COFACE

Binding Corporate Rules

approved by French Data Protection Supervisory Authority (CNIL) on 30 January 2025

JANUARY 2025

1. INTRODUCTION

Compagnie Française d'Assurance pour le Commerce Extérieur ("**Coface"**) is committed maintaining the privacy of data obtained in the course of its business activities and complying with applicable laws and regulations regarding the Processing of Personal Data and Special categories of Data.

Disclosing and sharing Coface standards through the BCR is of the utmost importance regarding the Data Subjects' legitimate expectations about how their Personal Data is Processed.

Coface decided to adopt a set of Binding Corporate Rules in order to set up adequate safeguards to ensure that Personal Data is protected while transferred within the Coface Group between Coface Entities based or not in a EEA jurisdiction and Coface Entities located in a third country which do not offer an adequate level of protection according to the European Commission ("**Non-adequate third country**") and where the data has been subject to prior lawful transfer to a third-country, any subsequent Onward Transfer of that data to a Non-adequate third country. Where necessary additional measures might be required to carry out a transfer between two Coface Entities bound by the BCR.

As a consequence of the above and taking into consideration standards, regulations and laws applicable in the field of data protection, and the requirements introduced by the GDPR and other Applicable Data Protection Legislation, Coface Entities will process data in accordance with the following principles:

- **Lawfulness** – Personal Data shall be collected and Processed with the Data Subject having given consent to the Processing or when Processing is legitimate or necessary in accordance with Applicable Data Protection Legislation;

- **Fairness** – Personal Data Processing shall take into account the specific circumstances and context in which such Personal Data is Processed;

- **Transparency** - Information and communication relating to the Processing of Personal Data shall be easily accessible, easy to understand, clear and in plain and simple language;

- **Purpose limitation** – Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes;

- **Data minimisation** – Collected Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed

- **Accuracy** – Personal Data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without undue delay;

- **Storage limitation** – Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed or any other lawful retention;

- **Integrity and confidentiality** – Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful

Processing and against accidental loss, destruction or damage, using appropriate technical, physical and administrative measures;

Through the BCR Coface intends to share and specify the detail and the principles applicable to all Coface Entities and provide certain group-wide standards allowing the implementation of the BCR. Furthermore, Coface Group may make available specific, local or sectorial policies. Should there be a contradiction between the BCR and such specific, local or sectorial policies, the terms of the BCR shall prevail.

The BCR aims at ensuring an adequate and consistent approach throughout the entire Coface Group regarding Personal Data Processing. Local legislation may impose exceptions to the BCR, which impose a higher level of protection for Personal Data in which case the local legislation will take precedence.

No transfer of Personal Data shall be carried out by any Coface Entity to an entity not bound by the BCR unless such entity has provided the sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing and obligations attached to such Processing will meet the requirements of the BCR and ensure the protection of the rights of the Data Subjects.

2. DEFINITIONS

As used in the BCR, the following terms and expressions, when written with a capital letter, shall have the following meanings set out below and be read in light of the GDPR:

*"**Applicable Data Protection Legislation**"*. should be understood to mean "the GDPR, the EU Member States national laws and regulations relating the Processing of Personal Data and implementing GDPR" and, in the case of BCR members located outside the EEA receiving personal data transferred under the BCR, the law of the country in which the data exporter is located.

*"**Binding Corporate Rules**" or "**BCR**"* has the meaning given to by the Article 4 of the GDPR and refers the present Binding Corporate Rules, including the Appendixes listed and amendments as the case may be, entered into by and between Coface and all other Coface Entities.

*"**Coface**" means* Compagnie Française d'Assurance pour le Commerce Extérieur (COFACE), Société Anonyme having its principal offices at 1 Place Costes et Bellonte, 92270 Bois Colombes, registered on the Commercial Registry of Nanterre under the number 552 069 791.

*"**Coface Entities**"* mean Coface and any other company controlled by Coface, or controlled by Coface's mother company or any other company controlling Coface, with a company being considered as controlling another based on the criteria of Article L 233-3 of the French Commercial Code (individually a ***"Coface Entity"***).

*" **Data Steering Committee**"* is a committee specifically dedicated to supervision of data matters, including GDPR and the BCR, consisting of Coface Group senior management representatives and GDPO.

*"**Coface Employees**"* are all the employees of the Coface Entities including directors, trainees, apprentices and assimilated status.

*"**Coface Group**"* means, together, all Coface Entities.

*"**Competent Supervisory Authority**" means EEA data protection Supervisory Authority competent for the Data Exporter.*

*"**Controller**"* means a Coface Entity which, alone or jointly with others, determines the purpose(s) and means of the Processing of Personal Data.

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

*"**Data Exporter**"* means any Controller, which transfers Personal Data under the BCR pursuant to a Relevant Transfer or Onward Transfer.

*"**Data Importer**"* means any Controller or Processor Processing Personal Data on behalf of a Controller who receives Personal Data from Data Exporter under a Relevant Transfer or Onward Transfer.

*"**Data Protection Coordinators**" or "**DPC**"* means the person in charge of data protection matters at Coface regional level, responsible for coordinating with the Group Data Protection Officer and the Local Compliance Officers for ensuring the Coface Entities' compliance with the Binding Corporate Rules and applicable local legal / regulatory requirements.

*"**Data Subject**"* means any natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

*"**European Data Protection Board**" ("EDPB")* means the body of the European Union composed of the head of one Supervisory Authority of each Member State and of the European Data Protection Supervisor.

*"**EEA**" or "**European Economic Area**"* means the European Economic Area that combines the countries of the European Union, Iceland, Liechtenstein, and Norway.

*"**EU Model Clauses**"* are the standard contractual clauses issued by European Commission which offer sufficient safeguards as required by the GDPR for the transfer of Personal Data to third countries which do not ensure an adequate level of data protection according to European Commission.

*"**GDPR**"* means Regulation (EU) 2016/679 of the European Parliament and of the Council 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 data, and repealing Directive 95/46/EC.

*"**Group Data Privacy Officer**" or "**GDPO**"* means the person in charge of the overall supervision of these Binding Corporate Rules through a network of Data Protection Coordinators and Local Compliance Officers, the GDPO report directly to the highest management at the Coface Group level through various committees, including the Risk Committee with external board members and the Data Steering Committee. The GDPO is responsible for ensuring the Coface Entities' compliance with the Binding Corporate Rules and applicable local legal / regulatory requirements. The GDPO enjoys the highest management support for the fulfilling of its tasks.

*"**Local Compliance Officer**"* means the person in charge of data protection matters in each Coface Entity, reporting to the relevant Data Protection Coordinator and being the main point of contact of the GDPO for its Coface Entity.

