MAERSK DATA PRIVACY
BINDING CORPORATE RULES ('BCR')
for transfer of HR Personal Data within Maersk

TABLE OF CONTENTS

Indhold

1 BACKGROUND AND OVERVIEW 4

1.1 Introduction 4

1.2 Definitions 4

1.3 Scope of the BCR 6

1.4 Maersk entities bound by the BCR 7

1.5 Data Subjects who benefit from the BCR 7

1.6 Third-party beneficiary rights 7

1.7 Survival of third-party beneficiary rights 8

1.8 Data Privacy Compliance Officer and HR Privacy Leads 8

1.9 Contact details 8

2 MAERSK COMMITMENTS 10

2.1 Compliance with local law 10

2.2 Lawfulness, fairness and transparency 10

2.3 Information to be provided to Data Subjects 11

2.4 Processing of Personal Data for a new purpose 12

2.5 Accuracy and Data Minimisation 13

2.6 Privacy by Design 13

2.7 Privacy by Default 13

2.8 Data retention 13

2.9 Special Categories of Personal Data 14

2.10 Automated individual decisions 14

2.11 Transfers to third parties in non-EEA countries 15

2.12 Security 15

2.13 Processing by data processors 16

2.14 Data Subjects' Rights 17

3 SUPERVISION OF DATA PRIVACY COMPLIANCE 18

3.1 Accountability 18

3.2 Records of processing activities 18

3.3 Data Protection Impact Assessments 19

3.4 Training 19

3.5 Audit 19

3.6 Complaint handling 19

3.7 Co-operation with Supervisory Authorities 20
3.8 Update of the BCR 20

4 RELATIONSHIP BETWEEN THE BCR AND LOCAL STATUTORY REGULATIONS 20

APPENDIX 1 DATA SUBJECTS' REQUESTS AND COMPLAINTS PROCEDURE 21

APPENDIX 2 AUDIT PROCEDURE 28

APPENDIX 3 CO-OPERATION WITH AUTHORITIES 30

APPENDIX 4 UPDATING PROCEDURE 31

APPENDIX 5 – GROUP STRUCTURE CHART 32

APPENDIX 6 – LIST OF MAERSK ENTITIES BOUND BY THE BCR 33

APPENDIX 7 – OVERVIEW OF DATA PROCESSING ACTIVITIES COVERED BY THE BCR
(enclosed separately)

1 BACKGROUND AND OVERVIEW

1.1 Introduction

Maersk is committed to protecting the privacy of the individuals who work, or apply to work, for Maersk. These Binding Corporate Rules (BCR) set out the minimum requirements for processing these individuals' Personal Data within Maersk and are binding for all participating corporate entities within Maersk towards these individuals, by virtue of third-party beneficiary rights.

The BCR are internal rules adopted by A.P. Møller-Mærsk A/S and its participating corporate entities, to present "adequate safeguards for the protection of the privacy and fundamental rights and freedoms of data subjects" within the meaning of the Data Protection Legislation.

Maersk Binding Corporate Rules (BCR) are part of Maersk Commit Rule, which is Maersk's Governance Framework, and Mandatory Instructions on Data Privacy compliance.

Maersk BCR defines the responsibilities that Maersk has with regard to protecting the privacy of Data Subjects and explains how Maersk complies with such responsibilities.

1.2 Definitions

The terms used in the BCR will be interpreted in accordance with the GDPR. Further, in the BCR the defined terms have the meanings ascribed to them below:

Term	Definition
Audit Procedure	means the audit procedure set out in Appendix 2 to the BCR.
Binding Corporate Rules or BCR	means the Maersk Binding Corporate Rules, including its appendices and the Unilateral Declaration and Confirmation Letters.
Confirmation Letter	means the confirmation letters, which are signed by authorised signatories of the EEA Maersk entities in order to make the BCR legally binding for said entities.
Control	means in relation to any entity (i) the ownership or control (directly or indirectly) of shares/ownership interests in that entity carrying more than 50 % of the votes exercisable at general meetings of that entity on all or substantially all matters; or (ii) the right to appoint or remove a majority of directors of that entity or having a majority of voting rights at board meetings of that entity; or (iii) the right under any contract or other legally binding arrangement to direct the business or affairs of that entity; or (iv) the ability by virtue of a direct or indirect participation in the respective entity to exercise a dominating influence. Controlled,

	Controlling and any other phrasing of the word control shall be construed accordingly.
Co-operation Procedure	means the procedure on Maersk's cooperation with authorities set out in Appendix 3 of the BCR.
Data Privacy Compliance Officer or DPCO	means Maersk's Data Privacy Compliance Officer appointed by A.P. Møller-Mærsk A/S.
Data Protection Legislation	means the data protection laws applicable to the relevant Maersk entity established within an EEA member state, including the GDPR.
Data Subject	For the purpose of the BCR, the term "Data Subject" has the meaning given to it in clause 1.5 of the BCR.
Data Subjects' Requests (DSRS) and Complaints Procedure	means the procedure on the Data Subjects' rights to request access, rectification, restriction, portability and deletion of Personal Data and to object and complain about Maersk's processing of Personal Data set out in Appendix 1 to the BCR.
(EEA) Supervisory Authority	means an independent public authority which is established by a Member State pursuant to article 51 of the GDPR.
General Data Protection Regulation or GDPR	means Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such Personal Data, and repealing Directive 95/46/EC.
Maersk	means A.P. Møller-Mærsk A/S and all affiliates under A.P. Møller-Mærsk A/S' Control which are subject to the BCR and which have duly signed the Unilateral Declaration or Confirmation Letter as applicable.
Mandatory Instruction	means instructions to individuals working for Maersk, which are issued under Maersk's governance framework Commit. All employees, consultants and other persons who work for Maersk are required to comply with Mandatory Instructions issued under Commit.
Member State	means a country within the EEA.
Personal Data	mean any information relating to an identified or identifiable natural person ('Data Subject')
Service Level Agreement (SLA)	means an agreement between a Maersk entity acting as a service provider and another Maersk entity acting as a service recipient that defines the

	level of service expected from the Maersk entity acting as a service provider.
Special Categories of Personal Data	means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Unilateral Declaration	means the unilateral declaration signed by authorised signatories of A.P. Møller – Mærsk A/S in order to make the BCR legally binding.
Updating Procedure	means the updating procedure set out in Appendix 4 of the BCR.

The following acronyms are used in the BCR:

Term	Definition
BCR	Binding Corporate Rules
EEA	European Economic Area
HR	Human Resources
GDPR	General Data Protection Regulation
SLA	Service Level Agreement

1.3 Scope of the BCR

The BCR establishes Maersk's global approach to compliance with Data Protection Legislation and covers all Personal Data transferred between Maersk entities for HR purposes.

The categories of Personal Data which will be covered by the BCR are mainly general employee data, such as: identification details (name, address, contact information etc.), bank account details, age, CV, interview conclusions, test results (from personality tests and logical tests used in the recruiting process), social security number/personal identity number, education, position with Maersk, seniority, commencement and duration of the employment relationship, terms of employment, performance assessments, salary, bonus and benefits, working hours, absence such as sickness, annual leave, maternity leave etc., visas, work and residence permit, warnings, terminations and the reason for terminations and signature for use with insider lists. The processing may also include sensitive data such as information on criminal records, health, trade union membership, as well as information received through the Maersk's whistleblowing scheme.

The BCR is applied by Maersk to establish a minimum level of protection for a Data Subject's Personal Data. Any exceptions to this principle follow directly from the specific context in the clauses of the BCR and Appendices 1-4.

