Data Processing Agreement

(hereinafter referred to as "**Data Processing Agreement**" or "**DPA**")
by and between

1. ESAB (as defined in the ESAB Digital Terms of Service)

and

2. the Client (as defined in the ESAB Digital Terms of Service and Order Form)

- ESAB and Client hereinafter referred to as "**Parties**" and each as "**Party**" -

PREAMBLE

ESAB offers the licensing and maintenance of a cloud platform for managing, and analyzing the performance of, certain ESAB machines, hereinafter altogether called (the "**Services**") in accordance with the ESAB Digital Terms of Service and Order Form entered into by Client and ESAB ("**Agreement**"). In the course of providing the Services, ESAB will process personal data of Client and/or Client's affiliates who are beneficiaries under the Agreement.

This DPA and its Exhibits regulate the data protection obligations of the Parties when processing Client Personal Data under the Agreement. This DPA is supplemental to and subject to the terms and conditions of the Agreement. In the event of a conflict between any of the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail.

DEFINITIONS

1. DEFINITIONS

1.1 Unless otherwise set out below, each capitalised term in this DPA shall have the meaning set out in the Agreement. In this DPA, unless the context requires otherwise:

"**Affiliates**" means the affiliated offices of Client that are expressly identified in the Agreement as beneficiaries under the Agreement;

"**Applicable Law**" means all laws, rules and regulations applicable to either party's performance under this DPA, including but not limited to those applicable to the Processing of Client Personal Data;

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., including any amendments and any implementing regulations thereto that become effective on or after the effective date of this DPA;

"**CCPA Consumer**" means a "consumer" as such term is defined in the CCPA;

"**CCPA Personal Information**" means the "**personal information**" (as defined in the CCPA) about CCPA Consumers that ESAB Processes on behalf of the Client and/or the Client's Affiliates in connection with ESAB's provision of the Services;

"**Controller**" has the meaning given in the GDPR;

"**Client Personal Data**" means information that relates to an identified or identifiable person that is provided to ESAB by Client or its Affiliates, and Processed by ESAB in connection with providing the Services under the Agreement, including, but not limited to the CCPA Personal Information and the GDPR Personal Data;

"**Data Processing Services**" means the Processing of CCPA Personal Information for any purpose permitted by the CCPA, such as for a permitted "business purpose," as such term is defined in the CCPA, or for any other purpose expressly permitted by the CCPA;

"**Data Subject**" has the meaning given in the GDPR;

"**EU Data Protection Laws**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council (the "**GDPR**") and any applicable national legislation implementing or supplementing the GDPR, in each case as amended, replaced or superseded from time to time, and all applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the Processing of GDPR Personal Data as well as the data protection laws of Switzerland and the UK (including the UK Data Protection Act 2018);

"**European Economic Area**" or "**EEA**" means the Member States of the European Union together with Iceland, Norway, and Liechtenstein and – for the purpose of this DPA – also the UK and Switzerland;

"**Instruction**" means any documented instruction submitted in writing by an authorized representative of Client to a designated recipient for ESAB that directs ESAB to perform a specific action with regard to Client Personal Data. Such Instructions may, from time to time thereafter, be amended, supplemented or replaced pursuant to additional Instructions by an authorized representative of Client to a designated recipient for ESAB, provided that such amended, supplemental or replacement Instructions still fall within the scope of the Services. Instructions issued for the purpose of complying with statutory claims under the EU Data Protection Laws or the CCPA, including but not limited to statutory claims under the GDPR with respect to rectification, erasure, restriction or portability, fall within the scope of the Services;

"**GDPR Personal Data**" means the "**personal data**" (as defined in the GDPR) about Data Subjects located in the EEA that ESAB Processes on behalf of the Client and/or the Client's Affiliates in connection with ESAB's provision of the Services;

"**Processing**" has the meaning given in the GDPR, and "**Process**" will be interpreted accordingly;

"**Processor**" has the meaning given in the GDPR;

"**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Client Personal Data;

"**Sell**" and "**Sale**" have the meaning given in the CCPA;

"**Services**" means the service(s) provided by ESAB to the Client under the Agreement, including the Data Processing Services;

"**Standard Contractual Clauses**" means the Standard Contractual Clauses (processors) approved by the European Commission Decision C(2010)593or any subsequent version thereof released by the European Commission, attached as Exhibit F of this DPA;

"**Subprocessor**" means any Processor engaged by ESAB who agrees to Process Client Personal Data in connection with providing the Services to ESAB; and

"**Supervisory Authority**" has the meaning given in the GDPR.

2. AMENDMENT OF AGREEMENT

2.1 This DPA is an integral part of and amends the Agreement with respect to any Processing of Client Personal Data provided by Client or Affiliates in connection with the Agreement.

3. SUBJECT MATTER, DURATION, NATURE AND PURPOSE, AND SPECIFICATION OF PROCESSING OPERATIONS

3.1 The subject matter, duration, nature and purpose of the Processing are described in Exhibit A, this Sec. 3 and the Agreement.

3.2 The categories of data and data subjects which may be affected by the Processing are listed in Exhibit A.

3.3 The duration of the Processing shall correspond to the duration of this Data Processing Agreement as set forth in Sec. 9.

4. ESAB'S OBLIGATIONS

4.1 ESAB shall in the course of providing Services Process Client Personal Data only on behalf of and under the documented Instructions of Client unless such Processing is permitted or required by Applicable Law.

4.2 ESAB shall take steps reasonably necessary to ensure that any natural person acting under its authority who has access to Client Personal Data does not Process such data except on Instructions from Client, unless otherwise required to do so by Applicable Law.

4.3 ESAB ensures that persons authorized to process the Client Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that the obligation will remain after termination of this Data Processing Agreement.

