

**DATA PROCESSING AGREEMENT**

1. **PARTIES**
   1. This Data Processing Agreement is entered into by and between [name of Oerlikon entity] [acting on its behalf and on behalf of its affiliates] (“**Oerlikon**”) and [ name of Supplier] (“**Supplier**”) (together the “**Parties**”).
2. **PREAMBLE**
   1. As part of the agreement signed on [date] for the provision of [describe services/name of software license] (hereafter the “Agreement”), **Supplier** (“**Processor**”) will Process Personal data on behalf of **Oerlikon** (“**Controller**”). This Processing of Personal Data is described in **Annex I.**
   2. Controller and Processor have agreed to sign this Data Processing Agreement to comply with Applicable Data Protection Law. In the event of a conflict between this Data Processing Agreement and the Agreement, this Data Processing Agreement shall prevail concerning the data protection terms, obligations and responsibilities of the Parties relating to the Processing to be carried out by the Processor on behalf of Controller. Annexes I, II, III form an integral part of this Data Processing Agreement
   3. **Definitions: i)** Applicable Data Protection Law shall mean all data protection laws and regulations applicable to the Processing of Personal Data described in Annex I to this Data Processing Agreement, and in particular the EU Regulation 2016/679 (GDPR), the implementing legislations in the EU/EEA, but also any applicable non-EU data protection laws including, without limitation, the Swiss Federal Data Protection Act (Swiss FADP) and the UK data protection laws; **ii)** the terms “Controller”, “Processor”, “Processing”, “Personal data” “Sensitive Personal Data” have the meaning given to those terms under Applicable Data Protection Law. Processor acknowledges that the Oerlikon legal entity signatory and each individual company of the Oerlikon Group on behalf of whom this Data Processing Agreement is signed are Controller(s) with respect to their Personal data Processed by Processor. “Sub-processor” shall mean a subcontractor engaged by Processor to perform any part of the Processing described in Annex I; **iii)** “Restricted Transfer” means a transfer (directly or via onward transfer) of Personal data subject to GDPR, UK data protection laws or Swiss Federal Data Protection Act to a country outside of Europe that is not subject to an adequacy decision by the European Commission, or the competent UK or Swiss authorities (as applicable); **iv)** EU Standard Contractual Clauses: shall mean the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, and applicable approved amendments.
3. **OBLIGATIONS OF THE PROCESSOR**
   1. Processor shall Process Personal data only under documented instructions of the Controller – as specified in the Agreement and this Data Processing Agreement - and solely for the purpose of providing its services as described in the Agreement. Processor shall immediately inform the Controller if, in its opinion, an instruction infringes Applicable Data Protection Law.
   2. Processor shall not subcontract any part of the Processing without the prior written authorization of the Controller. The Sub-processors authorised by the Controller are listed **in Annex III**.
      1. Controller agrees that Processor may change and engage new Sub-processors to perform all, or part of the Processing defined in Annex I provided Processor informs in writing Controller of any intended change concerning the addition or replacement of Sub-processors at least one month in advance, thereby giving Controller the opportunity to object to such changes based on reasonable data protection grounds.
      2. When Processor engages a Sub-processor, it shall do so by way of a contract that imposes on the Sub-processor in substance, the same obligations as in this Data Processing Agreement.
      3. Where a Sub-processor fails to fulfil its obligations, Processor remains fully liable and accountable to the Controller for the performance of its Sub-processors. Processor shall provide a copy of the contracts signed with its Subcontractors upon request of the Controller (parts of such contracts not related to the Processing of Personal data and confidential can be masked).
   3. Processor ensures that the personnel authorised to process the Personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and have a real need to know based on their functions. Processor shall set up and maintain appropriate technical and organizational security measures, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing carried out for the Controller, as well as the risk of varying likelihood and severity for the rights of individuals. These technical and organisational security measures are described in **Annex II.** Processor shall not reduce the level of security described in Annex II during the Agreement.
   4. Processor assists the Controller in demonstrating compliance with Applicable Data Protection Law in relation with the Processing in Annex I and undertakes to: i) make promptly available to the Controller, upon request, all information necessary to demonstrate such compliance; ii) permit and contribute, at the Controller’s request, to audits of the Processing, at reasonable intervals or if there are reasonable indications of non-compliance. The Controller may choose to conduct the audit by itself or mandate an independent auditor bound by a contractual confidentiality obligation. Audits may include inspections at the premises or physical facilities of the Processor (or a Sub-Processor) where the Processing is carried out and shall be carried out with reasonable written notice.
   5. Any transfer of Personal Data overseas shall be performed in compliance with Applicable Data Protection Law. Processor shall not perform any transfer of Personal Data overseas without the prior authorization of the Controller.
      1. Restricted transfers: when the transfer of Personal data from Controller (as “data exporter”) to Processor (as “data importer”) is a Restricted Transfer, the transfer will be subject to the EU Standard Contractual Clauses, which are deemed incorporated into and form a part of this Data Processing Agreement, as follows : in relation to transfers of Controller’s Personal data governed by the EU GDPR and processed in accordance with this Data processing Agreement, the EU Standard Contractual Clauses will apply, completed as follows: (a) Module Two (Controller to Processor) will apply; b) in Clause 7, the optional docking clause will not apply; c) in Clause 9, the time period for prior notice of Sub-processor changes is set out in this Data Processing Agreement; d). in Clause 11, the optional language will not apply; e). in relation to Claude 13, the competent data protection authority is the data protection authority of the EU Member State in which the data exporter is established, f) in Clause 17, the governing law is the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights (i.e. Germany); g) in Clause 18(b), disputes will be resolved before the courts of the EU Member State in which the data exporter is established. Annexes I, II and III of the EU Standard Contractual Clauses are deemed completed respectively with the information set out in Annexes I, II, III to this Data Protection Agreement, as applicable. Any onward Restricted transfer by Processor to a Sub-processor shall be covered by the EU Standard Contractual Clauses “Processor-Processor”.