*"**Onward Transfer**"* means the Onward Transfer of Personal Data by a Coface Entity that has been previously exported pursuant to a Relevant Transfer: to another Coface Entity that is in a third country which (but for the operation of the BCR) does not offer an adequate level of protection ; and which is not subject to any of the permitted derogations, conditions, other mechanisms and additional measures enabling to ensure an adequate protection of the Personal Data transferred.

*"**Personal Data**"* means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

*"**Processing**", "**Process**"* or *"**Processed**"* means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

*"**Processor**"* means a Coface Entity which processes Personal Data on behalf of another Coface Entity acting as a Controller.

*"**Relevant Transfer**"* means a transfer of Personal Data (to the extent such Personal Data has not previously been the subject of a Relevant Transfer or Onward Transfer):

(i) from a Coface Entity that is a Data Exporter to another Coface Entity that is in a third country which does not offer an adequate level of protection in line with GDPR requirements; and

(ii) which is not subject to any of the permitted derogations or conditions contained in Application Data Protection Regulation (which may include the consent of the Data Subject, existing contractual protections such as EU Model Clauses, and/or establishment in a third country approved by the European Commission under the GDPR as ensuring an adequate level of protection).

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

*"**Supervisory Authority**"* means an independent public authority which is established by a Member State pursuant to Article 51.

*"**Third Party**"* shall mean any natural or legal person (including Coface Entities), public authority, agency or any other body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the Personal Data of a Data Subject.

3. SCOPE

3.1 MATERIAL SCOPE

The BCR is applicable when a Coface Entity Processes Personal Data as Controller relating to its employees, business partners, customers, and customers' debtors, and by a Coface Entity acting as an internal Processor, i.e. Processing Personal Data on behalf of a Coface Entity acting as Controller. The scope of the BCR includes Processing of Personal Data carried out in the course of its business activities, employment administration and vendor management – such as:

- Human resources data: including personal data of past and current employees, independent contractors, temporary staff and job applicants;
- Customer data: including personal data relating to representatives of customers who use our products and services, other customer contact information, billing and financial information, website use, and information necessary to authenticate customers and to provide our services;
- Provider data: including personal data relating to representatives of third-party providers other third-party provider information, billing information;
- Financial Data: including personal data relating to the customer's and the customer's debtor's economic situation to permit us to evaluate the credit risk and appropriately price the insurance policy, as well as undertake collection action as necessary.
- Publicly available data: including personal data displayed on governmental and institutional public lists; and
- Supply chain management data: including personal data of individual contractors and of account managers and staff of third-party suppliers who provide services to us

Based on the nature of the Coface Centralized Hosting approach, any Personal Data Processed by a Coface Entity is stored in the EEA. This approach entails that Coface Entities can be provided with logical access to Personal Data stored by another Coface Entity in the EEA. Centralized hosting in the EEA means a single and consistent set of data, closer control on data protection and security with a better supervision of hardware configuration, capacity and performance. By focusing the efforts in one centralized place, the risk relating to data protection and security is reduced especially due to the strong governance in place.

Due to these diverse ranges of Processing activities covered by the Coface Entities may have to process and transfer various categories of Personal Data which are detailed in the table provided as Appendix 8.

3.2 GEOGRAPHICAL SCOPE

Coface Group wants to ensure a consistent approach within Coface Entities where Personal Data are being Processed. Consequently, all Coface Entities irrespective of the country in which they are located are subject to the BCR, to which they adhere in signing the Coface Intra-Group Agreement ("***Coface IGA"***). Each Coface Entity, as a signing party to the Coface IGA, will be bound by the BCR incorporated as an appendix to the Coface IGA. No transfer of Personal Data performed under this BCR shall be carried out by any Coface Entity bound by the BCR to an entity not yet bound by the BCR and unable to demonstrate compliance with the BCR. Any Entity joining the

Coface Group shall adhere to the BCRs through signing the Coface IGA. The list of entities bound by the BCR is set out in Appendix 1 to the BCR. Every Coface Entity bound by the BCR acting as Controller shall be responsible for and able to demonstrate compliance with the BCR.

Where a Coface Entity located outside the EEA ceases to be part of the Coface Group or to be bound by the BCR, no Personal Data shall be transferred to this entity under the BCR. Moreover, any Personal Data transferred prior to the withdrawal of such Coface Entity shall be deleted or returned, unless Data Exporter and Data Importer agree that the Personal Data may be kept by the Data Importer, In the latter case, such Coface Entity undertakes to continue to apply the BCR requirements to the Processing of those Personal Data and a protection must be maintained in accordance with Chapter V of the GDPR. In the future, transfer of Personal Data to this former Coface Entity will require ensuring that appropriate safeguards have been implemented to ensure an adequate level of protection including the conclusion of a written agreement detailing them.

4. BINDING NATURE

4.1 UPON EMPLOYEES OF COFACE

Each Coface Employee, as a Data Subject, benefits from the provisions of the BCR. As protecting Personal Data is a matter of individual and organisational commitment, each Coface Employee must also comply with the requirements specified under the BCR.

The BCR falls within the set of policies Coface Employees are required to comply with as part of their employment contract, such as the Coface Code of Conduct in which the present BCR are incorporated by references. Coface Employees are or will be specifically trained for the handling of Personal Data in the course of their business activities. Failure to comply with the principles and rules of the BCR may lead to disciplinary action that could result in the termination of the employment and, in certain circumstances, to criminal charges.

In accordance with applicable labour law, the present BCR are made binding and enforceable upon Coface Employees of all Coface Entities through any of the following at each Coface Entity:

- through respect of binding Coface Group internal policies, or
- through respect of a binding collective agreement, or
- through respect of a clause in the employment contract, or
- through any other means suitable to make the BCR binding on Coface Employees in their respective country.

4.2 UPON ENTITIES OF THE COFACE GROUP

Coface Group will ensure that all Coface Entities are bound in the same or a similar manner to the principles and obligations specified under the BCR and will comply with the requirements specified herein.

For this reason, the BCR is binding upon all the entities of the Coface Group by virtue of each Coface Entity's signing the Coface IGA, an intragroup agreement incorporating the BCR and adhesion to the BCR.