4.4 **Technical and Organizational Data Security Measures**

4.4.1 The appropriate technical and organizational data security measures implemented at the date of the signing of this Data Processing Agreement are specified in Exhibit B. The measures specified in Exhibit B are subject to technical advancements and development.

4.4.2 When assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Personal Data transmitted, stored or otherwise Processed.

4.4.3 If ESAB significantly modifies measures specified in Exhibit B, such modifications have to meet the obligations pursuant to Sec. 4.4.2. ESAB shall make available to Client a description of such modified measures. By notifying, ESAB grants to Client the opportunity to object to such modifications within four (4) weeks. Client shall only be entitled to object to any modification in the case that the modification does not meet the requirements pursuant to Sec. 4.4.2. If Client does not object to the modification within the objection period, consent regarding the modifications shall be assumed. In case of an objection, ESAB may suspend the portion of the Service which is affected by the objection of Client. Client shall not be entitled to a pro-rata refund of remuneration for the Services, unless Client can prove that the obligations pursuant to Sec. 4.4.2 has not been met.

4.5 **Documentation and Audit Rights**

4.5.1 Upon request and subject to signing the non-disclosure agreement attached as Exhibit C and Applicable Law, ESAB shall make available to Client information reasonably necessary to demonstrate ESAB's compliance with its obligations under this DPA, in particular with the agreed technical and organizational data security measures. ESAB shall have the right to limit unreasonable or overly burdensome requests by the Client and charge Client a reasonable fee for the production of such information. ESAB may, in its discretion provide data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, by a publicly certified auditing company or by another Client of ESAB.

4.5.2 If Client has justifiable reason to believe that ESAB is not complying with the terms and conditions under this Data Processing Agreement, in particular with the obligation to implement and maintain the agreed technical and organizational data security measures, and only once per year (unless there are specific indications that require a more frequent inspection), Client is, subject to signing the non-disclosure agreement attached as Exhibit C, entitled to audit ESAB. This audit right can be exercised by (i) requesting additional information, (ii) accessing the databases which process Client Personal Data or (iii) by inspecting ESAB's working premises whereby in each case no access to personal data of other Clients or ESAB’s confidential information will be granted. Alternatively, Client may also engage third party auditors to perform such tasks on its behalf in accordance with

Sec. 4.5.4. The costs associated with such audits and/or for providing additional information shall be borne by Client.

4.5.3 If Client intends to conduct an audit at ESAB's working premises, Client shall give reasonable notice to ESAB and agree with ESAB on the time and duration of the audit. In the case of a special legitimate interest, such audit can also be conducted without prior notice. Inspections shall be made during regular business hours and in such a way that business operations are not disturbed. At least one employee of ESAB may accompany the auditors at any time. ESAB may memorialize the results of the audit which shall be confirmed by Client.

4.5.4 Client may not appoint a third party as auditor who (i) ESAB reasonably considers to be in a competitive relationship to ESAB or (ii) is not sufficiently qualified to conduct such an audit, or (iii) is not independent. Any such third-party auditor shall only be engaged if the auditor is bound by a non-disclosure agreement in favor of ESAB prior to conducting any audit or is bound by statutory confidentiality obligations.

4.6 **Notification Duties**

4.6.1 ESAB shall inform Client without undue delay in text form (e.g., letter, fax or email "**Text Form**") of the following events:

- Requests from third parties including such from a Supervisory Authority regarding Client Personal Data; in which case it is permitted to inform the third party of the name of Client and the fact that it has forwarded the request to Client.

- Threats to Client Personal Data in possession of ESAB by garnishment, confiscation, insolvency and settlement proceedings or other incidents or measures by third parties. In such case, ESAB shall immediately inform the respective responsible person/entity that Client holds the sovereignty and ownership of the Client Personal Data.

4.6.2 For the purpose of enabling Client to comply with its own Security Incident notification obligations, ESAB shall notify Client without undue delay after becoming aware of a Security Incident. Such notice will, if possible, include the following information:

- a description of the nature of the Security Incident including where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Client Personal Data records concerned;

- a description of the measures taken or proposed to be taken by ESAB and/or Client to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects; and

- any further information which is available and known to ESAB and (i) that is necessary for Client to comply with Client's notification obligations and (ii) which Client does not otherwise have access to.

4.6.3 ESAB will take any additional steps, at Client's request and expense, that are reasonably necessary to remedy any non-compliance with this DPA.

4.7 **Instructions**

4.7.1 ESAB shall inform Client immediately if, from its point of view, an Instruction of Client may lead to a violation of Applicable Law. Until Client either confirms or alternates the Instruction, ESAB may refuse to comply with the Instruction issued.

4.8 **Duration and Retention**

4.8.1 Except as otherwise provided in clause 4.8.2, ESAB shall, upon completion of the Services in consultation with Client, either delete or return all Client Personal Data in its possession to Client.

4.8.2 ESAB may retain Client Personal Data to the extent required by Applicable Laws after the termination of this DPA, provided that ESAB shall ensure the confidentiality of all such Client Personal Data in accordance with this DPA and the Agreement and shall ensure that such Client Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage.

4.8.3 If a Data Subject addresses ESAB with claims for access, rectification, erasure, restriction, objection or data portability, ESAB shall refer the data subject to Client.

4.9 ESAB will inform Client of the name and the official contact details of its data protection officer if ESAB is, by Applicable Law, required to appoint a data protection officer.

4.10 Without limitation to the foregoing, ESAB's Processing of GDPR Personal Data is subject to the additional terms set forth in Exhibit D and ESAB's Processing of CCPA Personal Information is subject to the additional terms set for in Exhibit E.