      2. UK Addendum and UK International Data Transfer Agreement: in relation to transfers of Personal data governed by EU GDPR and UK Data Protection Law, the EU Standard Contractual Clauses will apply and are deemed amended as specified by the UK Addendum “International Data Transfer Addendum to the EU Commission Standard Contractual Clauses” which is deemed executed by the Parties and incorporated into and forming an integral part of this Data Processing Agreement. Any conflict between the terms of the EU Standard Contractual Clauses and the UK Addendum will be resolved in accordance with the terms of the UK Addendum. When transfers of Personal Data are governed solely by UK Data Protection Law, the Parties agree to be bound by the UK International Data Transfer Agreement (“IDTA”) incorporated herein by reference.
      3. Swiss Addendum: In relation to transfers of Personal data governed by the Swiss FADP, the EU Standard Contractual Clauses will apply, with the following modifications: i. any references in the EU Standard Contractual Clauses or “Regulation (EU) 2016/679” will be interpreted as references to the Swiss FADP, and references to specific Articles of “Regulation (EU) 2016/679” will be replaced with the equivalent article or section of the Swiss FADP; ii. references to “EU”, “Union”, “Member State” and “Member State law” will be interpreted as references to Switzerland and Swiss law, as the case may be, and will not be interpreted in such a way as to exclude data subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU Standard Contractual Clauses; iii. Clause 13 of the EU Standard Contractual Clauses and Part C of Annex 1 are modified to provide that the Federal Data Protection and Information Commissioner (“FDPIC”) of Switzerland will have authority over data transfers governed by the Swiss FADP. Subject to the foregoing, all other requirements of Clause 13 will be observed; iv. references to the “competent supervisory authority” and “competent courts” will be interpreted as references to the FDPIC and competent courts in Switzerland; v. in Clause 17, the EU Standard Contractual Clauses will be governed by the laws of Switzerland; and vi. Clause 18(b) states that disputes will be resolved before the applicable courts of Switzerland.
      4. It is not the intention of either party to contradict or restrict any of the provisions set forth in the EU Standard Contractual Clauses and, accordingly, if and to the extent the EU Standard Contractual Clauses conflict with any provision of the Agreement or this Data Processing Agreement, the EU Standard Contractual Clauses prevail to the extent of such conflict.
   6. To the extent required by Applicable Data Protection Law, Processor assists Controller in the drafting of any Privacy Impact Assessment, consultation with data protection authorities and implementation of any required safeguards and mitigation measures in relation to any Processing or Restricted Transfer performed on behalf of Controller.
   7. Processor shall assist Controller in responding to:
      1. any allegation of non-compliance or demand addressed by any court, law enforcement authority to Processor (or any of its Sub-processors) for disclosure of the Personal Data. In the event that any request, correspondence, enquiry or complaint is made directly to Processor in relation with the Processing in Annex I, Processor will not respond to such communication directly but will inform Controller for Controller to respond. If Processor is legally required to respond to such a request, Processor will promptly notify Controller in advance and provide it with a copy of the request unless legally prohibited from doing so. Where EU Regulation 2016/679 applies to the Processing of Personal data under this Data processing Agreement, such prohibition should be exclusively based on EU or EU Member State Law. Where not prohibited by the EU law, the abovementioned notification shall take place promptly and before any disclosure of Personal Data by Processor or its Sub-processors.
      2. any request for exerting their rights or complaint from data subjects about their Personal data (covered in Annex I). Processor shall not respond directly to those requests or complaints but assist the Controller in fulfilling its obligation to respond in timely and legally compliant manner. In performing this obligation, Processor shall comply with the Controller’s instructions.
   8. In the event of a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the Personal data Processed by Processor or its Sub-Processors for Controller (“Personal Data Breach”), the Processor must:
      1. notify the Controller without undue delay, and in any case by no later than 48 hours after becoming aware of a Personal Data Breach. The notification shall describe the nature of the Personal Data Breach, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal data records concerned, the name and contact details of the data protection officer or other contact point where more information can be obtained, the likely consequences of the Personal Data Breach; the measures taken or proposed to be taken to address the Personal Data Breach and mitigate its possible adverse effects. Where it is not possible to provide the information at the same time, it may be provided in phases without undue delay.
      2. collaborate and set up at its own cost all reasonable and relevant remediation measures to resolve the Personal Data Breach and avoid or limit to the lower extent possible any adverse effect for data subjects.
      3. provide reasonable support to Controller to perform any legally required notification to the data subjects and data protection authority and update its register of Personal Data Breaches.
   9. At the choice of Controller, Processor deletes or returns all Personal data to the Controller at the end of the Agreement, unless Applicable Data Protection Law requires storage of the Personal data. When GDPR is applicable this legal requirement must be based on EU law or EU Member State law.
4. **NON-COMPLIANCE AND TERMINATION**