4.3 TOWARDS COFACE'S CUSTOMERS

Coface Entities may Process Personal Data relating to their customers, and customers' debtors, in the context of Coface Group's business activities, including:

- Credit insurance for companies including reinsurance. This activity involves a broad range of products and services designed for domestic and international transactions made by companies around the world including international insurance for corporate clients;
- Risk analyses and assessments: Coface Entities offers clients global risk analyses and assessments enabling them on the one hand to assess the risk of default from the debtors of Coface Group's clients and on the other to evaluate the overall quality of the business environment in the country to which the customer wishes to export goods or services;
- Factoring;
- Provision of business information;
- Debt collection;
- Bonds; and
- Direct marketing in order to support our core business;

Where a Coface Entity is Processing the Personal Data of Data Subjects of its customers, it undertakes to ensure the protection of the rights of such Data Subject and provide an adequate level of protection to the Personal Data in accordance with the BCR, subject to the provision of Section 8 – Rights of Data Subjects.

4.4 TOWARDS COFACE'S PROCESSORS

Where a Coface Entity engages a Processor such as another Coface Entity or Third Party provider for carrying out specific Processing activities, such Processor shall provide sufficient guarantees and implement appropriate technical and organisational measures in a manner that the Processing will meet the requirements of the BCR, and if necessary the service agreement between Coface Entity and a Controller.

Any Processing activity undertaken by Coface Entities' Processors shall be governed by a written contract or other binding legal act containing all the provisions provided for under Article 28.3 of the GDPR. Such contract or legal act shall stipulate, in particular:

- Processor will process Personal Data only on Controller documented instructions;
- Persons authorised to Process Personal Data have committed themselves to confidentiality or under an appropriate statutory obligation of confidentiality;
- Processor has taken appropriate technical and organisation measures to ensure a level of security appropriate to the risk incurred in line with the Article 32 of the GDPR;
- Processor ensures that it will not engage another processor without prior specific or general written authorisation of the Controller and such processor will undertake to comply with the same Personal Data protection obligations as set out in the contract between the Controller and the Processor;

- Processor has taken into account the nature of the Processing and will assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to Data Subject Requests;

- Processor undertakes to assist the Controller to ensure compliance with Personal Data security and Data Breach requirements;

- Processor, at the choice of the Controller, undertakes to delete or return all Personal Data to the Controller at the end of the provision of services relating to Processing and to delete existing copies unless Applicable Data Protection Legislation requires storage of such Personal Data;

- Processor will make available to the Controller all information necessary to demonstrate compliance with the obligations contained herein and allow for and contributor to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

In any case, such written contract shall set out the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of Coface Entities.

5. PRINCIPLES FOR PROCESSING PERSONAL DATA

The Applicable Data Protection Legislation defines a set of principles to be observed when Processing Personal Data. Coface Group undertakes to comply with these principles whether it is acting as Controller or as an internal Processor.

5.1 DEFINING A LEGAL BASIS FOR PROCESSING

When Personal Data is being Processed, it is required that such Processing relies upon an appropriate legal basis, such legal basis being the foundation that allows for lawful Processing.

In this respect, Coface Group undertakes to lawfully Process Personal Data only where it has a valid legal basis to do so pursuant to the requirements of the Applicable Data Protection Legislation. Accordingly, Coface Entities rely on one of the following legal bases:

- Consent of the Data Subject;

- Performance of a contract to which Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;

- Compliance with a legal obligation;

- Protection of vital interests of the Data Subjects or of another natural person;

- Performance of a task carried out in the public interest or in the exercise of official authority vested in the Coface Entity; and

- Legitimate interests pursued by the Coface Entities, except where such interests are overridden by the interests or rights and freedoms of the Data Subject;

5.2 PURPOSE LIMITATION

Unless specifically authorised by Applicable Data Protection Legislation, Coface Entities shall ensure that it has ascertained a lawful, fair, explicit and legitimate purpose prior to any collection or Processing of Personal Data.

Coface Entities undertake to ensure that the purposes it defines do not breach the Applicable Data Protection Legislation and are legitimate while ensuring Personal Data is not further Processed in a manner that is incompatible with those purposes.

For example, Personal Data will only be processed for the defined purposes for which they have been collected and Data Subjects are informed of such purposes and further Processing operations.

5.3 DATA MINIMISATION

Coface Entities commit to collecting and Processing Personal Data, which is strictly adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

Personal Data shall not be collected widely in the perspective of a further undefined purpose.

As a matter of principle, due to the BtoB activities exclusively carried out by Coface Entities, very few personal data are collected and when these are collected they are strictly necessary for the defined purposes.

Coface Entities will only Process Personal Data necessary to achieve the purposes for which they are collected and further Processed and will delete Personal Data as soon as they are no longer necessary in accordance with Coface data wiping policy or must be retained for instance for a legal obligation.

5.4 RECORDING PROCESSING ACTIVITIES

Coface Entities shall maintain a record in writing, including in electronic form of all categories of Personal Data Processing activities under its responsibility (e.g. payroll Processing, management of customer relationship) that should be made available to the relevant Supervisory Authority upon request.

Such records should at least mention when Coface Entities are Controllers :

- The name and contact details of the relevant Coface Entity that is Controller, the potential joint Controller and the Data Protection Officer;
- The purposes of the Processing;
- The description of the categories of Data Subjects and of Personal Data;
- The categories of recipients of the Personal Data;
- The potential transfers of Personal Data to a third country or an international organisation;
- The Personal Data storage duration;
- A general description of the technical and organisational security measures to ensure a level of security appropriate to the risk of the Processing.

Such records should at least mention when Coface Entities are Processors :

- The name and contact details of the relevant Coface Entity that is Processor and of each Controller on behalf of which it is acting, the potential Controller's or the Processor's representatives, and the Data Protection Officer;
- The categories of processing carried out on behalf of each Controller;
- The potential transfers of Personal Data to a third country or an international organisation;
- A general description of the technical and organisational security measures to ensure a level of security appropriate to the risk of the Processing.

5.5 DATA ACCURACY

Coface Group shall implement adequate measures and controls to ensure that the Personal Data it collects and processes remains accurate and, where necessary kept up to date. To this end, Coface Entities undertake to implement any required actions and to take reasonable steps to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is Processed, are erased or rectified.

Coface Entities offer means for Data Subject to correct and modify any inaccurate Personal Data.

5.6 STORAGE LIMITATION

Coface Group will not keep the Personal Data for a longer period than is strictly necessary having regard to the purpose for which such Personal Data is collected. In this respect, Coface Entities commit to determine a data retention period before implementing each Processing.

To ensure compliance with this requirement, Coface Entities implement a data retention procedure and specify guidelines to be applied with respect to a given Processing activity.

Coface Entities shall ensure that Personal Data are no further processed when it is no longer needed and any copy deleted once legal retention periods and, as applicable, relevant statute of limitation expire.

5.7 DATA SECURITY AND INTEGRITY

Coface Group has implemented appropriate technical, physical and administrative measures and controls to ensure that Personal Data is not unlawfully accessed and/or Processed (Appendix 7). Such technical, physical and administrative measures shall ensure a level of security appropriate to the risk, including, but not limited to, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by a Coface Entity and any Processor.

