

BINDING CORPORATE RULES

SHIPPING **THE** FUTURE



CMA CGM LOG

CMA TERMINALS

CMA SHIPS



CONTENTS

Article 1 - Introduction.....	5
Article 2 - Definitions	5
Article 3 - Scope	6
3.1. Type of data processed (material scope)	6
3.2. Scope of transfers (geographical scope).....	6
Article 4 - Personal data protection principles.....	6
4.1. Purpose Limitation	6
4.2. Data minimization Data quality and storage limitation	6
4.3. Lawfulness of processing of Personal Data.....	7
4.4. Lawfulness of Processing of Special categories of Personal Data.....	7
4.5. Data protection by design and by default	8
4.6. Security of personal data	8
4.7. Onward transfers to organizations not bound by BCRs.....	8
Article 5 - Transparency and right of information.....	9
5.1. Information of Data Subjects.....	9
5.2. Accessibility of the BCRs.....	10
Article 6 - Right of access, rectification erasure, and portability of Data, rights to the restriction of Processing and right to object to the Processing	10
Article 7 - Automated Individual Decisions-making, including profiling	12
Article 8 - Security and confidentiality policy of Personal Data	13
Article 9 - Data transfer to a BCR Company acting as Processor	13
Article 10 - Restriction on transfers and onward transfers to External Processors or Controllers	15
10.1. Exportation to External Controllers	15
10.2. Exportation to External Processors.....	15
Article 11 - Audit concerning compliance with the BCRs	15
Article 12 - Training concerning the BCRs	16
Article 13 - Binding nature of the BCRs.....	17
13.1. Internal binding nature	17
13.2. Compliance and supervision of compliance	17
13.3. Sanctions.....	18
Article 14 - Mutual assistance and Cooperation with the Supervisory Authorities	18
Article 15 - Application of regional legal specificities.....	19
15.1. Relationships between national laws and the BCRs	19
15.2. Actions in case of national legislation preventing respect of BCRs.....	19
Article 16 - Updating the BCRs.....	19
Article 17 - Claim process.....	20

Claim conditions by Data Subjects.....20

Article 18 - Right of beneficiary third parties22

Article 19 - Liability.....23

Article 20 - Entry into effect and termination.....24

Article 21 - Interpretation of terms24

Article 22 - Applicable law / Jurisdiction.....24

Article 1 - Introduction

Personal data protection legislation aims at guarantying that individuals have a high level of control of their private life and personal data. As of May 2018, Regulation (EU) 2016/679 (the General Data Protection Regulation or "GDPR") and the 2002/58/EC Directive (together, and with any other applicable European regulations applicable to the processing and protection of Personal Data, the "European Data Protection Regulations") define the applicable legal framework in order to guarantee this level of protection for personal data.

The CMA CGM Group undertakes to comply with the European Data Protection Regulations. The person in charge of ensuring compliance is, the Chief Privacy Officer of the CMA CGM Group who has been appointed as Data Protection Officer for certain CMA CGM entities.

The European Data Protection Regulations which ensure that Personal Data of individuals who are in the European Union is protected require the CMA CGM Group to implement appropriate safeguards for Personal data transferred to any entity located outside the EEA.

Therefore, the CMA CGM Group is legally bound to protect Personal Data transferred (or accessible) from its information system, or by any other means, to the companies of the CMA CGM Group and all CMA CGM Group partners located outside the EEA.

In this context, BCRs are at the core of the GDPR, which explicitly recognizes them as an adequate safeguard for transfers of Personal Data outside of the EEA. The adoption and the implementation of BCRs to facilitate and protect international flows of Personal Data is thus an important part to ensure an adequate level of protection for cross-border transfers of Personal Data throughout the organization, regulating and protecting all intra-group cross-border transfers of Personal Data and, in particular outside of the EEA.

Consequently, the CMA CGM Group has decided to identify the companies of the CMA CGM Group likely to export and import Personal Data to each other (hereinafter jointly referred to as the "BCR Companies").

An exhaustive list of the BCRs Companies which are bound by the present BCRs either by signing the present document or by signing the "Undertaking to comply with the Binding Corporate Rules for personal Data Protection (Privacy Policy)" is provided in Appendix 5 of the BCRs and is regularly updated by the CPO.

BCR will apply whenever the transfer of Personal Data is not otherwise permitted by Article 49 of the GDPR and/or any other applicable law and to any subsequent onward transfer that is not otherwise permitted by applicable law.

Each of these BCR Companies shall comply with the present BCRs and ensure that their Employees comply with their provisions as well as with all applicable local laws and regulations in relation to the protection of Personal Data under penalty of internal sanctions (against the local Data Controller and/or a local Employee, if allowed under the respective local legislation). These sanctions may include prohibition of access to the CMA CGM information system or any other relevant corrective necessary measures (legal, technical or organizational) or appropriate sanction.

These rules are binding and mandatory for the BCR Companies and their Employees.

In compliance with the CNIL recommendations, and the recommendations of the "Group Article 29" in its working document WP154 dated 24 June 2008, the CMA CGM Board of Directors has accepted to procure that the BCR Companies will comply with these rules.

Article 2 - Definitions

All the definitions of the terms used are appended to these rules: Appendix 1 – Definitions.

Article 3 - Scope

3.1. Type of data processed (material scope)

The nature of the Personal Data being transferred within the scope of the BCRs and the purposes of the Processing therefore are detailed in Appendix 4.

3.2. Scope of transfers (geographical scope)

Appendix 5 includes a list of the BCRs Companies that are bound by the present BCRs and which will be updated by the CPO and communicated to all BCR Companies whenever amended.

It is specified that the present BCRs aim at framing Data Transfers between the BCRs Companies listed in Appendix 5, as amended from time to time, which act either as Data Exporters or as Data Importers.

Article 4 - Personal data protection principles

Any Data Transfer within the scope of the BCRs shall comply with the following data management principles as defined in the GDPR.

Each BCR Company shall be responsible for and be able to demonstrate compliance with the present data protection principles (accountability).