5. CLIENT'S OBLIGATIONS

5.1 Client shall provide all Instructions pursuant to this Data Processing Agreement to ESAB in Text Form or verbally. Verbal Instructions shall be confirmed immediately in Text Form thereafter.

5.2 Client shall notify ESAB in Text Form of the names of the persons who are entitled to issue Instructions to ESAB. Any consequential costs incurred resulting from Client's failure to comply with the preceding sentence shall be borne by Client. In any event, the managing directors and personnel/human resource management of Client are entitled to issue Instructions.

5.3 Client shall inform ESAB immediately if Processing by ESAB might lead to a violation of Applicable Law.

5.4 In the case claims based on Applicable Law are raised against ESAB, Client shall reasonably support ESAB with its defense to the extent the claim arises in connection with the Processing of Client Personal Data by ESAB in connection with performing the Services to Client or Affiliate.

5.5 Client shall name a person responsible for dealing with questions relating to Applicable Law and data security in the context of performing this Data Processing Agreement.

6. LIABILITY

6.1 The Parties agree that notwithstanding anything contained hereunder, when providing the Services, ESAB's liability for breach of any terms and conditions under this Data Processing Agreement shall be subject to the liability limitations agreed in the Agreement.

6.2 No Affiliate shall become beneficiary of this Data Processing Agreement without being bound by this Data Processing Agreement and without accepting the liability limitation set out in Sec. 6.1 above.

6.3 Client will indemnify ESAB against any losses that exceed the liability limitations in the Agreement suffered by ESAB in connection with any claims of Affiliates or Data Subjects who claim rights based on alleged violation of the GDPR or this Data Processing Agreement.

7. COSTS FOR ADDITIONAL SERVICES

If Client's Instructions lead to a change from or increase of the agreed Services or in the case of ESAB's compliance with its obligations pursuant to Sec. **Error! Reference source not found.** or **Error! Reference source not found.** to assist Client with Client's own statutory obligations, ESAB is entitled to charge reasonable fees for such tasks which are based on the prices agreed for rendering the Services and/or notified to Client in advance.

8. CONTRACT PERIOD

The duration of this Data Processing Agreement coincides with the duration of the Agreement. It commences and terminates with the provision of the Services under the Agreement, unless otherwise stipulated in the provisions of this Data Processing Agreement.

9. MODIFICATIONS

ESAB may modify or supplement this Data Processing Agreement, with notice to Client, (i) if required to do so by a Supervisory Authority or other government or regulatory entity, (ii) if necessary to comply with Applicable Law, (iii) to implement standard contractual clauses laid down by the European Commission or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Applicable Law.

10. WRITTEN FORM

Any side agreements to this Data Processing Agreement as well as changes and amendments of this Data Processing Agreement or the Services hereunder, including this Sec. 10, shall be in writing.

11. CHOICE OF LAW

11.1 This DPA and any dispute or claim arising out of it or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in

accordance with the laws of the EU Member State in which the Client is established; provided, however, that to the extent any such dispute or claim relates to the CCPA, such dispute shall be governed by and construed in accordance with the laws of California.

11.2 Any claim or dispute between the Parties arising out of, or in connection with, this DPA (a "Dispute") that cannot be resolved by direct discussions between the Parties shall be resolved in accordance with the procedure set out in the Agreement, if any.

12. MISCELLANEOUS

12.1 With respect to any issues arising of or in connection with the Processing of Client Personal Data, this Data Processing Agreement shall prevail over all other agreements between the Parties. This DPA sets forth the entire understanding and agreement between the Parties with respect to the subject matter hereof.

12.2 **Severability**

12.2.1 If any court or competent authority decides that any term of this DPA is held to be invalid, unlawful, or unenforceable to any extent, such term shall, to that extent only, be severed from the remaining terms, which shall continue to be valid to the fullest extent permitted by law. The Parties will mutually agree on modifications to the Agreement to the extent necessary to ensure compliance with Applicable Law.

12.3 **No Waiver**

12.3.1 Either Party's failure to enforce any provision of this DPA shall not constitute a waiver of that or any other provision and will not relieve the other Party from the obligation to comply with such provision.

Exhibit A – Data Processing Specification

Data Exporter

The Client subscribed to the Services that include Processing of GDPR Personal Data.

Data Importer

ESAB, providing the Services as described in the Agreement and in the DPA.

Subject matter, Nature and Purpose of Processing

ESAB offers Client the Services for managing and analyzing the performance of welding machines. Information regarding the welding machines and the welding activities is send to ESAB's online platform(s). Client can use the platform(s) to manage their worldwide welding equipment. With the help of the Services, the performance and work of the machines can be analyzed.

Categories of Data

The Client determines the categories of data entered onto the Services. The transferred GDPR Personal Data typically relates to the following categories of data.

- Data of the welding and cutting machines, incl. status and location
- Data regarding welding and cutting activities, incl. data on the welding method, welded material (including 3D model containing the design of the product being welded, geometry of joints, work and travel angle of welding torch, and speed of welding torch), parameters of welding source (and volts, amperes, and wire feed speed parameters of the welding source), welding job number, usage of power and material
- Information on user accounts, such as user names, passwords, information of usage of the Services, information on operation of welding and cutting machines, user's welding authorization.

Categories of Data Subjects

Unless provided otherwise by the Data Exporter, transferred GDPR Personal Data relates to the following categories of data subjects:

- Users of the Services – potentially employees, contractors or agents of the Client.
- Machine operators/ Welders – potentially employees, contractors or agents of the Client.

Data Retention

ESAB stores the Client's Personal Data in the Services for the period of the Agreement. Data will be deleted earlier upon Client's request.

Exhibit B – Description of the Technical and Organizational Security Measures

1. Pseudonymization and Encryption

Pseudonymization contains measures that enable one to process personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures. Encryption contains measures that enable one to convert clearly legible information into an illegible string by means of a cryptographic process.