Coface Entities have implemented robust technical and organisational security measures to ensure the protection of Personal Data when accessed by Coface personnel and stored in Coface Entities systems.

5.8 DATA PROTECTION IMPACT ASSESSMENT

The Data Protection Impact Assessment (DPIA) is a risk-based process introduced by the GDPR that enables the Controller to describe the Data Processing, to prove its necessity and proportionality and to help manage the risks to the rights and freedoms of natural persons resulting

from the Processing of Personal Data by assessing them and determining the measures to address them. Coface Group is committed to conduct DPIAs in accordance with the procedures set forth in Appendix 6 Privacy by Design, Privacy by Default and DPIA Procedure.

Where a type of Processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the Processing, is likely to result in a high risk to the rights and freedoms of Data Subjects, Coface Entities shall, prior to the Processing, carry out a DPIA. This requirement shall also apply to existing Processing operations where a modification of the Processing operation is expected and where such modification may result in a high risk to the rights and freedoms of Data Subjects.

Proposed Processing will generally require a Data Protection Impact Assessment if two or more of the following criteria are satisfied, but a casuistic analysis must be performed:

- The Processing includes systematic evaluation or scoring of personal aspects relating to natural persons, including profiling and predicting;
- The Processing is based on automated decision making with legal or similar significant effect upon Data Subjects;
- The Processing is done on Sensitive Data or Personal Data of highly personal nature;
- The Personal Data is Processed on a large scale;
- The Processing combines or matches two or more Processing operations or datasets;
- The Processing includes a systematic monitoring of a publicly accessible area;
- The Processing relates to vulnerable Data Subjects' or children's Personal Data;
- The Processing includes innovative use or application of new technological or organisational solutions; and
- The Processing prevents the Data Subjects from exercising their rights or using a service or contract.

Where a Data Protection Impact Assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk and where a DPIA reveals high residual risks, Coface Group will seek prior consultation of the Supervisory Authority before carrying out this Processing.

5.9 TRANSFERS OUTSIDE THE COFACE GROUP

Coface Group undertakes not to transfer any Personal Data to Controllers and/or Processors which are not part of the Coface Group unless such Controllers and/or Processors provide sufficient guarantees and have implemented appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of the BCR.

In this respect, Coface Entities have implemented appropriate technical, physical and administrative measures to ensure and control that Personal Data is not unlawfully accessed and/or Processed.

Any Coface Entity is required to enter into a written contract or other binding legal act with any Controllers or Processors outside the Coface Group if they are Processing Personal Data, in line

with GDPR requirements, including in particular regarding Processors a written agreement containing all the provisions provided for under Article 28 of the GDPR pursuant to the same requirements described under Article 4.4 of the BCR. The above-mentioned contract or other binding legal act, shall set out (amongst other things) the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects, the obligations and rights of Coface Entities and describe any technical and organisational measures required to Process securely Personal Data.

5.10 DATA BREACH

Where a Data Breach occurs, Coface Entity shall comply with the applicable Data Breach procedure adopted by Coface Group.(Appendix 5 – Procedure for collecting operational incidents and losses).

In any case, Coface and/or the relevant Coface Entity shall without undue delay, and where feasible, not later than 72 hours after having become aware of it, notify the Data Breach to (1) the Controller when such Coface Entity is acting as a Processor of another Coface Entity, (2) the Supervisory Authority when acting as a Controller, unless the Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons, (3) the GDPO, the Data Protection Coordinator or the Local Compliance Officer, as applicable and (4) Coface.

Coface Entities undertake to document Data Breaches, including information about the factual background, effects and the remedial action taken and such documentation must be made available to the relevant Supervisory Authority upon request.

The above-mentioned notification shall cover at least the following information:

- Nature of the Data Breach and scope of the Data Breach, including when possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

- Name and contact detail of the Group Data Protection Officer (“GDPO”) and the Data Protection Coordinator or Local Compliance Officer or other contact point where more information can be obtained;

- Describe the consequences likely to result from the Data Breach;

- Describe the measures taken or proposed to be taken by the Controller to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

A Coface Entity, when Processing Personal Data on its own behalf, may also need to communicate to the Data Subjects about the Data Breach where it results in a high risk to the rights and freedoms of natural persons. In such circumstances, the communication shall take place without undue delay, and shall cover the above-mentioned elements as the one which would be communicated to the Supervisory Authority.

5.11 NON – COMPLIANCE

Coface Entity acting as Data Importer should promptly inform Coface Entity acting as Data Exporter and Coface if it is unable to comply with the BCR, for whatever reason, including the situations

further described under Article 7 of the BCR. Where the Data Importer is in breach of the BCR or unable to comply with them, the Data Exporter should suspend the transfer.

The Data Importer should, at the choice of the Data Exporter, immediately return or delete the Personal Data that has been transferred under the BCR in its entirety, where:

- the Data Exporter has suspended the transfer, and compliance with this BCR is not restored within a reasonable time, and in any event within one month of suspension; or

- the Data Importer is in substantial or persistent breach of the BCR; or

- the Data Importer fails to comply with a binding decision of a competent court or Competent SA regarding its obligations under the BCR.

The same commitments should apply to any copies of the Personal Data. If applicable, the Data Importer should certify the deletion of the Personal Data to the Data Exporter.

Until the Personal Data is deleted or returned,the Data Importer should continue to ensure compliance with the BCR.

In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred Personal Data, the Data Importer should warrant that it will continue to ensure compliance with the BCR, and will only process the Personal Data to the extent and for as long as required under that local law.

6. PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA AND DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES

Special Categories of Personal Data require specific protection measures because the Processing of such Personal Data could create significant risks in relation to fundamental rights and freedoms of Data Subjects.

Coface Group undertakes to Process Special Categories of Personal Data in accordance with any Applicable Data Protection Legislation or any other applicable legislation in order to carry out its legitimate business activities.

Such Processing shall be limited and specific, in particular in relation to Coface Group's employees.

Processing of personal data relating to criminal convictions and offences shall be prohibited, unless the same exemptions as the ones envisaged by Article 10 GDPR apply. Coface Group may request extract of criminal record before job applicants join a Coface entity but these extracts cannot be retained and are immediately deleted.

Where it intends to Process Special Categories of Personal Data on its own behalf, Coface Entities will ensure that:

- The Processing is necessary and lawful;

- The Processing is carried out with appropriate safeguards and controls; and

- When necessary, and exceptionally, the Data Subject has given explicit consent to the Processing of those Special Categories of Personal Data for one or more specified purposes.

