tessi®

BINDING CORPORATE RULES (BCR-C)

Tessi acts as Controller

REFERENCE	
Document type:	Policy
Centre:	ALL
Customer:	ALL
Reference:	Binding Corporate Rules (BCR-C), Tessi acts as Controller
Version:	1.0

tessi®

CONTENTS

I. BACKGROUND 5

II. DEFINITIONS 6

III. SCOPE 9

1. Geographic scope 9
2. Material scope 9
2.1 Categories of personal data and categories of data subjects 9
2.2 Purposes of the processing 9
2.3 Type of the processing 10
2.4 Third Countries 10

IV. THIRD COUNTRIES' LAWS AND PRACTICES 11

1. Laws and practices affecting compliance with the BCR-C 11
2. Government access requests 13

V. TESSI GROUP ENTITIES' LIABILITY REGIME 16

VI. RIGHTS OF DATA SUBJECTS 17

1. Right to enforce the BCR-C as third-party beneficiaries 17
2. Rights to request access, rectification and erasure of personal data and other rights of data subjects 17
3. Right to judicial remedies, redress and compensation 21
4. Right of information 22

VII. PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA 23

1. Transparency 23
2. Fairness, lawfulness and purposes limitation 25
3. Legal basis 26
4. Accuracy and data minimisation 28
5. Security of personal data 29
5.1 Security governance 30
5.2 Human Resources 30
5.3 Physical security 30
5.4 Incident management 30
5.5 Identity management 30
5.5.1 Access controls 30
5.5.2 Management of remote access and mobile devices 31

5.6 Operational security 31
5.7 Protection against malicious code 31
5.8 Vulnerability management 31
5.9 Development security 31
5.10 Security of communications 32
5.11 Backing-up of personal data 32
5.12 Encryption 32
5.12.1 Database encryption 32
5.12.2 Transfer encryption 32
5.13 Maintenance and destruction of personal data 32
5.14 Traceability management 33
5.15 Auditing of security measures 33
6. Data protection by design and data protection by default 33
7. Notification of personal data breaches 35
VIII. DECISION BASED SOLELY ON AUTOMATED PROCESSING AND PROFILING 38
IX. STORAGE PERIOD OF PERSONAL DATA 40
X. ONWARD TRANSFER OF PERSONAL DATA 41
1. Onward transfer 41
XI. PROCESSING OF SENSITIVE DATA AND CRIMINAL DATA 42
1. Processing of sensitive data 42
2. Processing of criminal data 44
XII. COOPERATION WITH THE COMPETENT SUPERVISORY AUTHORITIES 46
XIII. COMPLAINT HANDLING PROCESS 47
XIV. BCR-C UPDATING PROCESS 48
APPENDIX 1: LIST OF TESSI GROUP ENTITIES BOUND BY THE BCR 49
APPENDIX 2: DESCRIPTION OF THE MATERIAL SCOPE OF THE TESSI GROUP BCR-C 60

tessi®

I. BACKGROUND

The protection of personal data is a major concern for the Tessi Group. As part of its activities, the Tessi Group undertakes to protect the personal data processed, whether during its collection, processing, storage or transfer. The Tessi Group undertakes to comply with Union and Member State laws and regulations applicable in this area.

The Tessi Group has therefore put in place a specific governance structure to ensure the protection of personal data at group level. This governance structure has been approved by senior management and is overseen by a Data Protection Officer (Group DPO). This governance structure is intended to build, maintain and coordinate the personal data protection programme within the Tessi Group and is strategically aligned with risk reduction issues. It must be implemented by all Tessi Group entities referred to in this document.

Pursuant to Article 46(2)(b) of 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 (the "GDPR"[1]), the Tessi Group has decided to adopt binding corporate rules setting out appropriate safeguards, harmonised at group level, to provide a framework for the transfers of personal data carried out by its entities referred to in this document.

Consequently, this document sets out the binding corporate rules of the Tessi Group where it acts as controller or internal processor.

[1] Article 46(2)(b) of the GDPR states: *"The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by binding corporate rules in accordance with Article 47".*

I. DEFINITIONS

For the purposes of these BCR-C, the terms listed below, whether or not capitalised, shall have the meanings given to them in this Section:

BCR-C

Means these Tessi Group Binding Corporate Rules.

Competent Supervisory Authority

Means the EEA Supervisory Authority competent for the data exporter.

Controller

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

For example: The relevant Tessi Group entity is the controller for the personal data of its employees, prospective customers or suppliers, etc. Where it carries out processing on behalf of its customers as part of a service provided under an agreement, the entity's customers are then the controllers.

Criminal data

Means personal data relating to criminal convictions and offences.

Data exporter

Means the controller or internal processor that transfers personal data in a Third Country.

Data importer

Means the controller or internal processor located in a Third Country that receives personal data from the data exporter.

Data Protection Authority (or Supervisory Authority)

Means the independent public authority responsible for the protection of personal data in each EEA State.

For example: In France, this is the Commission Nationale de l'Informatique et des Libertés (CNIL) while, in Spain, this is the Agencia Española de Protección de Datos (AEPD).

Data subject

Means 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

EEA

Means the European Economic Area[2].

Internal processor

Means the Tessi Group entity that processes personal data in its capacity as processor on behalf of another Tessi Group entity that acts as controller.

Lead Supervisory Authority

Means, for the purposes of these BCR-C, the French Supervisory Authority, namely, the *Commission Nationale de l'Informatique et des Libertés* ("CNIL").

Liable Tessi Group Entity

Shall have the meaning given to it in Section V.

Personal data

Means any information relating to an identified or identifiable natural person (see "data subject" above); 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.

Some examples of personal data: (i) the surname and first name, the identity photo or a personal email address (which directly identify the natural person), and (ii) the social security number, security pass number, customer identifier, connection logs, or identification number (which do not directly identify the individual but make it possible to indirectly identify the natural person to which they relate).

Processing of personal data

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.

[2] The European Economic Area includes European Union countries and Iceland, Liechtenstein and Norway.

Some examples of processing: collection, digitisation, storage, retrieval, adaptation or modification, consultation, use, disclosure by transmission, transfer, dissemination, erasure, archiving or destruction.

Processor

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

For example: In providing services to customers, the relevant Tessi Group entity processes personal data on behalf of its customers as processor, in particular concerning the processing of their own customers' data (cheques, invoices, etc.).

Sensitive data

Means special categories of personal data, namely (i) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, (ii) genetic data, (iii) biometric data for the purpose of uniquely identifying a natural person, (iv) data concerning health, and (v) data concerning a natural person's sex life or sexual orientation.

Standard contractual clauses

Means the standard data protection clauses adopted by the European Commission to provide a framework for transfers of personal data to a third country as provided for in Article 46(2)(c) of the GDPR[3].

Tessi Group

Means all the Tessi Group entities defined below.

Tessi Group entity(ies)

Means Tessi SA and the legal entities controlled by Tessi SA and bound by these BCR-C, as listed in Appendix 1 to these BCR-C. For the purposes of this definition, "control" means the holding of more than 50% of the economic and voting rights.

Third Country(ies)

Means countries out of the EEA that have not been recognised as providing an adequate level of protection pursuant to the GDPR.

[3] Article 46(2)(c) of the GDPR states: *"The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2)".*

II. SCOPE

1. Geographic scope

The list of Tessi Group entities bound by these BCR-C is set out in Appendix 1.

These BCR-C apply to all transfer of personal data from Tessi Group entities established in the EEA, acting as controller, to Tessi Group entities established in a Third Country, acting as controller or internal processor, as well as to their onward transfers to other Tessi Group entities established in a Third Country acting as controller or internal processor.

As such, these BCR-C apply to all data subjects whose personal data are transferred within the scope of these BCR-C, being understood that these BCR-C apply to transfers of personal data carried out by Tessi Group entities established in Third Countries, to Tessi Group entities also established in Third Countries, insofar as the GDPR applies to such processing in accordance with the conditions provided for in Article 3.2 of the GDPR[4]. *For example: if a Tessi Group entity established in Tunisia transfers personal data concerning its Tunisian employees to a Tessi Group entity established in Mauritius, such transfer and the related processing will not be governed by the GDPR and these BCR-C will not apply to those transfers and the related processing.*

2. Material scope

The material scope of these BCR-C is presented below and more fully described in Appendix 2.

2.1 Categories of personal data and categories of data subjects

These BCR-C cover the categories of personal data and categories of data subjects described in Appendix 2.

⇨ Note: The BCR-C apply to automated and manual processing.

2.2 Purposes of the processing

These BCR-C cover the processing purposes described in Appendix 2.

[4] Article 3.2 of the GDPR states: *"This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or b) the monitoring of their behaviour as far as their behaviour takes place within the Union."*

2.3 Type of the processing

These BCR-C cover the following types of processing:

1. Collection and recording;
2. Access and disclosure;
3. Reading and consultation;
4. Use and exploitation;
5. Organisation and structuring;
6. Copying and extraction;
7. Modification and adaptation;
8. Erasure and destruction;
9. Hosting, storage and archiving;
10. Transmission, dissemination or any other form of provision;
11. Alignment or combination.

2.4 Third Countries

The list of Third Countries to which personal data may be transferred under these BCR-C is provided in Appendix 1.

tessi®

III. THIRD COUNTRIES' LAWS AND PRACTICES

1. Laws and practices affecting compliance with the BCR-C

The Tessi Group entity acting as data exporter and the Tessi Group acting as data importer will use the BCR-C as a tool for transfers only where they have assessed that the law and practices in the Third Country of destination applicable to the processing of the personal data by the Tessi Group entity acting as data importer, including any requirements to disclose personal data or measures authorising access by public authorities, do not prevent it from fulfilling its obligations under these BCR-C.

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 to safeguard one of the objectives listed Article 23(1) of the GDPR[5], are not in contradiction with these BCR-C.

In assessing the laws and practices of the Third Country which may affect the respect of the commitments contained in the BCR-C, the Tessi Group entities should take due account, in particular, of the following elements:

i. The specific circumstances of the transfers or set of transfers, and of any envisaged onward transfers within the same Third Country or to another Third Country, including:

   - purposes for which the data are transferred and processed (e.g., marketing, HR, storage, IT support);
   - types of entities involved in the processing (the data importer and any further recipient of any onward transfer);
   - economic sector in which the transfer or set of transfers occur;

[5] Article 23(1) of the GDPR states: *"Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); (i) the protection of the data subject or the rights and freedoms of others; (j) the enforcement of civil law claims."*

- categories and format of the personal data transferred;
- location of the processing, including storage; and
- transmission channels used.

ii. The laws and practices of the Third Country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities and those providing for access to these data during the transit between the country of the Tessi Group entity acting as data exporter and the country of the Tessi Group entity acting as data importer, as well as the applicable limitations and safeguards.

iii. Any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the BCR-C, including measures applied during transmission and to the processing of the personal data in the country of destination.

Where any safeguards in addition to those envisaged under the BCR-C should be put in place, the Liable Tessi Group Entity and the Group DPO or the relevant DPO relay will be informed and involved in such assessment.

The Tessi Group entities should document appropriately such assessment, as well as the supplementary measures selected and implemented. They should make such documentation available to the Competent Supervisory Authorities upon request.

Any Tessi Group entity acting as data importer should promptly notify the Tessi Group entity acting as data exporter if, when using these BCR-C as a tool for transfers, and for the duration of the BCR membership, it has reasons to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the BCR-C, 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 the Liable Tessi Group Entity.

