

**SAP FIONEER SUPPLIER PERSONAL DATA PROCESSING AGREEMENT**  
**(“SDPA”)**  
**(Controller to Processor / Processor to Processor)**

**1. DEFINITIONS**

Capitalized terms not defined herein will have the meanings given to them in the Agreement or in the Data Protection Law.

- 1.1 **“Cloud Services”** means any distinct, subscription-based, hosted, supported and operated on-demand solution as defined in the Agreement. For clarification, this includes but is not limited to SaaS.
- 1.2 **“Controller”** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
- 1.3 **“Data Protection Law”** means the applicable legislation protecting the fundamental rights and freedoms of natural persons and their right to privacy with regard to the Processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the Parties regarding the processing of Personal Data by Supplier on behalf of Pioneer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).
- 1.4 **“Data Subject”** means an identified or identifiable natural person as defined by Data Protection Law.
- 1.5 **“EEA”** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.
- 1.6 **“GDPR”** means the 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.
- 1.7 **“List of Subprocessors”** means a compilation of the name, address and role of each Subprocessor Supplier uses to provide Supplier Services as described in Appendix I Annex III of this SDPA.
- 1.8 **“Personal Data”** means any information relating to a Data Subject. For the purposes of the SDPA, it includes only Personal Data which is:
- (a) processed by the Supplier as part of the Supplier Services; or
  - (b) supplied to or accessed by the Supplier or its Subprocessors in order to provide support under the applicable Agreement or in connection with Supplier Services; or
  - (c) in Cloud Services provided as a subset of processed data
- 1.9 **“Personal Data Breach”** means cases of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized access to Personal Data.
- 1.10 **“Processor”** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller, be it directly as Processor of a Controller or indirectly as Subprocessor of a Processor which processes Personal Data on behalf of the Controller.
- 1.11 **“Professional Services”** means implementation services, consulting services and/or other related services as defined in the Agreement and may also be referred to in the Agreement as “Consulting Services”, “Education Services”, “Individual Software Development” or “Services”. For clarity: Professional Services does not include Cloud Services and Support including Software Maintenance.
- 1.12 **“SCC Relevant Transfer”** means the transfer and onwards transfer of Personal Data to a Third Country.
- 1.13 **“SCC UK Addendum”** The SCC UK Addendum (Version B1.0) is a specific addendum for transferring personal data from UK to the outside of the UK created by the UK Information Commissioner’s Office (ICO) under S119A (1) Data Protection Act 2018.

- 1.14 “**Standard Contractual Clauses / SCCs**” or sometimes also referred to the “EU Model Clauses” mean the Standard Contractual Clauses (Module 2 – Controller to Processors and Module 3 – Processor to Processor) published by the European Commission on the basis of Decision 2021/914 or any subsequent version thereof (which will automatically apply)
- 1.15 “**Subprocessor**” has the meaning given in the GDPR and means any third party that are directly or indirectly engaged by Supplier in connection with the Supplier Services and that Process Personal Data in accordance with the terms of this SDPA.
- 1.16 “**Supplier Services**” means the services as set out in the Agreement.
- 1.17 “**Technical and Organizational Measures**” means implementation and maintenance of appropriate security measures within the meaning of Art. 32 GDPR and further Applicable Data Protection Law.
- 1.18 “**Third Country**” means any country, organization or territory not acknowledged by either the European Union under Article 45 of GDPR or under applicable Data Protection Law as a safe country with an adequate level of data protection.

## 2. BACKGROUND

### 2.1 Application.

- (a) This SDPA is incorporated into and forms part of the Agreement between Supplier and Fioneer about the Supplier Services and shall continue for the duration of the Agreement.
- (b) This SDPA sets forth the terms and conditions related to the Processing of Personal Data by Supplier and/or its Subprocessors in connection with delivering Supplier Services.

### 2.2 Structure and Schedules.

- (a) The Appendix I, including Annex I, Annex II and Annex III is incorporated into this SDPA, and if applicable to the Standard Contractual Clauses.
- (b) If applicable, the Appendix II is incorporated as the SCC UK Addendum.

### 2.3 GDPR.

Supplier and Fioneer agree that it is each Party's responsibility to review and adopt the respective requirements imposed on Controllers and Processors by the GDPR, in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Fioneer or (other) Controllers that is processed under the SDPA.

