data Subject;
- Possible use of automated decision-making, including profiling, including information about the logic behind such profiling as well as the significance and the expected consequences this will have for the Data Subject; and
- Where Personal Data are transferred to a third country (countries outside the EU/EEA), the appropriate safeguards implemented in relation to the transfer.

The Group shall furthermore provide a copy of the Data Subject's Personal Data undergoing Processing. Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the relevant copy of the Data Subject's Personal Data shall be provided in a commonly used

electronic form. The Data Subject's right to receive a copy of the Personal Data shall not adversely affect the rights and freedoms of others.

The Group shall ensure that the information which is to be provided to the Data Subject is sent in a secure manner (for example, using encrypted email), if the information is to be sent electronically (e.g. by using e-mail).

The representative of the Group receiving a request for access shall notify the DPO immediately and no later than 24 hours after receiving the request. The DPO is responsible for ensuring that the access is granted to the Data Subject, but the practical implementation may be delegated further.

10 Right to rectification of Personal Data

10.1 Purpose

The purpose of this Section 10 is to ensure that the Group in an adequate and timely manner responds to- and observes the Data Subject's right to rectification.

10.2 Data Subject's right to rectification

As further described in Section 7, Personal Data shall be accurate and, where necessary, kept up to date. The Group shall take every reasonable step to ensure that Personal Data that are inaccurate, having regard to the Legitimate Purposes for which they are processed, are erased or rectified without delay (‘accuracy’).

Inaccurate Personal Data concerning the Data Subject shall also be rectified/corrected upon the request of the relevant Data Subject.

A request for rectification of Personal Data from a Data Subject shall be immediately forwarded to the DPO. The DPO shall further ensure that the Group rectifies/corrects the inaccurate Personal Data. however, the practical follow-up can be delegated.

Correction of incorrect or incomplete Personal Data that may be of significance for documentation purposes, shall be done by clearly marking and supplementing the information with the correct information. The Data Subject also has the right, if he/she so desires, to submit a supplementary statement of information that he or she considers necessary.

Rectification/Correction shall be made without undue delay and no later than 1 month from the date the Group received the request (cf. also Section 8.1 above), or from the time the Group became aware of the inaccurate Personal Data.

11 Procedure for handling the right to erasure (right to be forgotten)

11.1 Purpose

The purpose of the procedure is to ensure that the Group complies with the Data Subject's request for his/her right to erasure (right to be forgotten).

11.2 Right to erasure (right to be forgotten)

The Data Subject has the right to the erasure of his or her Personal Data, and the Group shall have the obligation to erase Personal Data without undue delay where one of the following grounds applies:

- Personal Data is no longer necessary in relation to the Legitimate Purpose of the Processing;
- The Data Subject withdraws his/her consent, in cases where consent of the Data Subject is the legal basis for the Processing;
- The Data Subject has an objection to the Processing and there are no legitimate reasons for the Processing that exceeds the objection;
- The purpose of the Processing is direct marketing or profiling and the Data Subject objects to the Processing;
- Personal Data has been processed unlawfully;
- Personal Data should be deleted in order to comply with a legal obligation under Law; or
- The Personal Data have been collected in relation to the offer of information society services directly to a child, on the basis of the Data Subject's consent.

If the Group has made the relevant Personal Data public and is obligated to erase the Personal Data, reasonable measures shall be taken to inform the Controller Processing the Personal Data that the Data Subject has requested that all links, copies or representations of the relevant Personal Data shall be erased.

The Group is not required to delete Personal Data to the extent that the Processing of Personal Data is necessary:

- To exercise the right to freedom of expression and information;
- In order to comply with a legal obligation which requires processing under Law or to perform a task in the public interest or in the exercise of official authority vested in the Group;
- For Archiving purposes; or
- For the establishment, exercise and defence of legal claims.

If the Group receives a request from a Data Subject who wishes to exercise his/her right to erasure, or the Group discovers that Personal Data shall be erased in accordance with the provisions above, the DPO shall be contacted immediately and no later than 72 hours after receiving the request. The DPO, in consultation with the Group Data Protection Administrator is responsible for ensuring that the Group erases the relevant Personal Data in accordance with this Section 11. However, the practical follow-up can be delegated to others.

12 Procedure relating to the Data Subject's right to restriction of Processing

12.1 Purpose

The purpose of this Section 12 is to ensure that the Group complies with the Data Subject's right to restriction of Processing, and responds to the Data Subject's request for such restriction in an adequate manner.

12.2 Right to restriction of Processing

The Data Subject shall have the right to obtain from the Group restriction of Processing where one of the following applies:

(i) The accuracy of the Personal Data is contested by the Data Subject, for a period enabling the Group to verify the accuracy of the Personal Data;

(ii) The Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;

(iii) The Group no longer needs the Personal Data for the Legitimate Purposes, but is required by the Data Subject for the establishment, exercise or defence of legal claims; or

(iv) The Data Subject has objected to processing pending the verification whether the legitimate grounds of the Group override those of the Data Subject.

Where Processing has been restricted under this Section 12, such Personal Data shall, with the exception of storage, only be Processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU/EEA or of its Member State.

A Data Subject which obtains restrictions of Processing, shall be informed by the Group before the restriction of Processing is lifted.

13 Notification obligations relating to rectification, erasure or restriction

The Group shall communicate any rectification or erasure of Personal Data or restriction of Processing carried out in accordance with these BCRs to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. Furthermore, the Group shall inform the Data Subject about those recipients if the Data Subject requests it.

14 Procedure for data portability

14.1 Purpose

The purpose of this Section 14 is to ensure that the Group complies with the requirement to provide data portability to the Data Subject, .

14.2 Right to data portability

If the legal basis for the Group's Processing of Personal Data is consent or fulfilment of a contract with the Data Subject, and the Processing is carried out by automated means, the Data Subject has the right to

receive his/her Personal Data Processed by the Group in a structured, commonly used and machine-readable format. The Data Subject may alternatively, and on the same grounds, request that the Group transmits his or her Personal Data directly to another Controller.

The right to data portability shall not adversely affect the rights and freedoms of others.

The representative of the Group that receives a data portability request from a Data Subject shall contact the DPO immediately. The DPO is responsible for ensuring that the Group observers the Data Subject's right to data portability. However, the practical follow-up can be delegated.

15 Right to object and automated individual decision-making

The Data Subject has the right to object to the Group's Processing on grounds relating to his or her particular situation to Processing of the Data Subject's Personal Data which is based on the legal bases described in Sections 4.2(vi) or 4.2(ii) of these BCRs, including profiling based on these legal bases. The Group shall no longer Process the Personal Data unless the Group demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

Where Personal Data are processed for direct marketing purposes, the Data Subject shall have the right to object at any time to Processing of Personal Data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the Data Subject objects to the Processing of the Data Subject's Personal Data for direct marketing purposes, the Personal Data shall no longer be Processed for such purposes.

At the latest at the time of the first communication with the Data Subject, the right referred to in sub-paragraphs 1 and 2 of this Section 15 shall be explicitly brought to the attention of the Data Subject (and shall be presented clearly and separately from any other information) by the Group.

In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the Data Subject may exercise his or her right to object by automated means using technical specifications.

The Data Subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

16 Security of Processing and confidentiality

16.1 Introduction

The Group shall Process Personal Data in a manner which ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The measures in place shall always ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected, having regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing.

Special Categories of Personal Data are Processed with enhanced security measures.

Personnel with access to Personal Data must only be authorized to access Personal Data to the extent that this is necessary, in order for them to perform their assigned tasks, and otherwise in accordance with these BCRs and Law.

Personnel who access Personal Data must have committed themselves to confidentiality or be under an appropriate statutory obligation of confidentiality.

16.2 High level security measures

The Group has implemented security objectives and strategies, which constitute the framework for data and information security which must be complied with by the Group in relation to the processing of personal data.

The following high level security measures shall at all times be implemented and maintained by the Group:

(i) Security measures shall be implemented so that persons outside of the Group cannot cause security incidents/breaches;

(ii) Access to systems and information shall only be given on a need to know basis. Unauthorized access may have severe consequences for the persons concerned and shall be actively prevented;

(iii) Information shall be kept accurate and not changed or altered unintended and without legal basis;

(iv) Systems and services are resilient and available when authorized persons need access to information;

(v) Personal Data shall be protected against all threats, both internal and external as well as both intentional and unintentional;

(vi) Persons or systems shall not cause security incidents/breaches, neither within the Group nor against other businesses or individuals;

(vii) If discrepancies and/or data breaches occur, the reason for these shall be clarified and rectified;

(viii) Routines for handling of discrepancies and Personal Data Breaches shall be in place;

(ix) Requirements pursuant to applicable Law shall be complied with; and

(x) Employees and other personnel with access to the Group's IT systems shall have sufficient competence to comply with the Group's security objectives.

Additional security measures which shall be implemented and maintained by the Group are set out in Appendix 5 (Cyber Security Policy) to these BCRs.

17 Data protection by design and by default

17.1 Data protection by design

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the Processing, the Group shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data-protection principles, in an effective manner and to integrate the necessary safeguards into the Processing in order to meet the requirements of the GDPR and protect the rights of Data Subjects.