These situations shall be exceptional for narrow and specific situations where recourse to consent is strictly necessary and no alternative means exist, in particular as to employees, because of the concerns about the freely given nature of a consent given in an imbalance relationship. Such consent shall not be considered as necessary when (i) the Data Subject is not in a position to give its consent and the Processing is necessary to protect the vital interests of the Data Subject or of another person; (ii) the Data Subject itself has already manifestly rendered the affected Special Categories of Personal Data part of the public domain; (iii) when applicable, the Processing is explicitly permitted by Applicable Data Protection Legislation or any national law (e.g. processing of national ID and health data for subscribing insurance policies; Processing required under anti-money laundering laws); or

- When necessary, the Processing is essential for the purpose of establishing, exercising or defending legal claims, provided that there are no grounds for assuming that the Data Subject has an overriding legitimate interest in ensuring that such data is not Processed.

7. INTERNATIONAL TRANSFER OF PERSONAL DATA

In the course of their business, Coface Entities may Process Personal Data on behalf of another Coface Entity. Such Coface Entities may be located outside the European Economic Area. In such a case, transfers of Personal Data take place to the relevant Coface Entity outside the EEA. Where Personal Data is transferred, Coface Entities will implement specific guarantees in order to ensure that the Personal Data transferred benefit from an adequate level of protection as further described below:

Personal Data that have been transferred under the BCR may only be onward transferred outside the EEA to Processors and Controllers which are not bound by the BCR provided that the conditions for transfers laid down in Articles 44 to 46 GDPR are applied in order to ensure that the level of protection of natural persons guaranteed by GDPR is not undermined. In the absence of an adequacy decision or appropriate safeguards, Onward Transfers may exceptionally take place if a derogation applies in line with Article 49 GDPR .In any event, Coface Entities commit to use the BCR as a tool for transfers only where they have assessed that the law and practices applicable to the processing of Personal Data to Third Parties, including any requirements to disclose Personal Data or measures authorising access by public authorities, do not prevent them from fulfilling their obligations under these BCR. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society[1] to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the BCR.

For that purpose Coface Entities will take into account:

- the specific circumstances of the transfers or set of transfers and any intended Onward Transfers within the same third country or to another third country , including : the type of entities involved in the processing (the Data Importer and any further recipient of any Onward Transfer); the purpose of Processing and transfer; the categories and format of the transferred Personal Data; the economic sector in which the transfer or set of transfers occurs; the location of Processing including storage location; including the length of the processing chain, the number of actors involved and the transmission channels used;

- the relevant laws and practices of the third country in light of the circumstances of the transfer, including those requiring the disclosure of data to public authorities or authorising

[1] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

access by such authorities and those providing for access to these data during the transit between the country of the Data Exporter and the country of the Data Importer, as well as the applicable limitations and safeguards.

- any relevant contractual, technical or organisational safeguards put in place to supplement the BCR, including measures applied during the transmission and to the Processing of the Personal Data in the country of destination.

Where any safeguards in addition to those in the BCR should be put in place, Coface, the GDPO, the Data Protection Coordinators or the Local Compliance Officers will be informed and involved in such assessment.

Such assessment will be documented appropriately as well as the supplementary measures selected and implemented. Coface Entities should make such documentation available to the Competent Supervisory Authority upon request.

Coface Entities acting as Data Importers warrant that in carrying out this assessment, they have made their best efforts to provide Coface Entities acting as Data Exporters with relevant information.

In that respect, the Data Importer agrees to promptly notify the Data Exporter if, when using these BCR as a tool of transfers, and for the duration of the BCR membership, it has reason to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the BCR, including following a change in the laws in the third country or a measure (such as a disclosure request). This information should also be provided to Coface. In this case, it is being understood that the Data Exporter, with the support of Coface, the GDPO, the Data Protection Coordinators or the Local Compliance Officers, should promptly identify together the additional measures to be implemented by the Data Importer and/or Data Exporter, in order to enable them to fulfil their obligations under the BCR. The same applies if the Data Exporter has reasons to believe that a Data Importer can no longer fulfil its obligations under the BCR.

Where the Data Exporter, along with Coface and the GDPO, the Data Protection Coordinators or the Local Compliance Officers, assesses that the BCR – even if accompanied by supplementary measures- cannot be complied with for a transfer or set of transfers, or if instructed by the Competent Supervisory Authority, it commits to suspend the transfer or set of transfers at stake, as well as all transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the transfer is ended.

In case of suspension, the Data Exporter commits to end the transfer or set of transfers if the BCR cannot be complied with and compliance with the BCR is not restored within one month of suspension. In this case, Personal Data that have been transferred prior to the suspension, and any copies thereof, should, at the choice of the Data Exporter, be returned to it or destroyed in their entirety.

Coface, the GDPO, the Data Protection Coordinators or the Local Compliance Officers will inform all other Coface Entities of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of transfers is carried out by any other Coface Entity or, where effective supplementary measures could not be in place, the transfers at stake are suspended or ended.

Data Exporters should monitor, on an ongoing basis, and where appropriate in collaboration with Data Importers, developments in the third countries to which the Data Exporters have transferred

Personal Data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

Where transfers of Personal Data is carried out from a Coface Entity to Third Parties located outside of the EEA, such Coface Entity undertakes to comply with the requirements of the GDPR and notably its Chapter V.

8. RIGHTS OF DATA SUBJECTS

Due to the Processing of their Personal Data by a Coface Entity, Data Subjects are entitled to enforce the BCR as Third-Party beneficiaries.

Data Subjects must at least be able to enforce the following elements:

- Purpose limitation of the Processing (Article 5.2);
- Data minimisation (Article 5.3);
- Limitation of the storage periods (Article 5.6);
- Data accuracy (Article 5.5);
- Data protection by design and by default and measures to ensure data security (Articles 12 and 5.7);
- Legal basis for Processing (Article 5.1);
- Specific rules when Processing of Special Categories of Personal Data (Article 6);
- Transparency and easy access to the BCR (Article 13);
- Rights of access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to Processing, right not to be subject to decisions based solely on automated Processing, including profiling (Article 8.3);
- Right to complain through the internal complaint mechanism of the Coface Entities (Article 8.4 ; Article 6c);
- National legislation preventing respect of BCR (article 7);
- Public authorities' access requests (Article 13.3);
- Cooperation duties with Supervisory Authorities (Article 13.4);
- Security (Articles 1 "Integrity and confidentiality principle" and 5.7) including the duty to enter into written agreements with Third Parties Processing Personal Data (Article 5.10) as well as the duty to notify Data Breach to Supervisory Authority (Article 5.11) ;
- Right to lodge a complaint with the Supervisory Authority (choice between the Supervisory Authority in the member state of his habitual residence, place of work or place of the alleged infringement) and before the competent court of the EU member state (choice for the Data Subject to act before the courts where the Controller or Processor has an establishment or where the Data Subject has his or her habitual residence) (Article 8);

- Right to judicial remedies and the right to obtain redress and, where appropriate, compensation in case of any breach of one of the enforceable elements of the BCR (Appendix 3; Articles 8, 8.1 and 8.2);

- Right to enforce Third-Party beneficiary rights listed in this Article 8.