### 2.4 Governance.

- (a) **Role of Fioneer.** Fioneer acts as Controller and/or Processor as defined in Appendix I, Annex I of this SDPA
- (b) **Role of Supplier.** Supplier acts as a Processor or, where Fioneer acts as Processor, Supplier acts as a Subprocessor under this SDPA.
- (c) **Single Point of Contact.**
  - i. Supplier (for the Subprocessors) and Fioneer (for the (other) Controllers) act as central points of contact. To the extent permitted under Data Protection Law and subject to deviating Instructions by Controllers, all communication in connection with this SDPA and the processing of Personal Data thereunder shall be channeled through Fioneer and Supplier respectively.
  - ii. Between Fioneer and Supplier, Supplier shall inform its Subprocessors appropriately where required, and Fioneer shall inform the (other) Controllers appropriately where required.
  - iii. This Section (c) shall not, however, limit any rights of Controllers under this SDPA, Standard Contractual Clauses, the SCC UK Addendum or Data Protection Law.

## 3. OBLIGATIONS

3.1 **Instructions.** Supplier will process Personal Data only in accordance with documented instructions from Fioneer or (other) Controllers as forwarded to Fioneer respectively (including with regard to transfers of Personal Data to a Third Country or an international organization). The Agreement (including this SDPA) constitutes such documented instructions. Supplier will follow any additional instructions received from Fioneer or (other) Controllers respectively. If Supplier cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, Supplier will immediately notify Fioneer (email permitted).

3.2 **Processing on Legal Requirement.** Supplier may also process Personal Data for other purposes where required to do so by applicable law. In such a case, Supplier shall inform Fioneer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

3.3 **Personnel.** To process Personal Data, Supplier and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. Supplier and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

- 3.4 **Cooperation.** At Pioneer's request, Supplier will reasonably cooperate with Pioneer and (other) Controllers in dealing with requests from Data Subjects or regulatory authorities regarding Supplier's processing of Personal Data or any Personal Data Breach. In case Supplier receives a request from a Data Subject in relation to the Personal Data processing hereunder, Supplier will notify Pioneer in a timely manner and shall not respond to such request itself but instead ask the Data Subject to redirect its request to the respective Controller. In the event of a dispute with a Data Subject as it relates to this SDPA, the Parties shall keep each other informed and, where appropriate, cooperate in resolving them. Supplier shall provide functionality for production systems that supports Pioneer's or (other) Controller's ability to correct, block, delete or anonymize Personal Data from a Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, Supplier will correct, block, delete or anonymize any Personal Data, or restrict its processing, in accordance with Pioneer's instructions, instructions provided by Pioneer on behalf of (other) Controller's and in accordance with Data Protection Law.
- 3.5 **Data Protection Impact Assessment.** If, pursuant to Data Protection Law, Pioneer or (other) Controllers are required to perform a data protection impact assessment or prior consultation with a regulator, at Pioneer's request, Supplier shall provide reasonable assistance and shall promptly provide all required information and documents available to it and its Subprocessors relating to the processing of Personal Data in the context of the Supplier Service.
- 3.6 **Personal Data Breach Notification.** In the event that Supplier becomes aware of any Personal Data Breach (by itself or a Subprocessor), Supplier must report the same to Pioneer without undue delay and if possible within 24 hours. Personal Data Breaches must be reported to the designated Pioneer point of contact. The reporting of a Personal Data Breach shall contain all information (as set out in Clause 8.6 c) of Modules 2 and 3 of the Standard Contractual Clauses) which is available to Supplier or Subprocessors and which may be required to enable the Controller to assess the situation and comply with its reporting obligations towards authorities and/or Data Subjects.

#### 4. SECURITY OF PROCESSING

- 4.1 **Appropriate Technical and Organizational Measures.** Supplier is responsible for the implementation and maintenance of the Technical and Organization Measures. Supplier has implemented and will apply and maintain at least the Technical and Organizational Measures set forth in Appendix I, Annex II ("Technical and Organizational Measures"). Supplier will provide evidence of the implementation and maintenance of the Technical and Organizational Measures as requested, including by responding to any data protection questionnaire of Pioneer or of Pioneer on behalf of a (other) Controller.
- 4.2 **Changes.** Supplier shall carry out regular checks of the Technical and Organizational Measures to ensure that the Technical and Organizational Measures continue to provide an appropriate level of security. Supplier may change the Technical and Organizational Measures provided that Supplier maintains an equivalent or better level of security. Supplier will notify Pioneer in advance of any material changes to the Technical and Organizational Measures.

