Binding Corporate Rules (BCRs), for intra-group transfers of personal data to non EEA countries

1. INTRODUCTION 3

2. DEFINITIONS AND DATA PROTECTION PRINCIPLES 4

2.1. DEFINITIONS 4

2.2. DATA PROTECTION PRINCIPLES 4

3. SCOPE OF THE BCRs 6

3.1. GEOGRAPHICAL SCOPE 6

3.2. MATERIAL SCOPE 6

4. EFFECTIVENESS OF THE BCRs 6

4.1. TRANSPARANCY AND INFORMATION RIGHT 6

4.2. RIGHTS OF ACCESS, RECTIFICATION, ERASURE AND BLOCKING OF DATA 7

4.3. AUTOMATED INDIVIDUAL DECISION 8

4.4. INTERNAL COMPLAINT MECHANISM 8

4.5. SECURITY AND CONFIDENTIALITY / RELATIONSHIPS WITH PROCESSORS THAT ARE MEMBERS OF THE GROUP 9

4.6. TRAINING PROGRAMS 10

4.7. AUDIT PROGRAMME 10

5. BINDINGNESS OF THE BCRs 11

5.1. COMPLIANCE AND SUPERVISION OF COMPLIANCE 11

5.2. THIRD PARTY BENEFICIARY RIGHTS 12

5.3. LIABILITY 13

5.4. JURISDICTION 13

5.5. SANCTIONS 14

5.6. MUTUAL ASSISTANCE AND COOPERATION WITH DATA PROTECTION AUTHORITIES 14

6. FINAL PROVISIONS 15

6.1. RELATIONSHIP BETWEEN NATIONAL LAWS AND THE BCRs 15

6.2. RESTRICTIONS ON TRANSFERS AND ONWARD TRANSFERS TO EXTERNAL PROCESSORS AND CONTROLLERS 15

6.3. ACTIONS IN CASE OF NATIONAL LEGISLATION PREVENTING RESPECT OF BCRs 15

6.4. UPDATES OF THE BCRs 16

6.5. DEROGATIONS OF ARTICLE 26 EU DIRECTIVE 95/46 16

6.6. APPLICABLE LAW / JURISDICTION / TERMINATION / INTERPRETATION OF TERMS 17

7. APPENDIXES 17

1. INTRODUCTION

Because customers and employees are the most valuable assets of SOPRA HR SOFTWARE, the Group is committed to ensure the highest possible level of care and services in order to improve mutual trust. In this context, customers and employees' right to privacy is a prime consideration for SOPRA HR SOFTWARE.

Under the provisions of the the Regulation (EU) 2016/679 (General Data Protection Regulation) , any transfer of Personal Data outside the European Economic Area (EEA) shall be framed by specific safeguards, with a view to make the use of Personal Data compliant with European Data Protection Principles. Thus, the adoption and the implementation of Binding Corporate Rules (BCRs) within SOPRA HR SOFTWARE will aim to regulate intra-group data transfers related to Personal Data outside the European Economic Area (EEA), in accordance with the provisions of the the Regulation (EU) 2016/679 (General Data Protection Regulation)Beyond, SOPRA HR SOFTWARE and its employees are responsible for protecting and respecting personal information to which they have access. Therefore, we believe that our BCRs are an essential tool to effectively manage this important responsibility and to broadcast and share our culture on Privacy within the Group.

With regard to the scope of our BCRs, appropriate entities and employees of SOPRA HR SOFTWARE shall comply with the following provisions, as well as with applicable local laws.

At local level, and according to the terms of our BCRs, each Local Data Controller will have to sign a BCRs agreement and shall take every necessary step to ensure compliance with the provisions of the BCRs. Compliance with these provisions and procedures will especially rely on training programs and auditing activities, on a day to day basis.

Because of their wide scope in terms of privacy compliance, the use of BCRs at local level will, without any doubt, ease the management of privacy compliance and will help to ensure that local representatives take ownership of data protection.

Would a violation of the BCRs be established, any corrective measures (legal, technical or organizational measures) as well as any appropriate sanction (against the Local Data Controller or, according to local labor law, a local employee) may be taken on the initiative of the Head Controller, the EMEA Data Privacy Manager, the Local Data Controller or the Local Data Privacy Manager.

2. DEFINITIONS AND DATA PROTECTION PRINCIPLES

2.1. DEFINITIONS

The terms and expressions used in the BCRs are defined in Appendix 1, provided that these terms and expressions shall always be interpreted according to the Regulation (EU) 2016/679 (General Data Protection Regulation).

2.2. DATA PROTECTION PRINCIPLES

Within the scope of the BCRs (see paragraph 3), any transfer of Personal Data to a third country which does not ensure an adequate level of protection shall always comply with the following data protection principles, defined in specific paragraphs of the BCRs or in Appendix 2, in accordance with the provisions ofthe Regulation (EU) 2016/679 (General Data Protection Regulation).

