Data Processing Agreement ("DPA")

Contractual Clauses for the Subcontracting of Personal Data Processing

According to regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, and repealing Directive 95/46/EC - General Data Protection Regulation), the Parties have agreed as follow.

1. PURPOSE

In the course of the performance of the Services, the Supplier will have access to or will be provided by the Client, its affiliated companies, subsidiaries and holding company, with certain Personal Data which the Supplier will need to Process on behalf of the Client as specified in Clause 4. To ensure that all Personal Data at all times is processed in accordance with Data Protection laws, the Parties have agreed to execute this Data Processing Agreement, including its appendices (the “DPA”).

This DPA forms part and incorporates the terms of the Agreement. To the extent that the terms contained in this DPA conflict or are inconsistent with those terms relating to the same subject matter contained in the Agreement, the terms contained in this DPA shall prevail. Except as modified below, the terms of the Agreement shall remain in full force and effect.

2. DEFINITIONS

Capitalised terms used but not defined in this DPA shall have the meaning set forth in the Agreement. The following terms have the following meanings when used in this DPA:

Data Protection Laws means the General Data Protection Regulation (EU 2016/679) (GDPR), the Directive on privacy and electronic communications (2002/58/EC) and any other applicable laws, including any implementing national laws, any regulatory requirements, guidance and codes of practice applicable to the processing or Personal Data (as amended or replaced from time to time) in the various countries involved in the Services.

Personal Data, Process or Processing, Data Subjects, Data Controller (or Controller) and Data Processor (or Processor) have the meaning given to those terms under Data Protection Laws.

3. OBLIGATIONS

The Parties shall comply with the requirements of Data Protection Laws in respect of the provision of the services and otherwise in connection with this DPA and shall not knowingly do anything or permit anything to be done which might lead to a breach of Data Protection Laws.

Without prejudice to clause above, the Supplier shall in respect of the Processing of the Personal Data:

- Process the Personal Data only for the purposes of and in compliance with the terms set out in the Agreement and this DPA and on written instructions and directions received from the Client and comply promptly with all such instructions and directions received from the Client from time to time;
- immediately notify the Client if, in the the Supplier's reasonable opinion, any instruction or direction from the Client infringes the Data Protection Laws;
- not Process the Personal Data or permit it to be processed or access, in whole or in part, other than for the provision of the Services and only to the extent reasonably necessary for the performance of this DPA;
- Process the Personal Data in accordance with the specified duration, purpose, type and categories of Data Subjects as set out in Appendix 1 hereof (Particulars of the Data Processing);
- not copy, export or extract any Personal Data in any manner except as necessary to perform the Services and ensure full compliance of this obligation by its representatives and potential sub-processor, as defined under this DPA;
- taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the company and its affiliates shall in relation to Client Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.
- ensure full compliance with any complementary technical and organizational measures required from the Client;
- keep the Personal Data confidential, and not disclose, in whole or in part, the Personal Data to any person or entity, except to its employees:
    - on a need-to-know basis and only as necessary for the performance of the Services;
    - who are duly authorized to this effect as a result of their position and qualification and bound by obligations equivalent to those set out under this Clause;
    - who have received appropriate training about the Data Protection Laws concerning the handling of Personal Data;
    - who are informed of the confidentiality nature of the Personal Data; and

- who are subject to a duty of confidence .

- notify the Client without undue delay of becoming aware, of any actual or suspected accidental, unlawful or unauthorized access, loss and/or destruction of the Personal Data ("Personal Data Breach") in writing, with such notice to include all relevant details of the breach including (i) the time and nature of the incident, (ii) the affected system, the number of Data Subjects affected, the categories of Personal Data affected, (iii) the likely consequences of the Personal Data Breach, (iv) the name and contact details of the data protection officer or other point of contact at the Supplier where more information can be obtained and (v) the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate possible adverse effects of the Personal Data Breach. the Supplier shall reasonably co-operate and assist the Client with any investigation regarding the Personal Data Breach, including with the Client's notification obligations as mandated under Data Protection Laws. and take all reasonable measures to limit further unauthorized disclosure of or unauthorized Processing of Personal Data in connection with the Personal Data Breach. the Supplier shall further assist the Client to comply with its obligation to document any Personal Data Breach by performing a root cause analysis immediately upon becoming aware of such Personal Data Breach and sharing the outcome of such analysis with the Client;