17.2 Data protection by default

The Group shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific Legitimate Purpose of the Processing are Processed. That obligation applies to:

(i) The amount of Personal Data collected;

(ii) The extent of their Processing; and

(iii) The period of their storage and their accessibility. In particular,

(iv) Such measures shall ensure that by default Personal Data are not made accessible without the individual's intervention to an indefinite number of natural persons.

18 Personal Data Breach

18.1 General obligations related to Personal Data Breaches

All Group employees shall be responsible for reporting Personal Data Breaches from current procedures and other security related events to the person responsible for the particular area or security officer.

Personal Data breaches, security events and contingency events often require a quick response and must be reported promptly, orally or by email.

All employees/personnel shall report in accordance with the provisions in this Section 18 if they become aware that Personal Data are processed contrary to the BCRs or if there is otherwise a basis for suspicion of or an actual breach of security related to Personal Data.

The Group prohibits retaliation against anyone for making a good-faith report. All reports of suspected violations are taken seriously and shall be followed up, as appropriate. Reports may be made anonymously.

The Personal Data Breach shall be immediately reported to the DPO and the Exporting BCR Member. The notification shall contain an overview of the status of the Personal Data Breach and corrective measures initiated. The DPO, in consultation with the Global Personal Data Protection Administrator is responsible for ensuring that the Personal Data Breach is corrected and appropriately followed up the Group. However, the practical follow-up of this can be delegated to others.

If Personal Data Breaches and other security discrepancies are reported, detected or suspected, the Group Personal Data Protection Administrator shall inform IT:

(i) IT shall put into effect immediate measures if this is not already done, including for the purpose of assessing consequences of the Personal Data Breach;

(ii) IT shall put into effect corrective measures for the purpose of mitigating or reducing the risks associated with the Personal Data Breach; and

(iii) IT shall assess whether the corrective measures are working as intended, or whether further corrective measures should be implemented.

All burglaries and attempted burglaries and cybercrimes must be reported to the police.

The DPO shall document all Personal Data Breaches. This documentation shall include the following information:

- Date;
- Description of Personal Data Breach;
- Likely consequences of the Personal Data Breach;
- Source;
- Department / system area;
- Preliminary assessment of the likelihood of the Personal Data Breach resulting in risk to the rights and freedoms of natural persons;
- Status;
- Follow-up action/ corrective action;
- Responsible for follow-up; and
- Deadline for next follow-up point

Without limiting Sections 18.2 and 18.3 below, the above documentation shall be made available to the Competent Supervisory Authority, upon request.

18.2 Notification of a Personal Data Breach to the Supervisory Authority

Unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons, the Group shall notify the Competent Supervisory Authority without undue delay and, in any event, not later than 72 hours after the Group became aware of the Personal Data Breach. If the Personal data breach is not reported within 72 hours, the notification must be accompanied with a written reason for the delay.

However, if the BCR Member that became aware of the Personal Data Breach is acting as Processor on behalf of another BCR Member (i.e. the Controller) with respect to the affected Personal Data, then the

Processor BCR Member shall first notify the Controller BCR Member. This notification shall be made without undue delay after the Processor BCR Member became aware of the Personal Data Breach.

The notification to the Competent Supervisory Authority shall contain the following information:

(i) Description of the nature of the security breach, including, if possible, the categories and the approximate number of Data Subjects concerned and approximate number of Personal Data records concerned;

(ii) Name and contact information of the DPO or other contact person (if more appropriate);

(iii) Description of the likely consequences of the privacy breach; and

(iv) Description of the measures taken or proposed by the Group to address the Personal Data Breach, including, if appropriate, measures to mitigate its potential adverse effects.

If it is not possible to provide the above information together, the information can be provided gradually without unnecessary further delay.

The Group shall document any Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken by the Group. The documentation shall enable the Supervisory Authority to verify compliance with this Section 18.

18.3 Communication of a Personal Data Breach to the Data Subject

If it is likely that the Personal Data Breach will entail a high risk to the rights and freedoms of natural person, the Group shall notify the Data Subject of the Personal Data Breach without undue delay. The communication to the Data Subject shall describe in a clear an plain language the nature of the Personal Data Breach, and at least the information and measures referred to in Section 18.2, items (ii) – (iv).

However, the communication to the Data Subject is not required if one of the following conditions is met:

- The Group has implemented appropriate technical and organisational protection measures, and those measures were applied to the Personal Data affected by the Personal Data Breach (in particular those that render the Personal Data unintelligible to any person who is not authorised to access it, such as encryption);
- The Group has implemented subsequent security measures that ensure that the high risk of the Data Subject's rights and freedoms is no longer likely to materialise; or
- It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner.

19 Data protection impact assessment

19.1 Data Protection Impact Assessment

As further described in Section 16, the Group shall regularly assess the exposure to potential risks inherent to the Processing, and will implement measures to mitigate those risks. These measures shall ensure an

appropriate level of security, taking into account available technology, the costs of implementation in relation to the risk and the nature of the personal data to be protected.

Where a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons, the Group shall, prior to the Processing, carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data. A single assessment may address a set of similar Processing operations that present similar high risks.

The data protection impact assessment shall as a minimum include:

- A systematic description of the envisaged Processing operations and the purposes of the Processing, including, where applicable, the legitimate interest pursued by the Group;
- An assessment of the necessity and proportionality of the Processing operations in relation to the purposes;
- An assessment of the risks to the rights and freedoms of Data Subjects; and
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with the GDPR and the BCRs taking into account the rights and legitimate interests of Data Subjects and other persons concerned.

The Group's assessment of whether it is likely that the Processing of Personal Data may pose a high risk to the rights and freedoms of natural persons, in addition to the results of any data protection impact assessment must be documented.

The results of the data protection impact assessment shall furthermore be reported to the Group Personal Data Protection Administrator, which will report this to the Group Management Team and the Data Protection Officer.

The Group shall annually review whether the relevant Processing is performed in accordance with the data protection impact assessment, including when there is a change of the risk represented by Processing operations.

19.2 Responsibility and governance

The Group Personal Data Protection Administrator is responsible for ensuring that the Group's general data protection impact assessment is reviewed on a yearly basis and updated when necessary, including when there is a change of the risk represented by Processing operations. The Data Protection Officer shall be responsible for monitoring the performance of the Group's data protection impact assessments. If the Processing of a BCR Member is likely to result in a high risk to the rights and freedoms of natural persons, then that BCR Member shall be responsible for carrying out a data protection impact assessment in accordance with Section 19.1. As mentioned above, the results of the data protection impact assessment conducted by the relevant BCR Member shall be reported to the Group Personal Data Protection Administrator.

19.3 Consultation

The Group shall seek the advice of the DPO when carrying out a data protection impact assessment.

20 Prior consultation

If the data protection impact assessment indicates that the Processing of Personal Data would result in a high risk in the absence of measures taken by the Group to mitigate the risk, a written request for prior consultation must be sent to the Competent Supervisory Authority. The request to the Competent Supervisory Authority shall include the following information:

- The respective responsibilities of the Controller, and Processors involved in the Processing.
- The purposes and means of the intended Processing.
- The measures and safeguards provided to protect the rights and freedoms of Data Subjects pursuant to the GDPR.
- The contact details of the DPO.
- The data protection impact assessment conducted in accordance with Section 19.
- Any other information requested by the Competent Supervisory Authority.

The DPO must be contacted for assistance before contacting the Supervisory Authority for a "prior consultation".

21 Engaging internal Processors (within the Group)

This Section 21 sets forth the requirements that apply to the extent a Controller within the Group wishes to engage a Processor within the Group to Process Personal Data on behalf of the Controller.

It is noted, for the sake of clarity, that the Controller must ensure that the Legitimate Purposes set forth in Section 5 above are complied with, when the Controller shares Personal Data with a Processor.

The Controller shall ensure that the Processor provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of the GDPR and the BCRs and ensure the protection of the rights of the Data Subject.

Processing by a Processor shall be governed by a data processing agreement, that is binding on the Processor with regard to the Controller and that sets out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Controller.

The data processing agreement shall stipulate, in particular, that the Processor:

(i) Processes the Personal Data only on documented instructions from the Controller, unless required to do so by Law to which the Processor is subject; in such a case, the Processor shall

inform the Controller of that legal requirement before Processing, unless that Law prohibits such information on important grounds of public interest;

(ii) Ensures that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(iii) Takes necessary measures to ensure the security of Processing;

(iv) Does not engage another Processor without prior authorization from the Controller;

(v) Taking into account the nature of the Processing, assists the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights, such as right of information and access;

(vi) Assists the Controller in ensuring security of Personal Data;

(vii) At the choice of the Controller, deletes or returns all the Personal Data to the Controller after the end of the provision of services relating to Processing, and deletes existing copies unless otherwise provided by Law (it being understood that Section 29.2 last sub-paragraph shall apply correspondingly in the event the Processor, being an Importing BCR Member, is prohibited from deleting or returning the Personal Data due to applicable Third Country Law); and

(viii) Makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Section 21 and allows for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

The head of the IT department shall be involved if the data processing agreement in question concern the operation or maintenance of the Group's information systems.