#### 5. DATA EXPORT AND DELETION

- 5.1 **Export and Retrieval.** If and to the extent Supplier hosts Personal Data in a Cloud Service, during the Subscription Term of such Cloud Service and subject to the Agreement, Supplier ensures that Pioneer or the respective (other) Controller can access its Personal Data at any time in a structured, commonly used and machine-readable format.
- 5.2 **Return and Deletion.**
- (a) Before the Subscription Term of the Cloud Service expires, Supplier shall enable Pioneer and the respective (other) Controllers to perform a final data export which constitutes a final return of Personal Data from the Cloud Service.
  - (b) Notwithstanding Section (a) above, any Personal Data stored by Supplier or Subprocessors, and any copies thereof, shall be promptly returned to Pioneer upon the earliest of the following events: (i) upon Pioneer's first request; (ii) upon completion of all tasks for which the respective Personal Data was transferred to Supplier or Subprocessors; (iii) upon expiry or termination of this SDPA; or (iv) upon expiry

or termination of the Agreement. Alternatively, where such data cannot be returned, or if Pioneer chooses so, Supplier shall irreversibly delete or destroy, and certify to Pioneer in writing that it has deleted or destroyed, all such data within a reasonable time period in accordance with Data Protection Law (not to exceed three months) unless the retention of data is required by applicable law and permitted under Data Protection Law.

## 6. CERTIFICATIONS AND AUDITS

6.1 **Standard Audit.** Notwithstanding any rights under Module 2 and Module 3 of the Standard Contractual Clauses, Supplier agrees that Pioneer may request, and Supplier will provide, evidence of Supplier's compliance with the terms of this SDPA, including the Technical and Organizational Measures and any other information that is required in order that Pioneer may use Supplier as its (Sub-)Processor under applicable Data Protection Laws (such as information required by Pioneer to fulfil its transparency obligations regarding international processing) in the form of a questionnaire or a request for current relevant certifications both prior to commencement of Personal Data processing and at any time later during the term of this SDPA. Upon request, Supplier shall in particular provide all existing certifications and attestations with respect to its and its Subprocessor's IT control environment relevant for the Services (such as ISO 27001, SSAE18/ISAE3402, ISAE3000 like SOC2 or C5). Additionally, Pioneer or its independent third-party auditor reasonably acceptable to Supplier may conduct an audit to confirm Supplier's compliance with the terms of this SDPA where:

- (a) Supplier has not provided sufficient evidence of its compliance by responding to Pioneer's requests for information; or
- (b) an audit is formally requested by a competent data protection authority; or
- (c) Pioneer has indications of non-compliance i.e. to the extent that a Personal Data Breach has occurred, or Supplier is not able to perform its obligations under this SDPA; or
- (d) mandatory Data Protection Law provides Pioneer with a direct audit right, provided that Pioneer shall only audit Supplier once in any twelve-month period unless mandatory Data Protection Law requires more frequent audits.

6.2 **Limitations.** All standard audits will be subject to the following limitations: audits will be conducted upon reasonable notice (no fewer than thirty (30) calendar days unless shorter notice is required by a competent data protection authority or Data Protection Law), during regular business hours and without interrupting Supplier's business operations. The Parties will use reasonable efforts to leverage current certifications or other audit reports to avoid or minimize repetitive audits.

6.3 **Exceptional Audit.** Notwithstanding the foregoing, Pioneer may conduct additional audits on shortened notice either (i) where a Personal Data Breach has occurred, provided that the Parties will mutually agree on a timing that does not disrupt ongoing breach response or (ii) where Pioneer has reasonable grounds to suspect that Supplier is not in compliance with its obligations under this SDPA.

6.4 **Cost of Audit.** Each Party shall bear its own costs of any audit unless such audit reveals a breach by Supplier or Subprocessor of this SDPA in which case Supplier must reimburse Pioneer (or Controller) for all reasonable fees and expenses charged by any external auditor or incurred in the course of an audit. If an audit determines that Supplier (or a Subprocessor) has breached its obligations under the SDPA, Supplier (or Subprocessor) will promptly remedy the breach at its own cost.

6.5 **Other Controller Audit.** Any other Controller may assume and exercise Pioneer's rights under this Section 6 towards Supplier and Subprocessors. Pioneer shall use reasonable means to combine audits of multiple (other) Controllers to avoid multiple audits. For this purpose, Pioneer may share audit results with the (other) Controller.

## 7. SUBPROCESSORS

7.1 **Permitted Use.** Pioneer grants Supplier a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

- (a) Supplier shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this SDPA in relation to the Subprocessor's processing of Personal Data. Supplier shall be liable for any breaches by the Subprocessor in accordance with the terms of the Agreement;

- (b) Supplier will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to its selection in order to establish that it is capable of providing the level of protection of Personal Data required by this SDPA; and
- (c) Supplier provides to Pioneer the List of Subprocessors as defined in Appendix I, Annex III.