The Data Processing Agreement is in force from its date of signature until termination of the Agreement and full deletion of Personal data by Processor.

Processor shall promptly inform in writing the Controller, if it becomes unable to comply, for whatever reasons with this Data Processing Agreement and Applicable Data Protection Law. The Controller is entitled to terminate the Agreement and the Data Processing Agreement without prior notice, if the Processor (**i**) becomes unable to comply with this Data Processing Agreement and Applicable Data Protection Laws for whatever reason or (ii) violates this Data Processing Agreement or Applicable Data Protection Law. Processor shall indemnify, defend, and hold Controller harmless, to the fullest extent permitted by law, from and against all losses, judgments, liabilities, costs, expenses, that Controller suffers or incurs as a result of any claims, demands, suits, causes of action or enforcement proceedings (each, a “Claim”) arising from, relating to, any breach of this Data Processing Agreement or Applicable Data Protection Law by Processor or its Sub-processors or Personal Data Breach occurring while Processor (or its Sub-processors) were Processing Personal Data on behalf of Oerlikon.

**SIGNATURE OF THE PARTIESI**

**DateGNATURES**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **For Oerlikon**  **(Controller)** | **Name** | **Title** | **Signature** | **Date** |
|  |  |  |  |
|  |  |  |  |
| **For Supplier**  **(Processor)** |  |  |  |  |

**Annex I - Description of the Processing performed by Processor on behalf of Controller**

|  |  |
| --- | --- |
| **PURPOSE OF THE PROCESSING** |  |
| **NATURE OF THE PROCESSING**  (e.g. consultation, analysis, recording, storage, archiving, duplication, update, deletion, anonymisation,…). |  |
| **CATEGORIES OF PERSONAL DATA PROCESSED** |  |
| **CATEGORIES OF DATA SUBJECTS** |  |
| **SENSITIVE PERSONAL DATA PROCESSED (if any)**  (i.e. health data, social security number, sexual orientation or life, religion, trade union membership, political or philosophical belief, racial/ethnic origin, biometric or genetic data) |  |
| **COUNTRY WHERE PERSONAL DATA IS STORED AND PROCESSED BY PROCESSOR** |  |
| **DURATION OF THE PROCESSING** |  |

**ANNEX II - Technical and organisational security measures of Processor**

**INSTRUCTION: The Technical and Organisational security measures set up by the Processor to protect Personal Data shall be inserted in this Annex II.**

**Annex III : List of Sub-processors**

**The Controller authorises the use of the following Sub-processors for the Processing activities described below:**

|  |  |
| --- | --- |
| **SUBPROCESSOR’s NAME AND ADDRESS** |  |
| **PURPOSE OF PROCESSING** |  |
| **NATURE OF PROCESSING**  (e.g. consultation, analysis, update, recording, storage, anonymisation) |  |
| **CATEGORIES OF PERSONAL DATA** |  |
| **CATEGORIES OF DATA SUBJECTS** |  |
| **SENSITIVE PERSONAL DATA PROCESSED** |  |
| **COUNTRY WHERE PROCESSING IS PERFORMED** |  |
| **DURATION OF THE PROCESSING** |  |