

## 1. SCOPE OF APPLICATION

1.1 This data protection and processing annex (the “DPA”) is a supplement to and operates under the provisions of the Partner Agreement and any contractual document, services and activities duly agreed and concluded thereunder, as applicable and as amended from time to time (collectively the “Agreement”), the terms of which shall fully apply hereto.

1.2 This DPA serves as a written data protection and processing agreement between IFS and Partner and shall apply for all purposes of any personal data exchanged or processed under the Agreement, as further set forth herein.

1.3 Except as expressly stated otherwise, in the event of any conflict between the terms of the Agreement and the terms of this DPA, the relevant terms of this DPA shall take precedence. The Standard Contractual Clauses (as defined below) shall have precedence over this DPA, in the case of any conflict.

1.4 If any provision of this DPA is found by any court of competent jurisdiction to be invalid or unenforceable, the invalidity of such provision shall not affect the other provisions hereof, and all provisions not affected by such invalidity shall remain in full force and effect.

1.5 This DPA shall be effective for the term of the Agreement and any agreed service or delivery under the Agreement to which this DPA applies.

1.6 For the purposes of this DPA, the following definitions shall apply.

- (a) “Data Protection Law” means the legislation protecting the fundamental rights and freedoms of persons and, in particular, their right to privacy, with regard to the processing of Personal Data under the Agreement, including but not limited to local applicable law and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation) (referred to herein as the “GDPR”).
- (b) Other defined terms used herein, including “Data Subject”, “Personal Data”, “Personal Data Breach”, “Process”, “Processing”, and “Processor”, shall have the meaning given to such terms under the applicable Data Protection Law.
- (c) “EU Personal Data” means the Processing of Personal Data to which Data Protection Law of the European Union, or of a Member State of the European Union or European Economic Area were applicable prior to its Processing hereunder.
- (d) “Swiss Personal Data” means the Processing of Personal Data to which the Swiss Federal Acts on Data Protection were applicable prior to its Processing hereunder.
- (e) “UK Personal Data” means the Processing of Personal Data to which Data Protection Law of the United Kingdom were applicable prior to its Processing hereunder.
- (f) “IFS Customer” means any IFS/IFS Affiliate end-client on whose behalf Partner Processes Personal Data in its capacity as subprocessor to IFS in connection with the Agreement.
- (g) “Standard Contractual Clauses” means:
  - (i) for EU Personal Data, the standard contractual clauses adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 including the relevant modules of such clauses, not including any clauses marked as optional, and as further described in Exhibit 3 of this DPA (“EU SCCs”);
  - (ii) for UK Personal Data, the International Data Transfer Addendum to the EU SCCs, issued by the Information Commissioner in accordance with s.119A of the UK Data Protection Act 2018 but, as permitted by clause 17 of such addendum, the Parties agree to change the format of the information set out in the addendum so that (i) the details of the parties in table 1 shall be as set out in Annex 1 of the EU SCCs (with no requirement for further signature); (ii) for the purposes of table 2, the addendum shall be appended to the EU SCCs (including the modules and optional clauses noted

below) and Exhibit 3 selects the option and timescales for clause 9; and (iii) the appendix information listed in table 3 shall be as set out in the Annexes to the EU SCCs ("UK SCCs"); and

(iii) for Swiss Personal Data, the EU SCCs.

## 2. IFS INFORMATION SECURITY STANDARD

2.1 IFS has developed an IFS Information Security Standard to govern information security standards for non-IFS staff having access to IFS's systems and data, as amended from time to time.

2.2 It is acknowledged that the compliance by Partner's staff and permitted subcontractors at all times with the IFS Information Security Standard is a prerequisite for IFS to grant access to such persons to IFS's systems and data. Partner undertakes to ensure and shall remain fully liable for the strict adherence of its staff and permitted subcontractors to the IFS Information Security Standard, and undertakes, and shall maintain written records to this effect, to duly inform its staff and permitted subcontractors of the requirements of the IFS Information Security Standard and that any non-compliance thereof may involve a denial of access to IFS's information systems and services.

2.3 Partner acknowledges that IFS as part of its regular business consistently seeks to streamline and improve its security measures and infrastructure and that its information security standards may be developed and improved accordingly. IFS reserves the right to revise the IFS Information Security Standard to reflect such development and improvement and will notify Partner of such revisions when released.