Maersk BCRs applies both during the normal course of business as well as in situations in which one Maersk entity processes the Personal Data of another Maersk entity, e.g. by providing services to each other (such as hosting services or server facilities for Personal Data) and whether the processing takes place manually in filing systems (or originating from such) or by automatic means. The term processing is interpreted in accordance with the Data Protection

Legislation and include, for example, collecting storing, organising, destroying, amending, consulting, disclosing and transferring Personal Data.

1.4 Maersk entities bound by the BCR

The BCR apply to A.P. Møller – Mærsk A/S and subsidiaries owned and controlled indirectly or directly by A.P. Møller - Mærsk A/S which have undertaken to adhere to the BCR by signing as applicable a Unilateral Declaration or a Letter of Confirmation. All Maersk entities participating in the BCR Framework and their employees are bound to comply with the BCR, including all appendices hereto in respect of any transfer of Personal Data between Maersk entities covered by the BCR.

To receive a full and updated list of Maersk subsidiaries legally bound to comply with the BCR globally please contact Maersk's Data Privacy Compliance Officer (please see contact details in section 1.8. below).

1.5 Data Subjects who benefit from the BCR

Maersk BCR applies to the processing of Personal Data by Maersk about the following individuals (referred to as 'Data Subjects'):

a) Employees (current and former);

b) Managing directors and board members (current and former);

c) Individual consultants (externally employed/seconded into Maersk) (current and former);

d) Relatives and dependants of employees, managing directors, board members; and

e) Applicants to the first three categories above and individuals in the candidate pool (current and rejected).

1.6 Third-party beneficiary rights

Third-party beneficiary rights are afforded to Data Subjects whose Personal Data are processed by a Maersk entity in the EEA acting as a controller and transferred to a Maersk entity in a non-EEA country, whether such entity acts as a controller or as a processor.

This group of Data Subjects has the right to:

a) **Enforce Compliance:** Seek to enforce compliance by Maersk with the BCR (including the appendices), including but not limited to seeking enforcement of the following rights and principles:

   i) local statutory regulations in accordance with the BCR, insofar as such local law stipulates a higher level of protection of Personal Data than the BCR;

   ii) the substantive principles for the processing of Personal Data set out in clause 2; specifically;

   iii) the rights of the data subject set out in clause 2.14;

   iv) the right to make a complaint through the procedure set out in the Data Subjects' Requests and Complaints Procedure; and

   v) any support of or cooperation needed with EEA Supervisory Authorities pursuant to clause 3.7.

b) **Complain to Maersk:** Complain to a Maersk entity in the EEA responsible for exporting the Personal Data in accordance with Appendix 1 (Data Subjects' Requests and Complaints Procedure) and seek redress from the Maersk entity in the EEA responsible for exporting

the Personal Data including the remedy of any breach of the BCR by the non-EEA Maersk entity.

c) **Seek compensation:** Where required, receive compensation from the EEA Maersk entity responsible for exporting the Personal Data for any damage suffered as a result of a breach of the BCR by the non-EEA Maersk entity importing the Personal Data in accordance with the decision of an EEA court or other EEA competent authority.

d) **Complain to a Supervisory Authority:** Lodge a complaint with an EEA Supervisory Authority, in particular in the Member State of the data subject's habitual residence, place of work or place of the alleged infringement.

e) **Take judicial action:** Take action against a Maersk Entity in order to enforce compliance with the BCR in the courts of the jurisdiction in which the Maersk Entity responsible for the alleged breach is established, or the Maersk Entity responsible for exporting the personal data is established, or the data subject has his or her habitual residence.

f) **Burden of proof:** Where Data Subjects can demonstrate that they have suffered damage and can establish fact which show it is likely that the damage has occurred due to a breach of the BCR, Maersk has agreed that the burden of proof to show that no such breach took place, or that Maersk is not responsible for the breach, will rest with the EEA Maersk entity responsible for exporting the Personal Data of the Data subject as well as with the non-EEA Maersk entity importing the Personal Data of the Data subject.

1.7 Survival of third-party beneficiary rights

In the event that a non-EEA Maersk entity is no longer a party to the BCR or otherwise ceases to exist, the third-party beneficiary rights provided to Data Subjects under clause 1.6 will survive in order to ensure that the Data Subject's rights are not affected by such withdrawal from the BCR.

1.8 Data Privacy Compliance Officer and HR Privacy Leads

Maersk has appointed a Data Privacy Compliance Officer to oversee and ensure compliance with the BCR globally. Maersk's Data Privacy Compliance Officer enjoys the highest management support and advises the Board of Directors, deals with Supervisory Authorities' investigations and annual reports on compliance. Furthermore, Maersk's Data Privacy Compliance Officer ensures that changes to the BCR are notified to the Maersk entities, EEA Supervisory Authorities and other persons in accordance with Appendix 4 (Updating Procedure).

Maersk's Data Privacy Compliance Officer is supported by HR Privacy Leads who are responsible for overseeing and enabling compliance with the BCR on a day-to-day basis in the Maersk entities. The HR Privacy Leads are further responsible for handling local complaints from Data Subjects, reporting major privacy issues to Maersk's Data Privacy Compliance Officer and for ensuring compliance at a local level in accordance with Appendix 1 (Data Subjects' Requests and Complaints Procedure).

1.9 Contact details

Maersk has policies and procedures in place to oversee and ensure compliance with all aspects of the BCR. The governance on a local level is the responsibility of the HR Privacy Lead reporting to Maersk's Data Privacy Compliance Officer. The governance of the BCR on a global level is the responsibility of Maersk's Data Privacy Compliance Officer reporting to the Executive Management or General Counsel of A.P. Møller - Mærsk A/S.

If you have any questions regarding the provisions of the BCR, your rights under the BCR or any other data protection issues, please contact the HR Privacy Lead or relevant HR department if you are an employee of Maersk or Maersk's Data Privacy Compliance Officer at either of the contact points set out below. The Data Privacy Compliance Officer will either deal with the matter or forward it to the appropriate HR department, Legal Department or HR Privacy Lead within Maersk.

Maersk BCRs, including its appendices, are published on Maersk's intranet and externally on the Maersk website (www.maersk.com). Further, Data Subjects have the right to obtain a copy of the BCR by contacting Maersk's Data Privacy Compliance Officer.

Maersk's Data Privacy Compliance Officer:
Tel.: +45 33363 3363
Email: dataprivacy@maersk.com (Please mark 'BCR')

Postal address:
A.P. Møller - Mærsk A/S
Esplanaden 50
1263 Copenhagen K
Denmark
Att.: Maersk Legal, Data Privacy Compliance Officer

2 MAERSK COMMITMENTS

2.1 Compliance with local law

Maersk is committed to comply with any applicable legislation relating to Personal Data (in the EEA, e.g. the local laws implementing the GDPR and Directive 2002/58/EC (the "E-privacy Directive") and will ensure that where Personal Data is collected and processed, this is done in accordance with the local law.

Where there is no law or the law in non-EEA countries does not meet the standards set out by the BCR, Maersk will process Personal Data by adhering to the BCR, unless otherwise set out in the BCR, e.g. in the situations where local legal requirements may prevail and as set out in clause 4.

If there is reason to believe that local legislation applicable to any Maersk entity prevents it from fulfilling its obligations under the BCR or such legislation has a substantial effect on its ability to comply with the BCR, Maersk will comply with the procedures set out in clause 4 below.

2.2 Lawfulness, fairness and transparency

Any processing of Personal Data by Maersk must be lawful, fair and transparent to the Data Subject. Maersk will explain to Data Subjects, at the time their Personal Data is collected, about the processing of their Personal Data and will only obtain and process Personal Data for specified, explicit and legitimate purposes which are known to the Data Subject or which are within their reasonable expectations and which are relevant to Maersk.

Lawfulness

The processing of Personal Data by Maersk shall be done lawfully in compliance with the relevant statutory provisions and with due regard for the principles laid down in the BCR.