- deal promptly and properly with all enquiries from the Client relating to its Processing of the Personal Data;

- reasonably assist the Client in conducting any required privacy impact assessment upon request from the Client, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the Supplier ;

- implement privacy by design and privacy by default principles in relation to the tools and applications the company uses to provide the Services;

- implement and maintain a complete and updated record of Processing activities of the Personal Data in accordance with the Data Protection Laws. the Supplier will provide the Client a copy of such record upon Client 's request; reasonably assist the Client promptly for any exercise of Data Subjects' rights and cooperate with and support the Client in fulfilling its obligations as Data Controller in relation to such Data Subject requests at all times; assistance is limited to 1 (one) man-day, above this duration the Supplier shall charge the Client based on agreed fees.

- to the extent permitted by applicable law, notify the Client promptly upon receipt of any request from government office or other administrative body, or law enforcement authority, court order to disclose any of the Personal Data, including the basis for the requirement, the scope of the disclosure and to whom the Personal Data must be disclosed;

- the Supplier shall select any such sub-processor with due diligence, and verify whether the sub-processor is able to comply with their obligations under Data Protection Laws in relation to the Processing of Personal Data. Furthermore, the Supplier shall:

  - procure that sub-processors enter into written agreements with the Supplier which contain terms no less onerous than the terms set out under this DPA; and.

  - remain fully liable to the Client for the performance of the sub-processor's obligations under Data Protection Laws or for any acts or omissions of any sub-processors.

- In case of any intended changes concerning the addition or replacement of sub-processors, the Supplier shall inform the Client in advance, thereby giving the Client an opportunity to object based on reasonable grounds to such Processing of Personal Data.

- make available, upon Client's reasonable request, all information necessary to demonstrate compliance with their obligations under this DPA and with Data Protection Laws and allow for and contribute to audits, including inspections, conducted by the Client or another auditor as mandated by the Client who will have entered into a confidentiality undertaking covering the audit at any time. the Client shall therefore be entitled to enter the premises of the Supplier in order to perform inspections and audits. the Supplier shall grant to the Client all access rights and information required to perform such audits; provided, however, that information and audit rights only arise to the extent that the audit conducted under section 16 of the Agreement does not meet the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR);

4. SUB-PROCESSING

- The Client authorizes the Supplier to appoint new Processors to assist the Supplier with the performance of its obligations under the Agreement. Prior to giving any Processor access to Personal Data, the Supplier shall: (i) notify the Client by email; and (ii) ensure that such Sub-processor has entered into a written agreement with the Supplier requiring that the Sub-processor abide by terms no less protective than those provided in this Agreement, including terms sufficient to meet the requirements of Article 28(3) of the GDPR. As between the Client and the Supplier, the Supplier shall remain fully liable for all acts or omissions of any third-party Sub-processor appointed by it pursuant to this Agreement. If the Client has a reasonable basis to object to the use of any Sub-processor, the Client shall notify the Supplier. In the event the Client objects to a Sub-processor, the Supplier will make available a change in the Services or use of the affected Services to avoid Processing of Personal Data by the objected to Sub-processor. Any such change will be subject to prior agreement by the Client, such agreement not to be unreasonably denied or delayed. If the Supplier is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, the Client may terminate those Services which cannot be provided by the Supplier without the use of the objected to Sub-processor, by providing written notice. Such termination shall be without penalty to the Client, and where the Client has prepaid for such Services, the Client shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Services.

- The detailed list, of the Supplier's sub-processors providing data processing relevant services is available on the following link : https://www.aragoconsulting.eu/wp-content/uploads/2015/12/ARAGO-Consulting-Affiliates-and-sub-processors.pdf. It can be updated when required in accordance with required notification defined in article 5.