- **Legal basis for processing Personal Data and Sensitive Personal Data**: Personal Data and Sensitive Personal Data shall only be processed under the conditions defined in the the Regulation (EU) 2016/679 (General Data Protection Regulation) **Purpose limitation**: Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
- **Data quality, data minimisation and proportionality**: Personal Data shall be processed fairly and lawfully. Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Personal Data shall be accurate and, where necessary, kept up to date. Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.
- **Automated individual decisions**: each Data Subject has the right not to be subject to a decision which produces legal effects concerning him and which would be based solely on automated processing of data.
- **Information right**: Personal Data shall always be collected and further processed on a transparent basis (see paragraph 4.1)
- **Rights of access, rectification, erasure and blocking of data, right to restriction of processing , right to object, right to data portability** : Data Subjects are entitled to be told what information SOPRA HR SOFTWARE holds on them and to keep this information under control (see paragraph 4.2).
- **Security and confidentiality**: appropriate technical and organizational measures shall be implemented to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing (see paragraph 4.5).
- Lawfulness of processing
    - Processing shall be lawful only if and to the extent that at least one of the following applies:
    - 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 performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- 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.
- This last point of the list shall not apply to processing carried out by public authorities in the performance of their tasks

- **Storage Restriction** : Personal Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;

- **Ensure during the Processing of special categories of personal data** that the special data is processed by Sopra HR Software in accordance with the terms and conditions of Schedule 2 hereof.

- **Data protection by design and by default**:

  technical and organizational measures have been set up in order to preserve the privacy and the principles of data protection from the outset: in particular by setting limits on the fields to be filled in on the SIRH applications, adequate retention periods and limited accessibility.

- **Requirements for subsequent transfers to organizations not bound by BCRs:** these transfers must meet the requirements of Article 6.2 of these BCRs

3. SCOPE OF THE BCRs

3.1. GEOGRAPHICAL SCOPE

The BCRs shall apply to transfers of Personal Data from entities of SOPRA HR SOFTWARE established within the European Union to other SOPRA HR SOFTWARE throughout the world listed in Appendix 3.

Appendix 3 gives a list of all SOPRA HR SOFTWARE entities bound by the BCRs.

3.2. MATERIAL SCOPE

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

4. EFFECTIVENESS OF THE BCRs

4.1. TRANSPARANCY AND INFORMATION RIGHT

To make the data processing fair, Personal Data shall always be collected and further processed on a transparent basis. Thus:

1. The BCRs shall always be readily available to every Data Subject and therefore shall be uploaded on SOPRA HR SOFTWARE internet and intranet websites. A Data Subject shall always be able to obtain, upon request, a copy of the BCRs from the Local Data Privacy Manager, the Local Data Controller or the EMEA Data Privacy Manager.

2. Furthermore, specific FAQs shall be available for Data Subjects on SOPRA HR SOFTWARE internet websites, with a view to clarify any question Data Subjects may have about the BCRs or any related matter, such as concerns or requests related to submitting an access request to their Personal Data (see paragraph 4.2) or submitting a claim (see paragraph 4.3).

3. All data processing and, when appropriate, data transfers between entities of SOPRA HR SOFTWARE established throughout the world shall be associated with relevant data protection notices.

Local Data Privacy Managers, in coordination with the EMEA Data Privacy Manager, shall be able to provide templates of notices to every Local Data Controller within the Group, for any purpose that requires information to be made to the Data Subjects.

SOPRA HR SOFTWARE will provide a Data Subject with at least the following information, except where he already has it:

a. the identity of the controller and of his representative their contact details and the contact details of the DPO, if any, and, when appropriate, the place in which the Local Data Importer is based outside the EEA;

b. the purposes of the processing for which the data are intended, and, when appropriate, the purpose(s) of the transfer(s) outside the EEA;

c. any further information such as:

- the categories of personal data concerned;
- the Recipients or categories of Recipients of the data;
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;
- information, if any, of the intention of the controller to transfer personal data to a recipient in a third country.
-
- the length of time during which the personal data will be kept, or the criteria used to determine this duration when the duration is not possible to determine.

- the existence of the right of access to and the right to rectify or to erase the data concerning him. The right to restriction of processing the data concerning him , the right to object and the right to data portability

Where, with regard to an existing data processing, a new purpose or a new category of Recipient arises, the appropriate notice of information shall be consequently modified and the Data Subjects shall be informed.

Where the data has not been directly obtained from the Data Subjects, SOPRA HR SOFTWARE will provide with the information above at the time of undertaking the recording of Personal Data , as well as the source from which the personal data originates and, where appropriate, a statement that they are or are not from publicly available sources or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed.

According toRegulation (EU) 2016/679 (General Data Protection Regulation),, and notwithstanding any specific provision set out in national legislations, information will exceptionally not apply where the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law (see paragraph 6.3).

4.2. RIGHTS OF ACCESS, RECTIFICATION, ERASURE AND BLOCKING OF DATA Rights of Restriction of processing, the right to object and the right to data portability

4.3.

Data Subjects are entitled to be told what information SOPRA HR SOFTWARE holds on them and to keep this information under control. Thus:

1. Every Data Subject has the right to obtain from SOPRA HR SOFTWARE:

a. without constraint at reasonable intervals and without excessive delay or expense, and, where applicable, according to national legislations:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the Recipients or categories of Recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated individual decisions referred to paragraph 4.3.

b. as appropriate the rectification, erasure or blocking of Personal Data, , the Rights of Restriction of processing, the right to object and the right to data portability, in particular because of the incomplete or inaccurate nature of the data;

c. to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him.

According to theRegulation (EU) 2016/679 (General Data Protection Regulation), the exercise of those rights may be subject to certain limitations.