The processing of Personal Data by a Maersk entity is only permissible if at least one of the following prerequisites are fulfilled:

a) the Data Subject has given its unambiguous consent;

b) processing is necessary for the performance of a contract to which the Data Subject is party or to take steps at the request of the Data Subject to establish a contractual relationship with the Data Subject;

c) processing is necessary to safeguard legitimate interests of the controller and such legitimate interest is not overridden by the interest of the Data Subject; or

d) processing is necessary for compliance with the law of the Member State to which the controller is subject; or

e) processing is necessary to protect the vital interests of the Data Subject or of another natural person.

Fairness

Any processing of Personal Data by Maersk must be done for specified, explicit and legitimate purposes which are known to the Data Subject or which are within their reasonable expectations.

Transparency

Any processing of Personal Data by Maersk must be transparent for the Data Subject. Maersk will ensure that Data Subjects are provided with information as set out in articles 13 and 14 of the GDPR within the timelines for providing information set out herein. Maersk will ensure that the information provided is concise, easily accessible and easy to understand, and that clear and plain language is used. Where appropriate, Maersk will use visualisation to provide the information.

2.3 Information to be provided to Data Subjects

Prior to processing any Personal Data on Data Subjects, it must be ensured that the processing is covered by a privacy statement or privacy policy, which is consistent with the BCR and which provides the Data Subject with the information required pursuant to articles 13 and 14 of the GDPR, as set out below.

When providing the information, Maersk will ensure to observe the requirements set out in this clause 2.3.

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

Except where the Data Subject already has the information, each Maersk entity will provide Data Subjects (from whom Personal Data relating to the Data Subject is collected) with at least the following information:

a) the identity and contact details of the controller and its representative, if any;

b) the contact details of Maersk's Data Privacy Compliance Officer, i.e. dataprivacy@maersk.com;

c) the purpose(s) of the processing and the legal basis for the processing;

d) where the processing is based on a balancing of interests, the legitimate interest pursued by the relevant Maersk entity;

e) the recipients or categories of recipients;

f) where applicable that the Personal Data is intended to be transferred to a third country, including how adequate safeguards for the protection of data is ensured and the means by which to obtain a copy of or more information on such adequate safeguards.

In addition to the above, each Maersk entity will, at the time when the Personal Data are obtained, provide the Data Subject with the following further information necessary to ensure fair and transparent processing:

g) the period for which the Personal Data will be stored or if that is not possible, the criteria used to determine that period;

h) the existence of the right to request access to, rectification or restriction of and/or erasure of Personal Data as well as the right to object to the processing;

i) the right to data portability;

j) where a processing is based on consent, the right to withdraw such consent;

k) the right to lodge a complaint with an EEA Supervisory Authority;

l) whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, including whether the Data Subject is obliged to provide the Personal Data as well as the possible consequences of failure to provide such Personal Data;

m) whether automated decision making will be applied to the Personal Data, including information on the logic involved in such decision making and the significance and envisaged consequences of such processing.

Where a Maersk entity intends to process Personal Data for a different purpose than that for which the Personal Data were originally collected, the Maersk entity in question will notify the Data Subject prior to that further processing on the purpose of such processing and provide the Data Subject with any other relevant information pursuant to clause 2.3 a)- 2.3 m).

Information to be provided where Personal Data is not obtained from the Data Subject

Where the Personal Data has not been obtained from the Data Subject and where the Data

Subject does not already have the information, each Maersk entity will provide the Data Subject with the information set out in clause 2.3 a)-2.3 c)c) and clause 2.3 2.3g)-2.3 2.3m) and in addition the following information:

n) the categories of Personal Data concerned; and

o) where necessary to ensure fair and transparent processing information on:

   i) from which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources;

   ii) any relevant further information as set out in clause 2.3 e)- 2.3 f).

Timeline for providing the Data Subject with information

Each Maersk entity will provide the information set out in this clause 2.3:

a) within a reasonable period after obtaining the Personal Data, but no later than within one (1) month;

b) where the Personal Data are to be used for communication with the Data Subject, at the latest when the Maersk entity in question is first communicating to the Data Subject;

c) if disclosure to a third party is envisaged, at the latest when the Personal Data is first disclosed to such third party.

Where a Maersk entity intends to process Personal Data for a different purpose than that for which the Personal Data were originally collected, the Maersk entity in question will notify the Data Subject prior to that further processing on the purpose of such processing and provide the Data Subject with any other relevant information pursuant to this clause 2.3.

Exceptions to providing Individuals with information

When provided for by applicable law of an EU Member State, the Data Subject will not have a right to information under the following circumstances:

a) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in article 89(1) of the GDPR, or in so far as the obligation referred to in this clause 2.3 is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the relevant Maersk Entity will take appropriate measures to protect the Data Subject's rights and freedoms and legitimate interests, including making the information publicly available;

b) if obtaining or disclosure of the personal data is expressly laid down by EU or Member State law to which the relevant Maersk Entity is subject and which provides appropriate measures to protect the Data Subject's legitimate interests; or

c) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or Member State law.

2.4 Processing of Personal Data for a new purpose

Maersk will only process Personal Data for the specified, explicit and legitimate purposes for which it was collected, unless Maersk has a legal basis for processing the Personal Data for a new or different purpose and has otherwise observed the requirements under the GDPR.

If Maersk collects Personal Data for a specific purpose (as communicated to the Data Subject via the relevant privacy statement or otherwise) and subsequently, Maersk wishes to process the Personal Data for a different or new purpose, the relevant Data Subjects will be provided with information prior to that further processing on the purpose of such processing and any other relevant information pursuant to clause 2.3 above, unless:

a) the processing is compatible with the purposes for which the Personal Data were initially collected; or

b) there is a legal basis for not doing so, as described in clause 2.3 above.

In certain cases, for example, where the processing is of Special Categories of Personal Data, or where Maersk deems that no other legal basis applies, the Data subject's consent to the new use or disclosures may be necessary.

In some circumstances, for example where the new purpose of processing is for statistical, historical, or scientific research purposes, it will generally be permissible for Maersk to use a Data Subject's Personal Data for that new purpose, provided that this clause 2.4 is observed and provided that the data subject has been informed of such purpose and that the processing is subject to the conditions and safeguards referred to in article 89(1) of the GDPR.

2.5 Accuracy and Data Minimisation

Maersk will only process Personal Data, which is adequate, relevant and not excessive and will keep Personal Data accurate and up to date.

Maersk will only collect and use such Personal Data as may be necessary and proportionate in order to properly fulfil the purposes for which the Personal Data is processed.

Maersk will also keep Personal Data accurate and up to date. The main way of ensuring that Personal Data are kept accurate and up to date is by actively encouraging Data Subjects to inform Maersk when their Personal Data changes.

2.6 Privacy by Design

Maersk considers data privacy as an integral component of the design, development, operation and management of new projects, tools, applications and internal services where processing of Personal Data is taking place. When Maersk engages vendors and partner organizations as part of any design, development and implementation work, Maersk will ensure that privacy by design is an integral component.

2.7 Privacy by Default

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

2.8 Data retention

Maersk will only keep Personal Data for as long as is necessary for the purpose for which such data were collected or further processed.

Maersk will comply with any applicable internal guidelines, including but not limited to, privacy statements and guidelines (or equivalent) and information security policies (or equivalent) as revised and updated from time to time, including the provisions relating to data retention therein.

Personal Data, which is no longer required for the purposes for which it was originally collected and stored, is to be erased. In the event that statutory retention periods apply, the data shall be restricted rather than erased.

2.9 Special Categories of Personal Data

Maersk will only process Special Categories of Personal Data if it is necessary to do so.