## 3. PARTNER'S GENERAL DATA PROTECTION OBLIGATIONS IN REGARDS OF DATA PROVIDED BY IFS UNDER THE AGREEMENT

3.1 Partner acknowledges that in connection with the Agreement, it may receive or gain access to information and data, including Personal Data from IFS or any IFS Affiliate, such as, but not limited to data relating to staff (e.g. contact details, qualifications, roles, user data, etc), data related to customers / prospects (contact details, user data, etc) and data relating to other parties relevant for the Agreement (e.g. suppliers, partners, contractors, sub-contractors or other contract parties or business associates).

3.2 IFS/IFS Affiliate shall, in its sole discretion, determine the scope and purpose for which it shall provide Personal Data to the Partner hereunder and the manner in which the Personal Data shall be Processed by Partner as permitted under the applicable Data Protection Law. In the absence of explicit documented instruction(s) from IFS/IFS Affiliate, Partner shall Process Personal Data from IFS hereunder for the sole purpose of the Agreement and only to the extent necessary to maintain the relationship, manage the Agreement and facilitate any agreed activities under the Agreement.

3.3 Where such Personal Data referenced in Clause 3.1 is received or accessed by Partner in connection with the Agreement, Partner shall, and shall ensure that its staff and subcontractors will, adhere to the obligations provided under Clause 4.1(a)-(j) in regards thereof.

3.4 IFS retains, as between the parties, all rights, title and interest in any Personal Data provided by it to Partner hereunder including any amendments or alterations thereto.

## 4. PARTNER'S OBLIGATIONS AS PROCESSOR OR SUBPROCESSOR OF IFS OR CUSTOMER CONTROLLED PERSONAL DATA

4.1 Where Partner Processes Personal Data in the capacity as a Processor (or subprocessor) on behalf of IFS, an IFS Affiliate or any IFS Customer (including Personal Data provided by the IFS Customer on behalf of third parties) hereunder, it is Partner's responsibility to ensure (on its behalf and on behalf of any permitted subprocessor) the following:

(a) to be and remain at all times in compliance with all applicable Data Protection Law in connection with the Agreement;

(b) to implement and maintain, observing the IFS Information Security Standard as referenced in Clause 2 above and using good industry standards and practices, appropriate technical and organisational measures to protect the Personal Data against, *inter alia*, unauthorised or unlawful Processing, accidental loss, destruction, damage, alteration or disclosure; these measures shall ensure a level of security appropriate to the risks present at the Processing of Personal Data as required by Applicable Data Protection Law including guidelines and practice of competent data protection authorities and courts;

(c) to Process the Personal Data only in accordance with the documented lawful instructions of IFS and solely to perform the agreed services or activities under the Agreement, and not to access, use, export out,

transfer or otherwise handle the Personal Data for any other purposes whatsoever, regardless of whether or not the Personal Data is converted to an anonymized and/or aggregated format, nor to modify the Personal Data except per the documented lawful instructions of IFS; if Partner deems any such instruction to be in non-compliance with the applicable Data Protection Law, it shall promptly inform IFS thereof;