Thus, Coface Group acknowledges that Data Subjects are entitled to seek judicial remedies and/or remedies before a Supervisory Authority under the conditions defined below, for any non-compliance with the BCR and to receive compensation for any damages resulting from the violation of the BCR by any Coface Entity.

8.1 WHERE A COFACE ENTITY WITHIN THE EEA DOES NOT COMPLY WITH THE BCR

Where a Coface Entity within the EEA does not comply with the BCR, the Coface Entity within the EEA responsible for the non-compliance shall bear responsibility and shall take the necessary actions in order to remedy its acts.

The Data Subject shall be entitled to:

- lodge a complaint with a Supervisory Authority, in particular in the member state of its habitual residence, place of work or place of the alleged infringement; and/or;

- an effective judicial remedy where he or she claims that the BCR has been infringed by Coface Entity acting as a Controller or by a Coface Entity acting as a Processor. Coface Entities acknowledge that such claim can be brought either before the member state where the Coface Entity responsible for the non-compliance is established or before the court where the Data Subject has its habitual place of residence.

8.2 WHERE A COFACE ENTITY OUTSIDE OF THE EEA DOES NOT COMPLY WITH THE BCR

Where a Coface Entity outside of the EEA does not comply with the BCR, Coface (i) accepts and acknowledges responsibility for any damages resulting from the non-compliance, (ii) agrees to take the necessary actions in order to remedy the acts of such other Coface Entity and (iii) agrees to pay compensation for any damages resulting from the violation of the BCR by such other Coface Entity.

In such circumstances, Coface Group also acknowledges that the Data Subject shall be entitled to:

- lodge a complaint with a Supervisory Authority where the Data Subject has its place of residence, place of work or where the Coface Entity with delegated responsibility is established; and/or

- the right to an effective judicial remedy where the Data Subject claims that the BCR has been infringed by any Coface Entity as Controller or by a Coface Entity acting as a Processor Processing Personal Data on its behalf and such infringement has harmed the Data Subject.

Coface will be responsible for demonstrating that such Coface Entity outside the EEA is not liable for any violation of the rules specified under the BCR and which has resulted in the Data Subject claiming damages. In the event Coface can demonstrate that the other Coface Entity located outside the EEA was not responsible for the act, then it can also discharge itself from any responsibility.

8.3 DATA SUBJECTS' RIGHTS

Data Subjects are entitled to benefit from the following rights:

- Have access to the Personal Data relating to them and Processed by Coface Entities;
- Request the rectification or deletion of any inaccurate or incomplete Personal Data relating to them, and of any Personal Data with respect to which the purpose of Processing is no longer legal or appropriate;
- Request the limitation of the Processing of Personal Data relating to them;
- Object to the Processing of their Personal Data at any time, on grounds relating to the Data Subject's particular situation, which is based on the legitimate interests pursued by Coface Entities, unless the Coface Entity demonstrates compelling legitimate grounds for the Processing which are not overridden by the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.
- Be notified regarding rectification or erasure or restriction;
- Be informed about any update of the BCR and of the list of Coface Entities by way of publishing the new version without undue delay;
- Object to the Processing of their Personal Data for direct marketing purposes, including profiling;
- Not to be subject to decisions based solely on automated processing, including profiling which produces legal effects concerning them or similarly significantly affects them;
- Portability, i.e. to receive their Personal Data in a structured, commonly used, machine-readable format and interoperable when the Processing is carried out by automated means.

Where a Coface Entity is acting as Controller, it will handle such request without undue delay and in accordance with the complaint handling procedure specified under Section 9 below.

8.4 EXERCISING DATA SUBJECTS' RIGHTS

Data Subjects are entitled to enforce the BCR as Third-Party beneficiaries and to exercise their rights with respect to the Processing of their Personal Data by Coface Entities. Coface Entities shall ensure that any request or complaint from Data Subjects in relation to the exercise of their rights ("***Requests***") is addressed in a timely manner.

Data Subjects can make a request verbally or in writing. Coface Entities will provide Data Subjects with accessible means to exercise their rights and, in particular:

1 – A single dedicated contact email to be used irrespective of the country a Data Subject is located in to contact the GDPO directly Coface_dpo@coface.com

Local emails can be used in order to take into account local specificities, such as language.

2 – Privacy notices on Coface Group websites with a hyperlink to send a message to the single contact email address

3 – Single dedicated postal address to be used irrespective of the country a Data Subject is located in:

Data Protection Officer
1 Place Costes et Bellonte
92270 – Bois-Colombes
FRANCE

The GDPO, or any other individual or entity, internal or external, appointed by the GDPO, the Data Protection Coordinator or the Local Compliance Officer for the purpose of managing the Requests, shall (i) ensure that they have obtained the minimum required information from the concerned Data Subject to address his/her Request (ii), if deemed necessary, obtain as much information as possible to enable the Request to be duly handled.

If a doubt about the identity of the individual making the request exists, mainly when using distance communication means, Coface Entities may be required to ask for more information regarding the Data Subjects. Information collected shall be limited to information that is necessary to confirm who the individual making a request is. Proportionality shall always be assessed by the Controller.

In any case, the response to a Data Subject must occur within 1 month at the latest after receiving the Request (except in certain limited circumstances notably mentioned in Article 9 and further described in Appendix 3).

Where the Data Subject is not satisfied with the initial response provided by the Coface Entity, such Data Subject shall be entitled in any case to immediately ask for his or her Request to be re-examined. The Data Subject shall provide to the Coface Entity a detailed explanation of the unsatisfactory provisions of the solution provided. The Coface Entity shall take no longer than 2 months from receipt of the Request for re-examination to determine how it shall be handled and shall inform the Data Subject in writing accordingly.

In any case, if a Data Subject Request or complaint is rejected by the Coface Entity or the answer does not satisfy the Data Subject, the Data Subject can contact the GDPO, the Data Protection Coordinator or Local Compliance Officer.

In any case, Data Subjects can at any time lodge a complaint before a competent court and / or a Supervisory Authority, independently of any internal complaint mechanism.

Further details regarding this Article are available in the following Appendix 3 – Procedure to Process Data Subjects' Requests.