5. USE OF THE EU STANDARD CONTRACTUAL CLAUSES FOR INTERNATIONAL TRANSFERS

- To avoid the need for each of the Client affiliates, as data exporters, to enter into separate bilateral agreements with the Supplier, as data importer, this Agreement which the Client enters into on its own behalf and on behalf of the Client affiliates shall be deemed to constitute an agreement between each of the Client affiliates (each such the Client affiliate being a data exporter) and the Supplier, as data importer, on the terms of this Agreement.
- The Parties agree that each and every transfer of Personal Data from any one or more of the Client Affiliates, as data exporters to the Supplier as data importer, in each case, where such transfer would be prohibited by Data Protection Laws in the absence of the Standard Contractual Clauses, shall be subject to the terms of the Standard Contractual Clauses.
- This Agreement also shall apply with respect to transfers of Personal Data by non-European Client affiliates (as data exporters) if and to the extent the Standard Contractual Clauses are sufficient to satisfy the relevant local requirements.
- For the avoidance of doubt a transfer of Personal Data shall be deemed to occur if the Supplier accesses Personal Data of any Client affiliate by any means, including but not limited to electronic means notwithstanding that the physical location of the data does not change and that the Supplier does not obtain possession of such Personal Data.
- The Parties agree that the Client may amend the list of data exporters from time to time, notably by adding or removing any of its affiliates, by informing the Supplier.
- the Client will be entitled, for and on behalf of the Client affiliates, to enforce this Agreement. the Client will use commercially reasonable efforts to ensure that any claims that the Client affiliates may have under this Agreement against the Supplier are assigned by the Client affiliates to the Client, and the Client agrees that such claims may be so assigned.

6. APPLICATION OF STANDARD CONTRACTUAL CLAUSES

- This Agreement incorporates by reference the Standard Contractual Clauses.
- The Standard Contractual Clauses apply to all Personal Data, in particular Personal Data relating to the Client's employees, users, customers, vendors or other individuals in connection with the Agreement, that is transferred from or accessed remotely from outside the EEA, Switzerland or any country whose laws require an adequacy means for such international transfer or access and the required adequacy means can be met by entering into the Standard Contractual Clauses, either directly or via onward transfer to any country or recipient, in each case, where such transfer or access would be prohibited by Data Protection Laws in the absence of the Standard Contractual Clauses.
- The Standard Contractual Clauses apply to:
    - the Client affiliates listed in Appendix 4, each as a data exporter;
    - the Supplier, as a data importer; and
    - any other person, including Supplier Affiliates and subcontractors of the Supplier that have access to Personal Data in the course of providing any Services under the Agreement, each as Sub-processor.
- For the purposes of Clause 5(a) of the Standard Contractual Clauses, the Services provided under the Agreement set out the Processing instructions of each respective data exporter to the Supplier as data importer for the Processing of Personal Data. The Client, in its sole discretion, may provide additional or alternate instructions for the Processing of Personal Data under its control.
- The Parties agree that the copies of the Sub-processor agreements that must be sent by the Supplier to the Client pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercially sensitive or confidential information redacted.
- In relation to each transfer of Personal Data from a data exporter listed in Appendix 2 to the Supplier, as data importer, and for the purposes of Clause 9 (Governing Law) of the Standard Contractual Clauses, any dispute or claim arising out of or in connection with its interpretation shall be governed by the national law of the respective data exporter.
- The Supplier shall, upon reasonable request, make available to the Client a list of all Sub-processors currently providing Services under the Agreement, and make available for inspection all agreements with such Sub-processors as required under Clause 11(1) of the Standard Contractual Clauses. The Client shall bear its own costs in relation to such audit and inspection, unless a discrepancy is identified, in which case the cost of such audit and inspection shall be borne by the Supplier.
- The Standard Contractual Clauses shall be interpreted in light of the provisions of this Agreement. In the event of any conflict or inconsistency between this Agreement and the Standard Contractual Clauses, the following order of precedence shall apply:
    - the Standard Contractual Clauses;
    - this Agreement.
- Notwithstanding the foregoing, each Party shall promptly, on request from a national data protection authority, do all things necessary including executing such further documents and/or completing such further formalities (whether in the form of authorisation, registration or otherwise) as may be necessary to give effect to this Agreement and/or comply with applicable laws.