4.1. Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further Processing of data for archiving purposes in the public interest scientific or historical research purposes or statistical purposes shall not be considered as incompatible, provided implementation of appropriate safeguards for the rights and freedom of the Data Subjects and in particular technical and organizational measures in order to ensure data minimization.

In accordance with the principle of purpose limitation, Processing of Personal Data exported to BCR Companies must comply with the purposes mentioned by the Data exporter and listed in Article 3.1 of the BCRs.

The Data importer shall be held liable for any deviation from these purposes.

In case of doubt, the manager of the BCR Company must contact the Local Privacy Officer (LPO) in his/her region or directly contact the CPO in order to obtain further details concerning the purpose of the processing.

4.2. Data minimization Data quality and storage limitation

Data must be faithfully collected in order to guarantee the quality of Personal Data as regards the following aspects:

- Personal Data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy);
- Personal Data must be adequate, relevant and limited to what is necessary in relation to the

purposes for which they are collected and/or processed (data minimization);

- Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which it was collected and processed (storage limitation);
- Personal Data shall be processed fairly, lawfully and in a transparent manner in relation to the Data Subject (lawfulness, fairness and transparency).

4.3. Lawfulness of processing of Personal Data

Personal Data shall be processed only if:

- The Data Subject has given its Consent to the Processing for one or more specific purposes;
- 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;
- Processing is necessary for compliance with a legal obligation to which the Local Data Controller is subject;
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
- 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 Local Data Controller;
- Processing is necessary for the purposes of the legitimate interests pursued by the Local Data Controller or by the 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.

4.4. Lawfulness of Processing of Special categories of Personal Data

Special Categories of Personal Data shall be processed only if:

- The Data Subject gave his/her express Consent, for one or more specified purposes, except where the applicable law prohibits it. Such authorization must therefore be stored in order to be able to provide proof if necessary;
- The Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller and the Data Subject in the field of employment and social security and social protection law in so far as it is authorized by European Union or national law or a collective agreement providing for adequate safeguards for the fundamental rights and the interests of the Data Subjects;
- The processing in question is required to comply with the legislation of the country responsible for processing and provided that suitable guarantees will be implemented by the BCR Company;
- The processing is necessary to protect the vital interest of the Data Subject or of another person where the Data Subject is physically or legally unable to give his/her consent;
- The Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the Processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data is not disclosed outside the body without the Consent of the Data Subjects;
- The Processing relates to Special Categories of Personal Data which is manifestly made public by the Data Subject;

- The processing of Special Categories of Personal Data is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- The Processing of Special Categories of Personal Data is necessary for the purposes of preventive or occupational medicine, or the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatments or the management of health or social care systems and services, on the basis of national law or pursuant to contract with a health professional and subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Other Specific Categories of Personal Data may be subject to local data protection requirements provided by national law. In particular, Processing of data relating to criminal convictions and offences or related security measures may be carried out only under the control of official authority, or when the Processing is authorized by national law providing for appropriate safeguards for the rights and freedoms of Data Subjects. In addition, national law may further determine the specific conditions for the Processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the Data Subject pursuant to the national law.

4.5. Data protection by design and by default

Data protection by design: the Data Controller shall implement, both at the time of the determination of the means for Processing and at the time of the Processing itself, appropriate technical and organizational measures (such as Pseudonymization) designed to implement the data-protection principles (such as data minimization) in an effective manner and to integrate the necessary safeguards into the Processing.

Data protection by default: the Data Controller must implement appropriate technical and organizational measures to ensure that, by default, only Personal Data which is necessary for each specified purpose of the Processing is processed.

4.6. Security of personal data

Appropriate technical and organizational measures shall be implemented to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure of or access to and against all other unlawful forms of Processing (see Article 8 of the BCRs).

4.7. Onward transfers to organizations not bound by BCRs

When Personal Data is intended to be transferred to a non-BCR Company, adequate safeguards have to be implemented (see Article 10 of the BCRs).

The Data Controller shall be responsible for and be able to demonstrate compliance with the present data protection principles (accountability) which are reminded under the present Article 4 of the BCRs.

Article 5 - Transparency and right of information

5.1. Information of Data Subjects

Education materials shall be made available to the Data Subjects, with a view to clarifying questions with regard to the BCR or any related matters, such as submitting an access request with regards to their Personal Data held by a BCR Company (see Article 6) or submitting a claim (see Article 17).

Data Subjects are entitled to be informed of the Processing of their Personal Data. Consistent with this aim, relevant Local Privacy Officers, in coordination with the CPO, shall provide, when appropriate, templates of information notices to every local Data Controller.

When, with regard to an existing Processing, Data is processed for a new purpose or transferred to a new category of Recipients, the appropriate information notice shall be consequently modified and the relevant Data Subjects informed of such modification.

The Personal Data collected for the processing performed by the CMA CGM Group must be faithfully collected by notifying individuals of the following elements:

- a) the identity and contact details of the Data Controller or of his representative, if any;
- b) the contact details of the Local Privacy Officer (if the Data controller has nominated one);
- c) the purposes for which the Personal Data is processed as well as the legal basis for the Processing;
- d) the legitimate interests pursued by the Data Controller or by a Third Party (when the Processing is based on this ground);
- e) the Recipients or categories of Recipients of the Personal Data, if any;
- f) where applicable, the fact that the Data Controller intends to transfer Personal Data to a third country, the existence or absence of an adequacy decision by the European Commission or the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- g) the period for which the Personal Data will be stored (or the criteria used to determine that period);
- h) the existence of the right, to be exercised with the Local Data Controller, to obtain access to and request rectification or erasure of Personal Data or a restriction of the Processing or to object to Processing, as well as the right to data portability;
- i) where the Processing is based on the Data Subject's Consent (either as lawful basis for the Processing or for Processing of Special Categories of Personal Data), the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before withdrawal;
- j) the right to lodge a complaint with a Supervisory Authority;
- k) whether the provision of Personal Data is statutory or contractual, whether the Data Subject is obliged to provide the Personal Data and the possible consequences of failure to provide such data;
- l) the existence of Automated Decision-making, including profiling, meaningful information about the logic therefor, as well as the significance and the envisaged consequences of such Processing for the Data Subject;
- m) the intention to further process the Personal Data for a purpose other than that for which it was collected;
- n) the source of the Personal Data and, if applicable, whether it came from a publicly accessible source (where Personal Data has not been obtained directly from the Data Subject).