The Group Personal Data Protection Administrator is responsible for ensuring that the Group enters into data processing agreements before the Group engages a Processor to Process Personal Data on behalf of the Group.

22 Sharing Personal Data with external Processors and Controllers (outside the group)

22.1 External Processors located in the EU/EEA or a country recognised by the EU Commission as ensuring an adequate level of protection

If the Group engages external Processors (outside the Group) located in the EU/EEA or in a country recognised by the EU Commission as ensuring an adequate level of protection, a written data processing agreement must be entered into, in accordance with the requirements set out in Section 21, above.

22.2 External Processors located outside of EU/EEA and in a country that is not recognised by the EU Commission as ensuring an adequate level of protection

22.2.1 Respect the EU/EEA rules on international transfers

The Group shall ensure that the rules in the GDPR on international transfers are complied with when Personal Data are transferred to external Processors (outside of the Group) located outside of EU/EEA, in a country that is not recognised by the EU Commission as ensuring an adequate level of protection.

In the absence of an adequacy decision from the EU Commission, the Group shall only transfer Personal Data to such external Processors (outside of the Group), if the Group has provided appropriate safeguards, and on condition that enforceable Data Subject Rights and effective legal remedies for data subjects are available. Such appropriate safeguards may in particular be:

(i) Standard data protection clauses adopted by the EU Commission in accordance with the applicable examination procedure;

(ii) Standard data protection clauses adopted by a Supervisory Authority and approved by the EU Commission pursuant to the applicable examination procedure; or

(iii) A legally binding and enforceable instrument between public authorities or bodies.

Furthermore, in the absence of both an adequacy decision and appropriate safeguards, a transfer of Personal Data to an external Processor (outside of the EU/EEA) shall only take place (i.e. on a exceptional basis) on one of the following conditions:

(iv) The transfer is necessary for the performance of a contract between the Data Subject and the Group or the implementation of pre-contractual measures taken at the Data Subject's request;

(v) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Group and another natural or legal person;

(vi) The Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards;

(vii) The transfer is necessary for important reasons of public interest recognised in Law;

(viii) The transfer is necessary for the establishment, exercise or defence of legal claims; or

(ix) The transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.

22.2.2 Respect of the provisions in the GDPR relating to Processors

The Controller and the Processor must enter into an agreement as set out in Section 21, above.

22.3 International organisations and Controllers located outside of EU/EEA in a country that is not recognised by the EU Commission as ensuring an adequate level of protection

All transfers of Personal Data to an International Organization or to external Controllers (outside of the Group) located outside of EU/EEA in a country that is not recognized by the EU Commission as ensuring an adequate level of protection, must respect these BCRs, the provisions in the GDPR regarding such transfers, and in particular the requirements set forth in Section 22.2 above.

23 Supervision of compliance

23.1 The Data Protection Officer's tasks and responsibilities

The Group has appointed a Data Protection Officer with the responsibility to assist the Group to be compliant with the BCRs and the GDPR, and to monitor the Group's compliance with the BCRs and the GDPR.

The DPO shall, inter alia, be responsible for the following tasks:

(i) The DPO shall have the right to collect information to identify Processing activities, analyse and control the compliance of Processing activities, and inform, advise and issue recommendations to the Group;

(ii) Be the first point of contact for enquiries on data protection and Data Subject access requests, providing Data Subjects with appropriate advice, and guidance and answering their requests;

(iii) Administer the reporting of Personal Data Breaches in the Group, and ensure that the Supervisory Authority and/or the Data Subjects are notified when required;

(iv) Support and communicate with the Groups Personal Data Protection Administrators (PDPA's) in matters concerning Personal Data;

(v) To inform and advise the Group of their obligations pursuant to the BCRs, the GDPR and to other data protection Law, including privacy legislation in countries where the Group has its operations;

(vi) To monitor compliance with the BCRs, the GDPR, with other Laws regarding data protection provisions and with the Group's data protection policies, including the assignment of responsibilities, conduct awareness-raising and training of staff involved in Processing operations, and ensuring that audits are conducted on a regular basis;

(vii) Maintain and follow up on the yearly work plan for internal controls;

(viii) To provide advice where requested regarding data protection impact assessments and monitor its performance;

(ix) To cooperate with the Norwegian Data Authority and other Supervisory Authorities; and

(x) To act as the contact point for the Norwegian Data Authority and other Supervisory Authorities on issues relating to Processing, including the prior consultations, and to consult, where appropriate, with regard to any other matter.

Notwithstanding the above, the DPO shall not perform tasks which may result in conflict of interests. The DPO should therefore not be put in charge of carrying out data protection impact assessments (the DPO may, however, provide advice regarding- and monitor the performance of such assessments).

23.2 The Position of the Data Protection Officer

The following requirements shall apply to the position of the DPO:

(i) The Group shall ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of Personal Data;

(ii) The Group shall support the Data Protection Officer in performing the tasks referred to in Section 23.1 by providing resources necessary to carry out those tasks and access to Personal Data and Processing operations, and to maintain his or her expert knowledge;

(iii) The Group shall ensure that the Data Protection Officer does not receive any instructions regarding the exercise of the aforementioned tasks. He or she shall not be dismissed or penalized by the Group for performing his/her tasks. The Data Protection Officer shall report directly to the Group Management Team. The DPO may also notify the Group Management Team in the event any questions or problems arise regarding the performance of the DPO's tasks or duties;

(iv) Data Subjects may contact the Data Protection Officer with regard to all issues related to Processing of their Personal Data and to the exercise of their rights under this Regulation;

(v) The Data Protection Officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Law; and

(vi) The Data Protection Officer may fulfil other tasks and duties. The Group shall ensure that any such tasks and duties do not result in a conflict of interests.

The Group shall publish the contacts details of DPO on the Group's website and intranet, and specify therein that Data Subjects may contact the DPO directly.

23.3 DPO and PDPA management

As part of its operations, the Group processes Personal Data of Personnel, Business Partners and External Parties in over 120 countries. The Group has therefore established a network of Personal Data Protection Administrators. The management of this network of Personal Data Protection Administrators and their relationship to the DPO is further described in Appendix 6 (Personal data protection management in the Wilhelmsen Group).

As set out in Appendix 6 (Personal data protection management in the Wilhelmsen Group), the responsibility for the daily supervision of the Group's general data protection compliance has been assigned to the Group PDPA. For the avoidance of doubt, the foregoing shall not limit the DPO's responsibilities as inter alia set out in Section 23.1 and Section 23.2 of the BCRs.

23.4 Training program

The Group will provide appropriate and up-to-date training on these BCRs to Personnel with permanent or regular access to Personal Data, Personnel involved in the collection of Personal Data, and to Personnel involved in the development of tools used to Process Personal Data. For the avoidance of doubt, this

training will cover procedures for managing requests for access to Personal Data made by public authorities.

All Personnel shall furthermore complete mandatory training programs, including e-learning courses.

The above training will be provided with adequate intervals, and at least once per year.

24 Audit and monitoring program

24.1 Monitoring and internal audit

24.1.1 Monitoring

General monitoring is conducted within the Group to manage risk, and drive performance and learning, including the BCR Member's compliance with these BCRs.

Monitoring is performed by internal or external parties. The scope and frequency of internal monitoring depends on an assessment of risks performed by each BCR Member.

Internal monitoring consists of three main categories: follow-up, verification, and internal audit.

24.1.2 Internal audit

Internal audit is an independent, objective assurance and consulting activity performed in accordance with international standards to evaluate and improve the effectiveness of the Group's performance, management system and governance in accordance with the formal mandate from the Data Protection Officer and/or the Group PDPA.

The Group shall carry out audits related to the BCRs at least annually. The Group shall furthermore carry out audits if there are any indications of non-compliance, i.e., to ensure the verification of compliance with the BCRs, as well as upon the request of the DPO or the Group PDPA.

In relation to the BCRs, the aim of the audit is to ensure compliance with all aspects of these BCRs including, but not limited to the following elements:

(i) Legal basis for Processing Personal Data;

(ii) Purpose limitation;

(iii) Data minimisation;

(iv) Accuracy;

(v) Storage limitation;

(vi) Integrity and confidentiality;

(vii) Transparency and right to be informed;

(viii) Data Subject's right of access, rectification, erasure (right to be forgotten), restriction of Processing, objection to Processing and data portability;

(ix) Security;

(x) Transfer to internal Processors and external Processors and Controllers;

(xi) Training program;

(xii) Compliance and supervision of compliance;

(xiii) Internal complaint mechanisms;

(xiv) Third party beneficiary rights;

(xv) Liability; and

(xvi) Changes to the BCRs.

Audits shall be carried out by the DPO, the Group PDPA, or another requested party in the course of regular internal audit as described in this Section 24, or if requested by the DPO. The DPO may decide to appoint an external auditor to do the audit. The DPO shall ensure that applicable professional standards of independence, integrity and confidentiality is observed by such auditor in connection with the audit.

The results of the audit shall be communicated to the board of each BCR Member which have been audited, the relevant Exporting BCR Member and, if appropriate, the General Management Team and/or WWH's board of directors. In the event that the audit is not carried out by the DPO, reports from the audit shall also be made available to the DPO.

On the basis of the results of the audit, the DPO shall produce an annual data protection report for the General Management Team regarding the Group's compliance with these BCRs, and other relevant issues.