7. STANDARD CONTRACTUAL CLAUSES

For the specific purpose of providing the Services, Client authorizes Services Provider to transfer, if it is strictly necessary for the provision of the Services, the Client Personal Data to India, Morocco and Colombia where Services Provider's Affiliates providing Services for Client are located. To this end, the Parties agree that the EU Standard Contractual Clauses for the transfer of personal data to third countries of 4 June 2021 ("**EU SCC**") will apply in respect of that transfer of Client Personal Data as follows:

- Services Provider's Affiliates described in Appendix 4 will comply with the obligations of the "data importer" in the EU SCC and Client will comply with the obligations of "data exporter,
- When the Client acts as Data Controller and the Services Provider's Affiliates as Data Processor, the Module Two of the EU SCC will apply. When the Client acts as Data Processor and the Services Provider's Affiliates as Sub-Data Processor, the Module Three of the EU SCC will apply,
- in Clause 7 the optional docking clause applies,
- in Clause 9, Option 1 "SPECIFIC PRIOR AUTHORISATION" applies and the request for specific authorisation shall be submitted at least sixty (60) days prior to the engagement of the rank 2 Processor,
- in Clauses 17 and 18, the Parties agree that the governing law and forum for disputes for the EU SCC will be the French law and the courts of France,
- the Annexes of the EU SCC will be deemed completed with the information set out in Appendix 4,
- if and to the extent the EU SCC conflict with any provision of this DPA, the EU SCC will prevail to the extent of such conflict.

8. RETURN AND DESTRUCTION OF THE PERSONAL DATA

Except to the extent prohibited by applicable law, at the Client's written request at any time, the company and the authorized sub-processor (if any) shall promptly return all Personal Data as well as authorized copies (if any) of the Personal Data, including extracts or other reproductions (if any), whether in written, electronic or other readable and processable format or media, to the Client;

except to the extent prohibited by applicable law, upon termination of retention periods as defined by the Client for each category of Personal Data or upon termination or expiration of the Agreement, the Supplier shall securely delete, remove and destroy all Personal Data processed on behalf of the Client as well as authorized copies (if any) of the Personal Data, including extracts, backups or other reproductions (if any), whether in written, electronic or other form or media, except where necessary to retain such Personal Data strictly for the purposes of compliance with applicable law. the Supplier shall certify in writing to the Client that the Personal Data has been securely destroyed.

Notwithstanding the termination or expiry of the Agreement, the obligations of this DPA shall remain valid until return or complete destruction, deletion and removal of the Personal Data as set out in this Clause.

9. THE DATA PROTECTION OFFICER

The processor communicates to the controller the name and contact details of its data protection officer, if it has designated one in accordance with Article 37 of the GDPR.

He can be contacted at: David SAADA – dpo@aragoconsulting.com

10. CONTROLLER'S OBLIGATIONS WITH RESPECT TO THE PROCESSOR

The controller undertakes to:

1. provide the Processor with the data mentioned in the Appendix 1 Particulars of the Data Processing,
2. document, in writing, any instruction bearing on the processing of data by the processor,
3. ensure, before and throughout the processing, compliance with the obligations set out in the General Data Protection Regulation on the processor's part.,

Appendix 1 Particulars of the Data Processing

SUBJECT-MATTER OF THE PROCESSING

Technical assistance on parametrization, support and data load operation related to SAP Concur

CATEGORIES OF PERSONAL DATA TRANSFERRED

Identification data, Data related to professional life and Logs data

DURATION OF THE PROCESSING

Processing shall not to exceed the term of the Agreement and retention periods as defined by the Client. Especially, Personal Data of Client's employees shall not be processed upon termination of 6 months period further to labour agreement's termination.

NATURE AND PURPOSE OF THE PROCESSING

Collection, recording, structuring, organization, storage, retrieval, consultation, use, dissemination or otherwise making available and erasure or destruction and in particular: incident, service request, problem, change, enhancement actions or project works.