Where the data has not been directly obtained from the Data Subjects, the Data Controller will provide

such information to the relevant Data Subjects within a reasonable period after obtaining the Personal Data, but at the latest within one month, taking into consideration the specific circumstances under which the Personal Data are processed; if the Personal Data are to be used for communication with the Data Subject, such information will be provided at the latest at the time of the first communication to that Data Subject; or if a disclosure to another Recipient is envisaged, at the latest when the Personal Data are first disclosed.

Pursuant to Article 14(5) of the GDPR, which applies where the Personal Data have not been directly obtained from the Data Subjects, this disclosure of information to the Data Subject will exceptionally not apply (i) where the Data Subject already has the information, (ii) where the provision of such information proves impossible or would involve a disproportionate effort, (iii) if obtaining or disclosure is expressly provided by a law to which the Data Controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests or (iv) where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by law (including a statutory obligation of secrecy).

5.2. Accessibility of the BCRs

A Data Subject shall always be able to obtain, upon request, a copy of the BCR from the CMA CGM CPO or the relevant LPO. Information on access to the BCR will be provided as follows:

- Availability of these BCR at the CMA CGM Group intranet. This intranet can be accessed by any employee with an access account to the information system as well as an access to Internet.
- Availability of these BCR on the CMA CGM Group institutional website (<http://www.cma-cgm.com/>).

Article 6 - Right of access, rectification erasure, and portability of Data, rights to the restriction of Processing and right to object to the Processing

The Data Subject must be able (after having established his/her identity and made a specific request to the relevant Local Privacy Officer of CMA CGM or the BCR Company) to:

- a) Obtain without restriction at reasonable intervals and without excessive delay or expense:
 - confirmation as to whether or not his/her Personal Data is being processed;
 - the purposes of the Processing, the categories of Personal Data concerned, the Recipients or categories of Recipients to whom the Personal Data is disclosed, where possible the envisaged period for which the Personal Data will be stored or, if not possible, the criteria used to determine that period, the existence of the right to request from CMA CGM 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 as to their source (where the Personal Data are not collected directly from the Data Subject); the existence of Automated Decision-making, including Profiling and, at least, meaningful information about the logic therefore, as well as the significance and the envisaged consequences of such Processing for the Data Subject;
 - where Personal Data are transferred to a third country, information about the appropriate

safeguards used for the Data Transfer;

- communication to the Data Subject in an intelligible form of the Personal Data undergoing Processing;
 - any communication (including the copy of the personal data undergoing processing) and any action taken in response to a Data Subject's access right request shall be provided free of charge. However, the Data Subject may possibly be asked a reasonable fee based on administrative costs to for any further copies requested by the Data Subject;
 - where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form;
 - the right to obtain a copy shall not adversely affect the rights and freedoms of others.
- b) Obtain, without undue delay, the rectification of inaccurate Personal Data concerning him or her. Taking into account the purposes of the Processing, the Data subject shall have the right to have incomplete Personal Data completed, including by means of providing a supplementary statement.
- c) Obtain without undue delay, the erasure of any Personal Data where one of the following grounds applies: i) where the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; ii) where the Data Subject withdraws the Consent on which the Processing is based and there are no other legal grounds or overriding legitimate grounds for the Processing; iii) the Data Subject objects to the Processing and there are no overriding legitimate grounds for the Processing or the Data Subject objects to the Processing for the purposes of direct marketing; iv) the Personal Data has been unlawfully processed; v) the Personal Data has to be erased for compliance with a legal obligation to which CMA CGM and/or a BCR Company is subject; vi) the Personal Data has been collected in relation to the offer of information society services; which cover any service, normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data.

Where CMA CGM and/or a BCR Company has made the Personal Data processed public and is obliged to erase it, CMA CGM or the relevant BCR Company shall i) take reasonable steps, including technical measures, to inform any other Controllers processing the Personal Data concerned that the Data Subject has requested the erasure of any links to, or copy or replication of, such Personal Data (taking account of available technology and the cost of implementation) and ii) request that such Controllers comply with the request.

Exceptions to this right to erasure apply i) when the Processing is necessary for exercising the right of freedom of expression and information; ii) for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller; iii) for reasons of public interest in the area of public health; for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; for the establishment, exercise or defence of legal claims.

- d) Obtain restriction of Processing was one of the following grounds applies: i) when the accuracy of the Personal Data is contested (for the period necessary to verify the accuracy of the data), ii) when the Processing is unlawful and the Data Subject requests the restriction of use of his/her Personal Data, iii) when CMA CGM or a BCR Company no longer needs the Personal Data for the Processing but they are required by the Data Subject for the establishment, exercise or defence of legal claims and iv) when the Data Subject has objected to a Processing CMA CGM or a BCR Company has based on its legitimate interest (for the period necessary to verify whether the legitimate grounds of CMA CGM or the relevant BCR Company override those of the Data Subjects, if applicable).
- e) Have CMA CGM or the relevant BCR Company communicate to each Recipient to whom the Personal Data have been disclosed any rectification, erasure or restriction carried out in compliance with (b), (c), (d), unless this proves impossible or involves a disproportionate effort. The Controller shall inform the Data Subject about the Recipients if the Data Subject requests such information.

- f) Exercise his/her right to data portability and obtain from CMA CGM or a BCR Company the right to receive communication of his/her Personal Data which he/she has provided to CMA CGM or the relevant BCR Company, in a structured, commonly used and machine-readable format, and have the right to transmit those data to another data controller without hindrance from CMA CGM or the relevant BCR Company, when the Processing is based on Consent or on a contract and the Processing is carried out by automated means.
- g) Object at any time, for compelling legitimate grounds relating to the Data Subject particular situation to the Processing of Personal Data based on the legitimate interest of CMA CGM or a BCR Company. CMA CGM or the BCR Company shall no longer process the Personal Data unless the controller 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.