- The user data and the weld data are stored in separate databases
- The user data and the weld data are encrypted according to Microsoft Azure DB standard

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

Confidentiality and integrity are ensured by the secure processing of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

2.1 Confidentiality

2.1.1. Physical access control

Measures that prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

- Data processing systems are governed by the capabilities of Microsoft Azure. Furthermore, personal data is protected by unique and secure user credentials. Access to personal computers and PC are protected by security guards and secure room control access cards, limiting access only to authorized personnel. Access cards are provided and removed by Facility Administration staff.
- The Services use Microsoft Azure data centers and therefore Microsoft handles the physical access control to the data processing centers. More information can be read at the following link: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security#physical-security

2.1.2 System/Electronic access control

Measures that prevent data processing systems from being used without authorization.

- Unique two-step verification is required per application. Password change requests administered every 90 days.
- The Service uses Microsoft Azure access control. More information can be read at the following link: https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal#overview-of-access-control-iam

2.1.3 Internal Access Control

Measures that ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage.

- This process is managed by the ESAB IT Director. Credentials are distributed only to authorized users at time of account start-up. Unique two-step verification is required per application.

Password change requests administered every 90 days. ESAB maintains a policy to reset unique credentials in the event of a stolen computer or lost/compromised password.

2.1.4 Isolation/Separation Control

Measures to ensure that data collected for different purposes can be processed (storage, amendment, deletion, transmission) separately.

- Data collected for different purposes are stored in different databases (locations).
- Processing operations in the databases are not interlinked.
- Data collected for different purposes can be processed only by select authorized personnel for purposes of manual data separation.

2.1.5 Job Control

Measures that ensure that, in the case of commissioned processing of personal data, the data are processed strictly corresponding the instructions of the principal.

- Data are strictly processed corresponding to the instructions of the principal by authorized personnel automatically.
- By granting the Client an administrative account, the Client can activate the available Services features itself and initiate, stop or amend the processing operations offered by ESAB.
- The employees with access to the administrative accounts held and used by ESAB employees are contractually bound to use the accounts only to carry out instructions of the Clients and only to the extent such processing cannot be initiated by the Client itself. Employees with access to administrative accounts are trained on GDPR and other applicable data protection requirements on a regular basis.
- Employees providing maintenance services for the Services with potential access to personal data are contractually bound to access and process personal data in the Services only to the extent necessary to provide maintenance services. These employees are trained on GDPR and other applicable data protection requirements on a regular basis.

2.2. Integrity

2.2.1 Data transmission control

Measures ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.

- The Services support secured web connection (HTTPS), user authentication and role-based access control. Therefore, if the Client chooses to use the role-based access control, only authorized users can access specific personal data.
- Only authorized product users may read or copy data. Only authorized ESAB personnel may remove data from the database. The data provided can be downloaded to PDF, jpeg and excel format. PDF and jpeg cannot be modified without specific editing tools. Excel may be modified, but only with deliberate act to alter data. Access to alterations is highly restrictive and only authorized ESAB personnel have ability and are able to perform the alteration act with written consent from all authorized stakeholders.

2.2.2 Data input control

Measures that ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed.

- Authorized users are able to select users to have access to product. This limits who inputs personal data and it is the choice of the authorized user which data to check and establish.
- All modifications in the Services will be monitored and all data related thereto will be stored by Azure Monitor. This allows Client and ESAB to verify whether and by whom personal data has been processed.

2.3 Availability and Resilience of Processing Systems and Services

Availability includes measures that ensure that personal data is protected from accidental destruction or loss due to internal or external influences. Resilience of processing systems and services includes measures that ensure the ability to withstand attacks or to quickly restore systems to working order after an attack.

- Link to MS Azure security measures:

  https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-azure?view=o365-worldwide

  https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data

  https://docs.microsoft.com/en-us/azure/cosmos-db/compliance
- The data in the Services is located in two different Azure data centers (different physical locations). Therefore in case of an attack or lose of information from any other reason the data can be restored within a short time.
- The Azure virtual machines and WeldCloud databases are backed by Microsoft.
- The Services source code is version controlled and in case of malfunction it can be restored.

3. Disaster Recovery and Business Continuity

Organizational measures that ensure the possibility to quickly restore the system or data in the event of a physical or technical incident.

- ESAB is subjected and consistent with Microsoft Azure restoration of system or data protocol.
- The Services data is located in two different Azure data centers (different physical locations). Therefore in case of an attack or lose of information from any other reason the data can be restored within a short time.
- The Services databases are backed by Microsoft.
- The Services source code is versioned control and in case of malfunction it can be restored.

4. Risk Assessments

Organizational measures that ensure the regular review and assessment of technical and organizational measures.

- On a minimum of annual review cycle, or in event of special requirement, ESAB reviews technical and organizational measures. In the event of a special requirement, ESAB holds review and action meeting with all relevant key holders (IT, R&D) to ensure compliance with procedures and update if necessary.

Exhibit C – Non-Disclosure Agreement

Non-Disclosure Agreement

(hereinafter referred to as "**NDA**")
by and between

1. ESAB, as defined in the Data Processing Agreement

and

2. Client, as defined in the Data Processing Agreement

PREAMBLE

The Data Processing Agreement concluded between ESAB and Client grants Client the right to demand information and to audit ESAB for the purposes and within the restrains of Section 3.7 of the Data Processing Agreement. When exercising these auditing rights, Client can potentially gain access to proprietary and confidential information of ESAB relating to the Services or other aspects of ESAB's business. Wishing to protect all confidential information of ESAB, which could be disclosed to Client in the context of Client's document requests or auditing, the Parties enter into the following NDA.