7.2 **New Subprocessors.** Where Supplier intends to replace a Subprocessor from the List of Subprocessors in Appendix I, Annex III or to introduce a new Subprocessor not included in the List of Subprocessors by the date of conclusion of this SDPA, Supplier must list all relevant information on Subprocessors in the List of Subprocessors and notify Pioneer prior to the intended use of such Subprocessor within ninety (90) calendar days. Pioneer may object to the use of a new Subprocessor on reasonable grounds, including insufficient reliability in Pioneer's reasonable discretion or status as a competitor of Pioneer. If Pioneer objects to the use within ninety (90) calendar days after being notified, Supplier must ensure that the Subprocessor is not used for the provision of the Services.

## 8. LIABILITY

- 8.1 SAP Pioneer and the Supplier shall be liable to the Data Subjects in accordance with the provisions of Article 82 GDPR. Supplier shall coordinate with SAP Pioneer regarding any possible fulfilment of liability claims.
- 8.2 The Parties shall each release themselves from liability if/insofar as one Party proves that they are in no way responsible for the circumstance through which the damage occurred to a Data Subject. Apart from that, Article 82 (5) GDPR shall apply.

## 9. INTERNATIONAL PROCESSING

9.1 **Conditions for International Processing.** Supplier shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this SDPA outside the country in which Pioneer is located as permitted under Data Protection Law.

9.2 **Standard Contractual Clauses.** If Personal Data is processed in a Third Country and the required adequacy means can be met by entering into Standard Contractual Clauses, then:

- (d) where Supplier is located in a Third Country, Supplier and Pioneer hereby enter into the Standard Contractual Clauses (SCC) or the SCC UK Addendum. Pioneer enters as the data exporter and Supplier enters as the data importer. SCC Relevant Transfers, apply as follows:
  - Module 2 (Controller to Processor) shall apply where Pioneer is a Controller; and
  - Module 3 (Processor to Processor) shall apply where Pioneer is a Processor.

(b) To the extent required under applicable Data Protection Law, Supplier as the data exporter, has entered into the Standard Contractual Clauses Module 3 (Processor to Processor) or the SCC UK Addendum respectively with each Subprocessor, as the data importer, applicable for SCC Relevant Transfers.

Upon request to Pioneer from a Data Subject or upon request of a (other) Controller, Pioneer may make a copy of the Standard Contractual Clauses entered into between Pioneer and Supplier and provide this to the Data Subject and to the respective (other) Controller.

Any onward transfers must follow the rules set forth in the Module of the Standard Contractual Clauses that is applicable to the data importer and establish a third-party beneficiary clause in line with Clause 9 (e) of the Standard Contractual Clauses with all relevant Subprocessors in the processing chain.

The Parties choose the application of the optional clause 7 (docking clause) of the Standard Contractual Clauses.

9.3 **Relation of the Standard Contractual Clauses to the SDPA and the Agreement.** Nothing in this SDPA and in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses or, if applicable, the SCC UK Addendum. For the avoidance of doubt, where this SDPA further specifies audit and subprocessor rules in sections 6 and 7, such specifications also apply in relation to the Standard Contractual Clauses and the SCC UK Addendum.

9.4 **Governing Law of the Standard Contractual Clauses.** The Parties agree that the Governing Law of the Standard Contractual Clauses shall be German law and that any dispute in relation to the Standard Contractual Clauses shall be resolved by the Courts of Munich, Germany. In case the SCC UK Addendum is applicable, the governing law is the law of England and Wales and that any dispute in relation to the SCC UK Addendum shall be resolved by the Courts of England, London, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

#### 10. **DOCUMENTATION; RECORDS OF PROCESSING**

Supplier shall maintain comprehensive documentation about the processing of Personal Data in line with Data Protection Law with respect to its area of responsibility and shall provide such documentation to Fioneer upon request. The documentation shall enable Fioneer to verify Supplier's compliance with Data Protection Law, including the use of Subprocessors in accordance with Data Protection Law. Supplier shall further provide to Fioneer all information with respect to the Services that concern (i) Supplier, (ii) the Subprocessors, (iii) the processing of Personal Data, to the extent it is necessary for Fioneer to maintain records of Processing activities according to Data Protection Law.

#### 11. **MISCELLANEOUS**

- 11.1 **Interpretation.** If any provision in this SDPA is ineffective or void, this shall not affect the remaining provisions. The Parties shall replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. The Parties shall similarly add a necessary appropriate provision where such a provision is missing.
- 11.2 **Modifications.** This SDPA, excluding the Standard Contractual Clauses and the SCC UK Addendum, may be modified by a written agreement of the Parties. The same applies to a change of this written form requirement. This written form requirement can also be met by exchange of documents with an electronically transmitted signature (facsimile transmission, e-mail transmission with scanned signatures, or other electronically permissible form of contract conclusion).
- 11.3 **Termination.** In addition to the termination rights set out in Clause 16 of the Standard Contractual Clauses, either Party may terminate this SDPA if no contractual relationship between the Parties exist any longer where the processing of Personal Data is in scope.