TYPE OF PERSONAL DATA

Identification data, data relating to professional life and registration data

The categories of personal data concerned are as follows:

Expense module:

- Surname, first name, identity card, e-mail address, country of residence
- Personal or business vehicle registration

Travel module:

- - Travel details (place, location, departure date, arrival date)
- - Personal address
- - Loyalty card
- - Identity card
- - Travel preferences

CATEGORIES OF DATA SUBJECTS

Client's employees and external contractors.

AUTHORIZED SUB-PROCESSORS:

All sub-processors set forth in Appendix 2

APPENDIX 2 - Current Sub-processors

Name	legal details	Nature of subcontracted Personal Data Processing activities	Localization of subcontracted Personal Data Processing activities	Transfer mechanism if applicable
ARAGO Consulting LATAM Carrera 28D Nº 67B-30, Officinas 204 - 205, 170004 – Manizales, Caldas Colombia	NIT : 901010948-8	Support services for the SAP Concur	Colombia	Through SAP cloud services
Arago Consulting Iberia LDA, Rua Engº Ferreira Dias, 924, Piso 1, 22/23, 4100-246 Porto Registre du Commerce de Braga Portugal	514 134 305	Support services for the SAP Concur	Portugal	Through SAP cloud services
Arago Consulting SARL Route de Pré-Bois, 29 Case Postale 1215 Genève Switzerland	Numéro federal: CH-660.0.142.014-3	Support services for the SAP Concur	Switzerland	Through SAP cloud services
Company Consulting Minds LLP JAL 1304, UNICCA EMPORIS Apartments, Sorahunase, Varthur Main Road, Varthur Hobli, Bengaluru – 560087 Karnataka India	CIN AAY-1095	Support services for the SAP Concur	India	Through SAP cloud services
ARAGO CONSULTING ESPAÑA, S.L. Calle Puerto 14, 5-5, 29016, Malaga, España	ID : B19328145	Support services for the SAP Concur	Spain	Through SAP cloud services
ACAFRICA Florida Center Park Lot 9, N 28, Etage 4 Sidi Maarouf, Casablanca Morocco	ID : 433937	Support services for the SAP Concur	Morroco	Through SAP cloud services
ARCODE ArCoDe GMBH Königsallee 92a Düsseldorf Germany	HRB115801	Support services for the SAP Concur	Germany	Through SAP cloud services
Arago Consulting Belgium BV Leonardo Da Vincilaan 19A bus 8 1831 Diegem Belgium	BE0768.826.354	Support services for the SAP Concur	Belgium	Through SAP cloud services

APPENDIX 3 - Technical and Organizational measures

Below measures shall be completed by the Supplier (the "Service Provider") in order to ensure compliance with Data protection Laws, and especially with article 28 and 32 of the GDPR.

The Service Supplier is aware of the confidentiality or criticality (in terms of integrity or availability) of a significant part of the information of the Client hosted or processed in the context of the Agreement and the Services and ensure that it has in place, and shall maintain for the duration of the DPA or the destruction of Personal Data, whichever is later, all necessary or appropriate technical and organizational measures, taking into account the nature and volume of Personal Data.

The scope of these confidential or critical information include but is not limited to Personal Data.

For this reason, the Service Supplier undertakes to apply, maintain and update at all times safety practices at least equal to those commonly accepted in the field in view of the risks considered for The Client. The Service Supplier also undertakes to implement an information security governance in line with the ISO27000 family standards, covering the entire human, functional and technical scope of the Contract.

In particular, the Service Supplier undertakes to:

- protect the integrity, availability, resilience, confidentiality, and security of all Personal Data,
- protect the Personal Data against accidental or unlawful destruction, damage, or loss, alteration, or unauthorized disclosure or access ,
- pseudonymize and encrypt Personal Data as appropriate, and
- provide a level of security appropriate to the risk represented by the Processing and the nature of the Personal Data to be protected as required under Data Protection Laws ;
- comply with the Information Security Policies, Procedures and Standards that the Client brings to its attention, being aware that these requirements are likely to evolve over time, particularly in the light of changes in regulations, threats and risks, the business and technical context of The Client;
- notify the Client without delay of any difficulty in applying these Policies, Procedures and Standards, so that the Service Supplier and the Client jointly define an acceptable means of dealing with such a difficulty;
- inform, advise and warn without delay the Client when the Service Supplier identifies a risk for the Client in terms of information security, and even more so an incident involving the confidentiality, integrity or availability of the data and the information process of The Client.