1. INFORMATION

In this NDA "Confidential Information" means all information, know-how, samples and the like of ESAB, disclosed in any form or medium whatsoever, to Client in the context of Client's document request or auditing. For the avoidance of doubt, Client Personal Data is not considered Confidential Information.

2. CONFIDENTIALITY

2.1 Client undertakes to keep all Confidential Information secret and confidential and not to disclose Confidential Information to third parties. Client also undertakes to use the Confidential Information only to the extent necessary to conduct and evaluate the document review and auditing. All Confidential Information will be kept in safe custody by Client and will at all times remain the property of ESAB. Once the Confidential Information is no longer needed for the purposes of evaluating the document review or audit, Client will return all originals, copies, reproductions, summaries and other tangible forms of Confidential Information to ESAB and delete all Confidential Information in its possession irrespective of the form or medium of such Confidential Information.

2.2 In case ESAB has in advance agreed in writing that Client may disclose all or certain pieces of Confidential Information to a third party, Client will nevertheless be liable to ESAB in ensuring that such third party is bound to obligations not less onerous than Client's obligations assumed hereunder.

2.3 The term "third party" will not apply to Affiliates, as defined in the Data Processing Agreement, provided such Affiliate is bound to the same extent of secrecy as Client under this NDA.

2.4 If Client breaches the confidentiality obligations of this NDA, ESAB shall be entitled to claim a contractual penalty for each breach in the amount of USD 50,000.00. Any further claims of ESAB, including claims for cease-and-desist and for damages, are not affected.

3. EMPLOYEES

Client is entitled to disclose the Confidential Information to those employees who have a need to know such Confidential Information for the performance of the document review or audit and only to those employees who (i) have been bound, in writing, to maintain the Confidential Information in confidence both during and after the term of their employment to the extent permitted by the applicable law or (ii) are bound under their employment contracts by comparable confidentiality obligations.

4. RIGHTS

Client acknowledges that the right, title and interest in the Confidential Information are and remain the exclusive property of ESAB. Nothing in this NDA is intended to give or shall be interpreted as giving Client a license, express or implied, under any of ESAB's patents and/or other rights now owned or hereinafter acquired by ESAB.

5. NO ANALYSIS

Client will not analyze or have analyzed samples, including but not limited to reverse engineering or any observation of the chemical composition and/or physical characteristics, disclosed in the context of a document review or audit.

6. EXCEPTIONS

6.1 The preceding obligations of this NDA do not apply to Confidential Information which

(i) at the time of disclosure is in the public domain;

(ii) was in Client's possession at the time of disclosure by ESAB;

(iii) after disclosure becomes part of the public domain by publication or otherwise through no fault of Client;

(iv) was obtained by Client from a third party, having a lawful right to disclose the same;

(v) was developed by Client independently from any access to the Confidential Information supplied by ESAB; or

(vi) is required to be disclosed by applicable law, regulation or order of a court of competent jurisdiction provided, however, that Client takes all reasonable steps to restrict and maintain the confidentiality of such disclosure and provides reasonable prior written notice to ESAB of the requirement to disclose such Confidential Information and the specific disclosure(s) proposed to be made to satisfy such law(s), regulation(s) or legal process(es).

6.2 Facts according to (i) to (vi) above must be proven by Client.

6.3 Any Confidential Information disclosed hereunder will not be deemed within the foregoing exceptions merely because such Confidential Information is embraced by more general information in the public domain or in Client's possession, nor will any combination of items of Confidential Information be deemed within the exceptions unless the combination itself and its principle of operation are within the exceptions.

7. SEVERABILITY

Should any provision of this NDA be or become invalid or unenforceable, such invalidity or unenforceability will not affect the validity or enforceability of the entire NDA. Invalid or unenforceable provisions will be replaced by a legally valid and enforceable regulation which comes closest to the original intention of the Parties. The same applies accordingly to any involuntary omissions in this NDA.

8. MISCELLANEOUS

8.1 This NDA constitutes the entire agreement between the parties relating to the subject matter hereto.

8.2 This NDA may not be changed or amended orally, but only in writing and signed by both Parties. The writing must refer to this NDA and must expressly state that it is an amendment hereof.

8.3 This NDA will in all respects be interpreted in accordance with and its performance governed by the laws of Sweden, to the exclusion of its conflict of laws provisions.

Exhibit D – GDPR Data Processing Addendum

BACKGROUND

This GPDR Data Processing Addendum ("**GDPR Addendum**") is supplemental to and subject to the terms and conditions of the Agreement and the DPA and shall apply to ESAB's Processing of GDPR Personal Data on Client's behalf. In the event of a conflict between any of the provisions of this GDPR Addendum and the provisions of the Agreement or the DPA, the provisions of this GDPR Addendum shall prevail.

1. INTERPRETATION

1.1 Unless otherwise set out below, each capitalised term in this GDPR Addendum shall have the meaning set out in the Agreement and the DPA.

2. GDPR PERSONAL DATA PROCESSING

2.1 **Applicability to GDPR Personal Data.** This exhibit to the DPA shall only apply to the Processing of GDPR Personal Data by or on behalf of ESAB.

2.2 **Role of the Parties.** For the purposes of the EU Data Protection Laws, the Parties acknowledge and agree that ESAB acts as Processor and the Client and/or Affiliates act as Controllers, except when Client or Affiliate acts as a Processor of GDPR Personal Data, in which case ESAB is a subprocessor. The Client acts as a single point of contact for its Affiliates with respect to compliance with EU Data Protection Laws, such that where ESAB gives notice to the Client, such information or notice is deemed received by the Affiliates. The Parties acknowledge and agree that any claims in connection with EU Data Protection Laws under this DPA will be brought by the Client, whether acting for itself or on behalf of an Affiliate.