**Appendix I to the SDPA and  
if applicable Appendix to the Standard Contractual Clauses**

Appendix I consists of Annex I, Annex II and Annex III.

**Annex I to Appendix I of the SDPA and if applicable  
Annex I to the Standard Contractual Clauses**

**A. LIST OF PARTIES**

For the List of Parties please refer to the SoW / Order Form.

**B. DESCRIPTION OF TRANSFER**

**CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED**

Unless provided otherwise by the Pioneer, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, Business Partners or other individuals having Personal Data stored, transmitted to, made available to or accessed by the Data Importer.

For supplemental Categories of Data Subjects to the SDPA please refer to the SoW / Order Form.

**CATEGORIES OF PERSONAL DATA TRANSFERRED**

Unless provided otherwise by the Pioneer, transferred Personal Data relates to the following categories of Personal Data: name, phone numbers, e-mail address, time zone, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data transferred or entered into the Suppliers service by users and may include financial data such as bank account data, credit or debit card data.

For supplemental Categories of Personal Data to the SDPA please refer to the SoW / Order Form.

**SENSITIVE DATA TRANSFERRED (IF APPLICABLE) AND APPLIED RESTRICTIONS OR SAFEGUARDS, WHICH FULLY TAKE INTO CONSIDERATION THE NATURE OF THE DATA AND THE RISKS INVOLVED. THESE MAY INCLUDE 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.**

Unless provided otherwise by the Pioneer, the transferred Personal Data concerns Sensitive Data as may be set out in the Agreement (including the Order Form), if any. The Technical and Organizational Measures as set out in the SDPA and if applicable to the SCCs Annex II contain respective Security measures reasonable to protect Sensitive Data.

For supplemental Sensitive Data and applied restrictions or safeguards please refer to the SoW / Order Form.

**THE FREQUENCY OF THE TRANSFER (E.G. WHETHER THE DATA IS TRANSFERRED ON A ONE-OFF OR CONTINUOUS BASIS)**

Unless provided otherwise by the Pioneer, transferred Personal Data relates to the following frequency of transfer

For the frequency of transfer please refer to the SoW / Order Form.

**NATURE OF THE PROCESSING / PURPOSE(S) OF THE DATA TRANSFER AND FURTHER PROCESSING**

The transferred Personal Data is subject to the processing activities as set out in the Agreement which may include:

**Cloud Services.**

The Supplier and / or its Subprocessors operate the Cloud Service data centers and infrastructure remotely from their facilities and allowed remote locations. The Supplier and/or its Subprocessors provide support when the Cloud Service is not available or not working as expected for some or all Users. The Supplier answers phone calls and performs basic troubleshooting and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service. Personal Data is processed for including but not limited to:

- (a) provision of Cloud Services;
- (b) communication to Users;
- (c) storage of Personal Data in dedicated data centers (multi-tenant architecture);
- (d) Release, development and uploading of any fixes or upgrades to the Cloud Service;

- (e) back up and restoration of Personal Data;
- (f) computer processing of Personal Data, including data transmission, data retrieval, data access;
- (g) network access to allow Personal Data transfer;
- (h) in anonymized form for continuous improvement of service features and functionalities provided as part of the Cloud Service including automation, transaction processing and machine learning;
- (i) monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database;
- (j) Security monitoring, network-based intrusion detection support, penetration testing;
- (k) execution of instructions of Pioneer in accordance with the Agreement;
- (l) further Services as defined in the Agreement.

#### **Maintenance and Support.**

The Supplier and/or its Subprocessors provide support when the Software is not available or not working as expected. They answer phone calls and perform basic troubleshooting, and handle support tickets in a tracking system including but not limited to:

- (a) accessing systems containing Personal Data in order to provide maintenance and support;
- (b) use of Personal Data to provide maintenance and support;
- (c) storage of Personal Data related to the support process or the case;
- (d) computer processing of Personal Data for data transmission;
- (e) execution of instructions of Pioneer in accordance with the Agreement;
- (f) further Services as defined in the Agreement.

#### **Professional Services.**

Supplier and/or its Subprocessors provide Services subject to the Order Form and the applicable Scope Document. This includes but is not limited to:

- (a) accessing systems containing Personal Data in order to provide Professional Services;
- (b) execution of instructions of Pioneer in accordance with the Agreement;
- (c) further Services as defined in the Agreement.

#### **THE PERIOD FOR WHICH THE PERSONAL DATA WILL BE RETAINED, OR, IF THAT IS NOT POSSIBLE, THE CRITERIA USED TO DETERMINE THAT PERIOD**

Personal Data shall be retained for the duration of the Agreement and subject to Section 5.2 of the SDPA.