9. DATA SUBJECTS COMPLAINT HANDLING PROCEDURE

Data Subjects are entitled to lodge a complaint regarding the Processing of Personal Data they consider non-compliant with the BCR before the Coface Entity they deem to be non-compliant. Where the breach is likely to result from an act of a Coface Entity located outside the EEA, the Data Subject can lodge the complaint directly with Coface.

Such complaint will be handled by Coface and/or the relevant Coface Entity in due course and with particular care and attention according to the steps and timing defined herein. Such provisions are also applicable in relation to Data Subjects' Requests.

In practice, complaints made by Data Subjects will be handled according to the procedure defined under Appendix 3 – Procedure to Process Data Subjects' Requests

Coface Entities commit to reverting to a Data Subject with a reply to his/her complaint within one month from the date such complaint is lodged in accordance with the provisions herein. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Controller shall inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

In the event a Coface Entity decides to reject the request or complaint made by a Data Subject, this Coface Entity undertakes to inform such Data Subject about its decision and to provide him/her with information regarding the reason for such dismissal within one month.

In the event Coface Entity considers that a complaint made by a Data Subject is justified, Coface Entity commits to implementing the corrective measures it deems adequate to remedy such situation as soon as reasonably possible. In addition, Coface Entity will also promptly inform the concerned Data Subject once the corrective measures have been implemented and the situation is remedied.

In any case, Data Subjects are entitled to lodge a complaint before a court and/or a Supervisory Authority. Such right is not dependent on the data subject having used the complaint handling process beforehand.

Coface Entities acknowledge that Data Subjects may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) GDPR.

10. DATA PROTECTION GOVERNANCE

Coface Group has created a data protection organisation and governance structure which is presented in Appendix 2 – DPO Network and Data Protection Governance. This organisation is led by the Data Steering Committee and the GDPO who relies on a network of Data Protection Coordinators and Local Compliance Officers.

The roles and responsibilities of the network as well as its working governance are further described in Appendix 2.

11. TRAINING AND AWARENESS

Protecting Personal Data is not only a matter of compliance with Applicable Data Protection Legislation, but is part of the embodiment of Coface Group core values. In this context, fostering a privacy culture within the group is essential to make all employees, contractors, agents, trainees and other persons whose conduct, in the performance of work, is under the direct control of Coface Entities, accountable for the protection of Personal Data Processed as part of Coface Group operations.

To this end, Coface Group has adopted a privacy training program which aims at ensuring that Coface Employees, contractors, agents, trainees, and other persons whose conduct, in the performance of work is under the direct control of Coface Entities, are actually aware of the obligations, principles and procedures specified under the BCR. Such training program is further described in Appendix 9.

Such training carried out at least every (2) years is aimed at: (i) individuals having permanent or regular access to Personal Data; (ii) individuals involved in the collection of Personal Data; and/or (iii) individuals involved in the development of tools used to Process Personal Data.

The training program will aim at providing an up-to date :

- basic level core of knowledge regarding the applicable principles when Processing Personal Data and a good understanding of the existing procedures and their implementation, including procedures of managing requests for access to Personal Data by public authorities ; and

- Specific training adapted to the different functions within the organisation.

12. PRIVACY BY DESIGN/ PRIVACY BY DEFAULT

In order to ensure that the principles defined under the BCR are effectively taken into account and reflected in the different Processing it carries out, Coface Entities will take data protection into consideration from the very beginning of any new project.

In order to provide a high level of protection to Personal Data within the organisation, the principles and obligations defined herein will thus be integrated into the design of each project on the basis of privacy by design procedures adopted by Coface Group.

Details on the implementation at Coface Group of Privacy by design and by default are provided in Appendix 6.

13. TRANSPARENCY AND COOPERATION

13.1 COMMUNICATION OF THE BCR

Coface Entities will openly communicate the BCR to the Data Subjects and make it easily accessible to any individual. Such communication shall allow any Data Subject to obtain a copy of the BCR with no undue delay and in an open format.

Easy access to BCR will notably be ensured through the publication of the BCR on Coface and Coface Entities website.

Coface Entities will, in particular, allow the improvement of the privacy and security culture within its organisation by sharing the BCR through internal systems and means.

Where a Coface Entity contracts with a Processor, the Coface Entity commits to sharing information on BCR with the Processor and where practicable to refer to the BCR in the agreement concluded with the Processor.

13.2 INFORMATION TO DATA SUBJECTS

A Coface Entity, where acting as Controller, shall provide Data Subjects any information required by Applicable Data Protection Legislation. Such information shall be provided at the time when Personal Data is obtained, and shall include the following elements:

- The identity and the contact details of the Controller;

- The contact details of the Data Protection Officer;

- The purposes of the Processing and its legal basis;

- As the case may be, the existence of further Processing of Personal Data for a purpose other than that for which the Personal Data were collected and the relevant information on that other purpose with any relevant information contained hereunder;

- If the information is not collected directly from the Data Subject, the categories of Personal Data Processed;
- The recipients of the Personal Data;
- Where applicable, the existence of Data Transfers outside of the EEA, the countries where the Personal Data is transferred, the measures implemented to ensure an adequate level of protection and the means by which to obtain a copy of them;
- The data retention periods;
- The rights of the Data Subjects as defined under Section 8 above. (e.g. the existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability);
- The right to lodge a complaint before a Supervisory Authority;
- Where Personal Data is collected from the Data Subject, whether the Data Subject (i) is obliged to provide the Personal Data due to any statutory or contractual requirement, or (ii) has a requirement to provide the Personal Data as it is necessary to enter into a contract, and of the possible consequences of failure to provide such data;
- If the Processing is based on the consent of the Data Subjects, the right for them to withdraw their consent at any time without affecting the lawfulness of Processing based on consent before its withdrawal;
- If the Processing is based on Coface Entities' legitimate interest, explanations regarding the legitimate interest;
- As the case may be, the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject; and
- Where the Personal Data is not collected from the Data Subject, any available information as to their source.

Coface Entities undertake to provide such information to Data Subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

13.3 OBLIGATIONS IN CASE OF ACCESS REQUESTS BY PUBLIC AUTHORITIES

Coface Entity acting as Data Importer will promptly notify the Data Exporter and where possible, the Data Subject (if necessary with the help of the Data Exporter) if it:

- Receives a legally binding request by a public authority under the laws of the country of destination, or of another third country, for disclosure Personal Data transferred according to the BCR; such notification will include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided;
- Becomes aware of any direct access by public authorities to Personal Data transferred according to the BCR in accordance with the laws of the country of destination; such notification will include all information available to the Data Importer.

If prohibited from notifying the Data Exporter and/or the Data Subject, the Data Importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the Data Exporter.