2. Every Data Subject shall be clearly informed, in accordance with paragraph 4.1, on how he can exercise his rights.

3. Specific guidelines and procedures shall be in place within the Group, at local level, to ensure the exercise of the rights specified above. In particular, SOPRA HR SOFTWARE employees who collect, process or have access to Personal Data shall be trained to recognize a Data Subject access, rectification, erasure or blocking request the rights of Restriction of processing, the right to object and the right to data portability. Each request shall be acknowledged and handled according to the local procedure in place. A specific answer, given within a reasonable period of time, shall be systematically given to the Data Subject. if the request is found legitimate, SOPRA HR SOFTWARE shall take any necessary step to handle the matter in due times. If the request is denied, the reason for denial shall be communicated in writing to the Data Subject. In such a case, the Data Subject may follow the internal complaint mechanism specified in paragraph 4.4.

4. Local Data Privacy Managers, in coordination with the EMEA Data Privacy Manager, shall always be at the disposal of both Local Data Controllers and Data Subjects to provide any help.

4.4. AUTOMATED INDIVIDUAL DECISION

Subject to local applicable law, every Data Subject has the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, reliability, conduct, etc.

4.5. INTERNAL COMPLAINT MECHANISM

If a Data Subject believes that its Personal Data is not processed in accordance with the BCRs or the applicable local law, he may register a claim to obtain adequate correction measures and, where appropriate, adequate compensation (see paragraph 5.2 and 5.4). Therefore:

1. Specific guidelines and procedures shall be in place within the Group, at local level, to ensure a complaint mechanism to be consistent and to ensure sufficient information to be provided to the Data Subjects about these procedures. The complaints shall be dealt by a clearly identified local department which benefits from an appropriate level of independence in the exercise of its functions (for instance

the local compliance officer or the General counsel). When a complaint is registered, it must be acknowledged and handled within a reasonable period of time (one months).

2. If the Data Subject of SOPRA HR SOFTWARE representatives fail to solve the claim at local level, the complaint handling mechanism shall allow escalating the problem to the EMEA Data Privacy Manager who shall respond within 2 months. Each Local Data Controller and Local Data Privacy Manager shall regularly report to the EMEA Data Privacy Manager about the complaints settled at local level, with a view to take corrective actions and improve guidelines and procedures implemented within the Group, where the complaints may have revealed a "gap" in terms of Privacy compliance.

4. All SOPRA HR SOFTWARE representatives and employees shall, at local level, do their best efforts to help the Local Data Controller or the Local Data Privacy Manager to settle a complaint (see paragraph 5.3).

Prior to referring a case to the relevant court, each party should make its best efforts to solve a claim through the internal complaint mechanism described above.

4.6. SECURITY AND CONFIDENTIALITY / RELATIONSHIPS WITH PROCESSORS THAT ARE MEMBERS OF THE GROUP

Ensuring that personal information is appropriately protected from data breaches is a SOPRA HR SOFTWARE top priority. Thus:

1. Each Local Data Controller shall implement appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Consequently, appropriate information security policies and procedures shall be designed and implemented within the Group. These security policies set up all appropriate physical and logical measures with a view to prevent or deter accidental destruction, modification or unauthorized disclosure or access to Personal Data. These policies and procedures shall be regularly audited (see paragraph 4.7).

2. Sensitive Data shall be processed with enhanced and specific security measures.

3. Access to Personal Data is limited to Recipients for the sole purpose of performing their professional duties. Disciplinary sanctions may occur if a SOPRA HR SOFTWARE employee fails to comply with the appropriate information security policies and procedures.

Where a Local Data Controller requests that another entity of SOPRA HR SOFTWARE undertakes Processing of Personal Data on its behalf (for a short term period as well as for a long term period, depending on the case), the following safeguards shall be followed:

1. Where the data processing is carried out, the Local Data Controller shall choose a Processor providing sufficient guarantees in respect of the Technical and Organizational Security Measures governing the processing to be carried out, and must ensure compliance with those measures. The appointed entity of SOPRA HR SOFTWARE shall undertake in writing to provide those sufficient

guarantees. Local Data Privacy Managers, in coordination with the EMEA Data Privacy Manager, shall be able to provide templates of the appropriate clauses to a Local Data Controller within the Group.

2. The appointed entity of SOPRA HR SOFTWARE must not process the data except on instructions from the controller, unless he is required to do so by law.

3. Upon termination of the work to be done, the appointed entity of SOPRA HR SOFTWARE shall undertake to delete all the data transferred or, if any legal data retention requirement is applicable, to keep it recorded, provided that appropriate technical and organizational measures are taken to protect Personal Data against any unlawful form of processing.

4.7. TRAINING PROGRAMS

Any SOPRA HR SOFTWARE employee who collects, processes or has access to Personal Data shall be provided with specific training programs in order to improve its practical skills and knowledge that relate to data protection issues, especially the BCRs:

1. BCR's and all related guidelines, procedures or policies shall be uploaded on SOPRA HR SOFTWARE corporate intranet and permanently accessible to every employee.

2. Access to the BCRs and all related guidelines, procedures or policies shall be granted to every SOPRA HR SOFTWARE new employee. Internal notices shall also be transmitted within the Group to raise awareness on the BCRs.

3. New employees who collect, process or have access to Personal Data shall be required to follow a privacy compliance training program. Furthermore, all employees who collect, process or have access to Personal Data shall be required to follow such a program, on a regular basis. [All employees must pass a knowledge check (certification) following their completion of the training to confirm their knowledge and skills on privacy issues].

4. At local level, each data controller and/or Local Data Privacy Manager shall feel free to enhance the privacy training programs described above by adding any appropriate training material.