These commitments apply to all information security needs of The Client, whether personal data or not.

The service provider enables the Client to carry out an effective security audit implemented on its scope and undertakes to support the successful completion of this audit without financial compensation. This audit may involve the submission of documentary evidence or technical or on-site verifications. It takes place at most once a year at the request of the the Client and may also be required without limitation of occurrence in the event of an event likely to give rise to a serious doubt about the correspondence between the security implemented and the perceived risks.

Controls

THE CLIENT DATA ACCESS AND MANAGEMENT

- Supplier Staff access to the Client environment using nominative and dedicated account to ensure traceability.
- Supplier Staff do not have access to unencrypted Client Data unless the Client authorized it. If such access is granted, Supplier Staff are prohibited from storing unencrypted Client Data on local desktops, laptops, mobile devices, shared drives, removable media such as USB drives, or on public facing systems that do not fall under the administrative control or compliance monitoring processes of Provider.
- Supplier uses Client Data only as necessary to provide services to the Client, as provided in the Agreement/Contract.

ENCRYPTION AND LOGICAL SEPARATION OF THE CLIENT DATA

The Service in the production storage environment always encrypts the Client Data while at rest with state-of-the-art encryption protocol such as AES 256-bit.

The Service encrypts traffic with state-of-the-art encryption protocol like Transport Layer Security ("TLS") 1.2, when communicating across untrusted networks such as the public internet.

SERVICE GENERAL INFRASTRUCTURE SECURITY MANAGEMENT

Access to the systems and infrastructure that support the Service is restricted to Supplier Personnel who require such access as part of their job responsibilities.

Unique User IDs are assigned to Supplier Personnel requiring access to the Supplier servers that support the Service.

Password policy for the Service in the production environment adheres to the Client password requirements (or equivalent).

Access privileges of separated Supplier Personnel are disabled promptly. Access privileges of persons transferring to jobs requiring reduced privileges are adjusted accordingly.

All user access to the systems and infrastructure that support the Service is reviewed regularly at least two times in a year.

Access attempts to the systems and infrastructure that support the Service are logged, monitored, and alerted for suspicious activities.

RISK MANAGEMENT

Provider's Risk Management process is trusted and based on a well-known model.

Supplier conducts risk assessments of various kinds throughout the year, including self assessments and tests, automated scans, and manual reviews.

Changes to controls and threat mitigation strategies are evaluated and prioritized for implementation on a risk adjusted basis.

Threats are monitored through various means, including threat intelligence services, vendor notifications, and trusted public sources.

VULNERABILITY SCANNING AND PENETRATION TESTING

Each workstation or IT infrastructure is subject to regular patch management.

REMOTE ACCESS & WIRELESS NETWORK

Supplier corporate offices, including LAN and Wi-Fi networks in those offices, are considered as untrusted networks.

SYSTEM EVENT LOGGING, MONITORING & ALERTING

Monitoring tools and services are used to monitor systems including network, server events, and Cloud Supplier API security events, availability events, and resource utilization.

All Supplier endpoints have Endpoint Protection tools to monitor and alert for suspicious activities and potential malware.

All Cloud Private Networks leverage advanced threat detection tools to monitor and alert for suspicious activities and potential malware.

SYSTEM ADMINISTRATION AND PATCH MANAGEMENT

Supplier shall create, implement, and maintain system administration procedures for systems that access the Client Data that meet or exceed industry standards. It includes without limitation, system hardening, system and device patching (operating system and applications), and proper installation of threat detection software as well as daily signature updates of same.

Supplier Security team reviews vulnerabilities announcements weekly and assess their impact to Supplier based on a Provider-defined risk criteria, including applicability and severity.

Applicable security updates rated as "high" or "critical" are addressed within 30 days of the patch release and those rated as "medium" are addressed within 90 days of the patch release.

Supplier solution shall support any security updates that apply on systems where its solution is installed.

SECURITY TRAINING AND PERSONNEL

All Supplier Personnel acknowledge they are responsible for reporting actual or suspected security incidents or concerns, thefts, breaches, losses, and unauthorized disclosures of or access to the Client Data.