Upon verification of such notification, the Tessi Group entity acting as data exporter, along with the Liable Tessi Group Entity and the Group DPO or relevant DPO relay should promptly identify supplementary measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the Tessi Group entity acting as data exporter and/or the Tessi Group entity acting as data importer, in order to enable them to fulfil their obligations under the BCR-C. The same applies if the Tessi Group entity acting as data exporter has reasons to believe that a Tessi Group entity acting as data importer can no longer fulfil its obligations under these BCR-C.

Where the Tessi Group entity acting as data exporter, along with the Liable Tessi Group Entity and the Group DPO or the relevant DPO relay, assesses that the BCR-C – even if accompanied by supplementary measures – cannot be complied with for a transfer or set of transfers, or if instructed by the Competent Supervisory Authorities, 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.

Following such a suspension, the Tessi Group entity acting as data exporter has to end the transfer or set of transfers if the BCR-C cannot be complied with and compliance with the BCR-C 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 Tessi Group entity acting as data exporter, be returned to it or destroyed in their entirety.

The Liable Tessi Group Entity and the DPO Group or the relevant DPO relay will inform all other Tessi Group 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 Tessi Group entities or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended.

The Tessi Group entity acting as data exporter should monitor, on an ongoing basis, and where appropriate in collaboration with the Tessi Group entity acting as data importer, developments in the Third Countries to which the Tessi Group entity acting as data exporter have transferred personal data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

2. Government access requests

Without prejudice to the obligation of the Tessi Group entity acting as data importer to inform the Tessi Group entity acting as data exporter of its inability to comply with the commitments contained in the BCR-C (see clause 1 above), the Tessi Group entities also commit to the following obligations:

i. The Tessi Group entity acting as data importer will promptly notify the Tessi Group entity acting as data exporter and, where possible, the data subject (if necessary, with the help of the Tessi Group entity acting as data exporter) if it:

   a) receives a legally binding request by a public authority under the laws of the country of destination, or of another Third Country, for disclosure of personal data transferred pursuant to the BCR-C; such notification will include information about the

personal data requested, the requesting authority, the legal basis for the request and the response provided;

b) becomes aware of any direct access by public authorities to personal data transferred pursuant to the BCR-C in accordance with the laws of the country of destination; such notification will include all information available to the Tessi Group entity acting as data importer.

ii. If prohibited from notifying the Tessi Group entity acting as data exporter and / or the data subject, the Tessi Group entity acting as 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 Tessi Group entity acting as data exporter.

iii. The Tessi Group entity acting as data importer will provide the Tessi Group entity acting as data exporter, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the Tessi Group entity acting as data importer is or becomes partially or completely prohibited from providing the Tessi Group entity acting as data exporter with the aforementioned information, it will, without undue delay, inform the Tessi Group entity acting as data exporter accordingly.

iv. The Tessi Group entity acting as data importer will preserve the above-mentioned information for as long as the personal data are subject to the safeguards provided by the BCR-C, and shall make it available to the Competent Supervisory Authorities upon request.

v. The Tessi Group entity acting as 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 Tessi Group entity acting as data importer will, under the same conditions, pursue possibilities of appeal.

When challenging a request, the Tessi Group entity acting as 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.

vi. The Tessi Group entity acting as 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 Tessi Group entity acting as data exporter. It will also make it available to the Competent Supervisory Authorities upon request.

vii. The Tessi Group entity acting as 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, transfers of personal data by a Tessi Group entity to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

IV. TESSI GROUP ENTITIES' LIABILITY REGIME

For the purposes of this Section:

- "Importing Tessi Entity" means the Tessi Group entity established outside the EEA that has received personal data on the basis of these BCR-C from a Tessi Group entity established in the EEA or outside of the EEA;
- "Exporting Tessi Entity" means the Tessi Group entity established within the EEA that has transferred personal data on the basis of these BCR-C to a Tessi Group entity established outside the EEA.

If these BCR-C are breached by an Importing Tessi Entity, the Exporting Tessi Entity (the "**Liable Tessi Group Entity**") agrees, at any given time, to accept liability for the breach and, in this respect, to take the necessary action to remedy the breach and pay compensation for any material or non-material damages resulting from the breach.

Furthermore, where the Importing Tessi Entity violates the BCR-C, the courts or other judicial authorities in the EEA will have jurisdiction and the data subjects will have the rights and remedies against the Liable Tessi Group Entity as if the violation had been caused by the latter in the Member State in which it is based, instead of the Importing Tessi Entity. In that respect, the contact details of the relevant Liable Tessi Group Entity are provided to the data subjects in accordance with Section V.1.

Where data subjects can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of the BCR-C, it will be for the Liable Tessi Group Entity to prove that the Importing Tessi Entity was not responsible for the breach of the BCR-C giving rise to those damages, or that no such breach took place.

However, in case of a breach of the BCR-C in the context of the processing carried out exclusively by a Tessi Group entity established within the EEA, the Tessi Group entity involved in the processing shall be individually liable for the alleged breach and it is responsible for demonstrating that it is not liable for the breach.

V. RIGHTS OF DATA SUBJECTS

1. Right to enforce the BCR-C as third-party beneficiaries

Where Tessi acts as controller or internal processor, the data subjects have the right to enforce the following Sections of the BCR-C as third-party beneficiaries:

- **Section II**: Definitions;
- **Section IV**: Third Countries' laws and practices;
- **Section V**: Tessi Group entities' liability regime;
- **Section VI**: Rights of data subjects;
- **Section VII**: Principles relating to the processing of personal data;
- **Section VIII**: Decision based solely on automated processing and profiling;
- **Section IX**: Storage period of personal data;
- **Section X.1**: Onward transfer;
- **Section XI**: Processing of sensitive data and criminal data;
- **Section XII**: Cooperation with the Competent Supervisory Authorities (relating to compliance obligations covered by this third-party beneficiary clause);
- **Section XIII**: Complaint handling process;
- **Section XIV**: BCR-C updating process (relating to information to be provided to data subjects).

For sake of clarity, these third-party beneficiaries' rights do not extend to those elements of the BCR-C pertaining to internal mechanisms implemented within Tessi Group, such as compliance network, audit programme and mechanism for updating the BCR-C.

2. Rights to request access, rectification and erasure of personal data and other rights of data subjects

Principles:

Each data subject has the following rights:

- Right of access: the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the

case, access to the personal data as well as the information provided for by Article 15 of the GDPR[6];

- Right to rectification: the right to obtain from the controller (i) the rectification of inaccurate personal data concerning him or her and (ii) incomplete personal data completed, as provided in Article 16 of the GDPR[7];
- Right to erasure: the right to obtain from the controller the erasure of personal data concerning him or her on the grounds referred to in Article 17 of the GDPR[8];
- Right to restriction of processing: the right to obtain from the controller restriction of processing where one of the scenarios referred to in Article 18 of the GDPR[9] applies;

---

[6] Article 15 of the GDPR states: *"1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: a) the purposes of the processing; b) the categories of personal data concerned; c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; f) the right to lodge a complaint with a supervisory authority; g) where the personal data are not collected from the data subject, any available information as to their source; h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer."

[7] Article 16 of the GDPR states: *"The data subject shall have the right to obtain from the controller 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."*

[8] Article 17 of the GDPR provides for the following grounds: *"a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); d) the personal data have been unlawfully processed; e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)."*

[9] Article 18 of the GDPR provides for the following scenarios: "*a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject*."

- Right to data portability: the right to receive the personal data concerning him or her, which he or she has provided to the controller, in a structured, commonly used and machine-readable format, if the processing is carried out by automated means and is based on the consent of the data subject or on an agreement to which the data subject is a party, as provided in Article 20 of the GDPR[10];
- Right to object: the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her based on the legitimate interests pursued by the controller or a third party or when the data are processed for prospecting purposes, as provided in Article 21 of the GDPR[11]; and
- Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, as detailed more fully in Section VIII.

---

[10] Article 20 of the GDPR states: "*1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means.*
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others."

[11] Article 21 of the GDPR states: *"1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller 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.*
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.
6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest."

In order to exercise his or her rights, the data subject may send his or her request by post or email, as the case may be, to the relevant Tessi Group entity whose contact details have been provided to him or her for this purpose in accordance with Section VII.1.

Upon receipt of a request from a data subject, the Tessi Group entities must implement the Tessi Group's internal procedure in order to respond rapidly to the requests of the data subjects, so that they can fully exercise their rights.

If the controller does not comply with the request made by the data subject, it must inform the data subject without delay, and within one month of receiving the request at the latest, of the reasons for its inaction and inform the data subject that he or she can lodge a complaint with a Supervisory Authority and seek a judicial remedy.

In addition, as provided in Article 19 of the GDPR[12], any rectification or erasure of personal data or restriction of processing carried out in accordance with the above-mentioned principles shall be communicated by the relevant Tessi Group entity to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The relevant Tessi Group entity shall also inform the data subject about those recipients if the data subject requests it.

Operational application of the BCR-C:

Whenever personal data is to be processed, data subjects must be clearly informed of their rights and of the procedure to follow in order to exercise those rights.

EX-DPC-1: If the Tessi Group entity that receives the request acts as controller, it must ensure that it provides the data subject with information on the measures taken following its request without undue delay and in any event within one month of receiving the request, in accordance with the complaint handling procedure of the Tessi Group. Taking into account the complexity and number of the requests, that one month period may be extended at maximum by two further months; the relevant entity must then inform the data subject within one month of receiving the request, specifying the reasons for the delay.

EX-DPC-2: The Tessi Group entity, through its DPO relay, must centralise all requests made by data subjects to exercise their rights in order to ensure that requests are managed in a consistent and optimal manner.

---

[12] Article 19 of the GDPR states: *"The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it."*

EX-DPC-3: The person making the request must provide proof of his or her identity, in certain cases, so that the controller is certain that it is sending the personal data to the right person and not to someone with the same name or an identity thief.

EX-DPC-4: Where the data subject submits his or her request in electronic form, the information must be provided via electronic means where possible, unless the data subject requests otherwise.

Reference document: *Request and complaint management procedure*

3. Right to judicial remedies, redress and compensation

If any of the obligations of the Sections of the BCR-C listed above in paragraph 1 of this Section VI is breached, data subjects have the right to lodge a complaint with a Supervisory Authority and/or to lodge a claim before the competent court in accordance with the principles described below against the relevant Tessi Group entity in accordance with Section V. In this context, the data subjects have the right to judicial remedies and to obtain redress and, where appropriate, compensation.

Data subjects may also decide, before lodging such complaint or bringing such action, to submit the matter, by post or by email, as the case may be, to the relevant Tessi Group entity whose contact details have been provided to him or her for this purpose in accordance with Section VII.1. The list and the contact details of Tessi Group entities bound by these BCR-C are also available in Appendix 1 of these BCR-C.

Where the breach of the BCR-C is the result of a breach by a Tessi Group entity established within the EEA, the data subject has the right to lodge a complaint or seek a judicial remedy against that entity:

- with the Supervisory Authority, in particular in the Member State of the data subject's habitual residence, place of work or place of the alleged infringement; and/or,
- before the competent court of the EEA Member State in which the data subject habitually resides or in which the relevant Tessi Group entity is established.

