IN WITNESS WHEREOF, the parties have caused this ("**Data Processing Agreement**") to be executed by their authorized representative:

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

Weld Technologies ApS
CVR no. 41978104
Danneskiold-Samsøes Allé 41
1434 København K
Denmark
"the data processor"

and

“the data controller”

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble 3

3. The rights and obligations of the data controller 3

4. The data processor acts according to instructions 4

5. Confidentiality 4

6. Security of processing 4

7. Use of sub-processors 5

8. Transfer of data to third countries or international organisations 6

9. Assistance to the data controller 7

10. Notification of personal data breach 8

11. Erasure and return of data 8

12. Audit and inspection 8

13. The parties' agreement on other terms 9

14. Commencement and termination 9

Appendix A Information about the processing 10

Appendix B Authorised sub-processors 11

Appendix C Instruction pertaining to the use of personal data 11

Appendix D The parties' terms of agreement on other subjects. 14

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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 and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In the context of the provision of setting up a data platform for the data controller, including pulling data together from all of the data controller's different it-solutions into the data controller's central data warehouse, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

[1] References to ”Member States” made throughout the Clauses shall be understood as references to “EEA Member States”.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic review. Based on this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least seven (7) calendar days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). If data controller wishes to object against the change, data controller shall state so within five (5) calendar days after receiving the notification of the data processor. The objection of the data controller must be well-founded. Absence of any objections from data controller shall be deemed a consent to the sub-processing. Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures

in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

   a. transfer personal data to a data controller or a data processor in a third country or in an international organization

   b. transfer the processing of personal data to a sub-processor in a third country

   c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, considering the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than seventy-two (72) hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicating the personal data breach to the data subject when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within forty-eight (48) hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

   a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

   b. the likely consequences of the personal data breach;

   c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so or return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller’s and data processor’s facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor’s physical facilities on presentation of appropriate identification.

13. The parties’ agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties’ signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

On behalf of the data processor

Name Jonas Thordal
Position CEO
Date 24 June 2024
Signature

On behalf of the data controller

Name
Position
Date
Signature

Appendix A Information about the processing

A.1. The purpose of the data processor’s processing of personal data on behalf of the data controller is:

1. To aggregate, centralize, and streamline personal data from different it-solutions of the data controller, ensuring it's consolidated within a singular, cohesive data warehouse operated by the data controller.

A.2. The data processor’s processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

1. The data processor is tasked with transferring personal data from multiple IT solutions owned by the data controller to a data warehouse managed by the data controller. The data processor does not retain any data; it's momentarily held in memory during the synchronization process. Once the data has been successfully migrated to the data warehouse, it's immediately purged. The duration of these synchronization tasks can range from mere minutes to several days.

A.3. The processing includes the following types of personal data about data subjects:

1. Ordinary non-sensitive personal data, including but not limited to:
    1. Name
    2. Contact information
    3. Gender
    4. Personal identification number
    5. Email
    6. Phone number, etc.

2. In certain special cases, sensitive personal data may be processed but, in most situations, the data controller opts not to include IT systems in the data warehouse containing such data considering its nature and category.

A.4. Processing includes the following categories of data subject:

1. Job applicants
2. Employees
3. Contact persons at customers/business partners

A.5. The data processor’s processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

1. The processing will continue for as long as the customer maintains an active subscription with the data processor.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

1. By signing this Data Processing Agreement, Data Controller authorises the Data Processor to engage sub-processors to assist with the performances of the Data Processor. At the time of signing this Data Processing Agreement the following sub-processors are engaged:

NAME	PURPOSE	LOCATION
Amazon Web Services	Cloud Server and database hosting	US based / EU hosted data center in Germany)
Auth0	User authentication system	US based / EU hosted
Stripe	Payment system	US based / EU hosted

2. In case of replacements or engagements of new sub-processors, the data processor shall, where possible, notify data controller no less than seven (7) calendar days prior to the change. If the data controller wishes to object against the change, the data controller shall state so within five (5) calendar days after receiving the notification from the data processor. The objection of the data controller must be well-founded. Absence of any objections from the data controller shall be deemed a consent to the sub-processing.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

1. The data processor’s processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:
    a. Transferring data between multiple IT systems and databases via a data warehouse that is owned by the data controller. The data processor will not store any personal data beyond what is necessary for user authentication and billing.