A copy of the results of the audit shall be provided to the Norwegian Data Protection Authority and other Competent Supervisory Authorities, upon request.

24.1.3 Requirements regarding impartiality and independence

The persons in charge of the audit shall be guaranteed independence in the performance of their duties in connection with the audit, by the Group. In addition, the DPO and/or the Group PDPA may only be put in charge of an internal audit if the DPO and/or the Group PDPA (as applicable) are free of any conflicting interests in relation to the audit.

24.2 Audits by the Norwegian Data Protection Authority

The Norwegian Data Protection Authority and the Competent Supervisory Authorities shall also be entitled to perform audits.

24.3 Corrective Actions

The Data Protection Officer shall ensure that all adequate steps are taken by the Group to rectify breaches of these BCRs that are identified in relation to the audit and monitoring program in accordance with this Section 24, including steps to minimize the harm of breaches that have already occurred and to prevent future breaches.

25 Internal complaint mechanism

25.1 Complaints to the Data Protection Officer

Data Subjects have the right to complain if any part of the Group is non-compliant with these BCRs. Such complaints may be filed to the Data Protection Officer, either by email or ordinary mail. The Group has established an internal complaint mechanism, in accordance with this Section 25, for the purpose of receiving and processing complaints. Upon receipt of a complaint, the Data Protection Officer shall do an assessment, and if required, initiate an investigation and consult with relevant parts of the Group.

If a complaint is considered as justified, the Data Protection Officer shall give advice on what actions to take and, in case of doubt, consult with the Norwegian Data Protection Authority or any other Competent Supervisory Authority.

In the response to the Data Subject the Data Protection Officer shall provide information about measures that have been or will be implemented on the basis of the complaint and the stipulated timing for such measures.

In case a complaint is rejected, the Data Subject shall receive information about the result and the reason for the result from the Data Protection Officer.

If a Data Subject is not satisfied with the response to the complaint, the Data Subject can choose to lodge claims based on these BCRs in accordance with the provisions in Section 33, below.

25.2 Time limits

Without undue delay, and in any event within one (1) month after receipt of a complaint, the Data Protection Officer shall, as further described in Section 25.1 above, revert to the Data Subject in writing to inform him/her of the result of the complaint handling. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Data Protection Officer shall inform the Data Subject of any such extension within one month of receipt of the complaint, together with the reasons for the delay. Where the Data Subject makes the request by electronic form means, the response to the complaint shall be provided by electronic means where possible, unless otherwise requested by the data subject.

25.3 Information regarding the internal complaint mechanism

Information regarding the Group's complaint mechanism, as included in Appendix 8 (Template Complaint Form) to these BCRs, will be made available on the Group's website and intranet, e.g. on the Group's privacy notices and the published version of the BCRs. The Group shall furthermore make available the complaint form included in Appendix 8 on its website and intranet.

As further described in Appendix 8 to the BCRs, the information which the Group will provide to Data Subjects regarding its complaint system will include, without limitation, information on:

(i) Where to complain, i.e. the non-mandatory points of contact which may be used (it being understood that a physical address at all times shall be provided and presented as one of the points of contact);

(ii) In what form the complaint may be submitted;

(iii) Consequences in the event that the complained is not responded to within the time limits set out in Section 25.2 above;

(iv) Consequences in case the complaint is considered as justified;

(v) Consequences in case the Group rejects a complaint; and

(vi) Consequences in the event the Data Subject is not satisfied with the response to the complaint, i.e. that The Data Subject has the right to lodge a claim before the competent court within the EU/EEA and/or before the Supervisory Authorities in accordance with Section 33 of the BCRs (while clarifying that such right will not depend on the Data Subject having first lodged a complaint to the Group, i.e. used the internal complaint mechanism described in this Section 25).

26 Third party beneficiary rights

Data Subjects whose Personal Data is Processed under these BCRs shall have the right to enforce the following elements/rights of these BCRs as third party beneficiaries:

(i) The right to have Personal Data Processed according to the data protection principles, in particular the principles regarding:

- Lawfulness and fairness (cf. Section 4), and transparency (cf. Section 8)
- Purpose limitation (cf. Section 5);
- Data minimisation, limited storage periods, data quality and accuracy (cf. Section 7);
- Data protection by design and by default (cf. Section 17);
- Legal basis for Processing of Personal Data and Special Categories of Personal Data (cf. Section 4);
- Security, integrity and confidentiality (cf. Section 16), including the right to be notified of Personal Data Breaches in accordance with Section 18 of the BCR; and
- Restrictions on onward transfers to Third Parties not part of the Group (cf. Section 21 and Section 22).

(ii) Right with respect to transparency and easy access to the BCRs (cf. Section 8), including the right to receive information about changes to these BCRs and the list of BCR Members (cf. Section 34);

(iii) Right of information (cf. Section 8.2), access (cf. Section 9), rectification (cf. Section 10), erasure (cf. Section 11), restriction (cf. Section 12), objection to processing (cf. Section 15), right not to be subject to decisions based solely on automated processing, including profiling (cf. Section 15), and the right to data portability (cf. Section 14);

(iv) Rights in case of national laws and practices affecting compliance with the BCRs, and in case of government access requests (cf. Section **Error! Reference source not found.**);

(v) Right to complaint through the Group's internal complaint mechanism, cf. Section 25;

(vi) Rights related to the Group's cooperation duties with the Supervisory Authority (cf. Section 27);

(vii) The right to judicial remedies, as well as the right to obtain redress and compensation in accordance with Section 28.2 and Section 33, below; and

(viii) The right to hold the Exporting BCR Member responsible for any material or non-material damages resulting from the breach of the BCR by the BCR Member not established in the EU/EEA, including the right to demand remedy, redress and compensation from the Exporting BCR Member in such an event (cf. Section 28.2).

For clarity, this Section 26 will in itself be regarded as a third party beneficiary right, which Data Subjects whose Personal Data is processed under these BCRs will have the right to enforce.

However, the above third party beneficiary rights do not extend to those elements of the BCRs pertaining to internal mechanisms implemented within the Group, such as detail of training, audit programs, compliance network, and mechanism for updating the BCRs.

Data Subjects that wishes to exercise their third party beneficiary rights shall have a right to do so by lodging a complaint in accordance with Section 25 or Section 33 of these BCRs.

27 Mutual assistance and duty to cooperate with the Supervisory Authorities

All BCR Members shall:

(i) Cooperate with the Competent Supervisory Authorities;

(ii) Provide the Competent Supervisory Authorities, upon request, with any information about the Processing operations covered by these BCRs;

(iii) Accept to be audited and/or inspected (including on-site) by the Competent Supervisory Authorities;

(iv) Abide by any decisions of the Competent Supervisory Authorities and comply with the advice of the Supervisory Authorities on any issue related to the BCRs.

Furthermore, all BCR Members shall cooperate and assist each other to (i) handle requests or complaints from Data Subjects and/or a Supervisory Authority, and (ii) to handle an investigation or inquiry by a Supervisory Authority.

Any dispute between a BCR Member and the Competent Supervisory Authority related to the Supervisory Authority's exercise of supervision of the BCR Member's compliance with these BCRs will be resolved by the courts of the EU/EEA member state of the applicable Supervisory Authority, in accordance with that member state's procedural law. The BCR Members agree to submit themselves to the jurisdiction of these courts, in accordance with the preceding sentence.

28 Third Country laws and practices, Third Country government access requests

28.1 Third Country laws and practices which may affect these BCRs

28.1.1 TIAs and Supplementary Measures

The Group will use these BCRs as a tool for transferring Personal Data to an Importing BCR Member only where the Group has assessed that the laws and practices in the relevant Third Country of the Importing BCR Member (including any requirements to disclose Personal Data to- or measures authorising access by Third Country public authorities) do not prevent the Importing BCR Member from fulfilling its obligations under these BCRs (such assessments shall be referred to as a "**Transfer Impact Assessments**" or "**TIAs**"). For the avoidance of doubt, Third Country laws and practices that respect the essence of the fundamental rights and freedoms, and which do not exceed what is necessary and proportionate in a democratic society to safeguard one of the following objectives, shall not be regarded as in contradiction with these BCRs:

(i) National security;

(ii) Defense;

(iii) Public security;

(iv) The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(v) Other important objectives of general public interest of the Third Country, in particular an important economic or financial interest of the Third Country, including monetary, budgetary and taxation matters, public health and social security;

(vi) The protection of judicial independence and judicial proceedings;

(vii) The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(viii) A monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (i) to (v) and (vii);

(ix) The protection of the Data Subject or the rights and freedoms of others;

(x) The enforcement of civil law claims.

When carrying out the Transfer Impact Assessment, the Group shall take due account, in particular, to the following elements:

(xi) The specific circumstances of the transfers or set of transfers of Personal Data to the Importing BCR Member, and of any envisaged onward transfers within the same Third Country of that Importing BCR Member or to another Third Country, including:

- Purposes for which the Personal Data is transferred and Processed;
- Types of entities involved in the Processing (e.g. the Importing BCR Member and any further recipient of any onward transfer);
- Economic sector in which the transfer or set of transfers occur;
- Categories and format of the Personal Data transferred;
- Location of the Processing, including storage; and
- Transmission channels used.