#### **FOR TRANSFERS TO (SUB-) PROCESSORS, ALSO SPECIFY SUBJECT MATTER, NATURE AND DURATION OF THE PROCESSING**

Subject Matter, nature and duration of the processing by (Sub-) processors are generally equal to these described in this section B, subject to the role as described in Annex I A

### **C. COMPETENT SUPERVISORY AUTHORITY**

The supervisory authority of the Data Exporter according to Clause 13 (a) of the Standard Contractual Clauses Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

**Annex II to Appendix I of the SDPA and if applicable  
Annex I to the Standard Contractual Clauses**

*Description of the Technical and Organizational Measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

Supplier is responsible for the implementation of appropriate security measures. This Annex II describes three possible processing scenarios and the minimum requirements Supplier must implement for each.

In some scenarios, the responsibility for ensuring Technical and Organizational Measures may not be in the sole responsibility of Supplier. For example, where Supplier provide support services solely on Pioneer’s premises, Pioneer is responsible for the physical security of the buildings. However, Suppliers which provide Cloud Services would control all aspects of the Technical and Organizational Measures listed below. The following table outlines the typical scenarios for the provision of Supplier Services:

Definition of scenarios:

<b>Scenarios</b>	<b>Location Where are services provided?</b>	<b>IT-systems/-infrastructure In which systems are services provided?</b>
<b>Scenario I</b>	Supplier Services provided also from own / rented premises / offices of the Supplier or its Subprocessors (including home office).	Service provisioning includes the processing and storage of personal data also in systems / infrastructure of the Supplier or its Subprocessors.
<b>Scenario II</b>	Supplier Services provided also from own/rented premises / offices of Supplier or its Subprocessors (including home office).	Services provided exclusively in systems / infrastructure of Pioneer and / or (other) Controllers (including remote access granted by other Controllers, e.g. VPN, etc.)
<b>Scenario III</b>	Supplier Services provided exclusively from Pioneer’s premises and / or (other) Controllers’ premises (e.g. onsite at Pioneer Customers and Partners	Services provided exclusively in systems/ infrastructure of Pioneer and / or other Controllers (including remote access granted by other controllers, e.g. VPN, etc.)

With respect to these scenarios, tables at the end of the individual Technical and Organizational Measures described hereinafter indicate Suppliers responsibility (fields marked with an “X”).

<b>1. <u>Physical Access Controls</u></b> Only authorized persons can physically access premises, buildings or rooms where Data is stored. Data importer protects its assets and facilities using the following means:  (mark fields with an “X” as applicable)	<b>Scenarios</b>		
	<b>I</b>	<b>II</b>	<b>III</b>
1.1. Data centers and infrastructure systems are designed to minimize the impact of environmental risks including damage caused by natural disasters.	X		
1.2. As a minimum requirement, the physical entrance points of the office buildings and the data center facilities are fitted with a key system.	X	X	

<b>1. <u>Physical Access Controls</u></b> Only authorized persons can physically access premises, buildings or rooms where Data is stored. Data importer protects its assets and facilities using the following means:	Scenarios		
1.3. Depending on the security classification, buildings, specific areas and surrounding premises are further protected by additional security measures. These include specific access profiles, video surveillance, intruder alarm systems, smart card access control, active key management and biometric access control systems.	X	X	
1.4. Access rights are granted to authorized persons on an individual basis according to the System Access Controls and Data Access Controls measures. This also applies to visitor access. Guests and visitors to Supplier's buildings have to register at the reception and will be accompanied by authorized personnel.	X	X	
1.5. Only authorized persons have access to systems and infrastructure within the data center facilities.	X		
1.6. Every person has to wear their ID cards at all Supplier's locations.	X		
1.7. Additional measures for Suppliers's operated data centers:			
(a) All data centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and data center facilities from being compromised. To protect proper functionality, physical security equipment (e.g. motion sensors, cameras) undergo regular maintenance.	X		
(b) Supplier logs the names and times of authorized personnel entering and leaving Supplier's dedicated areas within the data centers.	X		

<b>2. <u>System Access Controls</u></b> Systems processing Personal Data can only be accessed with authorization. Supplier protects its systems and controls access using the following means:	Scenarios		
(mark fields with an "X" as applicable)	I	II	III
2.1. Multiple authorization levels are used when granting access to systems, including those processing Data. Authorizations are managed via defined processes.	X		
2.2. All personnel access Supplier's systems using a personalized account (user ID).	X	X	
2.3. Personnel have only access to the systems that they require to access in order to fulfill their duties. Supplier has procedures in place to implement the need-to-know principle for allowing system access. When personnel change their assigned role within the company, their access rights are timely revoked or adapted. As soon as personnel leave Supplier, their access is revoked generally within 24 hours. Supplier uses authorization concepts that document grant processes and assigned roles per personalized account (user ID). Furthermore, authorization and privileges are reviewed on a regular basis.	X	X	
2.4. Supplier has established a password policy that prohibits the sharing of personalized passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized accounts (user IDs) are assigned for authentication and must not be shared. All passwords fulfill defined minimum requirements, in particular for complexity and storage. Each end-user device has a password-protected screensaver.	X	X	