C.2. Security of processing

1. The data processor will implement the following minimum-security measures agreed upon with the data controller:

    2. Encryption:

    a. The data pipeline at Weld is fully encrypted in transit and at rest, using the in-memory data structure store Redis running our ephemeral workers. We do therefore not see the data we are moving.

    b. Weld uses recent SSL and TLS versions for all connections between systems. From your browser to the Weld application, from our servers to your data warehouse or SaaS application, as well as internally between our own services and databases.

   c. Our own core backend application is located in our HIPAA-compliant AWS deployment, where our servers are in a private subnet without connection to the Internet.

3. **Data storage:**
   a. Weld is running on top of Amazon Web Services (AWS). We host our servers in the European Union and only work with cloud providers whose datacenters are SOC 2 and ISO 27001 certified. These cloud providers guarantee a best-in-class state of the physical and network security of Weld’s servers and help us ensure that our server software is always up to date and protected from any newly discovered threats.

4. **Data handling:**
   a. Weld does not require super-user access to your data warehouse and will request the fewest OAuth scopes needed for your SaaS applications in order to provide the Weld solution. The secrets we store with enterprise-grade AWS Secrets Manager which is both PCI and SOC 2 compliant.
   b. For connection to data warehouses, we support an SSH connection in case the data warehouse is located in a private subnet.

5. **Authentication:**
   a. Two-factor authentication can be implemented for access to the SaaS platform upon request. Our authentication system, also fully encrypted, is handled by enterprise - grade solution Auth0 - more details can be found at https://auth0.com/security.

6. **Resilience:**
   a. Regular backups to restore availability in case of incidents.

7. **Monitoring:**
   a. Real-time monitoring and alerts for unusual activities.

C.3. Assistance to the data controller

1. The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organizational measures at the data controller’s expense:
   a. Assist in fulfilling data subject requests, to the extent applicable.
   b. Notify the data controller within seventy-two (72) hours in the event of a data breach or unauthorized data access.

C.4. Storage period/erasure procedures

1. Personal data is stored for the duration of a user's subscription plus an additional 12 months post-cancellation. Following this period, the data processor will automatically erase the personal data, unless otherwise directed by the data controller.

C.5. Processing location

1. Data processing takes place in Amazon AWS data centres located in Germany. The data processor may update or change these data processing locations. In case of location updates or changes, the data processor shall notify the data controller no less than seven (7) calendar days prior to making the change. If the data Controller wishes to object to the change, they must do so within five (5) calendar days after receiving the notification from the data processor. Any objection from the Data Controller must be well-founded. The absence of any objections from the data controller within this period shall be deemed consent to the new and/or additional processing location.

C.6. Instruction on the transfer of personal data to third countries

1. The data controller accepts that data processor may transfer personal data to a country outside the EEA. The data processor will be required to ensure that such transfer is at all times lawful and in compliance with the GDPR Chapter V, including that there is an adequate level of protection pursuant to the General Data Protection Regulation prior to the transfer of personal data to a country outside the EEA. The same obligation applies in relation to data processor's use of sub-processors in third countries, cf. clause 3 in this data processing agreement.

C.7. Procedures for the data controller’s audits, including inspections, of the processing of personal data being performed by the data processor

1. The Data Controller shall have the right to conduct audits and inspections to ensure the Data Processor's compliance with GDPR, applicable EU or Member State data protection provisions, and the Clauses of this Agreement. Given that all data processing operations are performed within Amazon AWS environments, these audits and inspections will be restricted to virtual audits and inspections of the system configurations, access controls, and data processing activities on Amazon AWS.

2. To facilitate such audits, the Data Processor shall provide the Data Controller with all necessary documentation, including but not limited to, system architecture, data flow diagrams, and any compliance or security certifications obtained concerning Amazon AWS.

3. In case the Data Controller deems it necessary to conduct further investigations, the Data Processor shall cooperate by providing additional information and clarifications regarding data processing operations carried out via Amazon AWS.

4. The Data Controller may elect to involve a third-party auditor to conduct these virtual audits, subject to prior written approval by the Data Processor regarding the choice of auditor.

5. The costs related to audits shall be borne by the Data Controller.

6. The Data Controller shall provide the Data Processor with a minimum of seven (7) days’ notice before initiating any audit or inspection.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

1. The data processor warrants and ensures that the sub-processing is lawful and that any and all sub-processors undertake and are subject to the same terms and obligations as data processor as set out in this Data Processing Agreement. Should the sub- processors not comply with their obligations, the data processor shall remain responsible towards the data controller for all acts and omissions of its sub-processors.

Appendix D The parties' terms of agreement on other subjects.

1. The data processor is entitled to receive payment from the data controller for assistance in relation to clause 9.1, clause 9.2. and clause 10.3.