(xii) The Third Country laws and practices of the Importing BCR Member which are relevant in light of the circumstances of the relevant transfer of Personal Data, including those requiring disclosure of Personal Data to public authorities, authorising access by such authorities and those providing for access to these Personal Data during the transit between the country of the Exporting BCR Member and the Importing BCR Member, as well as the applicable limitations and safeguards in such laws and practices.

(xiii) Any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these BCRs, including measures applied during the transfer of Personal Data to the Importing BCR Member and to the Processing of the Personal Data in the Third Country of destination (hereinafter "**Supplementary Measures**").

Should the Transfer Impact Assessment reveal that any Supplementary Measure should be implemented (cf. item (iii) above), the Exporting BCR Member and the DPO shall be informed thereof, and be involved in the work of determining which Supplementary Measure to implement.

The Group shall document appropriately the Transfer Impact Assessment it has carried out, including the Supplementary Measures which it has selected and implemented in connection with the TIA. This document will be made available to the Competent Supervisory Authorities, upon request.

The Exporting BCR Member and the DPO will inform all other BCR Members of the TIA carried out and of its results, so that any identified Supplementary Measures will be applied in case the same type of transfers is carried out by any other BCR Member or, where effective Supplementary Measures could not be put in place, the relevant transfer is suspended or ended.

28.1.2 Ongoing monitoring of Third Country laws and practices, notifications

The Exporting BCR Member will monitor, on an ongoing basis, and where appropriate in collaboration with the relevant Importing BCR Members, developments in the Third Countries to which the Exporting BCR

Member has transferred Personal Data to, that could affect the initial TIAs, and the decisions taken in connection therewith concerning Personal Data transfers.

The Importing BCR Member will promptly notify the Exporting BCR Member and the DPO if it has reasons to believe that it is or has become subject to Third Country laws or practices that would prevent it from fulfilling its obligations under these BCRs (including without limitation following a change in such laws or following a disclosure request from a Third Country authority). Upon receiving such a notification, the relevant Exporting BCR Member shall, along with the DPO, promptly identify the Supplementary Measure(s) which should be adopted, in order to enable the Exporting and Importing BCR Member to fulfil their obligations under the BCRs.

The foregoing paragraph shall also apply if the Exporting BCR Member has reason to believe that its Importing BCR Member can no longer fulfil its obligations under this BCRs due to the relevant Third Country laws and practices.

28.1.3 Suspensions and terminations of Third Country transfers

If the Exporting BCR Member, with the DPO, assesses that these BCRs cannot be complied with for a transfer or set of transfers to an Importing BCR Member, even if accompanied by Supplementary Measures, the Exporting BCR Member will suspend the relevant transfer (as well as all other transfers for which the same assessment and reasoning would apply) until compliance is again ensured or the transfer is ended. The Exporting BCR Member shall also suspend a transfer to a Third Country/Importing BCR Member, if instructed to do so by a Competent Supervisory Authority.

If these BCRs cannot be complied with, and compliance with the BCRs is not restored within one month of the above suspension of a Third Country transfer, the Exporting BCR Member will end the transfer. The Personal Data that has been transferred prior to the suspension, and any copies thereof, will at the choice of the Exporting BCR Member, be returned to the Exporting BCR Member or destroyed in its entirety (and the Importing BCR Member shall certify that it has done so).

28.2 Obligations in the event of Third Country government access requests

Without prejudice to the Importing BCR Members obligations under Section 28.1 above, the Importing BCR Member will promptly notify the Exporting BCR Member and, where possible, the Data Subject (if necessary with the help of the Exporting BCR Member) if it:

(i) Receives a legally binding request by a public authority under the laws of Importing BCR Member's country, or of an another Third Country, for disclosure of Personal Data transferred under these BCRs (such notification will include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided);

(ii) Becomes aware of any direct access by Third Country public authorities to Personal Data transferred under these BCRs in accordance with the laws of the applicable country (such notification will include all information available to the Importing BCR Member).

If prohibited from notifying the Exporting BCR Member and/or the Data Subject, the Importing BCR Member will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as

much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the Exporting BCR Member.

Furthermore, the Importing BCR Member will provide the Exporting BCR Member, at regular intervals, with as much relevant information as possible on any requests received, and in particular information regarding the:

(i) Number of requests;

(ii) Type of data requested,

(iii) Requesting authority or authorities, and

(iv) Whether requests have been challenged and the outcome of such challenges.

If the Importing BCR Member is or becomes partially or completely prohibited from providing the Exporting BCR Member with the aforementioned information, it will, without undue delay, inform the Exporting BCR Member thereof.

The Importing BCR Member will preserve the abovementioned information for as long as it Processes the relevant Personal Data under these BCRs, and shall make the information available to the Competent Supervisory Authority upon request.

The Importing BCR Member will review the legality of the Third Country authority's request for disclosure, in particular whether it remains within the powers granted to the requesting authority. The Importing BCR Member will challenge the aforementioned request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the applicable Third Country laws, applicable obligations under international law, and/or principles of international comity.

The Importing BCR Member will, under the same conditions, pursue possibilities of appeal. When challenging a disclosure request, the Importing BCR Member will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. The Importing BCR Member will not disclose the Personal Data requested until required to do so under the applicable procedural rules.

The Importing BCR Member will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the applicable Third Country laws, make the documentation available to the Exporting BCR Member. The aforementioned parties will also make the documentation available to the Competent Supervisory Authorities upon request.

The Importing BCR Member will provide the minimum amount of information permissible when responding to a request for disclosure from a Third Country authority, based on a reasonable interpretation of the request.

Notwithstanding the above, disclosures of Personal Data by a BCR Member to any Third Country authority can – as a general principle - not be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society (cf. Section 28.1 above).

29 Non-compliance with these BCRs

29.1 General requirements

No transfer of Personal Data can be made to an Importing BCR Member under these BCRs, unless the Importing BCR Member is effectively bound by and able to comply with the BCRs.

The Importing BCR Member will promptly notify the Exporting BCR Member and the DPO if it is unable to comply with the BCRs for any reason (including, without limitation, for the reasons described in Section 28 above).

29.2 Consequences of non-compliance with these BCRs

If the Importing BCR Member is in breach of the BCRs or unable to comply with the BCRs, the Exporting BCR Member will *suspend* its transfers of Personal Data to the Importing BCR Member.

Furthermore, the Importing BCR Member will, at the choice of the Exporting BCR Member, immediately *return or delete* the Personal Data which the latter has transferred to the former under the BCRs (including any copies thereof), if:

(i) The Exporting BCR Member suspended the relevant transfer, and compliance with the BCR is not restored within a reasonable time, and in any event within one month of suspension; or

(ii) The Importing BCR Member is in substantial or persistent breach of the BCRs; or

(iii) The Importing BCR Member fails to comply with a binding decision of a competent court within the EU/EEA or Competent Supervisory Authority regarding its obligations under the BCRs.

For the avoidance of doubt, the Importing BCR Member shall continue to Process the relevant Personal Data in compliance with these BCRs, until the Personal Data has been deleted or returned. The foregoing shall also apply if Third Country laws applicable to the Importing BCR Member prohibit the return or deletion of the relevant Personal Data. The Importing BCR Member will in this event only Process the relevant Personal Data to the extent and for as long as required under the applicable Third Country laws.

30 Termination of BCR membership

Subject to Section 29 above, the following shall apply in the event an Importing BCR Member terminates its BCR membership under the Intra-Group BCR Agreement, or the Importing BCR Member for any other reasons ceases to be bound by the BCRs:

(i) The Importing BCR Member shall notify the Exporting BCR Member and the DPO before the termination of the BCR membership becomes effective;

(ii) The Importing BCR Member and the Exporting BCR Member shall in good faith and loyally agree on whether the Importing BCR Member will keep, return or delete the Personal Data it has received by the Exporting BCR Member under these BCRs; and

(iii) If the parties agree that the Importing BCR Member may keep the aforementioned Personal Data (whether in part or in its entirety), the Parties shall take such steps which are necessary to ensure that the kept Personal Data is Processed in accordance with the requirements for transferring Personal Data to Third Countries under the GDPR (cf. Section 22.2.1 of the BCRs, where these requirements are described).

31 Liability and burden of proof

31.1 Liability

The Exporting BCR Member will be responsible for, and agrees to take the necessary actions to remedy the acts of her BCR Members not established in EU/EEA, and to be liable to pay compensation for any material or non-material damages resulting from the breach of the BCR by the BCR Member not established in the EU/EEA.
In the event that a BCR Member outside the EU/EEA violates these BCRs, courts or other competent authorities in the EU/EEA will have jurisdiction, and Data Subjects will have rights and remedies against the Exporting BCR Member as if the breach had been caused by the latter.

The BCR Members acknowledge and accept that Data Subjects that wish to invoke their rights under this Section 31, or to file a complaint under Sections 25 and 33, may be represented by a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of an EU/EEA Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data.

31.2 Burden of proof

Where the Data Subject can demonstrate that the Data Subject has suffered damage, and establish facts which show it is likely that the damage has occurred because of the breach of these BCRs, the Exporting BCR Member shall be exempt from the liability described in Section 31.1 above, in whole or in part, only if it proves that the concerned BCR Member established outside the EU/EEA was not responsible for the breach of the BCR giving rise to those damages, or that no such breach took place.