For the purpose of the BCR, and taking into account local law variations, Special Categories of Personal Data, are defined as information relating to a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, sex life or sexual orientation, and criminal offences.

Maersk will in some situations process Special Categories of Personal Data about Data Subjects, such as information on trade union membership, health and criminal offences etc. However, Maersk will, in accordance with the principle of data minimization, assess whether Special Categories of Personal Data is actually required for the proposed use and when it is necessary in the context of the business.

Further, the collection and processing of Special Categories of Personal Data within Maersk must also take place with due consideration to any applicable anti-discrimination legislation.

Maersk will only process Special Categories of Personal Data where the Data Subject's explicit consent has been obtained unless Maersk has an alternative legitimate basis for the processing.

Data Subjects must explicitly consent to the collection and processing of their Special Categories of Personal Data by Maersk unless Maersk has another legal basis for doing so, for example, where the processing is necessary:

a) for the purposes of carrying out the obligations and exercising specific rights of a Maersk entity in the field of employment law or other applicable Member State laws and regulations;

b) to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his or her consent; or

c) for the establishment, exercise or defence of legal claims.

If relying on explicit consent to process Special Categories of Personal Data, it must be specific, informed and freely given. Further, the consent must represent an unambiguous indication of the Data Subject's wishes by which he or she, by a statement or clear affirmative action, signifies agreement to the processing of the Personal Data relating to him or her.

When collecting consent, Maersk will ensure to inform Data Subjects of their right to withdraw consent at any time.

2.10 Automated individual decisions

There are particular requirements in place under EEA data protection legislation to ensure that no evaluation of or decision about a Data Subject which significantly affects them can be based solely on the automated processing of Personal Data unless measures are taken to protect the legitimate interests of Data Subjects.

Where decisions are made by automated means which have a significant or legal effect on Data Subjects, Data Subjects must be provided with meaningful information about the logic involved in the decision, as well as information about the significance and envisaged consequences of such processing for the Data Subject. Maersk will take necessary measures to protect the legitimate interests of Data Subjects when applying automated individual decisions.

The above will not apply if the automated decision is authorised or required by applicable legislation of an EEA country, or taken in preparation for, or in relation to, a contract with the Data Subject concerned, and, is to give the Data Subject something they have asked for, or where steps have been taken to safeguard the legitimate interests of the Data Subjects, or is based on the Data Subject's explicit consent.

Such processing should be subject to suitable safeguards, which include implementing the right to obtain human intervention with the Maersk entity, to express his or her point of view and to contest the decision.

2.11 Transfers to third parties in non-EEA countries

Maersk will not transfer Personal Data collected by a controller in the EEA to a third-party outside Maersk in non-EEA countries without ensuring adequate protection for the Personal Data.

The transfer of Personal Data from a Maersk entity to a non-Maersk entity (i.e. a company that is not bound by the Maersk BCR) outside the EEA is only permissible under the following conditions:

a) the receiving entity demonstrates that it has an adequate level of protection for Personal Data within the meaning of Article 46 of the GDPR, e.g. by concluding an EU standard contract (Standard Contractual Clauses for Data Processors 2010/87/EU or Standard Contractual Clauses between Data Controllers 2001/497/EC or 2004/915/EC) or by concluding other appropriate contractual agreements between the transferring and the receiving entity; or

b) the transfer is permissible under the exceptions defined in Article 49 of the GDPR, to the extent such transfer is not massive, disproportionate or indiscriminate; and

c) transfers of Personal Data from a Maersk entity to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

Furthermore, if the receiving entity is a data processor, the conditions set out in Articles 24, 25, 28, 29 and 32 of the GDPR must additionally be satisfied.

2.12 Security

Maersk will adhere to appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures will ensure a level of security appropriate to the risks represented by the processing and the nature of the Personal Data to be protected (privacy by design).

Special categories of Personal Data will be subject to specific security and protection measures. Such measures will further ensure that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed (privacy by default).

Maersk complies with the Maersk information security policies as revised and updated from time to time together with any other security policies and guidelines applicable to a Maersk entity.

Maersk has implemented a data protection breach procedure setting out how all Personal Data breaches must be reported to the Data Privacy Compliance Officer and procedures for how the Data Privacy Compliance Officer and the Maersk entities must handle Personal Data breaches, including reporting such to dataprivacy@maersk.com. Furthermore, the data protection breach procedure sets out how Maersk will ensure to notify Data Subjects of a Personal Data breach where the Personal Data breach is likely to result in a high risk to the rights and freedoms of the Data Subjects. Furthermore, any Personal Data breaches will be documented (comprising the facts relating to the Personal Data breach, its effects and the remedial action taken) and the documentation will be made available to the EEA Supervisory Authorities on request.

Maersk will ensure that providers of services (data processors) to Maersk also adopt appropriate security measures.

2.13 Processing by data processors

If an external service provider to a Maersk entity has access to Personal Data about Data Subjects (e.g. an external hosting provider), the following requirements will be observed:

a) the service provider is carefully assessed and selected by the Maersk entity being the controller on the basis of the processor's ability to ensure the implementation and maintenance of necessary technical and organizational security measures required for complying with the Maersk BCR in relation to data processing;

b) the controller will ensure and regularly verify that the processor remains fully compliant with the agreed technical and organizational security requirements;

c) the rights and obligations of the processor must be regulated in a written agreement in which the rights and obligations of the processor are unambiguously defined. In particular, such agreement will stipulate that the processor:

   i) processes the Personal Data only on documented instructions from the controller;

   ii) ensures the confidentiality of persons processing the Personal Data;

   iii) will not engage another processor without prior authorisation from the controller;

   iv) takes all measures required to implement the necessary technical and organisational security measures;

   v) ensures that any processing by a sub-processor will be subject to the same data protection requirements as stipulated in the agreement between the controller and the processor;

   vi) assists the controller with answering requests from Data Subjects to exercise their rights;

   vii) that the processor remains liable to the controller for any breach of the data protection obligations by a sub-processor;

   viii) assists the controller in ensuring compliance with applicable security requirements, notification of EEA Supervisory Authorities and Data Subjects in case of a data breach and with conducting data protection impact assessments and prior consultations with EEA Supervisory Authorities, if necessary;

   ix) at the choice of the controller deletes or returns all copies of the Personal Data to the controller upon termination of the services;

   x) makes available to the controller all information necessary to demonstrate compliance with data protection legislation, in particular that the processor will contribute to audits, including inspections, conducted by the controller or a third party appointed by the controller; and

   xi) the controller retains responsibility for the legitimacy of the processing and continues to be the point of contact for the Data subject.

Where Maersk entities process Personal Data on behalf of other Maersk entities, a written agreement must be entered between the Maersk entities acting as processor and controller, respectively.

Where a service provider is a Maersk entity processing Personal Data on behalf of another Maersk entity, the Maersk entity which is the controller must ensure that the requirements set out in this clause 2.13 are observed and that a written agreement is entered with the Maersk entity acting as the processor (e.g. in the form of a Service Level Agreement). Such agreement must meet the requirements set out in this clause 2.13.

2.14 Data Subjects' Rights

Maersk will adhere to the Data Subjects' Requests and Complaints Procedure set out in Appendix 1, and will be receptive to any queries or requests made by Data Subjects regarding the processing of their Personal Data.