- (d) to keep the Personal Data strictly confidential and take all necessary steps to ensure that the Data is not accessed without authorization and not lost, damaged, altered or disclosed;
- (e) to take all reasonable steps to ensure the reliability of staff who have access to the Personal Data and ensure that such access is limited to such authorised staff only who require access to the Personal Data for the purpose of the Agreement and who are contractually or by statutory obligation bound to maintain confidentiality and security of the Personal Data;
- (f) to not engage any subprocessors for any part of the Processing of Personal Data hereunder except with the prior written specific authorization and mandate of IFS in accordance with Clause 5 below;
- (g) to not transfer Personal Data outside of the European Economic Area except with the prior written specific authorization and mandate of IFS in accordance with Clause 6 below;
- (h) to promptly (where possible within 24 hours and otherwise as promptly as practicably possible taking into account the narrow reporting deadlines set forth in the applicable Data Protection Law) alert and inform IFS of any security incident or personal data breach (whether concerning Partner or any subprocessor) relating to the Processing hereunder (including, but not limited to, any suspected or actual unauthorised or unlawful Processing, loss of, damage to or destruction of the Personal Data) and provide to IFS all reasonable information, co-operation and assistance to enable IFS to comply with its obligations under applicable Data Protection Law and required for IFS to investigate, handle and mitigate the security incident or personal data breach and to reduce the impact thereof on IFS's (or the relevant data controller's) business operations and reputation; Partner shall not disclose any information to any third party concerning such security incident or personal data breach without the prior written authorisation of IFS;
- (i) upon IFS's reasonable written request or as otherwise required under the applicable Data Protection Law:
  - (1) provide to IFS all information necessary to demonstrate Partner's (and any subprocessor's) compliance with this DPA and the applicable Data Protection Law; and (ii) subject to customary confidentiality covenants, allow for and contribute to audits, including inspections, of Partner and any subprocessor to verify such compliance, to be conducted by IFS or another auditor mandated by IFS,
  - (2) assist IFS (or the relevant data controller) by appropriate technical and organizational measures, insofar as this is possible and to the extent reasonable, in complying with its obligation to respond to requests of Data Subjects (including requests for exercising Data Subjects' rights under the applicable Data Protection Law), and
  - (3) provide to IFS (or the relevant data controller) all other reasonable assistance and cooperation to support it in complying with its obligations as data controller under the applicable Data Protection Law in regards of, without limitation, requests, demands or orders from supervisory authorities, security of Processing, personal data breach notification and communication rules, data protection impact assessments and prior consultations; and
- (j) to notify IFS promptly if it is or is likely to become unable to comply with any of its obligations under this DPA or the applicable Data Protection Law.

4.2 A more comprehensive description of the nature and purpose of the Processing of Personal Data hereunder, as well as the type of Personal Data and the categories of Data Subjects, is set forth in Exhibit 1 hereto as applicable from time to time, which may be provided to Partner by IFS upon written request.

## 5. PARTNER'S SUBPROCESSORS

5.1 Partner shall be permitted to delegate the Processing of Personal Data hereunder to a subprocessor (i) only with the express prior written consent, authorization and mandate of IFS; and (ii) which is bound to comply with provisions relating to confidentiality and data protection no less stringent than the terms of this DPA; and (iii) provided that the Partner shall remain responsible for the conduct of any of its subprocessors as for its own conduct, including their observance of any data transfer agreements entered into with regards to Clause 8.8 of the Standard Contractual Clauses.

5.2 Subject at all times to Clause 5.1, as per the date of this DPA IFS consents to and specifically authorizes and mandates Partner to delegate the Processing of Personal Data hereunder to the entities listed in Exhibit 2 hereto.

5.3 IFS reserves the right at any time to immediately withdraw any consent granted under this Clause 5 with written notice to the Partner.

## 6. TRANSFER OF PERSONAL DATA

6.1 It is acknowledged that the Partner's access (acting itself or through permitted subprocessor(s) referenced in Clause 5 above) to Personal Data located in the EU/EEA from locations outside of the EU/EEA constitutes a transfer of Personal Data under the terms of the applicable Data Protection Law. Partner agrees (and shall ensure its permitted subprocessors' compliance) that such transfers shall always be conducted in accordance with the applicable Data Protection Law. Partner shall not be permitted to transfer any data except where expressly authorized by IFS, as follows:

- (a) Where the parties have duly signed and executed the attached the Standard Contractual Clauses, Partner will be authorized to transfer data in connection with this DPA on behalf of IFS, an IFS Affiliate, and/or an IFS Customer as applicable and mandated by IFS on a case-by-case basis. Partner accepts that any such IFS Affiliate or IFS Customer will be designated as a third party beneficiary for the purposes of this DPA and such Partner Data Transfer Agreement. For the purpose of enabling transfers, this DPA incorporates the Standard Contractual Clauses by reference, and IFS and Partner hereby enters into the incorporated Standard Contractual Clauses, subject to the choices and clarifications set out in Exhibit 3 hereto, and with the additional information set out in Exhibits 4, 5 and 6.
- (b) Partner may also be authorized to conduct transfers of Personal Data in connection with this DPA subject to the express prior confirmation in writing of IFS that the Partner itself or the country or territory in which it operates (i.e. where or from where it Processes or accesses Personal Data) has been found to ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the Processing of Personal Data, including without limitation the EU-U.S. Privacy Shield or any subsequent or separately adopted equivalent provision, as determined by the European Commission and subject to the scope restrictions of any such determination.
- (c) Partner acknowledges that a Customer may request a data transfer agreement to be concluded directly between the IFS Customer and the Partner (and/or its permitted subprocessor), implementing the Standard Contractual Clauses for the purposes of transfers of Personal Data on behalf of the IFS Customer (including Personal Data provided by the IFS Customer on behalf of third parties) in connection with this DPA, and the Partner will use all reasonable measures to accommodate and facilitate such request in good faith and will only conduct any such transfers pursuant to the terms of such data transfer agreement.