32 Sanctions

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

33 Right to lodge a complaint

A Data Subject that is of the opinion that a BCR Member has infringed these BCR may, as further described in Section 25 above, lodge a complaint to the Group.

The Data Subject also has the right to lodge a complaint to;

(i) The Supervisory Authority in the EU/EEA Member State of his or her habitual residence, place of work, or place of the alleged infringement; and

(ii) Before the competent court of the EU/EEA Member State where the Group has an establishment or where the Data Subject has his or her habitual residence.

As also mentioned in Section 33 above, a Data Subject that wishes to lodge a complaint under these BCRs, may be represented by a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of an EU/EEA Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data.

34 Mechanism for reporting and recording changes of the BCRs

The BCRs may only be changed in accordance with the procedure and requirements set out in this Section 34. Without prejudice to the foregoing sentence, the Group has a general duty to maintain and keep the BCRs updated in compliance with the EDPB's Recommendations, and shall inter alia change/update these BCRs when necessary due to changes in Law, changes in the EDPB's Recommendations 01/2022 and/or changes to the scope of these BCRs (e.g. the categories of Personal Data which the Group intends to Process under the BCRs).

The Group's Data Protection Officer must approve all changes to these BCRs.

The Data Protection Officer shall be responsible for ensuring that approved changes are reported:

(i) To all BCR Members, without undue delay;

(ii) To Data Subjects, in accordance with Section 8 of the BCRs; and to

(iii) Competent Supervisory Authorities, upon request.

The Data Protection Officer shall furthermore keep a fully updated list of the BCR Members, and keep record of any updates and changes to these BCRs.

If a change to these BCRs would possibly be detrimental to the level of the protection offered by the BCRs or significantly affect them (e.g. due to changes to binding character of the BCRs, changes to the Exporting BCR Member(s)), the proposed change must, promptly and in advance, be communicated by the Data Protection Officer to the Norwegian Data Protection Authority, with a brief explanation of the reason for the change. In this event, the Competent Supervisory Authorities will also assess whether the proposed change to the BCRs will require a new approval (it being understood that such changes will not become effective until the necessary approval has ben obtained).

Any other changes to these BCRs or to the list of BCR Members should be notified once a year by the Data Protection Officer to the Norwegian Data Protection Authority, with a brief explanation of the reasons for the update. The Norwegian Data Protection Authority will also receive such an annual notification if no changes has made to the BCR that year. The annual notification will also include a renewed confirmation that the Exporting BCR Members have sufficient assets to pay compensation for damages resulting from a breach of these BCRs, in line with the EDPB Recommendations 01/2022.

A change to these BCRs shall enter into force and be binding upon all BCR Members after it has been approved by the Data Protection Officer (and the Norwegian Data Protection Authority, if necessary) and communicated/reported to the BCR Members.

35 Applicable version of the BCRs

Any request or complaint involving these BCRs shall be judged against the version of these BCRs that is in force at the time the request or complaint is set forth.

36 Governing law

The BCRs shall be governed by and interpreted in accordance with Norwegian law.

These For the avoidance of doubt, these BCRs shall not deprive Data Subjects of any rights or remedies provided to them under applicable data protection Law or the GDPR.

APPENDIX 1: MEMBERS OF THE BCRS

Company name	Country of incorporation
Wilh. Wilhelmsen Holding ASA (parent)	Norway
Wilhelmsen Chemicals AS	Norway
Wilhelmsen Business Service Center Sp z o.o.	Poland
Wilhelmsen Global Business Services AS	Norway
Wilhelmsen Global Business Services Sdn. Bhd.	Malaysia
Wilhelmsen Insurance Services AS	Norway
Ceataec AS	Norway
C-Loop AS	Norway
Consigli Portuali AS	Norway
Denholm Port Services Limited	United Kingdom
Marine Supply System AS	Norway
WAVESAPP AS	Norway
Wilhelmsen Maritime Services AS	Norway
Wilhelmsen Maritime Services Invest AS	Norway
Barber Ship Management Germany GmbH & Co. KG	Germany
Barber Ship Management Germany Verwaltungs GmbH	Germany
Barklav (Hong Kong) Limited	Hong Kong
Barklav S.R.L.	Romania
Diana Wilhelmsen Management Limited	Cyprus
Hecla Emissions Management AS	Norway
iRute Travel Pte. Ltd.	Singapore
OOPS (Panama) S.A	Panama
RightProc Pte. Ltd.	Singapore
RightProc Sdn. Bhd.	Malaysia
Verwaltung Wilhelmsen Ahrenkiel GmbH	Germany
Wilhelmsen Ahrenkiel Ship Management B.V	Netherlands
Wilhelmsen Ahrenkiel Ship Management GmbH & Co. KG	Germany
Wilhelmsen Marine Personnel (Hong Kong) Limited	Hong Kong
Wilhelmsen Marine Personnel (Norway) AS	Norway
Wilhelmsen Marine Personnel (Ukraine) Ltd	Ukraine
Wilhelmsen Marine Personnel d.o.o.	Croatia
Wilhelmsen Marine Personnel Germany GmbH & Co. KG	Germany
Wilhelmsen Marine Personnel Germany Verwaltungs GmbH	Germany
Wilhelmsen Marine Personnel Sp. z o.o.	Poland
Wilhelmsen Ship Management (India) Private Limited	India
Wilhelmsen Ship Management (Norway) AS	Norway

Wilhelmsen Ship Management (USA), Inc.	United States
Wilhelmsen Ship Management Denizcilik Ve Ticaret Anonim Sirketi	Turkey
Wilhelmsen Ship Management Holding AS	Norway
Wilhelmsen Ship Management Korea Ltd	Korea, Republic of
Wilhelmsen Ship Management Limited	Hong Kong
Wilhelmsen Ship Management Sdn Bhd	Malaysia
Wilhelmsen Ship Management Serviços Marítimos do Brasil Ltda.	Brazil
Wilhelmsen Ship Management Singapore Pte Ltd.	Singapore
Wilhelmsen-Smith Bell Manning, Inc	Philippines
WSM Global Services Limited	Hong Kong
WSM Invest AS	Norway
Alghanim Wilhelmsen Shipping Co.W.L.L	Kuwait
Almoayed Wilhelmsen (Ltd) W.L.L	Bahrain
Argomar - Navegacao e Transportes, S.A.	Portugal
Auxiliaire Maritime SAS	France
Baasher Barwil Agencies Ltd.	Sudan
Barwil (South Africa) Pty Ltd	South Africa
Barwil Abu Dhabi Ruweis L.L.C.	United Arab Emirates
Barwil Agencies Ltd. For Shipping	Saudi Arabia
Barwil Arabia Shipping Agencies SAE	Egypt
Barwil For Maritime Services Co. Ltd.	Iraq
Binzagr Barwil Marine Transport Co. Ltd.	Saudi Arabia
Cargomax Pty Ltd	Australia
Diize B.V.	Netherlands
Hunter Marine Surveyors Pty Ltd	Australia
International Shipping Co. Ltd.	Yemen
Intertransport Air Logistics, S.A.	Panama
Iraqi-Norwegian Co For Marine Navigation & Maritime Services Ltd	Iraq
Krew-Barwil (Pty) Ltd.	South Africa
Lowill S.A.	Panama
Ocean Shipping Co. Ltd	Sudan
Perez Torres Portugal Lda	Portugal
Scan Arabia Shipping Agencies S.A.E.	Egypt
Scan Cargo Services S.A.	Panama
Scan Logistics Ltda	Brazil
Tbilisi Dry Port LLC	Georgia
Triangle Shipping Agencies LLC	United Arab Emirates
Wilhelmsen Denizcilik Hizmetleri Ltd. Sti	Turkey
Wilhelmsen Huayang Port Services (Shanghai) Co., Ltd	China
Wilhelmsen Huayang Ships Service (Beijing) Co., Ltd.	China
Wilhelmsen Hyopwoon Port Services Ltd	Korea, Republic of