5. Privacy training programs shall be reviewed and approved by experienced SOPRA HR SOFTWARE officers, in coordination with the Local Data Controller, the Local Data Privacy Manager, the EMEA Data Privacy Manager. Procedures related to privacy training programs shall be regularly audited (see paragraph 4.7).

4.8. AUDIT PROGRAMME

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

1. Data Protection audits shall cover all aspects of the BCRs and all related policies, procedures or guidelines, including methods of insuring that corrective measures will take place. However, the scope of each audit can be strengthened to limited aspects of the BCRs and/or the related policies, procedures or guidelines, including methods of insuring that corrective measures will take place.

2. Data Protection audits shall be decided directly by the Compliance Department or upon specific request of the Head Controller, a Local Data Controller, a Local Data Privacy Manager or the EMEA Data

Privacy Manager. The ones in charge of handling an audit will always benefit from an appropriate level of independence in the exercise of their duties.

3. The results of all audits shall be communicated to the Head Controller (especially to the Head Controller's management), and the Local Data Controller, and/or the Local Data Privacy Manager, and/or the EMEA Data Privacy Manager.

4. The relevant Data Protection Authorities shall receive a copy of such audit upon request. Each Local Data Controller shall accept to be audited by a Data Protection Authority and to abide by the advice of a Data Protection Authority on any issue related to the BCRs.

5. As provided by section 3 of paragraph 5.1, Local Data Privacy Managers, in coordination with the EMEA Data Privacy Manager shall report every year to the Head Controller about all the actions and measures taken with regard to Data Protection issues (training programs, inventory of Personal Data processing implemented, management of complaints, etc.). Furthermore, each local data Privacy Manager shall take every necessary step to make sure that Local Data Controllers comply with the provisions of the BCRs. To this end, a "BCR compliance check-list" shall be used at local level to make compliance checks.

6. The EMEA Data Privacy Manager shall also regularly report to the Head Controller about the implementation of the BCRs within each Local Data Controller.

7. Thanks to the audit results and the reports mentioned above, the Head Controller (especially the Head Controller's management), and/or the EMEA Data Privacy Manager shall decide any appropriate legal, technical or organizational measure in order to improve Data Protection management within the Group, both at global and/or local level.

5. BINDINGNESS OF THE BCRs

5.1. COMPLIANCE AND SUPERVISION OF COMPLIANCE

At local level, each Local Data Privacy Manager shall be responsible for the implementation of the BCRs. Thus:

1. Each entity of SOPRA HR SOFTWARE shall take every necessary step to make sure that Local Data Controllers comply with the provisions of the BCRs. To this end, a "BCR compliance check list" shall be used at local level to make compliance checks. Data Protection audits decided by the Compliance Department or the EMEA Data Privacy Manager may focus on how these compliance checks are made at local level.

2. Local Data Privacy Managers, in coordination with the EMEA Data Privacy Manager, shall always be at the disposal of both Local Data Controller and Data Subjects to provide any help with regard to a data protection issue, especially the BCRs.

3. Local Data Privacy Managers, in coordination with the EMEA Data Privacy Manager, shall report every year to the Head Controller about all the actions and measures taken with regard to Data

Protection issues (training programs, inventory of Personal Data processing implemented, management of complaints, etc.), especially the implementation of the BCRs.

4. Each Local Data Controller and Local Data Privacy Manager shall regularly report to the EMEA Data Privacy Manager about the complaints settled at local level, with a view to take corrective actions and improve guidelines and procedures implemented within the Group, where the complaints may have revealed a "gap" in terms of Privacy.

5. Local Data Privacy Managers, in coordination with the EMEA Data Privacy Manager, shall be able to provide any appropriate templates (i.e. notices of information, clauses, etc.) to each Local Data Controller within the Group for any purpose related to a data protection issue.

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

1. The EMEA Data Privacy Manager shall regularly report to the Head Controller about the implementation of the BCRs within each Local Data Controller.

2. Data Protection audits shall be decided directly by the Compliance Department or upon specific request of a Local Data Controller, a Local Data Privacy Manager or the EMEA Data Privacy Manager. The results of all audits or reports shall be communicated to the Head Controller (especially to the Head Controller's management), and the Local Data Controller, and/or the Local Data Privacy Manager, and/or the EMEA Data Privacy Manager.

3. Thanks to the audit results and the reports mentioned above, the Head Controller (especially the Head Controller's management), the EMEA Data Privacy Manager, a Local Data Controller or a Local Data Privacy Manager shall decide any appropriate measure in order to improve Data Protection management within the Group, both at global and/or local level.

4. If a violation of the BCRs is established, any correction measure (legal, technical or organizational measure) as well as any appropriate sanction (against the Local Data Controller or, according to local labor law, a local employee) may be taken on the initiative of the Head Controller, the EMEA Data Privacy Manager, a Local Data Controller or a Local Data Privacy Manager.

5. Privacy training programs shall be reviewed and approved by SOPRA HR SOFTWARE senior officers, in coordination with the EMEA Data Privacy Manager and Local Data Privacy Managers. Procedures related to privacy training programs shall be regularly audited (see paragraph 4.7).