Where the breach of the BCR-C is the result of a breach by a Tessi Group entity established in a Third Country, the data subject has the right to lodge a complaint or seek a judicial remedy against the Liable Tessi Group Entity:

- with the Supervisory Authority, in particular in the Member State of the data subject's habitual residence, place of work or place of the alleged infringement; and/or,
- before the competent court of the EEA Member State in which the data subject habitually resides or in which the Liable Tessi Group Entity is established.

Data subjects may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) GDPR[13].

4. Right of information

All data subjects should be provided with information, including on their third-party beneficiary rights, with regard to the processing of their personal data, and on the means to exercise those rights.

Tessi Group will thus provide easy access to data subjects to the essential undertakings made under these BCR-C, as detailed below, by adopting a public version made available to data subjects via the website www.tessi.eu and, for employees, via the intranet (or any other internal communication channel).

The public facing document will at least reflect the following provisions of these BCR-C:

- **Section I**: Background;
- **Section II**: Definitions;
- **Section III**: Scope;
- **Section IV**: Third Countries' laws and practices;
- **Section V**: Tessi Group entities' liability regime;
- **Section VI**: Rights of data subjects;
- **Section VII**: Principles relating to the processing of personal data;
- **Section VIII**: Decision based solely on automated processing and profiling;
- **Section IX**: Storage period of personal data;
- **Section X.1**: Onward transfer;

[13] Article 80(1) of the GDPR states: "*The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.*"

- **Section XI**: Processing of sensitive data and criminal data;
- **Section XII**: Cooperation with the Competent Supervisory Authorities (relating to compliance obligations covered by the third-party beneficiary clause);
- **Section XIII**: Complaint handling process;
- **Section XIV**: BCR-C updating process (relating to information to be provided to data subjects);
- **Appendix 1**: List of Tessi Group entities bound by the BCR;
- **Appendix 2:** Description of the material scope of the Tessi Group BCR-C.

The information provided to data subjects should be up-to-date, and presented to data subjects in a clear, intelligible, and transparent way. Tessi Group entities will inform the data subjects about any update of the BCR-C, including of Appendix 1, by publishing the new version without undue delay.

VI. PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

The Tessi Group entities shall be responsible for and able to demonstrate compliance with the BCR-C.

1. Transparency

Principles:

When acting as controller, each Tessi Group entity undertakes to provide the data subjects with full information on the processing carried out as detailed below.

Operational application of the BCR-C:

EX-TRAN-1: Data subjects whose personal data are processed must receive the following information, as provided for by the GDPR, from the relevant Tessi Group entity, through their employment agreement, personal data collection forms, the entity's website, the internal regulations, the IT charter, an individual letter addressed to the data subject, a specific notice and/or by any other suitable means:

- The identity and contact details of the controller (and, if applicable, the relevant Liable Tessi Group Entity);
- The contact details of the Group DPO (who can be directly contacted in any event at dpo.tessi@tessi.fr) and, where applicable, of the DPO relay;

- The purposes of the processing for which the personal data are intended, as well as the legal basis for the processing;
- The recipients or categories of recipients of the personal data, if any;
- If the processing is based on legitimate interests, the description of the legitimate interests pursued by the controller or the third party;
- The existence of transfers of personal data in a Third Country, and the existence or absence of an adequacy decision by the European Commission or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- 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;
- Where the processing is based on the consent of the data subject, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- The right to lodge a complaint with a Supervisory Authority;
- The existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- Where the data has been collected from the data subject, whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into an agreement, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and
- Where the data has not been collected from the data subject, (i) the relevant categories of personal data; and (ii) the source of the personal data and, where applicable, a statement on whether or not it came from publicly available sources.

EX-TRAN-2: Where the personal data has been collected directly from the data subject, the relevant Tessi Group entity must provide him or her with the information referred to above at the time the relevant data is obtained, unless the data subject already has this information. Where the personal data has not been collected directly from the data subject, the relevant Tessi Group entity must provide him or her with the information referred to above, unless the data subject already has this information, within the following deadlines:

- Within a reasonable period (maximum 1 month) after obtaining the personal data, having regard to the specific circumstances in which the personal data are processed; or
- If the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to the data subject; or
- If a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

EX-TRAN-3: The relevant Tessi Group entity must ensure that the information is provided to the data subjects in an easily understandable and easily accessible manner.

2. Fairness, lawfulness and purposes limitation

Personal data must be processed fairly and lawfully with regard to the data subject. Personal data must only be collected for specified, explicit and legitimate purposes. They must not be further processed in any way incompatible with the purposes for which the personal data were collected. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with the GDPR, not be considered to be incompatible with the initial purposes.

Where the controller intends to further process the personal data for a purpose other than that for which the personal data was collected, the controller must provide the data subject prior to that further processing with information on that other purpose, in particular the legal basis for that further processing, as well as any other relevant information including the following:

- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- 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 and to object to processing as well as the right to data portability;
- Where the processing is based on the consent of the data subject, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- The right to lodge a complaint with a Supervisory Authority;
- The existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of this processing for the data subject;

- Where the data has been collected from the data subject, whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into an agreement, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and
- Where the data has not been collected from the data subject, (i) if the processing is based on legitimate interests, the description of the legitimate interests pursued by the controller or the third party, and (ii) from which source the personal data originate, and if applicable, whether it came from publicly accessible source.

In addition, where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) of the GDPR[14], the controller shall ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, taking into account the criteria set out by the GDPR.[15]

3. Legal basis

Principles:

Processing shall be lawful only if and to the extent that at least one of the following applies:

---

[14] Article 23(1) of the GDPR provides: *"1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); (i) the protection of the data subject or the rights and freedoms of others; (j) the enforcement of civil law claims*."

[15] Article 6(4) of the GDPR provides the following criteria: *"inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation."*

(i) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(ii) Processing is necessary for the performance of an agreement to which the Tessi group entity and the data subject are parties or in order to take steps at the request of the relevant party prior to entering into an agreement;
(iii) Processing is necessary for compliance with a legal obligation to which the controller is subject;
(iv) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(v) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(vi) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental data subject's rights and freedoms which require protection of personal data.

Operational application of the BCR-C:

All Tessi Group entities bound by the BCR-C must process personal data in accordance with the following principles, on the understanding that the legal bases defined in (iv) and (v) above will not apply to the processing carried out by Tessi Group entities or only exceptionally.

EX-BASELEG-1: The relevant Tessi Group entity must first determine whether the processing is necessary for compliance with a legal obligation to which the entity is subject. This will be the case, for example, for processing needed to comply with the legal anti-fraud and anti-corruption obligations provided for by Union and Member State laws.

EX-BASELEG-2: If this is not the case, the Tessi Group entity must determine whether the processing is necessary for the performance of an agreement between it and the data subject. This will be the case, for example, for processing associated with employee payroll management needed in order to execute the employment agreement between the relevant Tessi Group entity and its employees.

EX-BASELEG-3: If the first two legal bases mentioned above do not apply, the Tessi Group entity must determine whether the processing is necessary for the purposes of the legitimate interests pursued by the entity or by a third party. The Tessi Group entity concerned must demonstrate that these interests are not overridden by the interests or fundamental data subject's rights and freedoms which require protection of personal data. Evidence-based analysis must always be carried out for this purpose. This will be the case, for example, for

the processing needed to comply with the anti-fraud and anti-corruption legal obligations provided for by the law of a Third Country, in a Third Country.

EX-BASELEG-4: If none of the aforementioned legal bases applies to the case at hand (nor those defined in (iv) and (v) above), the Tessi Group entity must then obtain the express consent of the data subject(s) whose data is processed. In order for the consent to be validly obtained, the Tessi Group entity must ensure that it is obtained in accordance with the principles of the GDPR, notably before any personal data is collected.

4. Accuracy and data minimisation

Principles:

The personal data collected must be accurate and, where necessary, kept up to date. In this regard, 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.

The personal data must also be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Operational application of the BCR-C:

The Tessi Group entities must respect the principle of data minimisation and ensure that only the data needed for the purposes for which it is processed is collected and processed. In addition, the Tessi Group has put measures in place to ensure that any data that is inaccurate with regard to the purposes for which it is processed, is rectified or erased through the following mechanisms:

EX-EXA-1: If the data subject has access to a user space, he or she can rectify, complete and, depending on the case, erase his or her personal data when using the services offered by the Tessi Group: HR tools, activity monitoring tools, intranet, IT support tools, etc.

EX-EXA-2: If the data subject is unable to rectify, complete or erase his or her personal data, he or she may send a request to the relevant Tessi Group entity identified in accordance with the principles defined in Article 1 (Transparency) above. It must answer any request from a data subject in accordance with the principles defined in Section VI.2.

EX-EXA-3: The Tessi Group entity acting as controller must inform all recipients of the personal data about any rectification or erasure of personal data or any restriction of processing carried out, unless it proves impossible or disproportionate efforts are required

to inform them. If data subjects so request, the relevant Tessi Group entity must provide them with information on these recipients.

EX-EXA-4: Personal data that is no longer necessary in relation to the purposes for which it is processed must not be stored in a form that enables the data subjects to be identified.

EX-EXA-5: Technical and organisational measures must be implemented by Tessi Group entities to ensure that the personal data storage periods are limited in accordance with Section IX.

5. Security of personal data

Principles:

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for data subject's rights and freedoms posed by the processing, appropriate technical and organisational measures must be implemented to ensure a level of personal data security appropriate to the risks based on the stages of the data life cycle and the personal data concerned.

Personal data must be protected against accidental loss, destruction or damage, as well as against unauthorised or unlawful processing, including unauthorised or unlawful alteration, disclosure, access or dissemination, including when the processing involves the transmission of personal data over a network.

Operational application of the BCR-C:

EX-SEC-1: Tessi Group entities must put in place appropriate protection measures at all stages of the personal data life cycle (collection, operation, use, storage, hosting, transmission, destruction, etc.). These measures must comply with the requirements set out in the Tessi Group's General Information System Security Policy (GISSP). This policy uses a risk-based approach, in accordance with the ISO 27001 standard on information security management systems (ISMS).

EX-SEC-2: The personal data security measures described below, which apply to the Tessi Group enti ties that act as controller or internal processor, are described in Tessi Group Policy on Information Systems Security.

5.1 Security governance

The Tessi Group entities undertake to establish and apply an information security governance system to ensure and verify the implementation and operational functioning of the security measures relating to the protection of personal data.

Reference document: *Tessi Group Policy on Information Systems Security*

5.2 Human Resources

All Tessi Group employees and third parties that process personal data must undertake to respect data confidentiality. Tessi Group employees must be trained on and/or made aware of personal data protection issues.

Reference documents: *Tessi Group staff recruitment procedure, Personal data protection awareness-raising and training procedure and Tessi Group IT charter*

5.3 Physical security

Each Tessi Group entity must implement physical security measures and maintain an appropriate level of protection for its premises, in accordance with the physical security procedure.

Reference documents: *Tessi Group procedures on physical security*

5.4 Incident management

Each Tessi Group entity must implement a consistent and effective method for managing incidents relating to the security of personal data, including the disclosure of events, breaches and incidents affecting personal data.

Reference documents: *Tessi Group procedure on managing security incidents and Security incident sheet*

5.5 Identity management

5.5.1 Access controls

Each Tessi Group entity must put in place a process for managing access to the Tessi Group's information system, including an authorisation mechanism and security measures aimed at preventing unauthorised access to personal data.