All Supplier Personnel are required to satisfactorily complete regularly security training.

Supplier will ensure that its subcontractors, vendors, and other third parties (if any) that have direct access to the Client Data in connection with the services adhere to data security standards consistent with the Client requirements.

PHYSICAL SECURITY

When concerned, all physical security controls are managed by the Supplier or its Cloud Provider. Supplier reviews best practices annually to ensure appropriate physical security controls, including:

- Visitor management including tracking and monitoring physical access.
- Physical access point to server locations are managed by electronic access control devices.
- Monitor and alarm response procedures.

NOTIFICATION OF SECURITY BREACH

"Security Breach" is (a) the unauthorized access to or disclosure of the Client Data, or (b) the unauthorized access to the systems within the Service that transmit or analyze the Client Data.

- Supplier will notify the Client in writing within seventy-two (72) hours of a confirmed Security Breach.
- Such notification will describe the Security Breach and the status of Provider's investigation.
- Supplier will take appropriate actions to contain, investigate, and mitigate the Security Breach.

APPENDIX 4

LIST OF PARTIES subject to Standard Contractual Clauses

Data exporter(s):

1. Name: *The Client as described in the DPA*

   Address: *See the DPA*

   Contact person's name, position and contact details: *See the DPA*

   Activities relevant to the data transferred under these Clauses: *performance of the Services pursuant to the Agreement.*

   Signature and date: *See the DPA*

   Role: *Controller or Data Processor as described in article 18 of the DPA*

Data importer(s):

1. Name: *ARAGO Consulting LATAM*

   Address: *Carrera 28D Nº 67B-30, Officinas 204 - 205, 170004 – Manizales, Caldas - Colombia*

   Contact person's name, position and contact details: *Mr Mikael TUITEL managing Director*

   Activities relevant to the data transferred under these Clauses: *The data importer is a human resources solution implementation company, specialized in SAP SuccessFactors and Concur cloud services, providing services around solution implementation and application maintenance services.*

   Role (controller/processor): *Data Processor or Sub Data Processor as described in article 18 of the DPA*

   Signature and date: *See the DPA*

2. Name: *Company Consulting Minds LLP*

   Address: *JAL 1304, UNICCA EMPORIS, Varthur Hobli, Bangalore – 560087, Karnataka, India*

   Contact person's name, position and contact details: *Mr Pradeep VUDDANDI managing Director*

   Activities relevant to the data transferred under these Clauses: *The data importer is a human resources solution implementation company, specialized in SAP SuccessFactors and Concur cloud services, providing services around solution implementation and application maintenance services.*

   Role (controller/processor): *Data Processor or Sub Data Processor as described in article 18 of the DPA*

   Signature and date: *See the DPA*

3. Name: *ARAGO Consulting Africa (ACAfrica)*

   Address: *Casablanca Nearshore - 1100, Bld Al Quods, Shore 1, - 20270, Casablanca, Maroc*

   Contact person's name, position and contact details: *Mr Bouchta Toumani managing Director*

   Activities relevant to the data transferred under these Clauses: *The data importer is a human resources solution implementation company, specialized in SAP SuccessFactors and Concur cloud services, providing services around solution implementation and application maintenance services.*

   Role (controller/processor): *Data Processor or Sub Data Processor as described in article 18 of the DPA*

   Signature and date: *See the DPA*

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Employees and external contractors

Categories of personal data transferred

Identification data, Data related to professional life and Logs data

Processor Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

There is no sensitive data transferred

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Upon client request

Nature of the processing

Collection, recording, structuring, organization, storage, retrieval, consultation, use, dissemination or otherwise making available and erasure or destruction and in particular: incident, service request, problem, change, enhancement actions or project works.

Purpose(s) of the data transfer and further processing

Technical assistance on parametrization, support and data load operation related to SAP Concur

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Non retention unless on express request from the Client. In this specific case, the personal data will be retained for the duration of the request activity

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

N/A

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is the French Data Protection Authority: *the CNIL.*

D. Technical measures

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

All details contain in ARAGO Security and privacy policy