5.2. THIRD PARTY BENEFICIARY RIGHTS

A Data Subject shall have the right to enforce, as a third party beneficiary, the provisions of the BCRs related to:

- Purpose limitation, data quality, proportionality and legitimacy principles (see paragraph 2.2 and Appendix 2)
- Transparency principle and easy access to BCRs (see paragraph 4.1)
- Rights of access, rectification, erasure, blocking of data and object to the processing) the Rights of Restriction of processing, and the right to data portability
- (see paragraph 4.2)

- Rights in case automated individual decisions are taken (see paragraph 4.3)
- Security and confidentiality principles (see paragraph 4.5)
- Restrictions on onward transfers outside of the group of companies (see paragraph 6.2)
- National legislation preventing respect of BCR (see paragraph 6.3)
- Right to complain through the internal complaint mechanism (see paragraph 4.4)
- Cooperation duties with Data Protection Authority (see paragraph 5.6)
- Liability and jurisdiction provisions (see paragraphs 5.3 and 5.4)

5.3. LIABILITY

Either the Local Data Importer or the Local Data Exporter shall be liable for any breach of the BCRs, under the following conditions:

1. In cases involving allegations of breach by the Local Data importer, the Data Subject shall first request the Local Data Exporter to take appropriate action to enforce his rights against the Local Data importer. If the Local Data Exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the Data Subject may then enforce his rights against the Local Data Importer directly. A Data Subject shall also be entitled to proceed directly against a Local Data Exporter that has failed to use reasonable efforts to determine that the Local Data Importer is able to satisfy its obligations under the BCRs. Both Local Data Exporter and Local Data Importer shall agree to take necessary actions to remedy and to pay compensation for actual damages they may be recognized liable for. Both Local Data Exporter and Local Data Importer shall have therefore sufficient financial resources at their disposal to cover the payment of compensation for breach of the BCRs. Liability as between the parties shall be limited to actual damage suffered. Indirect or punitive damages shall be specifically excluded.

2. The burden of proof shall stay with the Local Data Exporter to demonstrate that the entity of SOPRA HR SOFTWARE outside the EEA is not liable for the violation resulting in the damages claimed by the Data Subject. The Local Data Exporter shall also have the burden to prove that it took reasonable efforts to determine that the Local Data Importer is able to satisfy its obligations under the BCRs. Either the Local Data Importer or the Local Data Exporter may be exempted from any liability, in whole or in part, if it is proved that they are not responsible for the event giving rise to the damage or that the Local Data Exporter took reasonable efforts to determine that the Local Data Importer is able to satisfy its obligations under the BCRs.

3. If a violation of the BCRs is established, any correction measure (legal, technical or organizational measure) as well as any appropriate sanction (against the Local Data Controller or, according to local labor law, a local employee) shall be taken on the initiative of the Head Controller, the EMEA Data Privacy Manager, the Local Data Controller or the Local Data Privacy Manager.

5.4. JURISDICTION

1. Each Data Subject shall have the right to take its case, at its best convenience, to the supervisory authority in the Member State of his habitual residence, place of work or the place where the violation was committed (in accordance with Article 77 of the GDPR) or in the competent court of the Member

States of the EU at the choice of the relevant parent before the courts or the data exporter has an establishment or the one in which the data subject has his habitual residence (Article 79 of the GDPR)

2. According to the relevant provisions in paragraph 5.3, each Data Subject who has suffered damage shall be entitled to receive compensation (e.g. judicial remedies), provided that the internal complaint mechanism failed to settle the case (see paragraph 4.4) when applicable.

3. The BCRs shall always be readily available to every Data Subject, in the conditions described in paragraph 4.1. Furthermore, a Data Subject shall always be able to obtain, upon request, a copy of the BCRs from the Local Data Privacy Manager, the Local Data Controller, the EMEA Data Privacy Manager.

5.5. SANCTIONS

Would a violation of the BCRs, either by Local Data Controller representatives or employees, be established, any appropriate disciplinary sanction or judicial action may occur, in accordance with local labor law, on the initiative of the Head Controller, the EMEA Data Privacy Manager, the Local Data Controller or the Local Data Privacy Manager.

Thus, each Local Data Controller and Local Data Privacy Manager shall pay specific attention to any audit results (see paragraph 4.7) establishing non-compliance issues against representatives or employees, especially in case of:

- non compliance with the Data Protection Principles set out in paragraph 2.2 and Appendix 2;
- non compliance with guidelines or procedures relating to the exercise of the rights specified in paragraph 4.1, 4.2 and 4.4 (information, access, rectification, erasure, blocking and internal complaint rights, rights of object to the processing, rights of Restriction of processing, and the right to data portability,);
- non compliance with security policies designed to implement appropriate technical and organizational measures to protect Personal Data;
- non compliance with training programs designed to raise employee's awareness on Data Protection issues.

5.6. MUTUAL ASSISTANCE AND COOPERATION WITH DATA PROTECTION AUTHORITIES

All SOPRA HR SOFTWARE entities are committed to a full cooperation with the EEA data protection authorities who have competent jurisdiction. Thus:

- The relevant Data Protection Authorities shall receive, upon request, an update copy of the BCRs or all related procedures, policies or guidelines.
- The Local Data Controller shall reply within a reasonable period of time to any request addressed by a relevant Data Protection Authority with competent jurisdiction, including audit requests.
- The Local Data Controller shall apply any relevant recommendation or advice from a relevant Data Protection Authority relating to the implementation of the BCRs.
- The Local Data Controller shall abide by a decision of a relevant Data Protection Authority with competent jurisdiction, related to the implementation of the BCRs, against which no further appeal is possible before competent courts.
- The EMEA Data Privacy Manager shall be at the disposal of the relevant Data Protection Authorities for any matter related to the implementation of the BCRs.