6.2 Partner shall comply with and participate in any successor program to the Standard Contractual Clauses related to the transfer of Personal Data, as and when mutually agreed in good faith.

## 7. ADDITIONAL DOCUMENTATION

7.1 The parties shall execute and deliver any necessary additional documentation (including the applicable Addendums to the Agreement and definitions of (i) the type of Personal Data and categories of Data Subjects, (ii) the subject-matter and duration of the Processing, (iii) the nature and purpose of the Processing) as may be required for the purposes of the parties complying with the applicable Data Protection Law regarding any Processing of Personal Data under this DPA.

## EXHIBIT 1A

### 1A IFS CONTROLLED DATA

#### PURPOSE OF DATA PROCESSING

Any Personal Data may be Processed by Partner solely for the purpose of delivering the services and performing the agreed obligations and commitments detailed in the Agreement, and in accordance with IFS's written instructions:

- to enable centralized administration or support the performance of administrative tasks and duties;
- to enable centralized support on IFS internal systems;
- to enable analysis and provide basis for aggregated reports;
- to comply with local legislative requirements;
- to assist the controller in providing services to IFS customers or business partners;
- to manage business relationships with controller contract parties, prospects or business associates; or otherwise
- to support IFS business processes and operations

#### DATA SUBJECTS

The Processing under the Agreement may concern the following categories of Data Subjects:

Employees, employment candidates, temporary staff, hired consultants and other representatives of the IFS entities themselves and of their associated companies, suppliers, partners, contractors, sub-contractors, customers, prospects, or other contract parties or business associates.

#### CATEGORIES OF PERSONAL DATA

The Processing under the Agreement may concern the following categories of Personal Data:

##### Identifiers

Examples: Employment Number, Person ID, User ID, Name, Birth name

##### Titles

Examples: Academic Title, Job Title

##### Personal data

Examples: Date of Birth, Gender, Citizenship

##### Contact information

Examples: Work phone, Work mobile, Work email, Work fax, Home address (if required for local salary systems or legal obligations), Emergency contact information, Work related comments entered by the employee that the employee want to show in IFS internal contact system, e.g. project participation and roles

##### Time and costs

Examples: Time reporting, Absence registration, Travel costs, Expenses

##### Customer/prospect Relationship Management information

Examples: Contact persons for customer/prospect, Contact information, User belonging organization

##### Partner Relationship Management information

Examples: Contact persons for customer, Contact information, User belonging organization

##### Supplier Relationship Management information

Examples: Contact persons for customer, Contact information, User belonging organization

##### Contractor Relationship Management information

Examples: Contact persons for customer, Contact information, User belonging organization

##### Business associates Relationship Management information

Examples: Contact persons for customer, Contact information, User belonging organization

**Product Support information**

Examples: User support organization belonging, User connection to queues, Support activities connected to cases and bugs, Solution comments to cases and bugs, Correspondence in connection with cases, Case time

**Product Implementation information**

Examples: Project activities, Project manager, Project assignees, Code Management items, Documents

**Product Development information**

Examples: Product Ownership, Requests, Project activities, Project manager, Project assignees, Code Management items, Documents

**Communication and Collaboration information**

Examples: Created Wiki articles, Contribution to blogs and forums, Created news and information items, Created media

**SPECIAL CATEGORIES OF PERSONAL DATA (IF APPLICABLE)**

No special categories will be subject to Processing for the purposes of the Agreement.