5.5.2 Management of remote access and mobile devices

Each Tessi Group entity must apply appropriate security measures to all methods of remote access and mobile devices to ensure the confidentiality and integrity of the personal data processed.

Reference documents: *Tessi Group procedure on logical access security and Tessi Group procedure on managing remote access to the IS*

5.6 Operational security

Each Tessi Group entity must ensure that the means of processing personal data operate properly and securely.

Reference documents: *Tessi Group server security procedure and Tessi Group workstation security procedure*

5.7 Protection against malicious code

Each Tessi Group entity must ensure that personal data and the means of processing such data are protected against viruses and malicious code.

Reference documents: *Tessi Group server security procedure and Tessi Group workstation security procedure*

5.8 Vulnerability management

Each Tessi Group entity must deploy appropriate measures to reduce the risks associated with the exploitation of published technical vulnerabilities. Exposure to vulnerabilities must be assessed and appropriate action must be taken to address the associated risk.

Reference document: *Tessi Group patch management policy*

5.9 Development security

Each Tessi Group entity must ensure the confidentiality and integrity of the personal data processed as part of its IT development activities. It must also ensure that the principles set out in Article 6 (Data protection by design and data protection by default) below are complied with as part of the application development cycle.

Reference documents: *Tessi Group procedure on development security and Tessi Group procedure on "Privacy by Design and Privacy by Default"*

5.10 Security of communications

Each Tessi Group entity must safeguard the protection of personal data as this data passes through the networks, whether it is transferred within the Tessi Group or to an external entity.

Reference documents: *Tessi Group procedure on network control and management and Tessi Group procedure on the security of network flows*

5.11 Backing-up of personal data

Each Tessi Group entity must put in place a backup policy on backing up personal data with the appropriate level of security.

Reference documents: *Tessi Group backup policy and Tessi Group personal data storage period procedure*

5.12 Encryption

5.12.1 Database encryption

Each Tessi Group entity must ensure a level of protection appropriate to the classification of the relevant data by using encryption on the personal data.

5.12.2 Transfer encryption

All personal data or personal data flows passing between a Tessi Group entity and an external third party must be exchanged via protocols that comply with the Tessi Group guidelines and that are encrypted during transit.

Reference document: *Tessi Group encryption policy*

5.13 Maintenance and destruction of personal data

Each Tessi Group entity must supervise all maintenance operations in order to control access to personal data by third parties. For example, personal data must first be erased from equipment destined for scrapping.

Reference documents: *Tessi Group procedure on the end of life of IT equipment, and Standard report on the destruction and erasure of data*

5.14 Traceability management

Each Tessi Group entity must record all operations carried out on personal data and be able to produce proof of the actions carried out on that data (access, modification, deletion, transfer, etc.).

Reference document: *Tessi Group IT trace security procedure*

5.15 Auditing of security measures

Each Tessi Group entity must undergo security audits based on the Tessi Group's security audit framework.

Reference document: *Tessi Group IT trace security procedure*

6. Data protection by design and data protection by default

Principles:

The Tessi Group entities that act as controllers undertake to comply with the principles of personal data protection by design and data protection by default by putting in place appropriate technical and organisational measures to implement the principles relating to the protection of personal data and to facilitate compliance with the requirements provided for in the BCR-C in practice.

More specifically, each relevant Tessi Group entity must implement appropriate technical and organisational measures in order to:

- Apply the data protection principles (e.g., data minimisation) in an effective manner and integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of the data subjects. These measures must be implemented both at the time of determining the means for processing and at the time of the processing itself, and must be determined taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for data subject's rights and freedoms posed by the processing.
    - For example, the design of the products, applications or processes must effectively incorporate the principles of personal data protection.
- Ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures must ensure that by default personal data

are not made accessible without the data subject's intervention to an indefinite number of natural persons.

- For example, the products, applications or processes must ensure that, by default, only the personal data which are necessary for the purpose of processing are processed with regard to the amount of data collected, the extent of their processing, the period of their storage and the number of persons who have access to it and ensure that the personal data processed are limited to the minimum necessary for the processing (i.e., proportionality of the processing relative to the purposes).

Operational application of the BCR-C:

EX-PBDD-1: The approach described in the Tessi Group's internal "Privacy By Design & Privacy By Default" procedure applies to the internal projects of the relevant Tessi Group entity, notably regarding the compliance of websites, business applications and mobile applications. The proposed approach aims to:

- Identify the technical, organisational and legal measures whose implementation appears essential as soon as the project begins, in order to protect personal data against accidental or voluntary loss, theft or misuse;
- Meet the data availability, integrity, confidentiality and traceability requirements;
- Identify the sensitivity and criticality of the personal data processing;
- Identify any processing that may result in a high risk for the data subject's rights and freedoms, requiring the implementation of a data protection impact assessment, and follow the Tessi Group Data Protection Impact Assessment Procedure;
- Ensure that the requirements of the Union and Member State laws applicable to the protection of personal data, notably concerning consent, profiling, the processing of sensitive and criminal data and the transfer of personal data in a Third Country are taken into account in the project's design.

EX-PBDD-2: The DPO relay of the relevant Tessi Group entity must validate the content of the "Privacy by Design/Default" file produced by the project manager or the person responsible for carrying out the processing. If necessary, the DPO relay consults the Group DPO, who will provide appropriate support.

Reference document: *Tessi Group "Privacy by Design & Privacy by Default" procedure*

7. Notification of personal data breaches

Principles:

A “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of personal data transmitted, stored or otherwise processed, or to unauthorised access to such data.

In the event of a personal data breach, the relevant Tessi Group entity shall, without undue delay, notify the personal data breach to the Liable Tessi Group Entity and to the Group DPO.

In the event the Tessi Group Entity is acting as a processor and becomes aware of a personal data breach, it shall, without undue delay, notify the Tessi Group entity acting as a controller.

The relevant Tessi Group entity, acting in its capacity as controller, shall also notify the personal data breach to the Competent Supervisory Authority without undue delay and, where feasible, no later than 72 hours after having become aware of the breach, unless the personal data breach is unlikely to result in a risk to the data subject’s rights and freedoms.

In addition, where the personal data breach is likely to result in a high risk to the data subject’s rights and freedoms, the relevant Tessi Group entity, acting as controller, shall notify the personal data breach to the data subjects without undue delay (except in the exceptional cases set out in Procedure for notifying personal data breaches).

Any personal data breach must be documented (comprising the facts relating to the personal data breach, its effects and the remedial action taken), and this documentation must be made available to the Competent Supervisory Authority on request, in accordance with the GDPR.

Operational application of the BCR-C:

Depending on the circumstances, a personal data breach may concern the confidentiality, availability and/or integrity of the personal data.

Personal data breaches may be associated with the following types of IT security incidents:

(i) Destruction of personal data;
(ii) Loss of personal data;
(iii) Unwanted alteration/modification of personal data;

(iv) Unauthorised disclosure of personal data;
(v) Unauthorised access to personal data.

EX-NVIO-1: The relevant Tessi Group entity must without undue delay report any personal data breach to the Liable Tessi Group Entity.

EX-NVIO-2: The Tessi Group entity, in its capacity as controller, must notify any personal data breach likely to result in a risk to the data subject's rights and freedoms to the Competent Supervisory Authority without undue delay, and if possible, no later than 72 hours after it becomes aware of the breach, while complying with the Tessi Group's procedure for notifying personal data breaches. Where the breach is not notified to the Competent Supervisory Authority by this deadline, the Competent Supervisory Authority must be informed of the reasons for the delay.

EX-NVIO-3: The Tessi Group entity, in its capacity as controller, must inform the data subjects without undue delay of any personal data breach that is likely to result in a high risk to their rights and freedoms (except in the exceptional cases set out in Tessi Group's procedure for notifying personal data breaches).

EX-NVIO-4: The information contained in the notification of the personal data breach to the Competent Supervisory Authority and to the data subjects must comply with the Tessi Group's procedure for notifying personal data breaches, and state the following:

- The nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned by the breach and the categories and approximate number of personal data records concerned;
- The name and contact details of the Group DPO or other contact point where more information can be obtained;
- The likely consequences of the personal data breach;
- The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse consequences.

EX-NVIO-5: Any detected personal data breach must be reported to the Group DPO either via the Tessi Group "ORQC" tool or via the report form contained in Tessi Group procedure for notifying personal data breaches.

EX-NVIO-6: Based on the information provided in the breach report form, the Group DPO must analyse the facts of the breach, its characteristics and, above all, its possible impacts for the data subjects.

EX-NVIO-7: Based on this analysis, the Group DPO must formalise an action plan to remedy the breach.

EX-NVIO-8: The Tessi Group entity must document any personal data breaches (record of personal data breaches), so that the Competent Supervisory Authority can check compliance with the GDPR.

Reference document: *Procedure for notifying personal data breaches*

VII. DECISION BASED SOLELY ON AUTOMATED PROCESSING AND PROFILING

Principles:

Data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling (as defined below), which produces legal effects concerning them or similarly significantly affects them, unless that decision (i) is necessary for entering into, or performance of, an agreement between the data subject and the controller, (ii) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or (iii) is based on the data subject's explicit consent[16].

In the cases referred to in (i) and (iii) above, the Tessi Group entity 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.

"Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person (e.g., an employee or a customer), in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Operational application of the BCR-C:

EX-PRO-1: The Tessi Group entity, acting as controller, must ensure that the decision based solely on automated processing, including profiling, that produces legal effects concerning the data subject or which similarly significantly affects him or her, (i) is necessary for entering

---

[16] Article 22 of the GDPR states:
"1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller 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.
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

into, or performance of, an agreement between the data subject and a controller, (ii) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or (iii) is based on the data subject's explicit consent.

EX-PRO-2: Where the applicable legal basis is that referred to in points (i) or (iii) of the "EX-PRO-1" application of the BCR-C, the Tessi Group entity acting as controller must allow the data subject to obtain human intervention from the relevant Tessi Group entity, to express his or her point of view and to contest the decision.

EX-PRO-3: The Tessi Group entity concerned must ensure that the decision based solely on automated processing, including profiling, that produces legal effects concerning the data subject or which similarly significantly affects him or her is not based on sensitive data, unless (i) the data subject has given explicit consent, or the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject, and (ii) suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

EX-PRO-4: Before carrying out the processing, the relevant Tessi Group entity must apply the Tessi Group's data protection impact assessment procedure to determine whether an impact assessment is required and consult the DPO relay or Group DPO, in particular to determine whether the Competent Supervisory Authority should be consulted, where applicable.

EX-PRO-5: The Tessi Group entity, acting as controller, must inform the data subject of the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such profiling for the data subject.

EX-PRO-6: Decision-making based solely on automated processing, including profiling, that produces legal effects concerning the data subject or which similarly significantly affect him or her, must be noted in the record of processing activities of the relevant Tessi Group entity, specifying the legal basis and appropriate measures implemented.

VIII. STORAGE PERIOD OF PERSONAL DATA

Principle:

Personal data must not be stored for longer than is necessary for the purposes for which it is processed.

Personal data may be stored for longer periods insofar as it will be processed solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with the GDPR, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the data subject's rights and freedoms.

Operational application of the BCR-C:

EX-DCO-1: The relevant Tessi Group entity must comply with the Tessi Group personal data storage period procedure.