Furthermore, members of SOPRA HR SOFTWARE shall cooperate and assist each other to handle a request or complaint from an individual (see paragraph 4.4) or inquiry by Data Protection Authorities.

6. FINAL PROVISIONS

6.1. RELATIONSHIP BETWEEN NATIONAL LAWS AND THE BCRs

SOPRA HR SOFTWARE undertakes that appropriate entities and employees of SOPRA HR SOFTWARE shall comply with the provisions of the BCRs, as well as with the provision of the Regulation (EU) 2016/679 (General Data Protection Regulation)

Where the local legislation requires a higher level of protection for Personal Data, it always will take precedence over the BCRs.

6.2. RESTRICTIONS ON TRANSFERS AND ONWARD TRANSFERS TO EXTERNAL PROCESSORS AND CONTROLLERS

Where a Local Data Controller requests that a non-SOPRA HR SOFTWARE entity undertakes Processing of Personal Data, the following safeguards shall be followed:

1. External Processors located inside the EEA or in a country recognized by the EU Commission as ensuring an adequate level of protection shall be bound by a written agreement stipulating that the Processor shall act only on instructions from the controller and shall be responsible for the implementation of the adequate security and confidentiality measures (see paragraph 4.5). Local Data Privacy Managers, in coordination with the EMEA Data Privacy Manager, shall be able to provide templates of the appropriate clauses to a Local Data Controller within the Group.

2. All transfers of Personal Data to external controllers located out of the EEA must respect the European rules on transborder data flows, for instance by making use of the EU Standard Contractual Clauses approved by the EU Commission

3. All transfers of Personal Data to external Processors located out of the EEA must respect the rules relating to the Processors in addition to the rules on transborder data flows, for instance by making use of the EU Standard Contractual Clauses approved by the EU Commission.

6.3. ACTIONS IN CASE OF NATIONAL LEGISLATION PREVENTING RESPECT OF BCRs

Shall a Local Data Controller have reasons to believe that the legislation applicable to him prevents the company from fulfilling its obligations under the BCRs and has substantial effect on the guarantees provided by the rules, he will promptly inform the EMEA Data Privacy Manager (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

Where there shall be conflict between national law and the commitments in the BCRs, the Local Data Privacy Manager and the Local Data Controller, in coordination with the EMEA Data Privacy Manager, shall take a responsible decision on what action to take and will consult the competent Data Protection Authorities in case of doubt.

6.4. UPDATES OF THE BCRs

In case of, for instance, changes in laws or SOPRA HR SOFTWARE procedures, the terms of the BCRs may be updated on the initiative of the Head Controller, in coordination with the EMEA Data Privacy Manager.

Any substantial or non substantial update of the BCRs shall be recorded and kept by the EMEA Data Privacy Manager. The EMEA Data Privacy Manager keeps as well a fully updated list of the members of the Group. '

Any substantial or non substantial update will lead to the communication, to each entity of SOPRA HR SOFTWARE, of an updated version of the BCRs for signature purpose.

SOPRA HR SOFTWARE undertakes that appropriate information will be given, once a year, to the Data Subjects, the appropriate Local Data Controllers and the competent Data Protection Authorities about any substantial update.

No transfer shall be made to a new SOPRA HR SOFTWARE entity until this new entity is effectively bound by the BCR and can deliver compliance.

6.5. DEROGATIONS OF ARTICLE 49 of the Regulation (EU) 2016/679 (General Data Protection Regulation)

In accordance with article 49 of the Regulation (EU) 2016/679 (General Data Protection Regulation)and applicable local law, a transfer or a set of transfers of Personal Data to a third country which does not ensure an adequate level of protection may take place from a Local Data Controller on condition that :

- the Data Subject has given his consent unambiguously to the proposed transfer;
- the transfer is necessary for the performance of a contract between the Data Subject and the controller or the implementation of precontractual measures taken in response to the Data Subjects request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the controller and a third party ;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims;
- the transfer is necessary in order to protect the vital interests of the Data Subject;
- the transfer is made from a register which according to laws or regulations 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 legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

6.6. APPLICABLE LAW / JURISDICTION / TERMINATION / INTERPRETATION OF TERMS

The BCRs shall be adopted by the Head Controller, in coordination with the EMEA Data Privacy Manager.

The BCRs shall take effect on the date when each entity of SOPRA HR SOFTWARE signs this BCRs agreement and, as a consequence, is legally bound. Each entity of SOPRA HR SOFTWARE recognizes to be bound by the BCRs, from the date of signature of the BCRs agreement and without any other formalities, with respect to other SOPRA HR SOFTWARE entities already bound or about to be bound from the date of their signature, notwithstanding the date and place of signature of a BCRs agreement by each other entity of SOPRA HR SOFTWARE involved, and provided that the terms of the BCRs are strictly identical between each other. Except if an entity of SOPRA HR SOFTWARE is able to prove that the signed BCRs agreement is not strictly identical to the ones signed by other entities, it expressly and irrevocably disclaims challenging the evidence that it is bound by the terms of the BCRs.

in the event that a Local Data Controller would be found in substantial or persistent breach of the terms of the BCRs, the Head Controller may temporarily suspend the transfer of Personal Data until the breach is repaired. Should the breach not be repaired in due times, the Head Controller shall take the initiative to terminate the BCRs Agreement. In such a case, the Local Data Controller shall take every necessary step in order to respect the European rules on transborder data flows, for instance by making use of the EU Standard Contractual Clauses approved by the EU Commission.