**1B IFS CUSTOMER CONTROLLED DATA****PURPOSE OF DATA PROCESSING**

The data importer's activities involve the delivery of services to the respective Customer via IFS on a subcontractual basis, in order to establish and provide services regarding the Customer's IFS application software solution in accordance with the agreed scope of work.

The data importer performs activities described in sub-section 2 of the sections 4.1 to 4.6 (in accordance with the particular IFS product(s) included as part of the IFS Customer agreement) of the IFS Data Processing Standard Standard.

**DATA SUBJECTS**

Data subjects whose data is processed as part of delivery of the IFS services provided in accordance with the IFS Customer agreement is identified in sub-section 4 of the sections 4.1 to 4.6 (in accordance with the particular IFS product(s) included as part of the IFS Customer agreement) of the IFS Data Processing Standard Standard.

**CATEGORIES OF DATA**

The personal data transferred may concern the categories of data identified in sub-section 5 of the sections 4.1 to 4.6 (in accordance with the particular IFS product(s) included as part of the IFS Customer agreement) of the IFS Data Processing Standard Standard.

**SPECIAL CATEGORIES OF DATA (IF APPROPRIATE)**

For most Customers the nature of their business will not require the handling or processing of any special categories of data. Access permissions required to perform their duties however provide the potential to access the special categories of data identified in sub-section 5 of the sections 4.1 to 4.6 (in accordance with the particular IFS product(s) included as part of the IFS Customer agreement) of the IFS Data Processing Standard Standard.

**PROCESSING OPERATIONS**

The personal data will be subject to the processing activities identified in section sub-section 2 of the sections 4.1 to 4.6 (in accordance with the particular IFS product(s) included as part of the IFS Customer agreement) of the IFS Data Processing Standard Standard.

**EXHIBIT 2****PERMITTED SUBPROCESSORS**

- [Enter Full Corporate Name of Subprocessor, and its service location]
- [Enter Full Corporate Name of Subprocessor, and its service location]

In the event of any agreed changes to this Exhibit 2, the exhibit shall be revised or replaced accordingly.

## EXHIBIT 3

Between IFS and Partner, module 2 (controller to processor) and module 3 (processor to processor) shall apply, as applicable in relation to the personal data that is transferred.

### OPTIONS REGARDING CLAUSES IN THE STANDARD CONTRACTUAL CLAUSES

The following provisions will be used to assist in the interpretation of the Standard Contractual Clauses incorporated as part of this DPA (for the purposes both module 2 and 3):

- in Clause 7, the optional provision (docking clause) shall not apply;
- in Clause 9(a), Option 1 (specific prior authorisation) shall apply, and the Partner as data importer shall submit the request for specific authorisation at least sixty (60) days prior to the engagement of the sub-processor;
- in Clause 11, the optional provision (redress mechanism) shall not apply;
- in Clause 17 (governing law), Option 1 shall apply and it is agreed that the governing law shall be the substantive laws of Sweden, without application of its conflict of laws principles;
- for Clause 18, (choice of forum and jurisdiction) the courts of Sweden shall have jurisdiction;
- with regard to Clause 13 (supervision), it is acknowledged that IFS is established in an EU Member State and that the competent supervisory authority (as indicated in Annex I.C) shall be the Swedish Authority for Privacy Protection (*Sw: Integritetsskyddsmyndigheten*); and
- for Swiss Personal Data, the DPA shall be deemed modified such that any reference to the GDPR shall refer to the Swiss Federal Acts on Data Protection 1992 and 2020, and the term 'Member State' shall not be interpreted in a way as to exclude Data Subjects in Switzerland from the possibility of enforcing their rights in their place of habitual residence in accordance with Clause 18(c) of the Standard Contractual Clauses.

### THE APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

References in this section to an "Annex" shall be construed as referring to the annexes set out in the appendix to the EU SCCs and the UK SCCs.

#### ANNEX I.A

In Annex I, Part A shall be populated as follows:

Data Exporter: IFS.

Data Exporter Role: Controller, and if applicable, Processor.

The activities relevant to the data transferred are, in relation to module 2:

- IFS process personal data in its capacity as legal entity, employer and supplier to customers under customer contracts.