2.3 **Specification of Processing Operations**

The subject matter, duration, nature and purpose of the Processing of GDPR Personal Data are described in the Agreement and Schedule 2 of Exhibit G. The categories of GDPR Personal Data and Data Subjects which may be affected by such Processing are listed in Schedule 2 of Exhibit G. The duration of such Processing is set forth in clause 8.

2.4 **Instructions for GDPR Personal Data Processing**

ESAB will only Process GDPR Personal Data in accordance with:

(a) the Agreement, to the extent necessary to provide the Services to the Client, and

(b) the Client's Instructions,

unless Processing is required by European Union or Member State law to which ESAB is subject, in which case ESAB shall, to the extent permitted by European Union or Member State law, inform the

Client of that legal requirement before Processing that GDPR Personal Data. In addition to any other fees set forth in the Agreement, ESAB shall have the right to charge the Client commercially reasonable rates for complying with the Client's Instructions relating to the Processing of GDPR Personal Data.

2.5 **Required consents and notices**

Where required by applicable EU Data Protection Laws, the Client will ensure that it has obtained/will obtain all necessary consents, and has given/will give all necessary notices, for the Processing of GDPR Personal Data by ESAB in accordance with the Agreement.

3. TRANSFER OF GDPR PERSONAL DATA

3.1 ESAB may engage Subprocessors for the Processing of GDPR Personal Data subject to the requirements of this Clause 3 of Exhibit D.

3.2 Any Subprocessor is obliged, before initiating the Processing of GDPR Personal Data, to commit itself in writing for the benefit of Client to comply with the same data protection obligations as the applicable obligations under this DPA. The agreement with the Subprocessor must provide at least the level of data protection required by the applicable sections of this DPA. Where the Subprocessor fails to fulfil such data protection obligations with regard to GDPR Personal Data, ESAB shall remain fully liable to Client for the performance of the Subprocessor's obligations.

3.3 Any Subprocessor that Processes GDPR Personal Data must in particular agree to comply with the applicable agreed technical and organizational security measures in accordance with clause **Error! Reference source not found.** herein and provide ESAB with a list of the implemented technical and organizational measures, which upon request by Client will also be made available to Client. Subprocessor's measures may differ from the ones agreed between Client and ESAB but shall not fall below the level of data security for GDPR Personal Data as provided by the measures of ESAB.

3.4 ESAB will inform Client in writing (email communication being sufficient) of any intended engagement of a Subprocessor for the Processing of GDPR Personal Data. Alternatively, ESAB may provide a website or another notice that lists all Subprocessors to access GDPR Personal Data of Client as well as the limited or ancillary services they provide. At least two (2) weeks before authorizing any new Subprocessor to access GDPR Personal Data, ESAB will notify Client thereof and, if applicable, update its website. By so notifying, ESAB grants to Client the opportunity to object to such change within two (2) weeks. If Client does not object to the engagement within the objection period, consent regarding the engagement shall be assumed. Upon Client's request, ESAB will provide all information necessary to demonstrate that the Subprocessor will meet all requirements pursuant to Sec. **Error! Reference source not found.** and 3.3. In the case Client objects to the Processing of GDPR Personal Data by a potential Subprocessor, ESAB can choose to either not engage the Subprocessor or to terminate the Agreement with two (2) months prior written notice. Until the termination of the Agreement, ESAB may suspend the portion of the Services that is affected by the objection of Client. Client shall not be entitled to a pro-rata refund of the remuneration for the Services, unless the objection is based on justified reasons of non-compliance with applicable EU Data Protection Laws.

3.5 Client herewith agrees also on behalf of its Affiliates to the following Subprocessors of GDPR Personal Data:

For Cloud Hosting Services:

- Microsoft Corporation, Redmond, WA 98052-6399, USA (Azure Cloud)

For Software Maintenance Services:

- PTC Inc., 121 Seaport Blvd, Boston Massachusetts 02210, USA (Thinkworx Software).

For all kinds of services:

- The ESAB Group, Inc., 411 South Ebenezer Road, P.O. Box 100545, Florence, SC 29501-0545, USA
- Colfax Corporation, 420 National Business Parkway, 5th Floor, Annapolis Junction, MD 20701, USA.
- Twillo Inc., 375 Beale St #300, San Francisco, CA 94105, USA.
- Transition Technologies S.A., ul. Pawia 55, 01-030 Warsaw, Poland.
- Vinnter AB, Kvarnbergsgatan 2, Göteborg, 411 05, Sweden.
- Goovin AB, Kvarnbergsgatan 2 411 05 Göteborg, Sweden.
- ENFO, Valgatan 30, Göteborg 405 22, Sweden.
- Google Inc., 600 Amphitheatre Parkway in Mountain View, California, USA.
- Mixpanel, San Francisco (HQ), 405 Ward Street, 2nd Floor, San Francisco, USA.
- Sentry, 132 Hawthorne St, San Francisco, CA 94107, USA.
- Stripe, 510 Townsend Street, San Francisco, CA 94103, USA.
- Fullstory, 1745 Peachtree St NE, Atlanta (HQ), GA, USA.
- PhotoeditoSDK, img.ly GmbH, Kortumstraße 68, 44787 Bochum, Germany.
- Heroku, 415 Mission Street, Suite 300, San Francisco, CA 94105, USA.
- Amazon AWS, 410 Terry Avenue North, Seattle, WA 98109-5210, USA.
- Crisp, 2 Boulevard de Launay, 44100 Nantes, France.
- Java, Oracle Corporation, 500 Oracle Parkway, Redwood Shores, California 94065, USA.
- Apache, The Apache Software Foundation, 1901 Munsey Drive, Forest Hill, Mayland 21050-274700, USA.
- Tomcat, The Apache Software Foundation, 1901 Munsey Drive, Forest Hill, Mayland 21050-274700, USA.
- Apache Maven, The Apache Software Foundation, 1901 Munsey Drive, Forest Hill, Mayland 21050-274700, USA.
- Hibernate, Red Hat, East Davie Street, Raleigh, North Carolina 27601, USA.
- Vaadin / Vaadin Report, Vaadin Ltd, Ruukinkatu 2-4, FI-20540, Turku, Finland.
- JasperReport, TIBCO Software Inc., 3307 Hillview Avenue, Palo Alto, California 94304, USA.
- Spring, VMware Inc., 3401 Hillview Avenue, Palo Alto, California 94304, USA.
- Microsoft MS-Sql, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052-6399, USA.