Wilhelmsen Port Services (Australia) Pty Ltd	Australia
Wilhelmsen Port Services (Gibraltar) Limited	Gibraltar
Wilhelmsen Port Services (Hong Kong) Limited	Hong Kong
Wilhelmsen Port Services (Japan) Pte. Ltd.	Singapore
Wilhelmsen Port Services (Japan) Pte. Ltd. - Japan Branch	Japan
Wilhelmsen Port Services (Myanmar) Limited	Myanmar
Wilhelmsen Port Services (S) Pte. Ltd.	Singapore
Wilhelmsen Port Services (Taiwan) Inc.	Taiwan (Province of China)
Wilhelmsen Port Services (Thailand) Ltd.	Thailand
Wilhelmsen Port Services Amsterdam B.V.	Netherlands
Wilhelmsen Port Services And Towell Co LLC	Oman
Wilhelmsen Port Services AS	Norway
Wilhelmsen Port Services B.V.	Netherlands
Wilhelmsen Port Services Belgium N.V	Belgium
Wilhelmsen Port Services Belgium NV, Anvers, Geneva branch	Switzerland
Wilhelmsen Port Services Brasil Ltda	Brazil
Wilhelmsen Port Services Bulgaria Ltd	Bulgaria
Wilhelmsen Port Services Canarias, S.A.	Spain
Wilhelmsen Port Services Egypt S.A.E	Egypt
Wilhelmsen Port Services France SAS	France
Wilhelmsen Port Services Georgia LLC	Georgia
Wilhelmsen Port Services Germany GmbH	Germany
Wilhelmsen Port Services Global Pte. Ltd.	Singapore
Wilhelmsen Port Services Hamburg GmbH	Germany
Wilhelmsen Port Services Hellas S.M S.A.	Greece
Wilhelmsen Port Services Holding BV	Netherlands
Wilhelmsen Port Services India Private Limited	India
Wilhelmsen Port Services Japan Co., Ltd.	Japan
Wilhelmsen Port Services Limited	New Zealand
Wilhelmsen Port Services LLC	United Arab Emirates
Wilhelmsen Port Services LLC (Dubai)	United Arab Emirates
Wilhelmsen Port Services Malaysia Sdn Bhd	Malaysia
Wilhelmsen Port Services Malta Ltd	Malta
Wilhelmsen Port Services Norway AS	Norway
Wilhelmsen Port Services Portugal S.A.	Portugal
Wilhelmsen Port Services Romania S.R.L.	Romania
Wilhelmsen Port Services Rotterdam B.V.	Netherlands
Wilhelmsen Port Services Senegal SUARL	Senegal
Wilhelmsen Port Services South Africa (Pty) Ltd	South Africa
Wilhelmsen Port Services Sp. z o.o.	Poland

Wilhelmsen Port Services Spain S.L	Spain
Wilhelmsen Port Services Sweden AB	Sweden
Wilhelmsen Port Services Terneuzen B.V.	Netherlands
Wilhelmsen Port Services, Inc.	United States
Wilhelmsen Port Services, S.A.	Panama
Wilhelmsen Ships Service (Mozambique), Limitada	Mozambique
Wilhelmsen Ships Service Agencia Maritima S.A.	Chile
Wilhelmsen Ships Service Algeria S.P.A.	Algeria
Wilhelmsen Ships Service Cote d'Ivoire SARL	Cote d'Ivoire
Wilhelmsen Ships Service Holdings Sdn. Bhd.	Malaysia
Wilhelmsen Ships Service Qatar Ltd.	Qatar
Wilhelmsen Ships Service QFZ LLC	Qatar
Wilhelmsen Ships Service Ukraine Ltd.	Ukraine
Wilhelmsen Sunnytrans Co., Ltd	Vietnam
Wilhelmsen W P S Dubai Port Services LLC	United Arab Emirates
Wilhelmsen WPS Dubai Port Services LLC - Jafza Jebel Ali Branch	United Arab Emirates
Wilhelmsen WPS Dubai Port Services LLC - Ras Al Khaimah Branch (RAK)	United Arab Emirates
Wilhelmsen WPS Dubai Port Services LLC -Sharjah Branch (SHJ)	United Arab Emirates
Wilhelmsen-Smith Bell (Subic), Inc.	Philippines
Wilhelmsen-Smith Bell Shipping, Inc.	Philippines
Wiltrans (Gibraltar) Limited	Gibraltar
WLB Shipping Pty. Ltd.	Australia
WWHI Property Australia Pty Ltd	Australia
Havtec Invest Pte. Ltd.	Singapore
Pelagus 3D Pte. Ltd.	Singapore
ShipDan ApS	Denmark
Timm Slovakia s.r.o	Slovakia
Unitor Cylinder Pte. Ltd.	Singapore
Unitor De Mexico, S.A. de C.V.	Mexico
Unitor Holding Inc.	United States
Unitor Ships Service NV Netherlands Anthilles	(Netherlands Antilles)
Wilhelmsen Lojistik Hizmetleri Ticaret Ltd. Sti	Turkey
Wilhelmsen Marine Products Contracting AS	Norway
Wilhelmsen Marine Products France SAS	France
Wilhelmsen Marine Products India Private Limited	India
Wilhelmsen Marine Products LLC -Abu Dhabi	United Arab Emirates
Wilhelmsen Marine Products Pty Ltd	Australia
Wilhelmsen Ships Service (Chile) S.p.A.	Chile
Wilhelmsen Ships Service (L.L.C.)	United Arab Emirates
Wilhelmsen Ships Service (Pty) Ltd. (South Africa)	South Africa

Wilhelmsen Ships Service (S) Pte. Ltd.	Singapore
Wilhelmsen Ships Service A/S	Denmark
Wilhelmsen Ships Service AB	Sweden
Wilhelmsen Ships Service Argentina S.A.	Argentina
Wilhelmsen Ships Service AS	Norway
Wilhelmsen Ships Service AS - Dubai Branch	United Arab Emirates
Wilhelmsen Ships Service AS - Fujairah Branch	United Arab Emirates
Wilhelmsen Ships Service AS - Ukraine Branch	Ukraine
Wilhelmsen Ships Service B.V.	Netherlands
Wilhelmsen Ships Service Bulgaria Ltd	Bulgaria
Wilhelmsen Ships Service Co. Ltd (Japan)	Japan
Wilhelmsen Ships Service Co., Ltd (S.Korea)	Korea, Republic of
Wilhelmsen Ships Service Co., Ltd. (China)	China
Wilhelmsen Ships Service Cyprus Ltd	Cyprus
Wilhelmsen Ships Service do Brasil Ltda.	Brazil
Wilhelmsen Ships Service GmbH	Germany
Wilhelmsen Ships Service Hellas S.A.	Greece
Wilhelmsen Ships Service Inc. (Canada)	Canada
Wilhelmsen Ships Service Inc. (USA)	United States
Wilhelmsen Ships Service Limited [New Zealand]	New Zealand
Wilhelmsen Ships Service Limited (UK)	United Kingdom
Wilhelmsen Ships Service LLC - Free Zone	Egypt
Wilhelmsen Ships Service Oy Ab	Finland
Wilhelmsen Ships Service Philippines Inc.	Philippines
Wilhelmsen Ships Service Polska Sp. z o.o.	Poland
Wilhelmsen Ships Service S.p.A.	Italy
Wilhelmsen Ships Service Spain S.A.	Spain
Wilhelmsen Ships Service Trading Sdn. Bhd.	Malaysia
Wilhelmsen Ships Service, S.A.	Panama
Eldøyane Holding AS	Norway
Norsea 123 Limited	United Kingdom
RTN AS	Norway
Bergen Porthandling AS	Norway
Blåse Energi AS	Norway
Elevon AB	Sweden
Elevon AS	Norway
Energy Innovation Holding AS	Norway
Maritime Waste Management AS	Norway
Norsea Denmark A/S	Denmark
Norsea Energy AS	Norway
Norsea Group (Australia) Pty Ltd	Australia

Norsea Impact AS	Norway
Norsea Offshore Wind I AS	Norway
Norsea UK Ltd	United Kingdom
Nsg Maritime AS	Norway
Westport AS	Norway
Windworks Jelsa AS	Norway
Narvikeiendommen AS	Norway
Norbase AS	Norway
NorSea Denmark Property A/S	Denmark
Norsea Logistics AS	Norway
Norsea Polarbase AS	Norway
OS Expressene AS	Norway
Polar Algae AS	Norway
Polar Lift AS	Norway
AQ-Utvikling AS	Norway
Averoy Eiendom AS	Norway
Dusavik Utvikling AS	Norway
Eldøyane Næringspark AS	Norway
Finnestadjordet 12 AS	Norway
Norsea Eiendom Dusavik AS	Norway
Norsea Eiendom Tananger AS	Norway
Norsea Property AS	Norway
Norsea Tananger 107 AS	Norway
Orvikan Eiendom AS	Norway
Polarbase Eiendom AS	Norway
Risavika Eiendom AS	Norway
Risavika Havnering 14 AS	Norway
Sørsea AS	Norway
Tananger Eiendom AS	Norway
Tangen 7 AS	Norway
Tangen 7 Eiendom AS	Norway
Tangen 7 Invest AS	Norway
Vestbase Eiendom AS	Norway
Vikan Næringspark Invest AS	Norway
CCB Energy Holding AS	Norway
CCB Holding AS	Norway
CCB Subsea AS	Norway
Coast Center Base AS	Norway
KS Coast Center Base	Norway
Logiteam AS	Norway
Norsea Industrial Holdings AS	Norway

Norsea Wind A/S	Denmark
Norsea Wind BV	Netherlands
Norsea Wind GmBH	Germany
Norsea Wind Holding AS	Norway
Norsea Wind Limited	United Kingdom
NSG Wind A/S	Denmark
Den Norske Amerikalinje AS	Norway
Olavsvern Group AS	Norway
Topeka Hagland Greenbulk AS	Norway
Treasure ASA	Norway
Wallenius Wilhelmsen ASA	Norway
Wilh. Wilhelmsen Holding Invest Malta Limited	Malta
Wilh. Wilhelmsen Invest AS	Norway
Wilhelmsen GRC Sdn Bhd	Malaysia
Wilhelmsen Invest Infrastructure AS	Norway
WILNOR Governmental Services AS	Norway
WilService AS	Norway
Massterly AS	Norway
Nordlys.Studio AS	Norway
Norsea Group AS	Norway
RAA Investment AS	Norway
Raa Labs AS	Norway
Topeka Holding AS	Norway
Topeka MPC Maritime AS	Norway
Topeka Nattruten AS	Norway
Wilhelmsen New Energy AS	Norway
Massterly AS	Norway
Norsea Group AS	Norway
RAA Investment AS	Norway
Raa Labs AS	Norway
Topeka Holding AS	Norway
Wilhelmsen New Energy AS	Norway
Norsea Wind Holding AS	Norway
Norsea 123 Limited	United Kingdom
Wilhelmsen GRC Sdn Bhd	Malaysia
Wilh. Wilhelmsen Holding Invest Malta Limited	Malta
Olavsvern Group AS	Norway
WILNOR Governmental Services AS	Norway
WilService AS	Norway

APPENDIX 2: MATERIAL SCOPE OF THE BCRS

1 Introduction

This Appendix 2 sets out the material scope of the BCRs, meaning:

(i) The types of Data Subjects affected;

(ii) The categories of Personal Data;

(iii) The type of Processing and its purposes;

(iv) The data transfers; and

(v) Identification of the third countries.