EX-DCO-2: The storage period for personal data must be defined in advance, before the processing is carried out, and be noted in the record of processing activities of the relevant Tessi Group entity.

EX-DCO-3: Other than in cases in which there is an archiving constraint (e.g., a legal obligation or obligation under a customer agreement), the personal data must be deleted within the defined deadlines with regard to the purposes pursued.

EX-DCO-4: The relevant Tessi Group entity must ensure that the data is effectively deleted.

EX-DCO-5: The DPO relay or Group DPO must regularly check compliance with the storage periods defined by the relevant Tessi Group entity.

Reference document: *Tessi Group personal data* storage *period procedure*

tessi®

IX. ONWARD TRANSFER OF PERSONAL DATA

1. Onward transfer

Principles:

Personal data that have been transferred under the BCR-C may only be onward transferred in a Third Country to processors and controllers which are not bound by the BCR-C if the conditions for transfers laid down in Articles 44 to 46 GDPR[17] 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[18].

---

[17] Article 44 of the GDPR states: "*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*"
Article 45 of the GDPR relates to transfers on the basis of an adequacy decision and Article 46 of the GDPR relates to transfers subject to appropriate safeguards such as binding corporate rules and standard data protection clauses.

[18] Article 49 of the GDPR states:
"*1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; (d) the transfer is necessary for important reasons of public interest; (e) the transfer is necessary for the establishment, exercise or defence of legal claims; (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in*

Operational application of the BCR-C:

EX-OT-1: Where personal data are transferred between Tessi Group entities bound by the BCR-C, the transfers are governed by these BCR-C.

EX-OT-2: Where personal data are transferred by Tessi Group entities to third parties in a Third Country, the relevant Tessi Group entity within the EEA must ensure that an appropriate safeguard is in place. In practice, Tessi Group entities generally rely on standard contractual clauses with that third parties, subject that the conditions for use of these standard contractual clauses are met[19].

X. PROCESSING OF SENSITIVE DATA AND CRIMINAL DATA

1. Processing of sensitive data

Principles:

In principle, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

As an exception, the relevant Tessi Group entity may process sensitive data under certain conditions.

---

addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.
2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.
3. [.]
4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.
5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.
6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30."

[19] The latest version of the standard contractual clauses dated 4 June 2021 is available at: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEXf:32021D0914&from=EN

Operational application of the BCR-C:

EX-SEN-1: Ensure that the processing of sensitive data is based only on one of the permitted cases listed below:

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provides that the prohibition on processing sensitive data may not be lifted by the data subject; or
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; or
- Processing is necessary to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent; or
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to certain conditions and safeguards.

EX-SEN-2: Where the relevant Tessi Group entity acts as controller, prior to processing any sensitive data, it must apply the Tessi Group's data protection impact assessment procedure to determine whether an impact assessment is required and consult the DPO relay or Group DPO, in particular to determine whether the Competent Supervisory Authority must be consulted, where applicable.

Reference document: *Tessi Group sensitive data procedure*

2. Processing of criminal data

Principles:

In principle, the processing of personal data relating to criminal convictions and offences shall be prohibited, in accordance with the conditions provided for in Article 10 of the GDPR[20].

As an exception, the relevant Tessi Group entity may process criminal data (in this case: criminal record) under specific conditions.

Operational application of the BCR-C:

EX-CRM-1: Ensure that the processing of criminal data (in this case: criminal record) is based only on one of the permitted cases listed below:

- The data subject has given consent to the processing of his or her personal data 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 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 purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

EX-CRM-2: In addition to the requirement mentioned above in EX-CRM-1, ensure that the processing of criminal data (in this case: criminal record) is authorised by Union or Member State law.

[20] Article 10 of the GDPR states: "*Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority*."

EX-CRM-3: Where the relevant Tessi Group entity acts as controller, prior to processing any criminal data (in this case: criminal record), it must apply the Tessi Group's data protection impact assessment procedure to determine whether an impact assessment is required and consult the DPO relay or Group DPO, in particular to determine whether the Competent Supervisory Authority must be consulted, where applicable.

XI. COOPERATION WITH THE COMPETENT SUPERVISORY AUTHORITIES

The Tessi Group entities undertake to cooperate with Competent Supervisory Authorities, to take into account their advice and to abide by their decisions.

The Tessi Group entities accept to be audited and to be inspected, including where necessary, on-site, by the Competent Supervisory Authorities.

Each Tessi Group entity shall provide the Competent Supervisory Authorities, upon request, with any information about the processing operations covered by these BCR-C.

Any dispute related to the Competent Supervisory Authorities' exercise of supervision of compliance with these BCR-C will be resolved by the courts of the Member State of that Competent Supervisory Authority, in accordance with that Member State's procedural law. In that respect, Tessi Group entities agree to submit themselves to the jurisdiction of these courts.

XII. COMPLAINT HANDLING PROCESS

Data subjects should be able to exercise their rights and complain about any Tessi Group entity as set out in Section VI. In that respect, data subjects can contact the relevant Tessi Group entity, by email (dpo.tessi@tessi.fr), by post or by other means, as the case may be, which have been provided to him or her for this purpose in accordance with Section VII.1.

The relevant Tessi Group entity, through the Group DPO or the DPO relay, must provide information on actions taken to the complainant without undue delay and in any event within one month of receiving the complaint. Taking into account the complexity and number of the requests, that one month period may be extended at maximum by two further months, in which case the data subject should be informed accordingly within one month of receipt of the request. The complaint must be handled by a department or person that/who has an appropriate level of independence in the exercise of his/her functions as identified in accordance with Tessi Group Request and complaint handling procedure.

If the relevant Tessi Group entity considers that the complaint is justified, the entity must process the complaint of the data subject without any delay and within the aforementioned deadlines at the latest.

If the relevant Tessi Group entity does not reply to the data subject in that period or rejects the complaint, it must inform the data subject without delay, and within the aforementioned deadlines at the latest, of the reasons for its inaction and inform the data subject that he or she can lodge a complaint with a Supervisory Authority and seek a judicial remedy.

If the data subject is not satisfied with the responses provided by the Tessi Group entity, the data subject has the right to lodge a claim before the competent court and a complaint before a Supervisory Authority. Such right is not dependent on the data subject having used the Tessi Group's complaint handling procedure beforehand.

Reference document: *Request and complaint handling procedure*

XIII. BCR-C UPDATING PROCESS

Principles:

The BCR-C have to be kept up-to-date in order to reflect the current situation (for instance to take into account modifications of the regulatory environment, the EDPB recommendations, or changes to the scope of the BCR-C).

Changes to the BCR-C, including to the list of the Tessi Group entities, shall be reported, without undue delay, to all Tessi Group entities.

Where a modification to the BCR-C would possibly be detrimental to the level of the protection offered by the BCR-C or significantly affect them (e.g., changes to the binding character, change of the Liable Tessi Group Entity), it must be communicated in advance to the Supervisory Authorities, via the Lead Supervisory Authority, with a brief explanation of the reasons for the update. In this case, the Supervisory Authorities will also assess whether the changes made require a new approval.

Any changes to the BCR-C or to the list of the Tessi Group entities should be notified once a year to the Supervisory Authorities, via the Lead Supervisory Authority, with a brief explanation of the reasons for the changes. This includes any changes made in order to align the BCR-C with any updated version of the EDPB recommendations. The Supervisory Authorities should also be notified once a year in instances where no changes have been made. The annual update or notification will also include the renewal of the confirmation regarding the assets of the Liable Tessi Group Entity.

Operational application of the BCR-C:

EX-MAJ-1: The Group DPO keeps a fully updated list of Tessi Group entities, keeps record of any updates to the BCR-C and provides the necessary information to the data subjects and Competent Supervisory Authorities upon request. It remains the responsibility of the Group DPO to keep the BCR-C up-to-date and in compliance with the GDPR and the EDPB recommendations.

EX-MAJ-2: No personal data transfer is made to a Tessi Group entity that is not listed in Appendix 1 until the new Tessi Group entity is effectively bound by the BCR-C and can deliver compliance.

APPENDIX 1:
LIST OF TESSI GROUP ENTITIES BOUND BY THE BCR

I. Entities established in the European Economic Area

France, Spain and Bulgaria

FRANCE

ADM COLLECTING, Simplified Joint-stock Company with sole shareholder, with a capital of €10,000, whose registered office is in ISSY-LES-MOULINEAUX (92130), 32 rue Henri Tariel, registered in the Trade and Companies Register of NANTERRE under number 789 618 584 00013, mail: dpo.tessi@tessi.fr

ADM PROCESSING, Simplified Joint-stock Company, with a capital of €100,000, whose registered office is in ISSY-LES-MOULINEAUX (92130), 32 rue Henri Tariel, registered in the Trade and Companies Register of NANTERRE under number 532 328 986 00023 mail: dpo.tessi@tessi.fr

ADM VALUE, Simplified Joint-stock Company, with a capital of €500,200, whose registered office is in ISSY-LES-MOULINEAUX (92130), 32 rue Henri Tariel, registered in the Trade and Companies Register of NANTERRE under number 418 657 763 00078, phone number: + 33 (0) 1 76 61 37 00 mail: dpo.tessi@tessi.fr

ADM VALUE ASSURANCES, Limited Liability Company (SARL), with a capital of €10,000, whose registered office is in ISSY-LES-MOULINEAUX (92130), 32 rue Henri Tariel, registered in the Trade and Companies Register of NANTERRE under number 521 671 149 00032, mail: dpo.tessi@tessi.fr

BIP-TESSI (SOCIETE BORDELAISE D'INFORMATIQUE PERIPHERIQUE), Simplified Joint-stock Company, with a capital of €7,622.45, whose registered office is in LE HAILLAN (33185), Immeuble Cassiopée, 1-3 avenue des Satellites, registered in the Trade and Companies Register of BORDEAUX under number 342 913 522 00054, phone number: +33 (0)5 57 57 25 33, mail: dpo.tessi@tessi.fr

C2I PRODUCTION, Simplified Joint-stock Company with sole shareholder, with a capital of €289,317.17, whose registered office is in RAMONVILLE SAINT AGNE (31520), 2 avenue de l'Europe, registered in the Trade and Companies Register of TOULOUSE under number 383 984 028 00118, phone number: +33 (0)5 62 57 19 80, mail: dpo.tessi@tessi.fr

CALLWEB, Simplified Joint-stock Company, with a capital of €128,600, whose registered office is in AMIENS (80000), 22D rue du Général Leclerc, registered in the Trade and Companies Register of AMIENS under number 517 813 960 00062, phone number +33 (0) 6 20 74 63 04, mail: dpo.tessi@tessi.fr

CERTIGNA, Simplified Joint-stock Company with sole shareholder, with a capital of €276,485, whose registered office is in VILLENEUVE D'ASCQ (59650), 20 allée de la Râperie, registered in the Trade and Companies Register of LILLE METROPOLE under number 481 463 081 00036, phone number +33 (0)3 20 79 24 09, mail: dpo.tessi@tessi.fr

GDOC LASERCOM FRANCE, Simplified Joint-stock Company with sole shareholder, with a capital of €15,000, whose registered office is in BOULOGNE-BILLANCOURT (92100), 27-33 quai Alphonse Le Gallo - Bâtiment ILEO, registered in the Trade and Companies Register of NANTERRE under number 512 067 877 00047, phone number: +33 (0)1 55 18 00 81, mail: dpo.tessi@tessi.fr