Each Maersk entity will ensure that all data subjects will be able to obtain:

a) confirmation as to whether or not Personal Data relating to the data subject is being processed and the following information:

   i) the purposes of the processing,

   ii) the categories of Personal Data concerned,

   iii) the recipients or categories of recipients to whom the Personal Data are disclosed,

   iv) the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period,

   v) the existence of the right to request from the Maersk entity rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the data subject or to object to such processing,

   vi) the right to lodge a complaint with an EEA Supervisory Authority,

   vii) where the Personal Data are not collected from the Data Subject, any available information as to their source, and

   viii) whether automated decision making will be applied to the Personal Data, including information on the logic involved in such decision making and the significance and envisaged consequences of such processing;

b) communication to the Data Subject in an intelligible form of the Personal Data undergoing processing and of any available information as to their source, including a copy of the Personal Data undergoing processing;

c) the rectification, restriction or erasure of Personal Data of which the processing does not comply with the provisions of the BCR or applicable local law, in particular because of the incomplete or inaccurate nature of the Personal Data;

d) notification to third parties to whom the Personal Data has been disclosed of any rectification, restriction or erasure carried out in compliance with (c), unless this proves impossible or involves a disproportionate effort, without constraint, at reasonable intervals and without excessive delay or expense. The response may be in a written form (e-mail will be sufficient);

e) restriction of a Maersk entity's processing of the Data Subject's Personal Data where:

   i) the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the Maersk entity 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 Maersk entity no longer needs the Personal Data for the purposes of the processing, but they are 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 Maersk entity override those of the Data Subject;

f) the Personal Data which the Data Subject has provided to the Maersk entity being the controller in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller where

   i) the processing is based on consent from the Data Subject or on a contract with the Data Subject in accordance with clause 2.2 b), and

   ii) the processing is carried out by automated means;

g) the right at any time to object, on grounds relating to the Data Subject's particular situation, where the processing of Personal Data is based on a balancing of interests, including profiling; and

h) 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.

Applicable Data Protection Legislation may restrict the Data Subject's right to access if this right is exercised repeatedly within a short period of time, unless the Data Subject can show a legitimate reason for the repeated assertion of claims for information.

Each Maersk entity may charge the Data Subject a reasonable fee for repeatedly providing the information, to the extent that applicable Data Protection Legislation permits this.

Further, each Maersk entity will ensure that all Data Subjects may at any time object to the Maersk entity's processing of Personal Data relating to the Data Subject. Where the objection is justified, each Maersk entity will ensure that the Personal Data is erased and will no longer be processed.

The Data Subject can assert the above rights by contacting the respective HR department, HR Privacy Lead or the Data Privacy Compliance Officer of Maersk.

3 SUPERVISION OF DATA PRIVACY COMPLIANCE

3.1 Accountability

Everyone who works for or on behalf of Maersk is:

a) responsible and accountable for processing Personal Data ethically and lawfully and in compliance with the provisions of the BCR;

b) expected to comply with Maersk's policies and data privacy practices when processing Personal Data; and

c) expected to understand the data privacy requirements which have relevance to the Personal Data they process on behalf of Maersk using our policies and training material.

Maersk has processes and procedures in place to manage and monitor our compliance with data privacy requirements, including the BCR. Further, Maersk has appropriate technical and organizational measures to meet these requirements. Everyone at Maersk is expected to follow these processes and comply with such procedures and measures.

3.2 Records of processing activities

Each Maersk entity has established and maintains a record of all categories of processing activities carried out by the Maersk entity. The record of processing activities contains the following information for each processing activity:

a) the name and contact details of the Maersk entity;

b) the purposes of the processing;

c) a description of the categories of Data Subjects and of the categories of Personal Data;

d) the categories of recipients to whom the Personal Data have been or will be disclosed, including recipients in countries outside of the EEA;

e) where transfers of Personal Data to a recipient in countries outside of the EEA, the country/-ies in which the recipient is established and the documentation of suitable safeguards (e.g. the Commission's standard contractual clauses);

f) where possible, the envisaged time limits for erasure of the different categories of data; and

g) where possible, a general description of the technical and organisational security measures implemented to protect the Personal Data.

The record is maintained in writing, including in electronic form, and will be made available to an EEA Supervisory Authority on request.

3.3 Data Protection Impact Assessments

Each Maersk entity will assess the risk of its processing activities and where it is assessed that a processing activity is likely to result in a high risk to the rights and freedoms of natural persons, the Maersk entity will in cooperation with the HR Privacy Lead carry out a data protection impact assessment in accordance with Article 35 of the GDPR.

If the data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Maersk entity to mitigate the risk, the HR Privacy Lead must consult the Data Privacy Compliance Officer and the Data Privacy Compliance Officer will consult the competent EEA Supervisory Authority, prior to processing Personal Data for the relevant processing activity.

3.4 Training

Maersk will provide appropriate training to employees who permanently or regularly handle Personal Data, who are involved in the collection of Personal Data relating to Data Subjects and employees who are engaged in the development of tools used to process Personal Data about Data Subjects or the acquisition of such tools/IT systems. Maersk has developed a Data Privacy Introduction video (available in English, Chinese, Portuguese and Spanish) as well as Data Privacy e-learning course for HR professionals. Both of these training tools are mandatory to complete. The e-learning course focuses on the processing of Personal Data during an entire employment, thus focusing on how to process Personal Data on applicants, current employees and former employees. HR continuously monitors the completion rate of the trainings and follows up upon reports.

3.5 Audit

Maersk will comply with the Audit procedure set out in Appendix 2. The purpose of the audits is to assess our compliance with our internal procedures and practices, applicable Data Protection Legislation and the BCR.

3.6 Complaint handling

Maersk will comply with the procedure on complaints set out in Appendix 1 (Data Subjects' Requests and Complaints Procedure).

3.7 Co-operation with Supervisory Authorities

Maersk will comply with the procedure for co-operation with EEA Supervisory Authorities set out in Appendix 3.

3.8 Update of the BCR

Maersk will comply with the Updating Procedure set out in Appendix 4.

4 RELATIONSHIP BETWEEN THE BCR AND LOCAL STATUTORY REGULATIONS

The legitimacy of the processing of Personal Data is judged on the basis of the applicable local law. To the extent that the applicable local law stipulates a higher level of protection of Personal Data than the BCR, data processing shall be in accordance with the applicable local law. Each Maersk entity shall check for itself, whether local data protection laws exist and shall ensure compliance with these. If the applicable local law provides a lower level of protection for Personal Data than the BCR, the present BCR shall be applied.

Maersk will ensure that if there is reason to believe that local legislation applicable to any Maersk entity prevents it from fulfilling its obligations under the BCR or such legislation has a substantial adverse effect on its ability to comply with the BCR, the Maersk entity will promptly inform the Data Privacy Compliance Officer unless prohibited by law or a law enforcement authority.

Maersk will ensure that if there is a conflict between the legislation applicable to it and the BCR, the Data Privacy Compliance Officer will make a responsible decision as to which action to take and will consult the EEA Supervisory Authority with competent jurisdiction in case of doubt.

In addition, where any legal requirement of a non-EEA country applicable to a Maersk entity is likely to have a substantial adverse effect on the guarantees provided by the BCR, the Maersk entity will promptly inform the Data Privacy Compliance Officer who will report such problem to the competent EEA Supervisory Authority.

This includes any legally binding request for disclosure of the Personal Data by a law enforcement authority or state security body. In such a case, the Data Privacy Compliance Officer will inform the competent EEA Supervisory Authority about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

If in specific cases the suspension and/or notification are prohibited, the requested Maersk entity will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible. The Maersk entity must document such efforts to be able to demonstrate that it did so.

If, in the above cases, despite having used its best efforts, the requested Maersk entity is not in a position to notify the competent EEA Supervisory Authorities, it must on an annual basis provide general information on the requests it received to the competent EEA Supervisory Authorities (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).