The activities relevant to the data transferred are, in relation to module 3:

- IFS and/or any of its Affiliates has been mandated by the respective Customer under a separate written agreement, to act on its behalf as data exporter with regard to transfers of personal data controlled by Customer for the purpose of providing Customer with an enterprise application software solution and supplemental services such as, as applicable, configuration, development, consultancy, maintenance, support, and managed cloud services, which may involve transfers of personal data between the data exporter and the data importer.
- In delivering the software solution and/or supplemental services, the Customer needs to undertake a range of activities with IFS in order to support the creation, and optionally day to day management, of the solution, each of which may result in the transfer of data. Such activities are described in the IFS Data Processing Standard.

- The Customer's business information will fall within the scope of the four core IFS business process which encompass service and asset based industries, project based activities/methodologies, manufacturing processes and the supporting supply chain. These core processes are supported within the following industry sectors:
  - Aerospace and Defense;
  - Automotive;
  - Retail;
  - Asset Intensive;
  - Energy & Utilities;
  - High Tech Manufacturing;
  - Industrial Manufacturing;
  - Oil & Gas;
  - Process Manufacturing;
  - Construction & Contracting
  - Service Providers.

Data Importer: Partner.

Data Importer Role: Processor.

The activities relevant to the data transferred are, in relation module 2:

- The data importer has been engaged as processor on behalf of the data exporter's (including any of its affiliates') personal data for the sole purpose of delivering services and performing agreed obligations and commitments specified under a separate written agreement (the "**Agreement**"), e.g. for the purposes of supporting IT-systems or handling administrative functions or other specified assignments in regards of HR, Marketing and Sales, Finance, Legal, Corporate Communications, Investor Relations or other areas within the IFS Group, as further set forth in the Agreement and in accordance with the instructions of the data exporter.
- The activities relevant to the data transferred are, in relation module 3:
  - The data importer is a provider of business software supplemental services.
  - The data importer's activities involve the delivery of services to the respective Customer via IFS on a subcontractual basis, in order to establish and provide services regarding the Customer's IFS application software solution in accordance with the agreed scope of work.
  - The data importer performs activities described in sub-section 2 of the sections 4.1 to 4.6 (in accordance with the particular IFS product(s) included as part of the IFS Customer agreement) of the IFS Data Processing Standard Standard.

## ANNEX I.B

In Annex I, Part B shall be populated with the information set forth in Exhibit 4 and Exhibit 5 to this DPA, as applicable for the Partner's assignment and in relation to the relevant module of the Standard Contractual Clauses.

## ANNEX I.C

In Annex I, Part C, the competent supervisory authority is that of the country where data exporter is registered as a company, which is identified above in this Exhibit 3.

## ANNEX II

Exhibit 6 to this DPA shall serve also as Annex II of the Standard Contractual Clauses.

## EXHIBIT 4

### **ANNEX I.B (1) TO THE STANDARD CONTRACTUAL CLAUSES – IFS CONTROLLED DATA**

This Exhibit 4 forms part of the Standard Contractual Clauses.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Exhibit 4.

#### **Data subjects**

The personal data transferred under the Agreement concern the following categories of data subjects:

Employees, employment candidates, temporary staff, hired consultants and other representatives of the IFS entities themselves and of their associated companies, suppliers, partners, contractors, sub-contractors, customers, prospects, or other contract parties or business associates.

#### **Purposes of transfers**

The purposes of transfers of personal data to the data importer are, as specified in the Agreement:

- to enable centralized administration or support the performance of administrative tasks and duties;
- to enable centralized support on IFS internal systems;
- to enable analysis and provide basis for aggregated reports;
- to comply with local legislative requirements;
- to assist the controller in providing services to IFS customers or business partners;
- to manage business relationships with controller contract parties, prospects or business associates; or otherwise

#### **Categories of data**

The personal data transferred may concern the following categories of data

##### **Identifiers**

Examples: Employment Number, Person ID, User ID, Name, Birth name

##### **Titles**

Examples: Academic Title, Job Title

##### **Personal data**

Examples: Date of Birth, Gender, Citizenship

##### **Contact information**

Examples: Work phone, Work mobile, Work email, Work fax, Home address (if required for local salary systems or legal obligations), Emergency contact information, Work related comments entered by the employee that the employee want to show in IFS internal contact system, e.g. project participation and roles