The categories of Data Subjects affected by the Group's Processing may be divided into two broad categories:

(i) Personnel; and

(ii) Business Partners and other External Parties.

On this background, the material scope of the BCRs relating to the Group's processing of Personnel Data is set out in Section 2 of this Appendix 2. The material scope of the BCRs relating to the Group's Processing of Business Partners and other External Parties is set out in Section 3 of this Appendix 2.

2 Personnel Data

2.1 The types of Data Subjects affected

The Personal Data Processed and transferred by the Group under the BCRs concern the following categories of Data Subjects:

(i) Personnel. As provided in Section 3 of the main body of the BCRs, Personnel means employees, candidates and former employees of the Group.

The term Personnel also includes present and former consultants and employees of Business Partners providing services to the Group through the Group’s information technology systems or from the Group’s premises, in the same manner as employees;

(ii) Next of Kin. As provided in Section 3 of the main body of the BCRs, Next of Kin means the spouse, partner or child of Personnel.

2.2 The categories of Personal Data

The Personal Data Processed under the BCRs concern the following categories of Personal Data:

(i) Categories of Personal Data concerning Data Subjects under Section 2.1(i), above:

- Name, address and title;
- Telephone numbers, fax number, email address and other contact information;
- Gender, birth date, signature;
- Birth location, country of citizenship/nationality, photograph;
- Citizen service number / social security number / other national identification number;
- Position, department, name of employer and location/business address;
- Family information and marital status (married or not, dependent spouse or children);
- Date of start and (if applicable) end of contract and contract / termination (information and documents);
- Working days, leaves of absence/holidays and other employment-related arrangements and information;
- Name of supervisor;
- Appraisal and evaluation information including courses and education followed;
- Personnel number;
- Financial information (such as salary, benefits and remuneration, lease car, options, credit card and telephone data);
- Pension and insurance information;
- Copy of a passport or other identity document and data thereon including photograph;
- Visa information and work permit information and results and input background screening;
- Bank account information, pay slips and data included therein;
- Other information relating to the individuals e.g. concerning their expertise, work experience, activities and memberships;
- Photograph on e.g. the passport, the intranet and internet;
- Details of any questions or disputes with or involving the individuals;
- Other data as necessary to comply with legal obligations and information provided by individuals.

(ii) Categories of Personal Data Concerning Data Subjects under Section 2.1(i), above (included to allow for a specification of purposes as set out below):

- Name, title;
- Telephone numbers, fax number, e-mail address, location/business address and other contact information;
- E-mails, attachments, appointments;
- Date and time of e-mail;
- Website visited, IP address;
- Other documents and use of the IT system; and
- User name and password.

(iii) Categories of Personal Data Concerning Data Subjects under Section 2.1(i)above (included to allow for a specification of purposes as set out below):

- Health data, such as health certificates: and

- Information regarding investigations of allegations of fraud, corruption or other criminal activity.

(iv) Categories of Personal Data concerning Data Subjects under Section 2.1(ii), above:

- Name and address, title;
- Telephone number, email address and other contact information;
- Gender;
- Birth date;
- Relationship with individuals referred to under Section 2.1(i); and
- Details concerning pension and/or insurance.

2.3 The type of Processing and its purposes

(i) The Processing of the categories of Personal Data under Section 2.2(i) and 2.2(iv), is made for the following purposes:

- Administration;
- Human resources and management of employees / personnel;

These purposes includes Processing that is necessary for the performance of an employment contract or a prospective employment contract, including Processing related to recruitment and deployment, performance and development, management and administration of payments, compensation, benefits and reward, tax issues, career planning, evaluations, training, travel and expenses, outplacement, communication with personnel, employee relations, change management and continuous improvement.

- Health, safety and security;

This purpose includes Processing that is necessary to protect health, provide safety and security related to Personnel and their Next of Kin or the public.

- Planning and control measures;

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

(ii) The Processing of the categories of Personal Data under Section (i)is furthermore made for the following purposes:

- Business operation and protection of business interests and security;

This purpose includes Processing in relation to business operations and protection of business interests and security; e.g. information security, logging, conduction of controls, surveys, analysis, reports and managing of daily operations and transactions/possible transactions involving the Group.

- Compliance with legal obligations and protection of legal position.

This purpose includes Processing that is necessary in order to ensure compliance with legal obligations and/or to protect a legal position of the Group (legal proceedings, investigations, questions from competent authorities).

(iii) The Processing of the categories of Personal Data under Section (ii), is made for the following purposes:

- Facilitate (and store) IT system/devices/documents/appointments, internet and e- mail traffic;
- Maintenance and correction of IT problems; and for
- Security purposes.

(iv) The Processing of the categories of Personal Data under Section (iii) is made for the following purposes:

- Health data is only processed for the purpose of complying with mandatory requirements and for carrying out obligations inter alia in the field of employment law and in the field of safety laws and regulations (such as maritime safety). The Group's seafarers are inter alia required under mandatory law to show health certificates before on-boarding vessels. Such Processing shall for the avoidance of doubt only be conducted to the extent that the Processing is permitted under Sections 4.2 and 4.3 of the main body of the BCRs (cf. Sections 4.3(i) and 4.3(vi)).
- Information regarding investigations of allegations of fraud, corruption or other criminal activity, is made for the purpose of complying with anti-corruption legislation, anti-bribery legislation, and similar obligations imposed on the Group, and for notifying the authorities and/or the Group's compliance officers of violations of such legislation. Such Processing shall for the avoidance of doubt only be conducted to the extent that the Processing is permitted under Sections 4.2 to 4.4 of the main body of the BCRs.

2.4 Data transfers and identification of the third countries

Most transfers of Personal Data will take place from Norway, where the Group’s head, Wilh. Wilhelmsen Holding ASA, is located, and where the Group's HR systems are hosted.

The Personal Data transferred under these BCRs will be transferred to and from, respectively, importers and exporters both in the EU/EEA and outside of the EU/EEA (i.e., to all BCR Members) in accordance with the BCRs..

3 Business Partners and other External Partners

3.1 The types of Data Subjects affected

The Personal Data Processed and transferred by the Group under the BCRs concern the following categories of Data Subjects:

(i) Business Partners. As provided in Section 3 of the main body of the BCRs, Business Partners means Data Subjects with whom the Group has a business relationship, either directly with the relevant Data Subject or with the relevant Data Subject's employer. Data Subjects that are also covered by the definition of Personnel shall be regarded as Personnel instead of Business Partners; and

(ii) External Party. As provided in Section 3 of the main body of the BCRs, an External Party means any natural or legal person, public authority, agency or any other body outside of the Group.

3.2 The categories of Personal Data

(i) The Personal Data Processed under the BCRs concern the following categories of Personal Data of Business Partners and other External Partners:

- Name, address and title;
- Telephone numbers, fax number, email address and other contact information;
- Gender, birth date, signature;
- Birth location, country of citizenship/nationality, photograph;
- Citizen service number / former social security number / other national identification number;
- Position, department, name of employer/company and location/business address; and
- Emails, attachments and appointments.

(ii) Furthermore, the Personal Data Processed under the BCRs also concern the following categories of Personal Data of Business Partners and other External Parties (Included to allow for a specification of purposes as set out below):

- Health data, such as health certificates.

3.3 The type of Processing and its purposes

The Processing of the categories of Personal Data under Section 3.2(i) is made for the following purposes:

- Customer administration;
- Supplier administration;
- Document and content management;
- IT administration and information security administration;
- Authentication and authorization;
- For the performance of contractual obligations either with Business Partners or External Partners, with their employers or the companies which they represent;
- To comply with legal obligations; and
- Customer relationship management

3.4 Data transfers and the identification of the third countries

Most transfers of Personal Data will take place from Norway, where the Group's head, Wilh. Wilhelmsen Holding ASA, is located. The Personal Data transferred under these BCRs will be transferred to and from,

respectively, importers and exporters both in the EU/EEA and outside of the EU/EEA (i.e., to all BCR Members) in accordance with these BCRs.