APPENDIX 1 DATA SUBJECTS' REQUESTS AND COMPLAINTS PROCEDURE

1. Background

EEA data protection law gives Data Subjects whose Personal Data is collected and/or used in EEA certain rights, and in Maersk, we extend this as our standard global procedure. This procedure explains how Maersk deals with the following rights:

Data Subjects' Rights	Sections below applicable
The right to be informed whether any Personal Data about them is being processed by the organisation and to request certain information about the processing of their Personal Data. This is known within Maersk as an **access request**.	Sections 2 and 3
Where a Data Subject's Personal Data is incomplete or inaccurate, the Data Subject has the **right to request rectification, restriction of processing and erasure** of their Personal Data.	Sections 2 and 4
Data Subjects have the **right to request portability** of the Personal Data, which they have provided to Maersk, where the processing by Maersk is based on consent or on a contract with the Data Subject and where the processing is carried out by automated means.	Section 2 and 4
The Data Subjects have the **right at any time to object** to the processing of Personal Data concerning him or her, on grounds relating to the Data Subject's particular situation, where the processing of Personal Data is based on a balancing of interests, including against being subject to automated decision making such as profiling, which produces legal effects or significantly affects the Data Subjects.	Section 2 and 4
The Data Subject has the **right to complain** to Maersk. This includes complaints about the way in which Maersk has responded to a Data Subject's access request, or request for the deletion, amendment or cessation of processing of the Data Subject's Personal Data, as well as complaints about Maersk's compliance with the BCR.	Sections 2 and 5

Where a Data Subject's request or complaint is subject to EEA data protection laws because it is made in respect of Personal Data collected and/or used within the EEA, such a request or complaint will be dealt with by Maersk in accordance with this procedure, however, the local EEA law will prevail if the EEA data protection law differs from this procedure.

2. Initial procedure for receipt of requests and complaints

Data Subjects can make requests/objections or complaints by contacting the relevant HR department, HR Privacy Lead or Maersk's Data Privacy Compliance Officer by contacting DataPrivacy@maersk.com.

Access requests are handled by the HR Privacy Lead.

Other requests and objections are handled by HR.

Complaints are handled by the HR Privacy Leads with an option to appeal a response to Maersk's Data Privacy Compliance Officer by contacting DataPrivacy@maersk.com.

If a request/objection is received by anyone other than the HR department then the request/objection must be forwarded to the relevant HR department or HR Privacy Lead immediately, indicating the date on which it was received together with any other information which may be of help in dealing with the request/objection. Similarly, complaints must be sent to the HR Privacy Lead.

2.1 Relevant information from a Data Subject

Both requests and complaints should preferably be made in writing (which can include email), and preferably in English (however, neither language nor format are firm requirements).

Data Subjects should indicate the following in their request or complaint:

a) Their full name, position and contact details (email address and telephone number, incl. country code (e.g. +45 for Denmark))

b) The name of the Maersk entity or at least the Maersk entity and country to which their request or complaint relates

Where a Data Subject is making an access request, requesting portability, rectification or erasure, or objecting to processing, the Data Subject must also specify:

a) the type of data to which the Data Subject is seeking access, requiring portability, rectification or deletion, or objecting to processing (as relevant);

b) the system in which the data are likely to be stored and the likely dates (if known); and

c) the circumstances in which Maersk obtained the data (if known)

Where a Data Subject is making a complaint, he/she must also provide:

a) a description of the reason why the Data Subject is making the complaint, including a detailed description of the circumstances leading to the complaint.

Maersk is only obliged to process a Data Subject's request or complaint if Maersk is supplied with the necessary information required to confirm the identity of the Data Subject making the request or complaint and to locate any Personal Data requested or complained about, if relevant.

2.2 Clarification of requests or complaints

Maersk will provide reasonable assistance to a Data Subject making a request or complaint to enable that Data Subject to provide Maersk with the information it needs in order to process the Data Subject's request or complaint. Where information which is necessary for Maersk to deal with the matter is missing, HR will for requests and the HR Privacy Lead will for complaints contact the Data Subject with a request to provide the necessary information and explain to the Data Subject that Maersk need not comply with a Data Subject's request or complaint if:

a) The request/complaint does not contain the information required under section 2.1 of this procedure where that information is necessary to enable Maersk to comply with the request/complaint;

b) The request/complaint is not sufficiently specific; or

c) The identity of the relevant Data Subject cannot be established by reasonable means.

In addition, Maersk need not comply with a Data Subject's access request if Maersk has previously complied with an access request made by the Data Subject, and where:

a) one or more further access requests are then made by the same Data Subject for identical Personal Data; and

b) no reasonable interval or specific interval as stipulated by applicable local law has elapsed between compliance with a previous request and the Data Subject's new request.

In making this decision, the HR Privacy Lead will take into account the nature of the Personal Data processed, how often that Personal Data is amended and the purpose of processing the Personal Data.

2.3 Initial assessment of all requests or complaints

When all requested information has been received from the Data Subject, HR will for requests and the HR Privacy Lead will for complaints send written confirmation of receipt of the request or complaint. Where Maersk cannot comply with the request or complaint for the reasons set out in section 2.2 of this procedure, Maersk will inform the Data Subject accordingly. The information to the Data Subject will contain the reasons for Maersk's inability to comply with the request or complaint as well as an explanation of the consequences hereof.

3. Access requests

3.1 Approach and scope

The request does not have to be official or mention data protection law to qualify as an access request.

A Data Subject making an access request to a Maersk entity is entitled to:

a) Be informed whether the Maersk entity holds and is processing Personal Data about that Data Subject.

b) Be given at least the following information:

i) the purposes for which the Personal Data are being processed;

ii) the categories of Personal Data processed about the Data Subject;

iii) the recipients or categories of recipients to whom the Personal Data have been, or may be, disclosed by Maersk;

iv) the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;

v) the existence of the right to request from the Maersk entity rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the Data Subject or to object to such processing as well as the right to lodge a complaint with an EEA Supervisory Authority;

vi) where the Personal Data are not collected from the Data Subject, any available information as to their source, and

vii) whether automated decision making will be applied to the Personal Data, including information on the logic involved in such decision making and the significance and envisaged consequences of such processing.

c) Receive communication in an intelligible form of the Personal Data held by the Maersk entity.

Usually no fee will be charged for an access request but this will be left to the discretion of the Maersk entity to which the access request relates in accordance with local applicable law.

3.2 Exemptions to a Data Subject's Right of Access

An access request may be refused on the following grounds:

Within the EEA. Where the access request is made to an EEA Maersk entity and relates to Personal Data controlled by that entity, the access request may be rejected if this is consistent with applicable Data Protection Legislation within that jurisdiction. Overall, the following grounds may according to general EEA-legislation justify not granting access:

a) national security, defence or public security;

b) the prevention, investigation, detection and prosecution of criminal offences;

c) the protection of the Individual or of the rights and freedoms of others.

Outside the EEA. Where the access request is made to a non-EEA Maersk entity and relates to Personal Data controlled by that entity and if, in the opinion of Maersk:

a) the information is subject to legal proceedings, litigation or legal privilege); or

b) it is necessary to refuse the access request in order to safeguard national or public security, defence, or the prevention, investigation, detection and prosecution of criminal offences; or

c) it is necessary to refuse the access request for the protection of the Data Subject or of the rights and freedoms of others; or

d) if the Personal Data are held by Maersk in non-automated form and are not or will not become part of a filing system; or

e) where the Personal Data do not originate from EEA nor have been processed by any establishment of a controller or processor in the EEA (i.e. where the processing relates to personal information which falls outside the scope of the GDPR), if:

   i) the Data Subject's interest in obtaining access is overridden by essential business interests of Maersk (which includes but is not limited to situations where the granting of access would cause material damages or have a material adverse effect on Maersk or the Maersk entity's business foundation, practices, and know-how, management planning, management forecasting, corporate finance or assessments or negotiations with a Data Subject, or where

   ii) the provision of the Personal Data requires Maersk to use disproportionate effort; or

   iii) the refusal to provide the Personal Data is consistent with the laws within that jurisdiction.