2. <b><u>System Access Controls</u></b> Systems processing Personal Data can only be accessed with authorization. Supplier protects its systems and controls access using the following means:	Scenarios		
2.5. The company network is protected from the public network by firewalls. Supplier operates an enterprise threat detection system to continuously and actively defend systems and infrastructure against attacks, using and analyzing audit logs.	X	X	
2.6. Supplier uses up-to-date commercially available antivirus/malware protection software intended to prevent, detect and remove known malicious code. This includes signature-based detections of malware, viruses, spyware and trojans as it applies to ingress and egress points such as email services and file transfers. It also mitigates security risks for malicious code on systems, endpoints and devices.	X	X	X
2.7. Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to Supplier's corporate network and critical infrastructure is protected by strong authentication.	X	X	

3. <b><u>Data Access Controls</u></b> Persons can access Personal Data only according to their authorization. Personal Data processed within the Supplier Services is classified as confidential information using the following means:	Scenarios		
(mark fields with an "X" as applicable)	I	II	III
3.1. Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require to access in order to fulfill their duties. When personnel leave or change their assigned role within the company, their access rights are timely revoked or adapted. As soon as personnel leave Supplier, their access is revoked generally within 24 hours. Data importer uses authorization concepts that document grant processes and assigned roles per account (user ID). Furthermore, authorization and privileges are reviewed on a regular basis.	X	X	X
3.2. Data and data carriers are securely deleted or destroyed once they are no longer required. If hardware is removed from data centers a physical decommissioning process is applied.	X	X	
3.3. Security measures that protect applications processing Data are regularly tested. To this end, Supplier conducts internal and external security checks and penetration tests on its IT systems.	X	X	
3.4. Supplier has policies in place to prevent installations of not approved software on workstations and servers. Mobile devices and workstations shall be locked manually when left unattended. The screensaver is configured to automatically lock the screen within a maximum of five minutes of inactivity. This time-dependent lock of devices must not be deactivated.	X	X	X
3.5. Display screens for all systems that could disclose information allowing access to another Supplier device or system or screens used to handle confidential information should be positioned so that unauthorized persons cannot readily view them through a window, over a shoulder, or by similar means.	X	X	X
3.6. Mobile devices that could provide access to devices or systems where Data is stored, have to be kept in the possession of personnel or locked in a secure location when not in use. Mobile devices must not be checked in as luggage when traveling.	X	X	X

4. <b><u>Data Encryption Controls</u></b> Supplier applies the following measures to prevent Personal Data from being read, copied, modified or removed without authorization during transfer and at rest:	Scenarios		
(mark fields with an "X" as applicable)	I	II	III
4.1. Personal Data is encrypted at rest using market accepted standards.	X		
4.2. Personal Data is encrypted using market accepted standards during transmission between secured networks in control of Supplier. Personal Data in transfer over secured networks in control of Supplier is appropriately secured.	X		
4.3. Mobile devices that could provide access to devices or systems where Personal Data is stored use Supplier controlled network encryption when connecting to Supplier's networks remotely.	X		
4.4. For the transfer of Personal Data between Pioneer, Pioneer Customers and Partners and Supplier, Supplier will provide adequate protection measures for the transferred Personal Data. The measures are defined in the product documentation or otherwise in the Agreement. This applies to both physical and network-based data transfer.	X		

5. <b><u>Data Integrity Controls</u></b> Supplier applies the following measures to keep Personal Data intact, complete and current during processing activities:	Scenarios		
(mark fields with an "X" as applicable)	I	II	III
5.1. Supplier only allows authorized personnel to access Personal Data as required in the course of their duty.	X	X	X
5.2. Supplier has implemented a system for logging and retaining Supplier's input, modification and deletion, or blocking of Personal Data within Supplier Services related to Pioneer's Cloud Service infrastructure.	X		
5.3. Supplier Services related to Pioneer's Cloud Service applications provide logging systems for input, modification and deletion, or blocking of Personal Data as required by Applicable Data Protection Law.	X		
5.4. Supplier uses the technical capabilities of the deployed software (e.g. multi-tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.	X		
5.5. The Personal Data of Pioneer (including Pioneer Customers and Partners and (other) Controllers) is logically separated from Personal Data of other customers. Access controls prevent the access of other customers to the relevant Personal Data.	X		
5.6. For Supplier Services related to Pioneer Support,			
(a) Pioneer, Pioneer Customers and Partners have control over their remote support connections at all times. Supplier cannot access a system of Pioneer and/or Pioneer Customers and Partners without the knowledge and consent of Pioneer, Pioneer Customers or Partners respectively. For Supplier Services related to Pioneer Support, Supplier provides a specially designated, secure support ticket facility in which Pioneer provides a special access-controlled and monitored security area for transferring access data and passwords. Pioneer, Pioneer Customers and Partners have control over their remote support connections at all times. Data importer's employees cannot access an on premise system of	X		