INNOVATION&TRUST FRANCE, Simplified Joint-stock Company with sole shareholder, with a capital of €435,800, whose registered office is in BOULOGNE-BILLANCOURT (92100), 27-33 quai Alphonse Le Gallo, registered in the Trade and Companies Register of NANTERRE under number 352 164 537 00099, phone number: +33 (0)1 55 18 00 18, mail: dpo.tessi@tessi.fr

LOGIDOC SOLUTIONS, Simplified Joint-stock Company with sole shareholder, with a capital of €142,100, whose registered office is in LIMOGES (87000), 4 rue Atlantis, Parc d'Ester Technopole, Bâtiment OXO, registered in the trade and companies register of LIMOGES under number 482 420 247 00033, phone number: +33 (0)5 55 77 11 79, mail: dpo.tessi@tessi.fr

MUTUA GESTION, Simplified Joint-stock Company with sole shareholder, with a capital of €4 300 000 whose registered office is in MURET (31600), 187 avenue Jacques Douzans, Trade and Companies Register of TOULOUSE under number 788 998 078 00026, phone number: +33 (0)5 61 43 83 83, mail: dpo.tessi@tessi.fr

ORONE FRANCE, Simplified Joint-stock Company with sole shareholder, with a capital of €1 250 000, whose registered office is in LE PETIT–QUEVILLY (76140), 72 avenue de la République, registered in the Trade and Companies Register of ROUEN, under number 521 071 324 00045, phone number: + 33 (0) 2 32 94 94 74, mail: dpo.tessi@tessi.fr

OWLIANCE, Simplified Joint-stock Company with sole shareholder, with a capital of €846 976 whose registered office is in BOULOGNE-BILLANCOURT (92100), 27-33 quai Alphonse Le Gallo, registered in the Trade and Companies Register of NANTERRE under number, 341 592 582 00124, phone number: + 33 (0) 1 82 70 16 00, mail: dpo.tessi@tessi.fr

OWLIANCE SERVICES INFORMATIQUES, Simplified Joint-stock Company with sole shareholder, with a capital of €1 500 000 whose registered office is in TOULOUSE (31100), 12 rue Louis Courtois de Viçose, Trade and Companies Register of TOULOUSE under number 510 435 696 00040, phone number: +33 (0)5 61 43 83 83, mail: dpo.tessi@tessi.fr

PERFO SERVICE, Simplified Joint-stock Company with sole shareholder, with a capital of €15,244.90, whose registered office is in SAINT JEAN BONNEFONDS (42650) - Bâtiment 7 du Parc Métrotech, registered in the Trade and Companies Register of SAINT ETIENNE under number 704 501 360 00074, phone number: +33 (0)4 77 43 97 30, mail: dpo.tessi@tessi.fr

PROCHEQUE NORD, simplified Joint stock Company, with a capital of 36,924, whose registered office is in VILLENEUVE D'ASCQ (59650), 24-26 rue du Carrousel Parc de la Cimaise, registered in the Trade and Companies Register of LILLE METROPOLE, under number 434 040 119 00043, phone number: +33 (0)3 20 94 50 35, mail: dpo.tessi@tessi.fr

RIB INFORMATIQUE DROME, Simplified Joint-stock Company with sole shareholder, with a capital of €7,622.45, whose registered office is in LYON (69007), 45 rue Saint Jean de Dieu, registered in the Trade and Companies Register of LYON under number 405 000 951 00039, phone number: +33 (0)4 26 68 86 00, mail: dpo.tessi@tessi.fr

RIP-TESSI (SOCIETE RHODANIENNE D'INFORMATIQUE PERIPHERIQUE), Simplified Joint-stock Company, with a capital of €7,622.45, whose registered office is in LYON (69007), 45 rue Saint Jean de Dieu, registered in the Trade and Companies Register of LYON under number 342 851 235 00032, phone number: +33 (04) 26 68 86 00, mail: dpo.tessi@tessi.fr

SATC (SOCIETE ALSACIENNE DE TRAITEMENTS DE CHEQUES), Simplified Joint-stock Company, with a capital of €7,622.45, whose registered office is in SHILTIGHEIM (67300), 1 allée d'Helsinki, registered in the Trade and Companies Register of STRASBOURG under number 394 003 081 00079, phone number: +33 (0)4 26 68 86 00, mail: dpo.tessi@tessi.fr

SEDI (SOCIÉTÉ D'ENRICHISSEMENT DE DONNÉES INFORMATIQUES), Simplified Joint-stock Company with sole shareholder, with a capital of €7,622.45, whose registered office is in BOULOGNE-BILLANCOURT (92100), 27-33 quai Alphonse Le Gallo, registered in the Trade and Companies Register of NANTERRE under number 342 568 565 00036, phone number: +33 (0)1 41 31 53 83, mail: dpo.tessi@tessi.fr

SIP-TESSI (SOCIETE D'INFORMATIQUE PERIPHERIQUE), Simplified Joint-stock Company, with a capital of €7,622.45, whose registered office is in COULOMMIERS (77120), 37 avenue du Général Leclerc, registered in the Trade and Companies Register of MEAUX under number 342 568 565 00036, phone number: +33 (0)1 64 20 73 60, mail: dpo.tessi@tessi.fr

SYNERCAM, Simplified Joint-stock Company with sole shareholder, with a capital of €457,347.05, whose registered office is in LESCAR (64230), rue Saint Exupéry ZAC Monhauba III, registered in the Trade and Companies Register of PAU under number 419 833 470 00026, phone number: +33 (0)5 59 40 13 90, mail: dpo.tessi@tessi.fr

T.D.C. TESSI, Simplified Joint-stock Company, with a capital of €7,622.45, whose registered office is in LYON (69007), 45 rue Saint Jean de Dieu, registered in the Trade and Companies Register of LYON under number 407 687 565 00033, phone number: +33 (0)4 26 68 86 00, mail: dpo.tessi@tessi.fr

TRAITEMENT DE DONNEES INFORMATIQUES (T.D.I), Simplified Joint-stock Company with sole shareholder, with a capital de €8,000, whose registered office is in MAMOUDZOU, Place du Marché – Immeuble Mahaba Club MAYOTTE, registered in the Trade and Companies Register of MAMOUDZOU under number 024 074 924 00010, phone number: +33 (0)2 69 61 02 57, mail: dpo.tessi@tessi.fr

TELETRAITEMENT ET INFORMATIQUE DE GESTION DE LA REUNION – T.I.G.R.E, Simplified Joint-stock Company with sole shareholder, with a capital of €40,000, whose registered office is in SAINT DENIS (97490), La Réunion, 1 rue Emile Hugo, Zone Technor - ZAC du Parc Technologique, registered in the Trade and Companies Register of SAINT DENIS, under number 310 851 324 00072, phone number: +33 (0)2 62 90 14 50, mail: dpo.tessi@tessi.fr

TESSI, Simplified Joint-stock Company with sole shareholder, with a capital of €6 524 342 whose registered office is in GRENOBLE (38000), 14 rue des Arts et Métiers, registered in the Trade and Companies Register of GRENOBLE under number 071 501 571 00237, phone number: +33 (0)4 76 70 59 10, mail: dpo.tessi@tessi.fr

TESSI ACCES, Simplified Joint-stock Company with sole shareholder, with a capital of €100,000, whose registered office is in AVON (77210), 44 avenue de Valvins, registered in the Trade and Companies Register of MELUN under number 338 621 972 00060, phone number: +33 (0)1 60 74 59 60, mail: dpo.tessi@tessi.fr

TESSI CHEQUE ILE DE FRANCE, Simplified Joint-stock Company, with a capital of €10,000, whose registered office is in MONTREUIL (93100), 240 rue de Rosny, registered in the Trade and Companies Register of BOBIGNY under number 439 202 698 00031, phone number: +33 (0) 1 41 58 65 32, mail: dpo.tessi@tessi.fr

TESSI CONTACT CENTER, Simplified Joint-stock Company with sole shareholder, with a capital of €400,000, whose registered office is in ISSY-LES-MOULINEAUX (92130), 32 Rue Henri Tariel, registered in the Trade and Companies Register of BOBIGNY under number 415 409 325 00024, phone number: +33 (0)1 41 31 53 83, mail: dpo.tessi@tessi.fr

TESSI 2M, Simplified Joint-stock Company with sole shareholder, with a capital of €37 000, whose registered office is in MAIGNELAY MONTIGNY (60420), 5 rue de Coivrel - Lieudit la Chapelle, registered in the Trade and Companies Register of BEAUVAIS under number 444 675 359 00053, phone number: +33 (0)3 44 50 00 90, mail: dpo.tessi@tessi.fr

TESSI DIGITAL SERVICES, Simplified Joint-stock Company, with a capital of €7,622.45 whose registered office is in LYON (69007), 45 rue Saint Jean de Dieu, registered in the Trade and Companies Register of LYON under number 383 587 557 00042, phone number: +33 (0)4 26 68 86 00, mail: dpo.tessi@tessi.fr

TESSI DOCUMENTS SERVICES, Simplified Joint-stock Company with sole shareholder, with a capital of €1,000,000, whose registered office is in BOULOGNE-BILLANCOURT (92100), 27-33 quai Alphonse Le Gallo, registered in the Trade and Companies Register of NANTERRE

under number 326 803 582 00062, phone number: +33 (0)1 41 31 53 83, mail: dpo.tessi@tessi.fr

TESSI DOCUMENTS SERVICES CENTRE DE RELATIONS CLIENTS, Simplified Joint-stock Company with sole shareholder, with a capital of €10,000, whose registered office is in LYON (69007), 13 rue Pierre Gilles de Gennes - Immeuble B, registered in the Trade and Companies Register of LYON under number 813 438 249 00043, phone number: +33 (0)4 72 02 52 53, mail: dpo.tessi@tessi.fr

TESSI EDITIQUE, Simplified Joint-stock Company with sole shareholder, with a capital of €355,600, whose registered office is in LONGJUMEAU (91160), 4 rue George Sand - ZI de la Vigne aux Loups, La Chapelle Saint Laurent, registered in the Trade and Companies Register of EVRY under number 722 057 593 00096, phone number: +33 (0)1 64 54 62 00, mail: dpo.tessi@tessi.fr

TESSI ENCAISSEMENTS Simplified Joint-stock Company with sole shareholder, with a capital of €500,000, whose registered office is in NANTERRE (92000), 39 rue des Hautes Pâtures, registered in the Trade and Companies Register of NANTERRE under number 449 587 500 00017, phone number: +33 (0)1 47 69 53 00, mail: dpo.tessi@tessi.fr

TESSI GESTION ASSURANCE, Simplified Joint-stock Company with sole shareholder, with a capital of €10,000, whose registered office is in BOULOGNE-BILLANCOURT (92100), 27-33 quai Alphonse Le Gallo, registered in the Trade and Companies Register of NANTERRE under number 822 481 115 00084, phone number: +33 (0)4 76 70 59 10, mail: dpo.tessi@tessi.fr

TESSI INFORMATIQUE, Simplified Joint-stock Company with sole shareholder, with a capital of €99,987.50, whose registered office is in SAINT JEAN BONNEFONDS (42650), Bâtiment 7 du Parc Métrotech, registered in the Trade and Companies Register of SAINT ETIENNE under number 331 618 520 00042, phone number: +33 (0)4 77 81 04 50, mail: dpo.tessi@tessi.fr