3.3 The search and the response

The relevant HR Privacy Lead will arrange a search of the relevant electronic and paper filing systems through the designated teams in Maersk.

The HR Privacy Lead may refer any complex/non-routine cases to Maersk's Data Privacy Compliance Officer for advice, particularly where the access request includes information relating to third parties or where the release of Personal Data may prejudice commercial confidentiality or legal proceedings.

The Personal Data requested will be collated by the HR Privacy Lead into a readily understandable format (internal codes or identification numbers used in Maersk which correspond to Personal Data shall be explained in connection with provision of the information).

The HR Privacy Lead will prepare a cover letter, which includes the Personal Data required to be provided in response to a Data Subject's access request.

Where the provision of the Personal Data in permanent (tangible) form is impossible or would involve disproportionate effort, there is no obligation to provide a permanent copy of the Personal Data. The other information referred to in section 3.1 above must still be provided. In such circumstances, the Data Subject should be offered the opportunity to have access to the Personal Data by inspection at Maersk premises or to receive the information in another form.

3.4 Deadline

The HR Privacy Lead must provide a response to an access request without undue delay and in any event within one (1) month of receipt of the request. The period for responding to the request may be extended by two (2) further months where necessary, taking into account the complexity and number of the requests. The BU HR Privacy Lead will inform the Data Subject of any such extension within one (1) 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 will be provided by electronic means where possible, unless otherwise requested by the data subject.

4. Procedure for requests for rectification, restriction of processing or erasure, portability and objections to processing of Personal Data

4.1 Receiving a request

If a request is received advising of a change in the Data Subject's Personal Data, such information must be rectified or updated accordingly if Maersk is satisfied that there is a legitimate basis for doing so.

If a request is received for restriction or erasure of a Data Subject's Personal Data, such a request must be considered and dealt with as appropriate by the relevant HR department.

If the request/objection is to restrict processing of the Data Subject's Personal Data because the rights and freedoms of the Data Subject are prejudiced by virtue of such processing by Maersk, or on the basis of other compelling legitimate grounds, the matter will be handled by the relevant HR department.

If a request concerns the portability of Personal Data which the Data Subject provided to Maersk in accordance with clause 2.14 f) of the BCR, Maersk will take steps to ensure that satisfying the request would not affect the rights and freedoms of other individuals. Such a request must be considered and dealt with as appropriate by the relevant HR department

If the request is received in conjunction with the Data Subject's right to object to the processing of their Personal Data by Maersk, there may be grounds for Maersk to continue certain types of processing where we can demonstrate that Maersk's legitimate interests override the rights of an individual or in instances where the processing is necessary for the establishment, exercise or defence of legal claims. The right to object request will be handled by the relevant HR department.

Maersk will respond to an individual's request within the specified timeframe. Where Maersk cannot process an objection, a notification explaining the reasons why will be sent.

The HR department may refer any complex/non-routine cases to the relevant HR Privacy Lead for handling or advice or to Maersk's Data Privacy Compliance Officer for advice.

4.2 The response and deadline

The HR department will provide a response to a request within one (1) month (or any shorter period as may be stipulated under local law) of receipt of all of the information required to process the request. If it is not possible to provide the response within one (1) month, the HR department will provide a reason for not providing the response and a time estimate of when a

response will be provided. However, a response must be provided within three (3) months of receipt of the request.

5. Complaint handling

5.1 Receiving a complaint

After the initial assessment described in section 2.2 and 2.3 above, the HR Privacy Lead will liaise with colleagues from relevant Maersk entities, as appropriate, to deal with complaints.

5.2 Deadline

The HR Privacy Lead will investigate and make a substantive response within four (4) weeks from the date the complaint was received (or any shorter period as may be stipulated under local law). If, due to the complexity of the complaint, a substantive response cannot be given within this period, the HR Privacy Lead will advise the Data Subject accordingly and provide a reasonable estimate for the timescale within which a response will be provided which will be no later than three (3) months from the date the complaint was submitted and all relevant information had been collected. This may e.g. be the case if the subject matter of the complaint is particularly complex or if involvement of third parties, including other data subjects, is necessary to resolve the complaint.

5.3 When a Data Subject disputes the response

If the Data Subject disputes the response of the HR Privacy Lead or any aspect of a finding and notifies the HR Privacy Lead, the matter will be referred to Maersk's Data Privacy Compliance Officer who will review the case and advise the Data Subject of his or her decision either to accept the original finding or to substitute a new finding. The Data Privacy Compliance Officer will respond to the Data Subject within one (1) month of the referral. As part of the review, the Data Privacy Compliance Officer may arrange to meet the parties in an attempt to resolve the complaint.

Data Subjects whose Personal Data are collected and/or used in accordance with EEA data protection law are afforded the third-party beneficiary rights set out in section 5.4 and may exercise these rights at any time, if he/she is not satisfied with the way in which the complaint has been resolved. Data Subjects entitled to such rights will be notified accordingly as part of the complaint handling procedure and will be given relevant information on how to lodge a complaint.

Data Subjects whose Personal Data is collected or otherwise processed is entitled to file a complaint to an EEA Supervisory Authority of competent jurisdiction or with a court as stated below in section 5.4, even if they have not beforehand filed a complaint with the relevant Maersk entity.

5.4 Third-party beneficiary rights

Third-party beneficiary rights are afforded to Data Subjects whose Personal Data are processed by a Maersk entity in the EEA acting as a controller and transferred to a Maersk entity in a non-EEA country, whether such entity acts as a controller or as a processor.

This group of Data Subjects has the right to:

g) **Enforce Compliance:** Seek to enforce compliance by Maersk with the BCR (including the appendices), including but not limited to seeking enforcement of the following rights and principles:

vi) local statutory regulations in accordance with the BCR, insofar as such local law stipulates a higher level of protection of Personal Data than the BCR;

vii) the substantive principles for the processing of Personal Data set out in clause 2; specifically

viii) the rights of the data subject set out in clause 2.14;

ix) the right to make a complaint through the procedure set out in the Data Subjects' Requests and Complaints Procedure;

x) any support of or cooperation needed with EEA Supervisory Authorities pursuant to clause 3.7.

h) **Complain to Maersk:** Complain to a Maersk entity in the EEA responsible for exporting the Personal Data in accordance with Appendix 1 (Data Subjects' Requests and Complaints Procedure) and seek redress from the Maersk entity in the EEA responsible for exporting the Personal Data including the remedy of any breach of the BCR by the non-EEA Maersk entity.

i) **Seek compensation:** Where required, receive compensation from the EEA Maersk entity responsible for exporting the Personal Data for any damage suffered as a result of a breach of the BCR by the non-EEA Maersk entity importing the Personal Data in accordance with the decision of an EEA court or other EEA competent authority.

j) **Complain to a Supervisory Authority:** Lodge a complaint with an EEA Supervisory Authority, in particular in the Member State of the data subject's habitual residence, place of work or place of the alleged infringement.

k) **Take judicial action:** Take action against a Maersk Entity in order to enforce compliance with the BCR in the courts of the jurisdiction in which the Maersk Entity responsible for the alleged breach is established, or the Maersk Entity responsible for exporting the personal data is established, or the data subject has his or her habitual residence.

l) **Burden of proof:** Where Data Subjects can demonstrate that they have suffered damage and can establish fact which show it is likely that the damage has occurred due to a breach of the BCR, Maersk has agreed that the burden of proof to show that no such breach took place, or that Maersk is not responsible for the breach, will rest with the EEA Maersk entity responsible for exporting the Personal Data of the Data subject as well as with the non-EEA Maersk entity importing the Personal Data of the Data subject.