##### **Time and costs**

Examples: Time reporting, Absence registration, Travel costs, Expenses

##### **Customer/prospect Relationship Management information**

Examples: Sales activities, Entered customer orders, Contact persons for customer/prospect, Contact information, User belonging organization

##### **Partner Relationship Management information**

Examples: Contact persons for customer, Contact information, User belonging organization

##### **Supplier Relationship Management information**

Examples: Contact persons for customer, Contact information, User belonging organization

##### **Contractor Relationship Management information**

Examples: Contact persons for customer, Contact information, User belonging organization

##### **Business associates Relationship Management information**

Examples: Contact persons for customer, Contact information, User belonging organization

#### Product Support information

Examples: User support organization belonging, User connection to queues, Support activities connected to cases and bugs, Solution comments to cases and bugs, Correspondence in connection with cases, Case time

#### Product Implementation information

Examples: Project activities, Project manager, Project assignees, Code Management items, Documents

#### Product Development information

Examples: Product Ownership, Requests, Project activities, Project manager, Project assignees, Code Management items, Documents

#### Communication and Collaboration information

Examples: Created Wiki articles, Contribution to blogs and forums, Created news and information items, Created media

Furthermore, since all internal systems marks each post with the identity of the person who last saved the post, this information will also be subject to the data transfer.

### **Special categories of data (if applicable)**

No special categories of data are transferred as a result of delivery of the contracted services by the data importer

### **Processing operations**

The personal data will be subject to the processing activities identified in the Agreement.

### **Frequency of the transfer**

### **Retention**

### **Transfers to (sub-) processors**

**EXHIBIT 5****ANNEX I.B (2) TO THE STANDARD CONTRACTUAL CLAUSES – CUSTOMER CONTROLLED DATA**

This Exhibit 5 forms part of the Standard Contractual Clauses.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

**Data subjects**

Data subjects whose data is processed as part of delivery of the IFS services provided in accordance with the IFS Customer agreement is identified in sub-section 4 of the sections 4.1 to 4.6 (in accordance with the particular IFS product(s) included as part of the IFS Customer agreement) of the IFS Data Processing Standard Standard.

**Categories of data**

The personal data transferred may concern the categories of data identified in sub-section 5 of the sections 4.1 to 4.6 (in accordance with the particular IFS product(s) included as part of the IFS Customer agreement) of the IFS Data Processing Standard Standard.

**Special categories of data (if appropriate)**

For most Customers the nature of their business will not require the handling or processing of any special categories of data. Access permissions required to perform their duties however provide the potential to access the special categories of data identified in sub-section 5 of the sections 4.1 to 4.6 (in accordance with the particular IFS product(s) included as part of the IFS Customer agreement) of the IFS Data Processing Standard Standard.

**Processing operations**

The personal data will be subject to the processing activities identified in section sub-section 2 of the sections 4.1 to 4.6 (in accordance with the particular IFS product(s) included as part of the IFS Customer agreement) of the IFS Data Processing Standard Standard.

**Frequency of the transfer****Retention****Transfers to (sub-) processors**

**EXHIBIT 6****ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES**

This Exhibit 6 forms part of the Standard Contractual Clauses.

**Description of the technical and organisational security measures implemented by the data importer:**

The data importer undertakes to set up and maintain physical, technical, and organizational security measures in order to protect the security of personal data created, collected, received, or otherwise obtained in connection with this agreement, and the processing operations provided thereunder, which measures are required for the processing of personal data in accordance with the relevant data protection laws in the European Union.

The technical and organisational security measures of the data importer shall include the following:

**1. SCOPE**

- 1.1 This applies to IFS systems and services containing personal data. Should an additional system or service be considered necessary by the data importer, the standard of security controls must be at least in alignment with this agreement and approved by IFS Corporate Services prior to taking such a system or service into use. In this Appendix "Corporate Services" means the central IT function of IFS AB and its subsidiaries)

**2. SECURITY ORGANISATION AND MANAGEMENT**

- 2.1 The data importer is responsible for creating local routines and processes that will reduce the risk of unauthorized access to the data and which complies with the content of this document and which is communicated to, and binding upon, the employees of the data importer involved in service delivery/processing IFS data.