TESSI MD, Simplified Joint-stock Company with sole shareholder, with a capital of €100,000, whose registered office is in PANNES (45700), 490 rue des Frênes, registered in the Trade and Companies Register of ORLEANS under number 300 647 609 00191, phone number: +33 (0)2 38 87 60 20, mail: dpo.tessi@tessi.fr

TESSI OUEST, Simplified Joint-stock Company, with a capital of €107,629, whose registered office is in ANGERS (49000), 35 rue du Nid de Pie, registered in the Trade and Companies Register of ANGERS under number 340 258 284 00074, phone number: +33 (0)1 41 31 53 83, mail: dpo.tessi@tessi.fr

TESSI PRINT, Simplified Joint-stock Company with sole shareholder, with a capital of €37,000, whose registered office is in LONGJUMEAU (91160), 4 rue George Sand – ZI de la Vigne aux Loups – La Chapelle St Laurent, registered in the Trade and Companies Register of EVRY under number 504 425 075 00042, phone number: +33 (0)1 30 13 92 00, mail: dpo.tessi@tessi.fr

TESSI SERVICES, Simplified Joint-stock Company with sole shareholder, with a capital of €37,000, whose registered office is in GRENOBLE (38000), 14 rue des Arts et Métiers, registered in the Trade and Companies Register of GRENOBLE under number 504 308 461 00020, phone number: +33 (0)4 76 70 59 10, mail: dpo.tessi@tessi.fr

TESSI TECHNOLOGIES, Simplified Joint-stock Company with sole shareholder, with a capital of €300,000, whose registered office is in LE HAILLAN (33185), 1-3 avenue des Satellites - Immeuble Cassiopée, registered in the Trade and Companies Register of BORDEAUX under number 382 105 823 00092, phone number: +33 (0)5 57 22 20 61, mail: dpo.tessi@tessi.fr

TESSI-T.G.D, Simplified Joint-stock Company with sole shareholder, with a capital of €100,000 whose registered office is in NANTES (44300), 8 rue de la Rainière - Parc Club du Perray, registered in the Trade and Companies Register of NANTES under number 393 046 784 00137, phone number: +33 (0)2 28 23 67 07, mail: dpo.tessi@tessi.fr

TESSI TMS, Simplified Joint-stock Company with a capital of €1,097,632.92, whose registered office is in VOISINS LE BRETONNEUX (78960), 130-136 avenue Joseph Kessel, registered in the Trade and Companies Register of VERSAILLES under number 649 801 826 00094, phone number: +33 (0)1 30 13 92 00, mail: dpo.tessi@tessi.fr

SPAIN

ADM VALUE ASSURANCES BARCELONA SUCCURSAL, a Succursal under Spanish Law, branch of ADM VALUE ASSURANCES, whose registered office is in BARCELONA, Spain, (08006), Calle AVILA, Num 61, registered in the Trade Register of BARCELONA, under number W2502949G, mail: dpo.tessi@tessi.fr

ADM VALUE BARCELONA SA, a public limited company (SA) under Spanish Law, with a capital of €60 000, whose registered office is in BARCELONA, Spain, (08006), C Tuset, Num 5 - Planta 5, registered in the Trade Register of BARCELONA, under number A67002808, mail: dpo.tessi@tessi.fr

GDOC ESPAÑA, a Limited Company (SL) under Spanish Law, with a capital of €8 000, whose registered office is in MADRID, Spain, (28033), Calle Golfo de Salonica 27, planta 7, registered in the Trade Register of MADRID, Volume 27369, Page 91, Sheet M-493218, Tax ID number (NIF) No. B85869824, phone number : +34 913 83 62 60, mail: dpo.tessi@tessi.fr

INNOVATION & TRUST SPAIN, a limited company (SL) under Spanish law, with a capital of € 3 000, whose registered office is in Madrid, Spain (28033) Calle Golfo de Salónica, 27, Planta 7, registered in the Trade Register of Madrid, Volume 46014, Page 145, Sheet M-808535, phone number: +34 913 83 62 60, mail: dpo.tessi@tessi.fr

INSYNERGY CONSULTING ESPANA, a public limited company (SA) under Spanish Law, with a capital of €63,665, whose registered office is in MADRID, Spain, (28033), Calle Golfo de Salonica 27, planta 7, registered in the Trade Register of MADRID, Volume 16660, Page

53, Sheet M-284237, with Tax ID number (NIF) No. A-83/032375, phone number: +34 913 83 62 60, mail: dpo.tessi@tessi.fr

TODO EN CLOUD, Sociedad limitada Unipersonal (SLU), with a capital of €20,000, whose registered office is in MADRID, Spain, (28033), Golfo de Salonica 27, planta 7, registered in the Trade Register, Volume 29.097, page 29, sheet M-523877, NIF: B-86266533, phone number: +34 910801233, mail: dpo.tessi@tessi.fr

BULGARIA

OWLIANCE BULGARIE, One-person joint-stock company, with a capital of €50 000 whose registered office is in SOFIA (1309),141 Todor Aleksandrov Blvd – Vazrazhdane District - Floor 7 – SOFIA Municipality, Trade and Companies Register of SOFIA under number 131346599, mail: dpo.tessi@tessi.fr

II. Entities established outside the European Economic Area

Madagascar, Mauritius, Morocco, Senegal, Switzerland, Tunisia, and United Kingdom

MADAGASCAR

ADM BLUE, a public limited company with board of directors (SA) under Malagasy Law, with a capital of MGA 30,000,000, whose registered office is in ANTANANARIVO (MADAGASCAR), Golden Business Center Bâtiment D, Morarano Alarobia, Analamanga 101 Antananarivo Renivohitra, registered in the Trade Register of Antananarivo under number 2018B01262, mail: dpo.tessi@tessi.fr

ADM VALUE ALAROBIA, a Non-resident Limited Liability Company (SARL) under Malagasy Law, with a capital of MGA 30,000,000, whose registered office is in ANTANANARIVO (MADAGASCAR), Golden Business Center Bâtiment D, Morarano Alarobia; Analamanga 101 Antananarivo Renivohitra, registered in the Trade Register of Antananarivo under number 2018B00202, mail: dpo.tessi@tessi.fr

ADM VALUE DIEGO, a Non-resident Limited Liability Company (SARL) under Malagasy Law, with a capital of MGA 30,000,000, whose registered office is in ANTANANARIVO (MADAGASCAR), Lot n° 2-5 Immeuble Assist Velo Rainimangalahy Ivandry – Analamanga 101 Antananarivo Renivohitra registered in the Trade Register of Antananarivo under number 2015B00878, mail: dpo.tessi@tessi.fr

MADA M VALUE, a Non-resident Limited Liability Company (SARL) under Malagasy Law, with a capital of MGA 30,000,000, whose registered office is in ANTANANARIVO (MADAGASCAR), Golden Business center Batiment "I" Morarano - 101 Antananarivo Alarobia, registered in the Trade Register of Antananarivo under number 2008B01052, mail: dpo.tessi@tessi.fr

MAURITIUS

BATCH IMAGE PROCESSING INDIAN OCEAN-BIPIO, Private Limited Liability Company under Mauritian Law, with a capital of €100,000, whose registered office is in EBENE (MAURITIUS), 8th floor, Cyber Tower II, Ebene Cybercity, registered in the Trade Register of Mauritius under number 48775, phone number: + (230) 467 9111, mail: dpo.tessi@tessi.fr

PROCESSURE COMPANY LIMITED, with a capital of MUR 1,000,000, whose registered office is in EBENE (Mauritius), Cybertower 2, registered in the Trade Register of Mauritius under number C086913, phone number: + (230) 467 9111, mail: dpo.tessi@tessi.fr

ADM VALUE ASSURANCES MAURITIUS BRANCH, Succursal under Mauritian Law, whose registered office is in EBENE (MAURITIUS), C/O Axis Fiduciary Lt, 2nd floor, The Axis, 26 Cybercity, registered in the Trade Register of Mauritius under number C22186640, mail: dpo.tessi@tessi.fr

MOROCCO

2T SERVICES MAROC, a Private Limited Liability Company under Moroccan Law, with a capital of MAD 100,000, whose registered office is in OUJDA (MOROCCO), Boulevard Mohamed VI, Rond-Point de l'Université, registered under ICE number 003214218000074 and in the Trade Register of OUJDA under number 40477, mail: dpo.tessi@tessi.fr

ADM CALL CENTER, a non-resident Limited Liability Company (SARL) under Moroccan Law, with a capital of MAD 1,400,000, whose registered office is in MEKNES (MOROCCO), 4 Rue Nehrou - N 26 Espace - Bureau 4ème étage JAWHARA VN, registered in the Trade Register of MEKNES under number 27263, mail: dpo.tessi@tessi.fr

ADM CALL ASSURANCES SUCCURSAL, a succursal under Moroccan Law, with a capital of MAD 0, whose registered office is in RABAT (MOROCCO), Rue Le Caire et Gandhi Résidence El Menzah APP20, registered in the Trade Register of RABAT under number 80325, mail: dpo.tessi@tessi.fr

ADM VALUE ASSURANCES ORIENTAL, a succursal under Moroccan Law, with a capital of MAD 10,000, whose registered office is in OUJDA (MOROCCO), BD Mohamed VI Rond point de l'université, registered in the Trade Register of OUJDA under number 32771, mail: dpo.tessi@tessi.fr

ADM VALUE GESTION, a non-resident Limited Liability Company (SARL) under Moroccan Law, with a capital of MAD 100,000, whose registered office is in RABAT (MOROCCO), 4 avenue Michlifen Agdal, registered in the Trade Register of RABAT under number 59021, mail: dpo.tessi@tessi.fr

ADM VALUE RABAT, a non-resident Limited Liability Company (SARL) under Moroccan Law, with a capital of MAD 100,000, whose registered office is in RABAT (MOROCCO), Immeuble Angle Avenue Hassan II et rue SIAM, registered in the Trade Register of RABAT under number 126115, mail: dpo.tessi@tessi.fr

CRM ON LINE, a non-resident Limited Liability Company (SARL) under Moroccan Law, with a capital of MAD 100,000, whose registered office is in RABAT (MOROCCO), 4 avenue Michlifen Agdal, registered in the Trade Register of RABAT under number 73385, mail: dpo.tessi@tessi.fr

CRM VALUE, a non-resident Limited Liability Company (SARL) under Moroccan Law, with a capital of MAD 3,300,000, whose registered office is in RABAT (MOROCCO), 4 avenue Michlifen Agdal, registered in the Trade Register of RABAT under number 55461, mail: dpo.tessi@tessi.fr

ID SWISS CALL SARL, a non-resident Limited Liability Company (SARL) under Moroccan Law, with a capital of MAD 100,000, whose registered office is in RABAT (MOROCCO), angle des rues El Koufa et Sana'a Hassan, registered in the Trade Register of RABAT under number 63721, mail: dpo.tessi@tessi.fr

NETWORK ONLINE, a non-resident Limited Liability Company (SARL) under Moroccan Law, with a capital of MAD 1,800,000, whose registered office is in RABAT (MOROCCO), angle des rues Koufa et Sanaa - Hassan, registered in the Trade Register of RABAT under number 58099, mail: dpo.tessi@tessi.fr