- Microsoft PowerBI, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052-6399, USA.
- Community Development: io springfox; com h2database; org postgres; org mapstruct; org jasypt.

3.6 **Prohibition on Transfers of GDPR Personal Data**

GDPR Personal Data may only be exported or accessed by ESAB or its Subprocessors outside the EEA or Switzerland (the "**International Transfer**"):

(a) if the recipient, or the country or territory in which it Processes GDPR Personal Data, ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of GDPR Personal Data as determined by the European Commission; or

(b) in accordance with Sec. 3.7.

3.7 **Standard Contractual Clauses**

(a) The Standard Contractual Clauses between Client, Affiliate and ESAB as set out in Exhibit F apply where there is an International Transfer to or within a country or territory that does not ensure an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of GDPR Personal Data as determined by the European Commission.

(b) For Subprocessors based outside the EEA and outside any country for which the European Commission has published an adequacy decision (the "**Third Country Subprocessors**"), ESAB will enter into an unchanged version of the Standard Contractual Clauses reflecting what has been agreed in Exhibit F with Third Country Subprocessors prior to the Subprocessor's processing of GDPR Personal Data. The Client hereby accedes to the Standard Contractual Clauses between ESAB and the Third Country Subprocessor. ESAB will enforce the Standard Contractual Clauses against the Subprocessor on behalf of the Client if a direct enforcement right is not available under EU Data Protection Laws.

(c) If there is an inconsistency between any of the provisions of this DPA and the provisions of the Standard Contractual Clauses, the provisions of the Standard Contractual Clauses shall prevail.

4. ACCESS REQUESTS AND DATA SUBJECT RIGHTS

4.1 Unless otherwise required by applicable law, ESAB shall promptly notify the Client of any request received by ESAB or any Subprocessor from a Data Subject in respect of the GDPR Personal Data of the Data Subject and shall not respond to the Data Subject.

4.2 Where applicable by virtue of Article 28(3)(e) of the GDPR, taking into account the nature of the Processing, ESAB shall assist the Client by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Client's obligation to respond to requests for exercising Data Subject rights laid down in the GDPR.

5. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

5.1 Where applicable by virtue of Article 28(3)(f) of the GDPR, ESAB shall provide reasonable assistance to the Client with any data protection impact assessments which are referred to in Article 35 of the GDPR and with any prior consultations to any Supervisory Authority of the Client which are referred to in Article 36 of the GDPR, in each case solely in relation to Processing of GDPR Personal Data and taking into account the nature of the Processing and information available to ESAB.

6. ADDITIONAL LIABILITY CLAUSES

6.1 Client and ESAB shall be each liable for damages of affected Data Subjects according to Art. 82 GDPR (external liability). Sec. 6.1 shall have no effect as regards the external liability.

6.2 Either Party shall be entitled to claim back from the other Party, ESAB or Client, that part of the compensation, corresponding to the other Party's part of responsibility for the damage (internal liability).

Exhibit E – CCPA Data Processing Addendum

BACKGROUND

This CCPA Data Processing Addendum ("**CCPA Addendum**") is supplemental to and subject to the terms and conditions of the Agreement and the DPA and shall apply to ESAB's Processing of CCPA Personal Information on Client's behalf. In the event of a conflict between any of the provisions of this CCPA Addendum and the provisions of the Agreement or the DPA, the provisions of this CCPA Addendum shall prevail.

1. INTERPRETATION

1.1 Unless otherwise set out below, each capitalised term in this CCPA Addendum shall have the meaning set out in the Agreement and the DPA.

2. CCPA PERSONAL INFORMATION PROCESSING

2.1 **Applicability to CCPA Personal Information.** This Exhibit F to the DPA shall apply to the Processing of CCPA Personal Information by or on behalf of ESAB.

2.2 **Role of the Parties.** For the purposes of the CCPA, the Parties acknowledge and agree that ESAB will act as a "Service Provider" as such term is defined in the CCPA, in its performance of its obligations pursuant to the Agreement. The Client will act as a single point of contact for its Affiliates with respect to CCPA compliance, such that if ESAB gives notice to the Client, such information or notice will be deemed received by the Client's Affiliates. The Parties acknowledge and agree that any claims in connection with the CCPA under this DPA will be brought by the Client, whether acting for itself or on behalf of an Affiliate.

2.3 **Instructions for CCPA Personal Information Processing**

ESAB shall not retain, use or disclose CCPA Personal Information for any purpose other than for the specific purpose of providing the Services, or as otherwise permitted by the CCPA, including retaining, using, or disclosing CCPA Personal Information for a commercial purpose other than providing the Services.

Processing CCPA Personal Information outside the scope of this DPA or the Agreement will require prior written agreement between the Client and ESAB on additional Instructions for Processing. In addition to any other fees set forth in the Agreement, ESAB shall have the right to charge the Client commercially reasonable rates for complying with the Client's Instructions relating to the Processing of CCPA Personal Information.