5.5 The complaint is considered justified by Maersk

If the complaint is considered justified either at the level of the HR Privacy Lead or the Data Privacy Compliance Officer on appeal, they will as appropriate inform the Data Subject thereof and arrange for the necessary steps to be taken by the affected Maersk entity in order to correct the matter at hand and in order to implement corrective actions for the future at the affected and other Maersk entities.

6. Contact

All queries relating to this procedure are to be addressed to the relevant HR Privacy Lead. A query may also be addressed to Maersk's Data Privacy Compliance Officer at DataPrivacy@maersk.com and the Data Privacy Compliance Officer will then distribute a request to HR and a complaint to the relevant HR Privacy Lead.

APPENDIX 2 AUDIT PROCEDURE

1. Background

As part of the BCR, Maersk has audit procedures in place. This document describes how Maersk deals with such audits.

2. Approach

2.1 Responsibility

Maersk's Data Privacy Compliance Officer will be responsible for performing the audits and will ensure that audits address all aspects of the BCR, including appendices thereto. The Data Privacy Compliance Officer will advise on any corrective actions to ensure that compliance takes place. The Data Privacy Compliance Officer may delegate the practical handling of the audits to internal or external resources.

2.2 Timing

Audit of the BCR will take place annually or more often at the request of:

- Maersk's Executive Board;
- Maersk's CEO;
- Head of Brand (affected);
- Head of Legal;
- Maersk's HR Board (and if not represented on the HR Board, the management of the affected Maersk entity);
- Group Internal Audit; or
- Maersk's Data Privacy Compliance Officer.

2.3 Scope

Maersk's audit effort is multi-layered, embedded in existing processes and covers the entire BCR framework and the requirements and activities thereunder.

The scope of the audit performed annually will be decided by Maersk's Data Privacy Compliance Officer based on the use of a risk-based analysis which will consider relevant criteria, for example: areas of current regulatory focus; areas of specific or new risk for Maersk; areas with changes to the systems or processes used to safeguard information; areas where there have been previous audit findings or complaints; and the nature and location of the Personal Data processed. Further, the scope of audit will be decided based on the period since the last review of the part of the BCR in question, ensuring that audit addresses all aspects of the BCR.

An audit may be conducted by forwarding questionnaires for completion by the local Maersk entity, interviews with employees and vendors processing information, conducting on-site audits, etc.

The coverage may include, but is not limited to, applications, IT systems, databases, sharing of data, disclosure, onward transfers, decisions taken as regards mandatory requirements under national laws which conflict with the BCR, review of contractual terms used for transfers out of Maersk to controllers or processors and corrective actions (advice and follow-up).

Audits of the Data Privacy Compliance Officer's performance of his/her duties and responsibilities under the BCR will be carried out at regular intervals by either Group Internal Audit or by external counsel.

2.4 Auditors

Audit of the BCR, including the HR Privacy Leads' handling of their duties, will be undertaken by the Data Privacy Compliance Officer but reliance on work performed by other accredited internal/external auditors may be determined by the Data Privacy Compliance Officer. The Data Privacy Compliance Officer will manage and provide quality assurance of audit work performed by third parties outside Maersk.

2.5 Report

Maersk has agreed to provide copies of the results of any audit of the BCR to an EEA Supervisory Authority upon request. Maersk's Data Privacy Compliance Officer will be responsible for liaising with the EEA Supervisory Authorities for this purpose.

Internally, all audit reports will be distributed to Maersk's HR Board and to the management of the entities on which information is included in the report.

Audit reports will also be presented to the Executive Board of A.P. Møller – Mærsk A/S if they highlight any irregularities and as part of Maersk's report on the Commit Framework. The report will be distributed further within Maersk, as appropriate, if deemed relevant, e.g. for the purpose of corrective actions or raising awareness of data protection compliance.

2.6 Audits by Supervisory Authorities

In addition, Maersk will co-operate with the EEA Supervisory Authorities as set out in Appendix 3 with regard to audits carried out by the EEA Supervisory Authorities. Maersk's Data Privacy Compliance Officer will also be responsible for liaising with the EEA Supervisory Authorities for this purpose and will involve the relevant HR Privacy Leads as appropriate.

APPENDIX 3 CO-OPERATION WITH AUTHORITIES

1. Background

This Co-operation Procedure sets out the way in which Maersk will co-operate with the EEA Supervisory Authorities in relation to the BCR.

2. Approach

When required, Maersk will make the necessary and relevant employees available for dialogue with an EEA Supervisory Authority in relation to the BCR. Maersk will abide by:

- Any decisions made by relevant EEA Supervisory Authorities on any data protection law issues that may affect the BCR; and
- The views of the European Data Protection Board as outlined in its published guidance on Binding Corporate Rules and the views of its predecessor the Article 29 Working Party, to the extent guidance from the Article 29 Working Party still applies.

Maersk will provide upon request copies of the results of any audit of the BCR to an EEA Supervisory Authority of competent jurisdiction.

Where any Maersk entity is located within the jurisdiction of a Supervisory Authority based in the EEA, Maersk agrees that the Supervisory Authority may audit that Maersk entity for the purpose of reviewing compliance with the BCR, in accordance with the applicable laws of the country in which the Maersk entity is located, or, in the case of a Maersk entity located outside the EEA, in accordance with the applicable law of the country from which the Personal Data is transferred under the BCR (or as otherwise set out in applicable local law).

Maersk agrees to abide by advice given by the relevant EEA Supervisory Authority on any issues related to the interpretation and application of the BCR. Finally, Maersk will abide by the updating procedure set out in Appendix 4 (Updating Procedure).

APPENDIX 4 UPDATING PROCEDURE

1. Background

This Updating Procedure of the BCR sets out the way in which Maersk will communicate changes to the BCR to the EEA Supervisory Authorities, Data Subjects and to the Maersk entities bound by the BCR.

2. Approach

2.1 Notification to authorities

Maersk's Data Privacy Compliance Officer will without undue delay communicate any material changes to the BCR to the Danish Data Protection Agency and any other relevant EEA Supervisory Authorities. The Data Privacy Compliance Officer will also provide a brief explanation of the reasons for any notified changes to the BCR. Maersk will once a year provide the Danish Data Protection Agency with an overview of changes made, which are not considered substantial.

2.2 Notification to Maersk entities and Data Subjects

Maersk will without undue delay communicate any changes to the BCR to the Maersk entities bound by the BCR and to the Data Subjects benefitting from the BCR.

The Data Privacy Compliance Officer will keep a change log which sets out the date on which the BCR has been revised and the details of the revisions made.

Maersk's internal communication process includes communication by the Data Privacy Compliance Officer of the changes to the HR Privacy Leads, who will communicate the changes to the individuals bound by the BCR in accordance with their area of responsibility. The internal communication process also includes publication of the updated BCR on Maersk's intranet and on Maersk's external website. Further, if deemed necessary, notice will be made by email or other individual means of communication.

2.3 List of Maersk entities

The Data Privacy Compliance Officer of Maersk maintains an up-to-date list of the Maersk entities and the HR Privacy Lead will ensure that all new Maersk entities are bound by the Maersk BCR and can deliver compliance before a transfer of Personal Data to the entity takes place.

The Data Privacy Compliance Officer will communicate any substantial changes to the list of Maersk entities once a year to the Danish Data Protection Agency. Otherwise, the Data Privacy Compliance Officer will communicate an up-to-date list of Maersk entities to the Danish Data Protection Agency and any other relevant EEA data protection authorities when required.

APPENDIX 5 – GROUP STRUCTURE CHART

Please see attached.

APPENDIX 6 – LIST OF MAERSK ENTITIES BOUND BY THE BCR

Please see attached.