In compliance with the GDPR, the exercise of the foregoing rights may be subject to certain limitations. In particular, CMA CGM or the relevant BCR Company may charge a reasonable fee or refuse to act on requests that are manifestly unfounded or excessive, in particular if repetitive.

- h) Object, at any time of the Processing, free of charge and without having to state legitimate grounds, to the Processing of Personal Data for the purposes of direct marketing (including Profiling to the extent that it is related to such direct marketing).

In order to enable Data Subjects to exercise their rights efficiently, specific guidelines and procedures shall be put in place within the CMA CGM Group, at local levels. In particular, CMA CGM Employees who collect, process or have access to Personal Data shall be trained to recognize a Data Subject's request for access, rectification, erasure, restriction, objection or portability. Each request shall be acknowledged and handled according to the local procedure in place.

A specific answer shall be given to the Data Subject within a reasonable period of time (i.e., no later than 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). CMA CGM or the relevant BCR Company shall inform the Data Subject of any extension within one month of receipt of the request together with the reasons for the delay.

If the request is found legitimate, CMA CGM or a BCR Company shall take necessary steps to handle the matter in due time. If the request is denied, the Data Subject shall be informed in writing or by email about the reason and the fact that the Data Subject may follow the internal claim process specified in Article 17 of the BCRs.

Article 7 - Automated Individual Decisions-making, including profiling

Subject to Applicable Data Protection, each BCR Company agrees not to make any decision based solely on automated Processing, including Profiling, which may significantly affect him/her or which produces legal effects with regard to such Data Subject.

Unless the decision in question:

- is necessary for the entering into or performance of, a contract between CMA CGM or a BCR Company and the Data Subject or is based on the Data Subject's explicit consent. In such case, CMA CGM or the relevant BCR Company shall implement suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

- is authorized by any Applicable Data Protection Law to which a BCR Company is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests.

Article 8 - Security and confidentiality policy of Personal Data

Each BCR Company shall implement appropriate technical and organizational measures to protect Personal Data against Personal Data Breaches, taking into consideration state-of-the-art technology and the cost of implementation, the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects.

Furthermore, the implemented measures shall ensure (i) a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected, including, where appropriate, the Pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

Consequently, appropriate information security policies and procedures shall be designed and implemented within the CMA CGM Group. In particular, all BCR Companies must comply with the CMA CGM Group Security Policy for the information system.

The ISSP (Information System Security Policy) of the CMA CGM Group which outlines the security rules connected with the technologies implemented in the CMA CGM Group information systems as well as the associated organisation measures are appended to these rules.

In accordance with Article 32, 1°, d) of the GDPR, these policies and procedures shall be regularly audited (see Article 11 of the BCRs).

In addition, the BCR Company acting as Data Processor shall comply with the minimum security criteria which are required to the processors (Ref. Article 9 - Data transfer to a BCR Company acting as Processor).

Special Categories of Personal Data shall be processed with enhanced and specific security measures.

Article 9 - Data transfer to a BCR Company acting as Processor

When subcontracting operations are performed by a BCR Company, the Data exporter bears the responsibility of the data exported. To this end, performance of the subcontracting service must be governed by a written legal deed binding the Data exporter to the Processor and which stipulates in particular that the Processor undertakes:

- To process the Personal Data only on documented instructions of the data controller unless the Data processor is required to do the Processing by law, in which case the Processor shall promptly notify the Data Controller (unless such notification is explicitly prohibited by law or important grounds of public interest);
- To take all the security and confidentiality measures in accordance with Article 8 of the BCRs;

- To ensure that persons authorized to process the Personal Data have committed to confidentiality or are under an appropriate statutory obligation of confidentiality;
- To respect the conditions for engaging another Processor. In this regard, the Processor undertakes:
 - Not to engage another sub-processor without prior specific or general written authorization of the Data controller. The Data controller agrees that a Processor may use another BCR Company for sub-Processing. In this case, the initial Processor undertakes to inform the Data Controller of any intended changes concerning the Processors, to give the Data Controller the opportunity to object to such changes;
 - To impose the same data protection obligations as set out in the present BCRs or another legal act between the controller and the processor.
- To assist the Data Controller, taking into account the nature of the Processing, by putting in place the appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Local Data Controller's obligation to respond to requests for exercising the Data Subject's rights as indicated in Article 6 of the BCRs;
- To assist the Data Controller in ensuring compliance with its obligations as regards the security of Personal Data, the notification of a Personal Data Breach, the data protection impact assessment and the prior consultation of the local Supervisory Authority (where necessary);
- At the choice of the Data Controller, to delete or return all the Personal Data to the Data Controller at the end of the provision of services relating to Processing, and to delete existing copies unless national law requires continued storage of the Personal Data;
- To make all information necessary to demonstrate compliance with these obligations available to the Data Controller and allow and contribute to audits of its Processing activities, including inspections conducted by the Data Controller or another auditor mandated by the Data Controller;
- To inform the Data Controller if in his opinion an instruction infringes the GDPR or the Applicable Data Protection Laws;
- To implement procedures for managing Personal Data Breaches and to notify the Data Controller without undue delay after becoming aware of a Personal Data Breach;
- Not to disclose Personal Data to any Third Party without the prior explicit Consent of the Data Controller (see also Article 10 below). In case of consented disclosure, the Processor will impose on such Third Party all of the same data protection obligations as set out herein, by way of a contract. Where such Third Party fails to fulfil its data protection obligations under such contract, the Processor shall remain fully liable to the Data Controller for the performance of the Third Party's obligations.

The Data Exporter makes sure, in particular, that the BCR Company has signed the Group PSSI (Information System Security Policy) in order to ensure that the security measures are implemented.

In addition, the Processor shall comply with the minimum security criteria (Ref. Appendix 2 – Minimum security criteria).

If a Data Processor determines the purposes and means of Processing, such Data Processor shall be considered to be the Data Controller in respect of that Processing.

The Data Processor must maintain a Record of Processing Activities carried out on behalf of the Data Controller.