ORIEN CALL, a non-resident Limited Liability Company (SARL) under Moroccan Law, with a capital of MAD 3,000,000, whose registered office is in OUJDA (MOROCCO), BD Mohamed VI Rond point de l'Université, registered in the Trade Register of OUJDA under number 18683, mail: dpo.tessi@tessi.fr

SENEGAL

ADM BLUE SENEGAL, a public Limited Company, with a capital of XOF 10,000,000, whose registered office is in DAKAR (SENEGAL), Point E – rue de Ziguinchor, registered in the Trade Register of DAKAR under number 2024B7107, mail: dpo.tessi@tessi.fr

ADM VALUE SENEGAL, a non-resident Limited Liability Company (SARL) under Senegalese Law, with a capital of XOF 130,000,000, whose registered office is in DAKAR (SENEGAL), Immeuble Yaye Fatou Dieng - Ex rue de Ziguinchor, registered in the Trade Register of DAKAR under number 2019B23586, mail: dpo.tessi@tessi.fr

SWITZERLAND

TESSI DOCUMENTS SOLUTIONS (Switzerland), GmbH under Swiss Law, with a capital of CHF 400,000, whose registered office is in URDOF (8902), - Switzerland, In der Luberzen 17w, having as identification number in the Handelsregister des Kantons Zürich, CHE-105.915.806, phone number: +41 22 308 68 10, mail: dpo.tessi@tessi.fr

GDOC LASERCOM, a Public Limited Company under Swiss law, with a capital of CHF 100,000, whose registered office is in PETIT-LANCY (1213) - Switzerland, 12 avenue des Morgines, registered in the Trade Register of Geneva under number CHE-113.330.973, phone number: +41 22 710 62 00, mail: dpo.tessi@tessi.fr

GDOC HOLDING, a Public Limited Company (SA) under Swiss law, with a capital of CHF 500,000, whose registered office is in PETIT-LANCY (1213) - Switzerland, 12 avenue des Morgines, registered in the Trade Register of Geneva under number CHE-437.210.137, phone number: +41 22 710 62 00, mail: dpo.tessi@tessi.fr

TUNISIA

OWLIANCE TUNISIE, Limited Liability Company under Tunisian Law, with a capital of 12 800 Dinars Tunisien, whose registered office is in ARIANA TUNIS (2083) – ZI De Chotrana II Lot AFI 114 Raoued, TUNISIE, Trade and Companies Register of TUNIS under number B03109322009, Matricule fiscal 946909 WAM 000, mail: dpo.tessi@tessi.fr

TUNIS DATA SERVICES, Non-resident Limited Liability Company, with a capital of 184000TND, whose registered office is in TUNIS (2035), rue 8612 - impasse n°2- zone industrielle la Charguia I, registered in the Trade Register of TUNIS under number of B2468682008 RC TUNIS, phone number: (+216) 71 284 721, mail: dpo.tessi@tessi.fr

TESSI TECHNOLOGY TUNIS, Non-resident Limited Liability Company, with a capital of TND 20,000, whose registered office is in TUNIS (2035), rue 8612 - impasse n°2 - zone industrielle la Charguia I, registered in the Trade Register of TUNIS under number B01237232017, phone number: (+ 216) 31 309 413, mail: dpo.tessi@tessi.fr

UNITED KINGDOM

DOCUPLUS LTD, a Limited Company under English Law, with a capital of GBP 40 000, whose registered office is at 22 Wycombe End - Beaconsfield - Buckinghamshire - HP9 1NB, registered in the Trade Register of England and Wales under number 03491827, phone number: +44 (0)1494 292602, mail: dpo.tessi@tessi.fr

XIV. APPENDIX 2: DESCRIPTION OF THE MATERIAL SCOPE OF THE TESSI GROUP BCR-C

Purposes of processing	Categories of personal data transferred[i]								Categories of data subjects[ii]	Third Countries
	Identification data	Professional life data	Connection data	Personal life data	Economic and financial data	Sensitive data	Criminal data	Location data		
Activities related to the development of applications of software solutions, websites and mobile applications of which the entities of the Tessi Group are publishers: study and design, creation, testing and acceptance	✓	✓	✓	✗	✗	✗	✗	✗	Employees, business partners, suppliers, service providers, processors and sub-processors	Tunisia, Mauritius, Madagascar, Morocco, Senegal
IT service management: support (telephone support, email), incident handling and operation	✓	✓	✓	✗	✗	✓	✗	✗	Employees, interns, job applicants, customers, business partners, suppliers, processors and sub-processors	Tunisia, Mauritius, Madagascar, Morocco, Senegal

Purposes of processing	Categories of personal data transferred[1]								Categories of data subjects[2]	Third Countries
	Identification data	Professional life data	Connection data	Personal life data	Economic and financial data	Sensitive data	Criminal data	Location data		
Human resources management: recruitment, personnel and salary management, human resources administration, career management, human resources communication, payroll management, teleworking, staff training, social action management, travel management, professional elections, etc.	✓	✓	✓	✓	✓	✓ Trade union membership (elected officials), medical data, social security, judicial, medical, RQTH, pregnant women, IRP, social security certificate or copy of carte vitale (if retained), date of sick leave, date of hospitalization, family events, existence of a disability (yes/no), membership union and type of mandate; occupational health opinion, occupational disease cases	✓ Extract from criminal record	✗	Employees, interns, job applicants, business partners, suppliers, processors and sub-processors	Tunisia, Mauritius, Madagascar, Morocco, Senegal
IT and physical security management	✓	✓	✓	✗	✗	✗	✗	✗	Employees, interns, job applicants, customers, business partners, suppliers, processors and sub-processors	Tunisia, Mauritius, Madagascar, Morocco, Senegal

Purposes of processing	Categories of personal data transferred[1]								Categories of data subjects[2]	Third countries
	Identification data	Professional life data	Connection data	Personal life data	Economic and financial data	Sensitive data	Criminal data	Location data		
Audit and internal control: quality, safety, compliance	✓	✓	✓	✗	✗	✓	✗	✗	Employees, interns, job applicants, customers, business partners, suppliers, processors and sub-processors	Tunisia, Mauritius, Madagascar, Morocco, Senegal
Business management (purchase, sale): suppliers, partners, customers, etc.	✓	✓	✓	✗	✓	✗	✗	✗	Employees, interns, customers, business partners, suppliers, service providers, processors and sub-processors	Tunisia, Mauritius, Madagascar, Morocco, Senegal
Customer relationship management (CRM)	✓	✓	✓	✗	✗	✗	✗	✗	Employees, interns, customers, business partners, suppliers, processors and sub-processors	Tunisia, Mauritius, Madagascar, Morocco, Senegal

Purposes of processing	Categories of personal data transferred[1]								Categories of data subjects[2]	Third countries
	Identification data	Professional life data	Connection data	Personal life data	Economic and financial data	Sensitive data	Criminal data	Location data		
Management of communications (internal, institutional) such as: management of websites, newsletters, events, and satisfaction survey	✓	✓	✗	✗	✗	✗	✗	✗	Employees, interns, job applicants, customers, business partners, suppliers, processors and sub-processors	Tunisia, Mauritius, Madagascar, Morocco, Senegal
Compilation of statistics for internal needs and social management control	✓	✓	✓	✓	✓	✓ Social security number, disability rate, recognition of the status of disabled worker	✗	✗	Employees, interns, job applicants, customers, business partners, suppliers, processors and sub-processors	Tunisia, Mauritius, Madagascar, Morocco, Senegal
Archiving	✓	✓	✓	✗	✗	✗	✗	✗	Employees, interns, job applicants, customers, business partners, suppliers, processors and sub-processors	Tunisia, Mauritius, Madagascar, Morocco, Senegal

Purposes of processing	Categories of personal data transferred[1]								Categories of data subjects[2]	Third countries
	Identification data	Professional life data	Connection data	Personal life data	Economic and financial data	Sensitive data	Criminal data	Location data		
Maintenance in operational condition and optimization of the performance of the solutions developed by the Tessi Group	✓	✓	✓	✓	✗	✗	✗	✗	Employees, interns, customers, business partners, suppliers, service providers, processors and sub-processors	Tunisia, Mauritius, Madagascar, Morocco, Senegal
Improvement of the company's performance	✓	✓	✓	✗	✗	✗	✗	✗	Employees, suppliers, processors and sub-processors	Tunisia, Mauritius, Madagascar, Morocco, Senegal
Individual monitoring of performance and progression of projects	✓	✓	✓	✗	✗	✗	✗	✗	Employees, interns, managers	Tunisia, Mauritius, Madagascar, Morocco, Senegal

Purposes of processing	Categories of personal data transferred[1]								Categories of data subjects[2]	Third countries
	Identification data	Professional life data	Connection data	Personal life data	Economic and financial data	Sensitive data	Criminal data	Location data		
Management of legal processes and related obligations	✓	✓	✗	✗	✗	✗	✗	✗	Employees, interns, customers, business partners, suppliers, service providers, processors and sub-processors	Tunisia, Mauritius, Madagascar, Morocco, Senegal
Human resources management: occupational medicine. (medical visit, disability monitoring)	✓	✓	✓	✓	✗	✓ Date of sick leave, date of hospitalization, Social security number	✗	✗	Employees, interns	Tunisia, Mauritius, Madagascar, Morocco, Senegal
Indexing of dematerialized HR (signing of contracts, electronic document management) and tax documents	✓	✓	✓	✓	✓	✓ Social security number, occupational medicine opinion, occupational disease files, disability, disability notification	✓ Extract from criminal record	✗	Employees, interns, managers	Tunisia, Mauritius, Madagascar, Morocco, Senegal

Purposes of processing	Categories of personal data transferred[1]								Categories of data subjects[2]	Third countries
	Identification data	Professional life data	Connection data	Personal life data	Economic and financial data	Sensitive data	Criminal data	Location data		
Recovery	✓	✓	✗	✗	✓	✗	✗	✗	Employees, interns, suppliers, customers	Tunisia, Mauritius, Madagascar, Morocco, Senegal
Inventory management and purchasing administration	✓	✓	✗	✗	✓	✗	✗	✗	Employees, interns, suppliers, customers	Tunisia, Mauritius, Madagascar, Morocco, Senegal
Provision of supplies	✓	✓	✗	✗	✓	✗	✗	✗	Employees, interns, managers	Tunisia, Mauritius, Madagascar, Morocco, Senegal
Reporting for statistics and analysis for management of activities	✓	✓	✗	✗	✓	✗	✗	✗	Employees, interns, suppliers, customers	Tunisia, Mauritius, Madagascar, Morocco, Senegal
Finance management	✓	✓	✗	✗	✓	✗	✗	✗	Employees, interns, suppliers, customers	Tunisia, Mauritius, Madagascar, Morocco, Senegal

[i] "**Connection data**" includes logs and IP addresses; "**Personal life data**" includes personal data related to individuals' families and emergency contacts; "**Economic and financial data**" includes income, taxes, banking information, ownership interests, financial position.

[ii] "**Customers**" includes current and potential customers (employees and representatives); "**business partners**" includes current and potential business partners (employees and representatives); "**suppliers**" includes current and potential suppliers (employees and representatives); "**service providers**" includes current and potential service providers (employees and representatives); "**processors**" and "**sub-processors**" include current and potential processors and sub-processors (employees and representatives).