The provisions of the BCRs shall be governed by the law of the EEA Member State in which the Local Data Exporter is located.

In accordance with paragraph 5.2 and 5.4, jurisdiction shall be attributed to the courts of the Local Data Importer or Local Data Exporter.

In case of contradiction between the BCRs and the appendixes, the BCR shall always prevail. In case of contradiction between the BCRs and other global or local policies, procedures or guidelines, the BCR shall always prevail. in case of contradiction or inconsistency, the terms of the BCRs shall always be interpreted and governed by the provisions of the Regulation (EU) 2016/679 (General Data Protection Regulation).

7. APPENDIXES

Appendix 1 - Definitions

Appendix 2 - Data Protection Principles

Appendix 3 - List of SOPRA HR SOFTWARE entities bound by the BCRs

Appendix 4 - Nature and purposes of the Personal Data, nature and purpose of the processing, the type of personal data and categories of data subjects being transferred within the scope of the BCRs

APPENDIX 1: DEFINITIONS

The terms and expressions used in the BCRs are defined in this Appendix, provided that these terms and expressions shall always be interpreted according to the Regulation (EU) 2016/679 (General Data Protection Regulation).

"**SOPRA HR SOFTWARE**" shall mean SOPRA HR SOFTWARE itself and/or any corporate entity of SOPRA HR SOFTWARE hold, directly or indirectly, by SOPRA HR SOFTWARE, according to article L. 233-3 of the French Commercial Code.

"**Head Controller**" shall mean SOPRA HR SOFTWARE Headquarters located in France which alone or jointly with others determines the purposes and means of the Processing of Personal Data and which is in charge of the formal adoption of BCRs to be implemented within SOPRA HR SOFTWARE.

"**Local Data Controller**" shall mean the legal entity of SOPRA HR SOFTWARE which alone or jointly with others determines the purposes and means of the Processing of Personal Data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

"**Local Data Exporter**" shall mean the legal entity of SOPRA HR SOFTWARE located within the EEA which transfers the Personal Data outside the EEA.

"**Local Data Importer**" shall mean the legal entity of SOPRA HR SOFTWARE located outside the EEA which agrees to receive from the Local Data Exporter Personal Data for further Processing.

"**Local Data Privacy Manager**" shall mean an experienced SOPRA HR SOFTWARE officer within a Local Data Controller who is responsible for managing business awareness and compliance with Applicable Data Protection Law and SOPRA HR SOFTWARE privacy policies, procedures and guidelines, especially the BCRs.

"**EMEA Data Privacy Manager**" shall mean the senior level manager who is responsible, within the Group at Global level, for managing business awareness and compliance with Applicable Data Protection Law and SOPRA HR SOFTWARE privacy policies, procedures and guidelines, especially the BCRs.

GDPR : Regulation (EU) 2016/679 (General Data Protection Regulation) for the treatment of the personal trainer and the self-circulation of the data, and abrogate the directive 95/46 / CE

"**Personal Data**": shall mean any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

"**Processing of Personal Data**" shall mean any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"**Processor**" shall mean a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the controller.

"**Recipient**" shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as Recipients.

"**Sensitive Data**" shall mean Personal Data revealing directly or indirectly the racial or ethnic origin, political, philosophical or religious opinions, trade union affiliation, or related to the health or sexual life of individuals.

"**Third Party**" shall mean any natural or legal person, public authority, agency or any other body other than the Data Subject, the controller, the Processor and the persons who, under the direct authority of the controller or the Processor, are authorized to process the data.

"**The Data Subject's Consent**" shall mean any freely given specific and informed indication of his wishes by which the Data Subject signifies his agreement to Personal Data relating to him being processed.

"**Applicable Data Protection Law**" shall mean the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the Processing of Personal Data applicable to a data controller in the EEA Member State in which the Local Data Exporter is established.

"**Technical and Organizational Security Measures**" shall mean measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

APPENDIX 2: DATA PROTECTION PRINCIPLES

Within the scope of the BCRs, any transfer of Personal Data to a third country which does not ensure an adequate level of protection shall always comply with the following data protection principles, set out by the Regulation (EU) 2016/679 (General Data Protection Regulation)..

LEGAL BASIS FOR PROCESSING PERSONAL DATA

Personal Data shall be processed only if:

- the Data Subject has unambiguously given his consent;
- 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;
- 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 or in a third party to whom the data is disclosed ;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the Data Subject which require protection.

LEGAL BASIS FOR PROCESSING SENSITIVE DATA

Sensitive Personal Data, especially Personal Data concerning health, shall be processed only if:

- the Data Subject has given his explicit consent to the processing of those Sensitive Data, except where the applicable laws prohibit it ;
- the processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards ;
- the processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his consent;
- the processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data is not disclosed to a third party without the consent of the Data Subjects;
- the processing relates to Sensitive Data which is manifestly made public by the Data Subject;
- the processing of Sensitive Data is necessary for the establishment, exercise or defense of legal claims ;

- the processing of the Sensitive Data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those Sensitive Data is processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

PURPOSE LIMITATION

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.

In accordance with the provisions of the Regulation (EU) 2016/679 (General Data Protection Regulation)., Sensitive Data shall only be provided with additional safeguards.

DATA QUALITY AND PROPORTIONALITY

Personal Data shall be processed fairly and lawfully.

Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; accurate and, where necessary, kept up to date. Every reasonable step shall be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for Personal Data stored for longer periods for historical, statistical or scientific use.

AUTOMATED INDIVIDUAL DECISIONS

Subject to local applicable law, every Data Subject has the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, reliability, conduct, etc.

APPENDIX 3: LIST OF THE SOPRA HR SOFTWARE ENTITIES BOUND BY THE BCRs

1. Local SOPRA HR SOFTWARE entities located within the EEA

WORLD

HEAD PROCESSOR	Sopra HR Software SAS
Form	Société par Actions Simplifiée
Registered address	PAE Les Glaisins 74940 Annecy-le-Vieux France
TVA communautaire	FR61519319651
Legal representative	Edgard DAHDAH
Group Data Privacy Manager	Eric Miroglio
Local Data Privacy Manager	Eric Miroglio

EUROPE

LOCAL DATA PROCESSOR	Sopra HR Software Limited
Form	Limited Liability
Registered address	30 Old Broad Street London EC2M 1RX United Kingdom
Local Data Privacy Manager	Alan Brennan

LOCAL DATA PROCESSOR	Sopra HR Software SPRL
Form	BVBA
Registered address	15-23 avenue Arnaud Fraiteurlaan 1050 Bruxelles Belgium
Local Data Privacy Manager	Julia Mateffi

LOCAL DATA PROCESSOR	Sopra HR Software SARL
Form	SARL
Registered address	8308 Capellen 89 E, Parc d'activités, Capellen Luxembourg
Local Data Privacy Manager	Julia Mateffi

LOCAL DATA PROCESSOR	Sopra HR Software GmbH
Form	GmbH
Registered address	Valoisplatz 2 26382 Wilhelmshaven Germany
Local Data Privacy Manager	Martin Junge

LOCAL DATA PROCESSOR	Sopra HR Software SRL
Form	SRL
Registered address	Assago, Strada Palazzo A7 4 cap 20090, frazione Milanofiori Italy
Local Data Privacy Manager	Pablo Roldan Jimenez

LOCAL DATA PROCESSOR	Sopra HR Software SLU
Form	Limited Liability
Registered address	Avenida de Manoteras 48 Planta 1 – Edificio B 28050 Madrid Spain
Local Data Privacy Manager	Pablo Roldan Jimenez

2. Local SOPRA HR SOFTWARE entities located outside the EEA

EUROPE

LOCAL DATA PROCESSOR	Sopra HR Software SARL
Form	société à responsabilité limitée
Registered address	18 avenue Louis Casaï 1209 Genève Switzerland
Local Data Privacy Manager	Eric Miroglio

AFRICA

LOCAL DATA PROCESSOR	Sopra HR Software SaRL
Form	SUARL société unipersonnelle à responsabilité limitée
Registered address	92, bd Anfa, Etage 6 20100 Casablanca Morocco
Local Data Privacy Manager	Zied Mokni

LOCAL DATA PROCESSOR	Sopra HR Software SaRL
Form	SARL société à responsabilité limité
Registered address	Immeuble Tunimara Rue du Lac Constance 1053 Les Berges du Lac Tunisia
Local Data Privacy Manager	Zied Mokni

APPENDIX 4: NATURE AND PURPOSES OF PERSONAL DATA Nature and purpose of the processing, the type of personal data and categories of data subjects BEING TRANFERRED WITHIN THE SCOPE OF THE BCRS

Nature and Purposes	Nature and categories of the data transferred
Customer*, prospects, partner and suppliers relationship management i.e. : - provide and charge for products or services purchase; - process electronic payments; - process electronic document exchange (e. g. dematerialized public bid); - provide customers with a more; - personalized level of service; - provide access to Sopra HR Software services (e.g. technical support system) and customers' own applications and environments; - conduct market research, customer satisfaction and quality assurance surveys, direct marketing and sales promotions ; - respond to any request from customer (information, claim, etc.); - organization of special events for clients; - suppliers management and payment; - administer general record keeping. * Sopra HR Software acting as data controller for the listed purposes	contact information (name, gender, home contact details, company, business title, date and place of birth, email, etc.); products or services purchased, location of the purchase, special requests made, observations about service preferences, etc.); billing details (amount of sells, credit card details, etc.); information provided regarding marketing preferences or in the course of participating in surveys or promotional offers.

Nature and Purposes	Nature and categories of the data transferred
Human Resource management i.e.: - payroll; - administrative management ; - management of careers and mobility; - organization of work; - training of employees; - management of the ICT equipment provided to the employees; - premises access control & video surveillance; - employees data for travel; - organizational charts and - employees directories; - health and retirement insurances.	identification data (corporate ID, name, sex, date and place of birth, nationality, professional contact, personal contact information, internal number, emergency contact, bank details, economic data for payroll, travel & expenses and taxes-, etc.); professional contact information (professional phone number, e-mall address, etc.); career information (date and condition of employment, changes in employment status, career simulation and development, disciplinary sanctions, professional evaluation, training performed, performance assessment history, assessment of knowledge, etc.); travel data information (passport details); holiday and leave information; Pictures Family information (identification of children and spouses); For retirement plan, information about beneficiary (when different to the legal ones).

In accordance with the meta-data field and the description of the transfers covered by the Sopra Hr Software Group controller BCRs and their appendices, personal data relating to the following categories of persons(described below) may be transferred for the purposes (described above):

- Employees and similar (former employees, candidates, trainees and temporary workers)
- customers (current or potential)
- partners
- providers