The Data Processor will be held liable for any damage caused by Processing where it has not complied with obligations of the BCR specifically applicable to a Data Processors or where it has acted outside or contrary to lawful instructions of the Data Controller (except if it proves that it is not in any way responsible for the event giving rise to the damage).

Where both a Data Controller and a Data Processor (or more than one Controller or Processor), are involved in the same Processing and where they are responsible for any damage caused by Processing, each of the Data Controller and the Data Processor shall be liable for the entire damage in order to ensure

effective compensation of Data Subjects. Where a Controller or Processor has paid full compensation for the damage suffered, that Controller or Processor shall be entitled to claim back from the other Controllers or Processors involved in the same Processing that part of the compensation corresponding to their part of responsibility for the damage.

Article 10 - Restriction on transfers and onward transfers to External Processors or Controllers

Where a Data Controller requests that a Third Party other than a BCRs Company undertakes Processing of Personal Data as a Processor or a Controller (an External Processor or an External Controller), the following safeguards shall be put in place.

External Processors located inside the EEA or in a country recognized by the EU Commission as ensuring an adequate level of protection shall sign a written agreement stipulating that the Processor shall act only on instructions from the local Data Controller and shall be responsible for the implementation of the appropriate technical and organizational measures (see Article 8). Relevant local Data Privacy Officers in coordination with the CPO, shall provide templates of the appropriate clauses to a local Data Controller within the CMA CGM Group.

10.1. Exportation to External Controllers

Any Personal Data transferred by a BCR Company to an External Controller located outside the EEA in a country not recognized by the EU Commission as ensuring an adequate level of protection shall be adequately protected and shall be governed by the standard contractual clauses adopted by the European Commission on 15 June 2001 or by those of 27 December 2004.

10.2. Exportation to External Processors

External Processors located inside the EEA or in a country recognized by the EU Commission as ensuring an adequate level of protection shall sign a written agreement stipulating that the Data Processor shall act only on instructions from the Data Controller and shall be responsible for the implementation of the appropriate technical and organizational measures (see Article 8 of the BCRs).

Any Personal Data transferred by a BCR Company to an External Processor located outside the EEA in a country not recognized by the EU Commission as ensuring an adequate level of protection shall be adequately protected and shall be governed by the standard contractual clauses adopted by the European Commission on 5 February 2010.

In any case, exportation shall be subject to prior approval from the Chief Privacy Officer who shall ensure that the rules in terms of security and protection of personal data are formalized and complied with.

Article 11 - Audit concerning compliance with the BCRs

These BCRs apply to the all BCR Companies. The internal audit department of CMA CGM checks that they are complied with, based on the BCRs.

Data protection audits shall be carried out on a regular basis (subject to more stringent local laws, but at least one audit every 3 years) by internal or external accredited audit teams to ensure that the BCRs and all related policies, procedures or guidelines are updated and applied

Data Protection audits shall cover all aspects of the BCR and all related policies, procedures or guidelines, including methods of ensuring that corrective measures will take place (see CMA CGM Data Protection audit work program). However, the scope of each audit can be adapted to limited aspects of the BCR and/or the related policies, procedures or guidelines, as necessary, including methods of ensuring that corrective measures will take place.

Data Protection audits shall be decided directly by the CPO either upon his/her own initiative or upon specific request of CMA CGM, or a LPO, or a Data Controller.

Based on the audit results and the reports mentioned in Article 13.2 below, the CPO and/or the LPO shall decide any appropriate legal, technical or organizational security measures in order to improve data protection management within the CMA CGM Group, both at global and local levels.

Results of the audit should be communicated to the CPO, to the board of directors of CMA CGM and of the BCR Company and should be available upon request to the competent Supervisory Authority.

The conclusions concerning the group Personal Data protection BCRs can be transmitted to the competent Supervisory Authorities upon express request. Each Local Data Controller shall accept to be audited by a competent Supervisory Authority if required under applicable law.

Article 12 - Training concerning the BCRs

Each BCR Company has a set of communication and training tools concerning the Group Personal data protection rules so as to make sure that they are fully and wholly applied in their entity. Training sessions are given to any Employee, and in particular to Employees with permanent or regular access to Personal data and who are associated with collecting personal data or development of Personal Data processing tools.

These tools contain the following elements:

- A distance training tool based on the “e-Learning” principle. This tool provides a didactic program explaining the Personal data protection principles. This training must enable Employees to understand the BCRs in their international and organisational dimension;
- A set of documents to be circulated internally concerning the best practices in Personal data protection and available on the CMA CGM intranet;
- An intranet dedicated to personal data protection. This intranet is maintained up to date under supervision of the CPO.

At local level, each local Data Privacy Officer shall, at its own discretion, enhance the data protection training program described above by adding any relevant local data protection requirement. The data protection training program shall be reviewed and approved by the CPO.

By signing these BCRs, each BCR Company’s CEO accepts to have its main managers attend the complete e-Learning training course.

For further details as to the E-learning tool see also Appendix 3.

Article 13 - Binding nature of the BCRs

13.1. Internal binding nature

These BCRs bind all BCR Companies which have signed the present BCR or the Undertaking to comply with the Binding Corporate Rules for personal Data Protection (Appendix 5).

Each BCRs Company that signs the BCRs or the Undertaking provided in Appendix 5 is responsible for administering and overseeing the implementation of these BCR, including making these BCR binding upon the Employees.

Pursuant to applicable local law, the BCRs are made binding towards the Employees either through work employment contracts or through collective agreements or through compliance with relevant company policies in which the BCR have been incorporated.

13.2. Compliance and supervision of compliance

CMA CGM has established a data protection network composed of the CPO and of LPO appointed at local levels. This LPO network is comprised of CMA CGM legal department representatives in the regions worldwide where the Group is present.

The regional breakdown of LPOs is as follows (this breakdown may change depending on the group activity, the CPO will inform the Leading Supervisory Authority on a regular basis concerning the change of these regions and LPOs):

- Europe & Eastern Europe Region,
- Middle East, Indian Subcontinent Region,
- Asia region,
- Africa, Maghreb region,
- Americas region,
- Noumea, Papeete, Australia and New Zealand Region.