2.4 Required consents and notices

Where required by applicable laws, the Client will ensure that it has obtained/will obtain all necessary consents, and has given/will give all necessary notices, for the Processing of CCPA Personal Information by ESAB in accordance with the Agreement.

3. TRANSFER OF CCPA PERSONAL INFORMATION

3.1 No Sale of CCPA Personal Information

The ESAB shall not Sell any CCPA Personal Information to another business or third party without the prior written consent of the Client unless and to the extent that such Sale is made to a Subprocessor for a business purpose, provided that ESAB has entered into a written agreement with Subprocessor which imposes the same obligations on the Subprocessor with regard to their Processing of CCPA Personal Information as are imposed on the ESAB under this DPA and the Agreement. Notwithstanding the foregoing, nothing in this DPA or the Agreement shall restrict the ESAB's ability to disclose CCPA Personal Information to comply with applicable laws or as otherwise permitted by the CCPA.

3.2 Subprocessors

ESAB may engage any Subprocessors for the Processing of CCPA Personal Information that commit in writing for the benefit of Client to comply with the same data protection obligations as the applicable obligations under this DPA, including but not limited to any applicable minimum technical and organizational security measures set forth in this DPA. The agreement with the Subprocessor must provide at least the level of data protection required by the applicable sections of this DPA. Where the Subprocessor fails to fulfil such data protection obligations, ESAB shall remain fully liable to Client for the performance of the Subprocessor's obligations. Client acknowledges and agrees that the following Subprocessors may Process CCPA Personal Information on behalf of Client and its Affiliates:

For Cloud Hosting Services:

- Microsoft Corporation, Redmond, WA 98052-6399, USA (Azur Cloud)

For Software Maintenance Services:

- PTC Inc., 121 Seaport Blvd, Boston Massachusetts 02210, USA (Thinkworx Software).

For all kinds of services:

- The ESAB Group, Inc., 411 South Ebenezer Road, P.O. Box 100545, Florence, SC 29501-0545, USA
- Colfax Corporation, 420 National Business Parkway, 5th Floor, Annapolis Junction, MD 20701, USA.
- Twillo Inc., 375 Beale St #300, San Francisco, CA 94105, USA.
- Transition Technologies S.A., ul. Pawia 55, 01-030 Warsaw, Poland.
- Vinnter AB, Kvarnbergsgatan 2, Göteborg, 411 05, Sweden.
- Goovin AB, Kvarnbergsgatan 2 411 05 Göteborg, Sweden.
- ENFO, Valgatan 30, Göteborg 405 22, Sweden.
- Google Inc., 600 Amphitheatre Parkway in Mountain View, California, USA.
- Mixpanel, San Francisco (HQ), 405 Ward Street, 2nd Floor, San Francisco, USA.
- Sentry, 132 Hawthorne St, San Francisco, CA 94107, USA.
- Stripe, 510 Townsend Street, San Francisco, CA 94103, USA.
- Fullstory, 1745 Peachtree St NE, Atlanta (HQ), GA, USA.
- PhotoeditoSDK, img.ly GmbH, Kortumstraße 68, 44787 Bochum, Germany.
- Heroku, 415 Mission Street, Suite 300, San Francisco, CA 94105, USA.
- Amazon AWS, 410 Terry Avenue North, Seattle, WA 98109-5210, USA.
- Crisp, 2 Boulevard de Launay, 44100 Nantes, France.
- Java, Oracle Corporation, 500 Oracle Parkway, Redwood Shores, California 94065, USA.
- Apache, The Apache Software Foundation, 1901 Munsey Drive, Forest Hill, Mayland 21050-274700, USA.
- Tomcat, The Apache Software Foundation, 1901 Munsey Drive, Forest Hill, Mayland 21050-274700, USA.
- Apache Maven, The Apache Software Foundation, 1901 Munsey Drive, Forest Hill, Mayland 21050-274700, USA.
- Hibernate, Red Hat, East Davie Street, Raleigh, North Carolina 27601, USA.
- Vaadin / Vaadin Report, Vaadin Ltd, Ruukinkatu 2-4, FI-20540, Turku, Finland.
- JasperReport, TIBCO Software Inc., 3307 Hillview Avenue, Palo Alto, California 94304, USA.
- Spring, VMware Inc., 3401 Hillview Avenue, Palo Alto, California 94304, USA.
- Microsoft MS-Sql, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052-6399, USA.
- Microsoft PowerBI, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052-6399, USA.
- Community Development: io springfox; com h2database; org postgres; org mapstruct; org jasypt.

4. CONSUMER RIGHTS REQUESTS

4.1 CCPA Consumer Rights Requests

Unless otherwise provided by applicable law, ESAB shall promptly notify the Client of any request received by ESAB or any Subprocessor from a CCPA Consumer in respect of the CCPA Personal Information of the CCPA Consumer, and shall not respond to the CCPA Consumer.

Exhibit F – Standard Contractual Clauses

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Client and Affiliates ("data exporter")

And

Name of the data importing organisation: ESAB ("data importer")

each a “party”; together “the parties”,

HAVE AGREED, as of the date of the last signature below, on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely the Member State in which the applicable data exporter's dependent office is located.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in

paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely the Member State in which the applicable data exporter's dependent office is located.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

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

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Client and Affiliates

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

ESAB

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

See Exhibit A to the DPA to which these Clauses are attached

Categories of data

The personal data transferred concern the following categories of data (please specify):

See Exhibit A to the DPA to which these Clauses are attached

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

See Exhibit A to the DPA to which these Clauses are attached

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

See Exhibit A to the DPA to which these Clauses are attached

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) ("TOMs") (or document/legislation attached):

See Exhibit B to the DPA to which these Clauses are attached