The Data Importer will provide the Coface Entity acting as Data Exporter, at regular intervals, with as much relevant information as possible on requests received (number of requests, type of data requested, requesting authority, whether requests have been challenged and the outcome of such challenges etc.). If the Data Importer is or becomes partially or completely prohibited from providing the Data Exporter with the aforementioned information, it will, without undue delay, inform the Data Exporter accordingly.

The Data Importer will preserve the abovementioned information for as long as the Personal Data are subject to the safeguards provided by the BCR and shall make it available to the Competent Supervisory Authorities upon request.

The Data Importer will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and principles of international comity.

The Data Importer will, under the same conditions, pursue possibilities of appeal.

When challenging a request, the Data Importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the personal data requested until required to do so under the applicable procedural rules.

The Data Importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter and also to the Competent Supervisory Authorities upon request.

The Data Importer will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

In any case, Coface Entities commit not to transfer Personal Data to public authorities in a massive and disproportionate and indiscriminate way that would go beyond what is necessary in a democratic society. Coface Entities will use its best efforts and shall take all reasonable actions to avoid and/or waive any legal prohibition to notify the Supervisory Authorities about a Transfer of Personal Data to authorities. Where it is not possible to avoid such prohibition, Coface must provide to Supervisory Authorities annual general information regarding the numbers of disclosure of Personal Data to the authorities carried out to the Coface Group.

In that regard, Coface Entities located in the EEA acknowledge that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring them to transfer or disclose Personal Data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to Chapter V of GDPR.

13.4 DUTY TO COOPERATE WITH SUPERVISORY AUTHORITIES

The Coface Entities agree to cooperate with Supervisory Authorities, including by enabling such Supervisory Authorities to perform audits thereof, including where necessary on-site, and to take into account any advice that may be provided in relation to the BCR and abide by the decisions issued by the Supervisory Authorities.

The Coface Entities shall make available to the Supervisory Authority, upon request, the records of Processing activities or any information about the processing operations covered by the BCR.

Any dispute related to the Supervisory Authority exercise of supervision of compliance with the BCR that may arise will be submitted to the courts located in the Supervisory Authority's country in accordance with its procedural law. The Coface Entities agree to submit themselves to the jurisdiction of these courts.

14. AUDIT

Coface Group's audit procedure is described in Appendix 4 – Procedure for Audits.

The audit covers all aspects of the BCR including methods for ensuring that corrective actions will take place. The result of the audit reports will be communicated :

- to the GDPO, Data Protection Coordinators and Local Compliance Officers of any impacted Coface Entity,
- to the board of Coface and where appropriate, of any impacted Coface Entity,
- where appropriate, to the Coface Group Risk and Compliance Committee.

The results of the audit reports and relevant internal audit reports will be maintained in a form such that Supervisory Authorities located in the EEA may access them if they utilize their audit right set out below.

Coface Group acknowledges that Supervisory Authorities can request communication of the audit results and thus agree to grant them access thereto upon request.

Coface Group commits to develop and integrate into its audit program the review of its compliance with the BCR. The audit program will enable Coface Entities to define:

- a reasonable frequency according to which audits shall be carried out;
- the expected scope of the audit; and
- the team in charge of the audit.

Coface Group commits to having audits conducted every 1 to 4 year based on risk assessment by an internal or external audit team, whose roadmap is initiated and advised by the GDPO and the concerned Data Protection Coordinators and Local Compliance Officers. The GDPO or any other competent function in the organisation can also trigger specific and ad hoc audit, in the scope of its missions. The GDPO is responsible for determining the scope of audits to be performed. To this end, it can also consult the Data Steering Committee.

The results of each audit will be submitted to the Data Steering Committee for information. The final report, defect identification and remedial actions are to be shared and enforced by the Data

Protection Coordinators and Local Compliance Officers and Data Protection Coordinators. Based on the Data Protection Coordinator's assessment, the report may be shared, where appropriate, with any concerned Local Compliance Officers, Data Protection Coordinator, local security manager, Process / system owners, board of Coface or any other required internal employee. Remedial actions will be defined with a prioritisation to determine a schedule for implementing such measures.

15. CHANGES TO THE BCR

Coface GDPO will ensure that it keeps a fully updated list of entities bound by the BCR and keeps track of and record any updates to the rules in order to reflect the current situation (for instance to take into account modifications of the regulatory environment, EDPB Recommendations or changes to the scope of the BCR) and provide the necessary information to the Data Subjects or Supervisory Authorities upon request. Coface GDPO is liable to keep the BCR up-to-date and in compliance with article 47 GDPR and EDPB Recommendations.

Where any new entity of Coface Group shall be bound by the BCR, Coface GDPO shall update the list, assisted by the Data Protection Coordinators and Local Compliance Officers and shall make available updated information at least once a year or when deemed necessary by the GDPO: (i) each Coface Entity and (ii) its employees.

Coface GDPO will ensure that any changes to the BCR, including to the list of BCR members, will be reported without undue delay to all BCR members, and to Data Subjects by way of publishing the new version.

Coface GDPO will ensure that any changes to the BCR or to the list of Coface Entities bound by the BCR will be reported at least once a year to the Supervisory Authority with a brief explanation of the reasons justifying the update. The Supervisory Authority must also be notified once a year in instances where no changes have been made.

The annual update or notification must also include the renewal of the confirmation concerning the assets of entities bound by the BCR.

To the same extent where a modification would significantly affect the BCR or would possibly affect the level of protection offered by the BCR, Coface GDPO undertakes to communicate it in advance to the Supervisory Authority with a brief explanation of the reasons for the update. In this case, the Supervisory Authority will assess whether the changes made require a new approval.

The information regarding any such updates and/or amendments will be made on a timely manner so as to enable Coface Group’s customers and contractual partners to acknowledge such updates and/or amendments and to take necessary actions where required.

* * *
* *
*

List of Appendixes:

Appendix 1 *List of Coface Entities bound by the BCR (publicly available)*

Appendix 2 *DPO Network and Data Protection Governance (non-publicly available)*

Appendix 3 *Procedure to Process Data Subject requests (publicly available)*

Appendix 3 bis *Internal Procedure to Process Data Subject requests (non-publicly available)*

Appendix 4 *Procedure for audits (non-publicly available)*

Appendix 5 *Procedure for Collecting Operation Incident and Losses (non-publicly available)*

Appendix 6 *Privacy by Design and by Default and DPIA Procedure (publicly available)*

Appendix 7 *Information Security Policy Counter Part (non-publicly available)*

Appendix 8 *BCR Material Scope (publicly available)*

Appendix 9 *Training program (non-publicly available)*