Each LPO shall be responsible for the implementation of the BCRs. Thus, each LPO shall:

1. inform and advise the BCR Company at their local level and the Employees who carry out Processing of their obligations;
2. take all reasonable steps to make sure that BCR Company comply with the provisions of the BCRs (including said provisions concerning training of staff involved in Processing operation and audits);
3. in coordination with the CPO, be at the disposal of the BCR Company, and Data Subjects to provide any help with regard to data protection issues, especially the implementation of the BCR, when necessary;
4. provide advice, where requested, with regard to the conduct of any data protection impact assessment and the monitoring of its performance where required (see Data Protection Impact Assessment methodology);
5. submit reports every year to the CPO concerning important questions and all the actions and measures taken connected to data protection issues (data protection training programs, Records of Processing Activities, management of complaints, etc.), and especially with regard to the implementation of the BCR;
6. regularly report to the CPO on the complaints settled at local levels, with a view to taking corrective actions and improving guidelines and procedures implemented within the BCR Companies, where the complaints may have revealed a "gap" in terms of data protection;

7. in coordination with the CPO, cooperate with the Supervisory Authorities and act as the contact point for the Supervisory Authorities on issues relating to Processing.

Furthermore, in terms of supervision of compliance, specific measures shall be taken to ensure the right implementation of the BCRs:

1. The LPO shall regularly report to the CPO on the implementation of the BCRs within each local BCR Company (including when acting as data Processor).
2. The results of all reports made by the CPO shall be communicated to CMA CGM board of directors and should be readily accessible to the competent Supervisory Authority.
3. Based on the audit results (see Article 11) and the reports mentioned above, the CPO, the LPO and the relevant local BCR Company shall decide on any appropriate measure in order to improve data protection management within the Organization, both at global and/or local levels. Any measure to be decided by one of the relevant stakeholders shall be taken in cooperation with the others who shall be duly informed about such decision, when appropriate.
4. The Data Privacy Officer will liaise with the Lead Supervisory Authority pursuant to Article 56 of the GDPR.

The list of Local Privacy Officers is provided in Appendix 7 of the BCRs.

13.3. Sanctions

In the event of a violation of the BCR by the Data Controller's Employees, any appropriate disciplinary sanction or judicial action may be imposed in accordance with local law, at the initiative of the CPO and the relevant local LPO.

The CPO and the local LPO shall pay specific attention to any audit results establishing non-compliance by Employees, especially in case of non-compliance with the Data Protection Principles or any of the applicable guidelines, procedures and policies related to the implementation of the BCR.

Article 14 - Mutual assistance and Cooperation with the Supervisory Authorities

The BCR Companies accept to cooperate with the competent Supervisory Authorities responsible for Personal data protection by promptly responding to any request made. The BCR Companies also agree to comply with the advice and recommendations of the competent Supervisory Authorities as regards the interpretation and application of these Corporate Rules.

The BCR Companies accept that the competent Supervisory Authorities responsible for Personal data protection initiate audits concerning data protection with CMA CGM, if necessary.

Furthermore, BCR Companies shall cooperate and assist each other to handle a request or complaint from a Data Subject (see Article 17) or an inquiry by a Supervisory Authority, under supervision of the Local Privacy Officer.

Each competent Supervisory Authority has the power to supervise the implementation of the BCR.

Article 15 - Application of regional legal specificities

15.1. Relationships between national laws and the BCRs

CMA CGM undertakes to ensure that the BCR Companies and their respective Employees shall comply with the provisions of the BCR, as well as with the provisions of Applicable Data Protection Laws.

Where the local Applicable Data Protection Laws require a higher level of protection for Personal Data, they will take precedence over the BCR.

15.2. Actions in case of national legislation preventing respect of BCRs

Whenever a BCR Company has reason to believe that the legislation which applies to it may prevent it from fulfilling its obligations under the BCRs and have a negative impact on the guarantees provided, the BCR Company shall immediately inform CMA CGM thereof through the CPO (unless this is prohibited by an authority responsible for enforcing any law such as for example a prohibition stipulated by the criminal code to preserve the secrecy of the inquiry). The CPO shall take a decision on the appropriate actions to be undertaken.

Moreover, in the event of conflict between national legislation and the commitments under these BCRs, the CPO will take a decision concerning the action to be taken and will consult with the competent Supervisory Authorities in case of doubts.

Article 16 - Updating the BCRs

The CPO is responsible within the group for updating the list of BCR Companies and recording any update of the BCRs.

Any update of the BCRs shall be recorded by the CPO. The CPO keeps an updated list of the BCR companies (available in Appendix 5). These changes shall also be communicated to the BCR Companies which have signed the present BCR or the Undertaking to comply with the Binding Corporate Rules for personal Data Protection (Appendix 5).

Any substantial modification of the BCRs must be notified at least once per year to the Supervisory Authorities issuing authorization. However, any changes which would affect the level of protection offered by the BCR or will significantly affect the BCR will be provided to the Leading Supervisory Authority promptly, which will consider whether this affects the approval previously issued for the BCR.

A transfer to a new BCR Company can only take place once the BCRs have been made restrictive for this company.

Article 17 - Claim process

If a Data Subject reasonably believes that there has been a violation of these BCR or that his/her Personal Data is being processed in a way that is incompatible with these BCR, he/she may lodge, in accordance with the BCR Claim Process, a complaint with a BCR Company to obtain adequate correction measures and, where appropriate, adequate compensation.

Specific guidelines and procedures shall be in place within CMA CGM, at local level, to ensure the consistency of the claim and to ensure sufficient information is provided to the Data Subjects about these procedures. The complaints shall be dealt with by a clearly identified local department which is appropriately independent in the exercise of its functions (normally, the Local Privacy Officer). When a complaint is registered, it must be acknowledged and handled within a reasonable period of time (i.e., closed out no later than three months from the receipt of the request. That period may be extended by three further months where necessary, taking into account the complexity and number of the requests. The relevant BCR Company shall inform the Data Subject of any extension within one month of receipt of the request together with the reasons for the delay).