<b>5. <u>Data Integrity Controls</u></b> Supplier applies the following measures to keep Personal Data intact, complete and current during processing activities:	<b>Scenarios</b>		
Fioneer, Fioneer Customers or Partners without the knowledge and active participation of Fioneer, Fioneer Customers or Partners respectively.			
(b) If Personal Data is required for Supplier to handle a support incident from Fioneer, Fioneer Customers or Partners respectively, the Personal Data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.	X	X	X

<b>6. <u>Availability Controls</u></b> Data is protected against accidental or unauthorized destruction or loss as follows:	<b><u>Scenarios</u></b>		
(mark fields with an "X" as applicable)	<b>I</b>	<b>II</b>	<b>III</b>
6.1. Supplier employs regular backup processes to provide restoration of Personal Data if and when necessary and provides disaster recovery services.	X		
6.2. Supplier uses uninterrupted power supplies (e.g. batteries, generators) for uninterrupted power availability to the data centers.	X		
6.3. Supplier has implemented reasonable network connection bandwidths and Denial-of-Service (DoS) prevention measures for the data center providing the Supplier Services.	X		
6.4. Supplier has defined business contingency plans for its own business-critical processes.	X	X	
6.5. Emergency processes and systems including data recovery are regularly tested.	X		

<b>7. <u>Governance Controls</u></b> Data is processed as follows:	<b>Scenarios</b>		
(mark fields with an "X" as applicable)	<b>I</b>	<b>II</b>	<b>III</b>
7.1. Data is processed in accordance with the Agreement, the SDPA and related instructions of the Data Controller and/or Fioneer	X	X	X
7.2. Supplier uses controls and processes to monitor compliance with contracts entered between Fioneer, Supplier and its, Subprocessors or other service providers respectively.	X	X	X
7.3. To process Personal Data, Supplier and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. Supplier and its Subprocessors will regularly train personnel having access to Data in applicable data security and data privacy measures.	X	X	X

*For transfers to (Sub-) Processors, also describe the specific Technical and Organizational Measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a Sub-processor, to the data exporter.*

Please refer to the SoW / Order Form.

**Annex III to Appendix I of the SDPA and if applicable  
Annex III to the Standard Contractual Clauses**

For the Supplier's List of Subprocessors please refer to the SoW / Order Form.

**Appendix II**  
**Standard Data Protection Clauses to be issued by the Commissioner**  
**under S119A (1) Data Protection Act 2018**

**International Data Transfer Addendum to the EU Commission Standard Contractual Clauses**  
**VERSION B1.0, in force 21 March 2022**  
 Reference to the SCC UK addendum:

<https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf>

The UK Addendum as referenced above is concretized below:

**Part 1: Tables**

**Table 1: Parties**

<b>Start date</b>	pls see in the contract / SDPA	
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties' details</b>	As laid out in Annex I of the SDPA	As laid out in Annex I of the SDPA
<b>Key Contact</b>	As laid out in Annex I of the SDPA	As laid out in Annex I of the SDPA
<b>Signature (if required for the purposes of Section 2)</b>	As laid out in Annex I of the SDPA	As laid out in Attachment 1 to Annex I of the SDPA

**Table 2: Selected SCCs, Modules and Selected Clauses**

<b>Addendum EU SCCs</b>	The EU SCCs according to article 1.11 of the SDPA, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs according to article 8.4 of the SDPA brought into effect for the purposes of this Addendum.
-------------------------	---

**Table 3: Appendix Information**

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties
Annex 1B: Description of Transfer
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data
Annex III: List of Sub processors (Modules 2 and 3 only)

**Table 4: Ending this Addendum when the Approved Addendum Changes**

<b>Ending this Addendum when the Approved Addendum changes</b>	<b>Which Parties may end this Addendum as set out in Section 19:</b> <input type="checkbox"/> Importer <input type="checkbox"/> Exporter <input checked="" type="checkbox"/> neither Party
--	---