**3. PERSONNEL SECURITY**

- 3.1 Each administrator of the systems and services will be required to be bound by written non-disclosure provisions to prevent distribution of any information in contradiction to the stipulations in the Data transfer agreement.
- 3.2 Employees' responsibilities pursuant to item 3.1 above can be included in terms and conditions of employment or documented as a separate agreement. In both cases the undertaking should extend beyond the period of employment and outside the organisation's premises and normal working hours.
- 3.3 All data importers are responsible for ensuring that all employees of the data importer with access to the data have the required competence and that the IFS Information Security Standard, to govern information security standards for non-IFS staff, are followed locally.

**4. SECURITY EDUCATION AND AWARENESS**

- 4.1 The data importer will encourage a security awareness culture by the provision of information security awareness policies that employees who are authorized by IFS to have access to IFS data, including contractors and non-permanent staff, are required to be updated on.

**5. SECURITY INCIDENTS AND REPORTING**

- 5.1 Employees and contractors who are authorized by IFS to have access to IFS data should be made aware of the procedures for reporting incidents that may have an impact on the security of information assets. They are required to report any observed or suspected security incidents or weakness to local management as well as the allocated IFS Partner Manager.
- 5.2 Incident reporting mechanisms should include the requirement to notify the data exporter of any breaches of security resulting in unauthorised access to, or disclosure of, personal data resulting in loss, misuse, or compromise of such personal data and will be in accordance with the applicable laws and regulations governing the data.

## 6. TECHNICAL SECURITY

6.1 The cross border transfer of personal data is limited to the minimum system management and user information required by the data importer to provide systems management and support services to each data exporter and where applicable each data exporter's clients and where required for competence data transfer and other purposes as described in Appendix 1. Privileged access rights required to conduct particular systems' management functions may, by default, enable the assigned employee of the data importer potentially further to access the data exporter's client's personal data placed on servers within and outside EU within those applications. Internal access by the data importer's assigned staff to application-level data owned by the data exporter's clients as controllers must not be given to any of the data importer's staff without the controller's consent.

## 7. SECURE TRANSPORT

7.1 Connectivity and access to IFS systems and services is permitted only in accordance with the IFS Information Security Standard which governs information security for non-IFS staff. Any additional required methods of connectivity to IFS systems and services not covered in these standards require the approval of IFS Corporate Services.

## 8. PROTECTION AGAINST MALICIOUS SOFTWARE

8.1 The data importer is responsible for ensuring that all employee, contractor and non-permanent staff that will connect to IFS or information systems or services have agreed security controls installed in accordance with industry good practice and, as a minimum include:

- malware protection and be free from known viruses or infections;
- Patching of operating system and application software to the latest security patch level;
- Secure password/pin code protection;
- Encryption of local storage;
- The use of legal, licenced software applications only from a trusted source.

8.2 Data access controls on each target system within the EU will be authorised, maintained and managed by each data exporter according to their access control standards.

## 9. LOGGING

9.1 To the extent permitted by law, and provided the data importer's consultants are working under IFS instructions and in IFS controlled environments IFS reserves the right to monitor, log and analyze all user activity on their systems and networks when it believes it has a legitimate business need including, but not limited to:

- In the course of an investigation triggered by indications of misconduct or misuse;
- In the course of an investigation of a suspected illegal act;
- As needed to protect health and safety;
- As needed to prevent interference with the IFS objectives;
- As needed to ensure the security of the IFS corporate network and connected services/devices;
- As needed to investigate an information security incident.

9.2 Computers available on the network as set out in Clause 9.1 above, will regularly be scanned and logged regarding hardware and software installations and configurations.

9.3 Usage of privilege account is logged in selected systems.

## 10. MONITORING AND AUDIT

10.1 The data importer is responsible for monitoring and auditing activities required for fulfilling all stipulations in the Data transfer agreement.

## 11. SECURITY RISK ASSESSMENT

11.1 Security risk assessment for internal systems holding personal data owned by IFS are performed on a regular basis by Corporate Services. The data importer is responsible for performing similar risk assessments for any systems or services owned by them and used in connection with delivery of their services.