If the relevant Local Privacy Officer fails to solve the claim at local level, the claim handling process shall allow escalation of the problem to the CPO who shall respond in the timeline indicated above. Each local Data Controller and each local LPO shall issue regular reports to the CPO on the complaints handled at local level.

All data protection complaints received by any Employee shall be communicated to the relevant Local Privacy Officer and the Chief Privacy Officer without any delay.

Each BCR Company shall make available practical tools or procedures allowing Data Subjects to lodge their complaints, including at least one of the below:

- Email address
- Postal address.

If the Data Subject is not satisfied by the replies received from the BCRs Company and ultimately, the CPO or LPO or if the Data Subject prefers to bypass the available internal claim process, the Data Subject has the right to lodge a complaint before the competent Supervisory Authority and/or the competent jurisdictions of the country of the local Data exporter (see Article 18). Consequently, the Data Subject shall be informed of the possibility to solve a claim through the internal claim process described above and the BCR claim process prior to referring a case to the relevant Supervisory Authority or competent jurisdiction.

- CMA CGM and BCR Companies agree to reply to any non-binding mediation procedure implemented by any individual or by the Supervisory Authority. BCR Companies may choose to participate in the procedures remotely (by telephone or other electronic means) if they are a party thereto.

CMA CGM and the BCR Companies also agree to examine the possibility of participating in any other arbitration, mediation or dispute settlement procedure put in place for the disputes pertaining to data protection.

- If a dispute has not been settled out of court within a reasonable timeframe (on average 3 months), it may be brought before the Court of the country of the Data exporter at the origin of the dispute in accordance with Article 19 of the BCRs.

Claim conditions by Data Subjects

The claim mechanism is published on the CMA CGM public website (<http://www.cma-cgm.com>) as well as in any form or new contractual document containing Personal data collection.

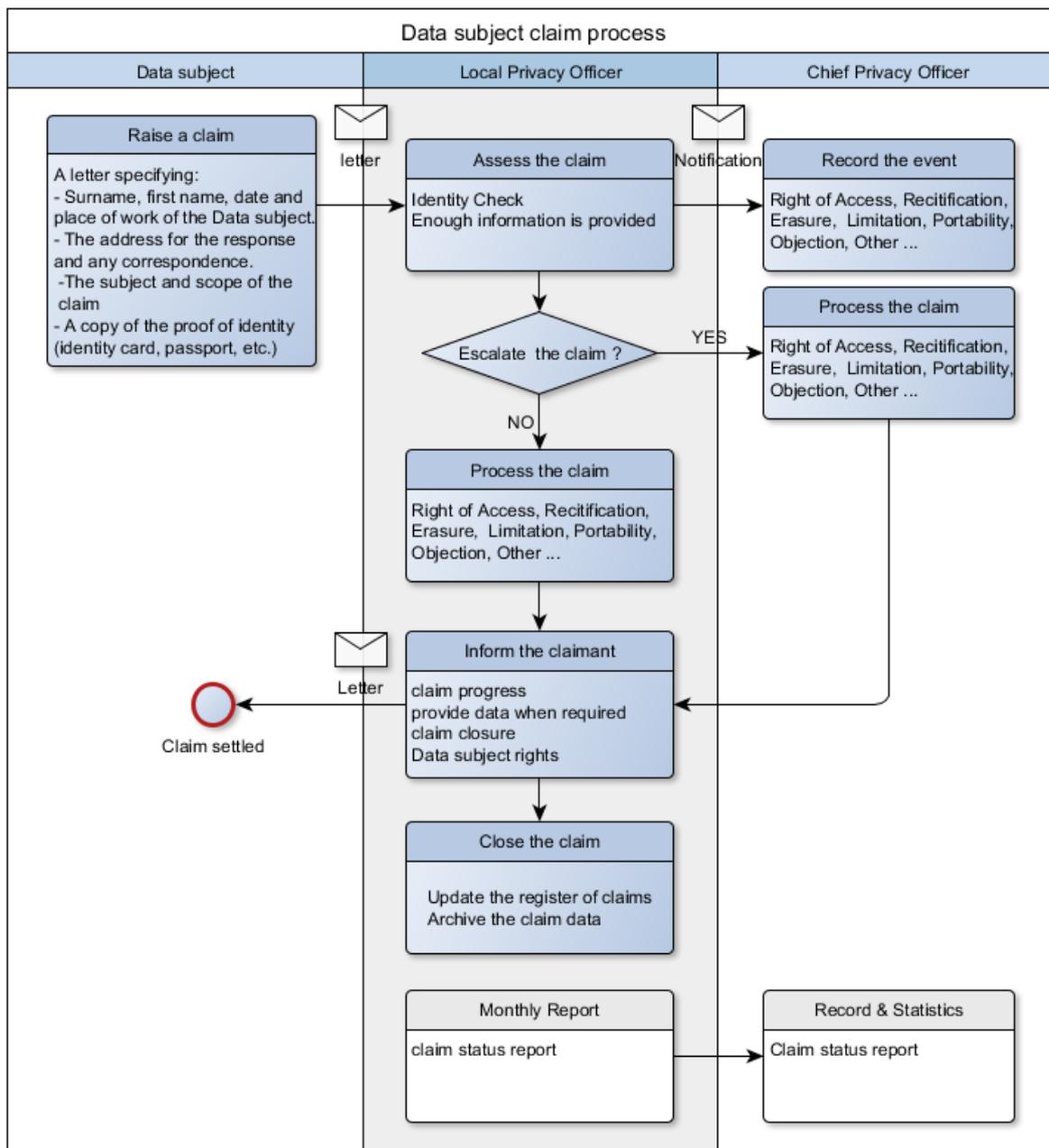
This claim procedure must allow individual to invoke non-compliance with the rules by any BCR Company. Each individual may also request the following operations:

- Access of his/her Personal data;

- Rectification of Personal data;
- Erasure of Personal data for legitimate reason;
- Limitation of Processing;
- Portability of his/her Personal Data;
- Objection to the Processing of his/her Personal data;
- Any other claim connected with use of Personal data.

All requests/claims must be sent as per the following conditions:

- A letter specifying:
 - Surname, first name, date and place of work of the Data subject;
 - The address for the response and any correspondence;
 - The subject and scope of the claim in order to make it easier to identify the data in question (HR, commercial or collaborative field).
- A copy of the proof of identity (identity card, passport, etc.).
- The request must be sent to the following addresses:
 - By post:
CMA CGM
Chief Privacy Officer
Legal Department
4, Quai d'Arenc
13235 Marseille Cedex 02
France
 - Email:
cpo@cma-cgm.com



Article 18 - Right of beneficiary third parties

A Data Subject who claims to have suffered damage as a direct result of a violation of the provisions of the BCRs or its Appendices and who either is not satisfied with the resolution of their complaint, as described in Article 17, or desires to bypass the internal complaint mechanism and bring their complaint directly to the competent Supervisory Authority or before the courts according to the principles and terms as set out below. The BCRs internal complaint mechanism shall support Data Subjects' ability to address any data protection complaint to a BCR Company. Data Subjects are however free to lodge a complaint directly with the competent Supervisory Authority or the courts as provided by Applicable Data Protection Laws.

Each Data Subject shall have the right to lodge a complaint at its choice with the competent Supervisory Authority, before the competent court of the Data Exporter or before the court of the Data Importer.

In addition, should the BCRs be breached, the Data subject who suffered prejudice may invoke these rules in order to obtain compensation from before the competent court, as may be ordered by the appropriate court or competent regulatory authority or as decided according to the internal complaint mechanism, if used.

The BCR shall always be readily available to every Data Subject, in the conditions described in Article 5.2.

Article 19 - Liability

Either the Local Data Importer or the Local Data Exporter shall be liable for breaches of the BCR under the following conditions:

1. Where the Data Importer is a Data Controller:
 - a) Where the Data Subject alleges a breach by the Data Importer, he/she shall first request the Data Exporter to take appropriate action to enforce the Data Subject's rights against the Data Importer. If the Data Exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the Data Subject may enforce his/her rights against the Data Importer directly. A Data Subject shall also be entitled to proceed directly against a Data Exporter unless the latter can prove that he has failed to use reasonable efforts to determine that the Data Importer is able to satisfy its obligations under the BCRs. Both the Data Exporter and the Data Importer shall agree to take necessary actions to remedy and to pay compensation for actual damages for which they may be held liable by a final decision of a court or Supervisory Authority. Both the Data Exporter and the Data Importer shall have sufficient financial resources at their disposal to cover the payment of compensation for breach of the BCRs. Liability as between the parties shall be limited to actual damage suffered. Indirect (i.e., consequential damages such as reputational damages) or punitive damages (i.e., damages intended to punish a party for its outrageous conduct) shall be specifically excluded.
 - b) The burden of proof will be with the Data Exporter to demonstrate that the BCR Companies involved are not liable for the alleged violation resulting in the damages claimed by the Data Subject. The Data Exporter will also have the burden to prove that it took reasonable efforts to determine that the Local Data Importer is able to satisfy its obligations under the BCR. The Data Exporter may be exempted from any liability, in whole or in part, if it is proven that it is not responsible for the event giving rise to the damage or that it took reasonable efforts to ensure that the Data Importer is able to satisfy its obligations under the BCR. The Data Importer may be exempted from any liability, in whole or in part, if it is proven that it is not responsible for the event giving rise to the damage.
2. Where the Data Importer is a Data Processor:
 - a) If a Data Subject is not able to bring a claim against the Data Exporter for a breach by the Data Importer or its sub-processor of any of their obligations under the BCR, either because the Data Exporter has factually disappeared or has ceased to exist in law or has become insolvent, the Data Importer agrees that the Data Subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, in which case the Data Subject must first enforce its rights against such entity. The Data Importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
 - b) If a Data Subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraph a for a breach by the sub-processor of any of their obligations under these BCR because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, then the sub-processor (provided such sub-processor is a BCR Company) agrees that the Data Subject may issue a claim against

the sub-processor with regard to its own Processing operations as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or the Data Importer by contract or by operation of law, in which case the Data Subject must first enforce his rights against such entity. The liability of the sub-processor BCR Company shall be limited to its own Processing operations.

Article 20 - Entry into effect and termination

Each BCR Company recognizes to be legally bound by the BCR, from the date of signature of the Appendix 6 of the BCRs (Undertaking to comply with the Binding Corporate Rules for personal Data Protection (Privacy Policy)”) by the relevant BCR company and without any other formalities, with respect to other BCR Companies already bound or about to be bound from the date of their signature, and provided that the terms of the BCR are strictly identical between each other. Except if a BCR Company is able to prove that its signed BCR agreement is not strictly identical to the ones signed by other entities, it expressly and irrevocably disclaims challenging the evidence that it is bound by the terms of the BCR.

In the event that a Data Exporter or a Data Importer is found to be in substantial or persistent breach of the terms of the BCR, the CPO may temporarily suspend the transfer of Personal Data from such Data Exporter or to such Data Importer until the breach is remedied. Should the breach not be remedied in due time, the CPO shall take the initiative to terminate the BCR intra-group agreement with respect to that specific Data Exporter or Local Data Importer. In such a case, the Data Exporter or Data Importer shall immediately take every necessary step in order to comply with the European rules on cross-border data flows (Article 46 of the GDPR), for instance by using the EU Standard Contractual Clauses approved by the EU Commission.

Article 21 - Interpretation of terms

In case of discrepancies between the BCR and the Appendices, the main body of the BCR shall prevail. In case of discrepancies between the BCR, including its Appendices, and other global or local CMA CGM policies, procedures or guidelines, the BCR shall prevail. In case of discrepancies or inconsistency, the terms of the BCR shall always be interpreted and governed by the provisions of the GDPR and 2002/58/EC Directive, as amended, if applicable.

Article 22 - Applicable law / Jurisdiction

These BCRs are governed by the Applicable Data Protection Laws.

In accordance with Article 19, jurisdiction shall be attributed to the courts of the Data Importer or Data Exporter.

SHIPPING **THE** FUTURE

WWW.CMA-CGM.COM