

General Terms and Conditions (GTC) for Software Use (Edition 2026)

Applicable to: SaaS – On-premises licence – Hybrid model

1. Scope

- 1.1 These general terms and conditions (hereinafter referred to as the 'Terms') govern the legal relationship between Steinemann Technology AG (hereinafter referred to as the 'Contractor') and the Customer (hereinafter 'Customer') regarding the use of the Contractor's software, irrespective of whether the software is provided as Software as a Service (SaaS), as an on-premises licence or as a hybrid model.
- 1.2 These Terms and Conditions apply exclusively to commercial customers (B2B). They are binding if they are declared applicable in the quotation or in the written acceptance of the quotation. Any terms and conditions of the Customer to the contrary shall only be valid insofar as they are expressly acknowledged in writing by the Contractor.
- 1.3 For one-off purchases of hardware components and implementation services, the Contractor's General Terms and Conditions of Delivery for Machinery and Plant and the General Terms and Conditions for Conventional Services shall apply.
- 1.4 In the event of any conflict between the general provisions of these terms and conditions and the provisions specific to the delivery model (Chapter 4), the latter shall take precedence.
- 1.5 The software is intended exclusively for commercial use and is not suitable for direct use as a control or safety system for machines, production plant or processes where a failure, without human intervention, could lead to personal injury or significant damage to property. The Customer bears sole responsibility for compliance with the applicable safety and usage regulations.
- 1.6 All agreements and legally relevant declarations by the contracting parties must be in writing (handwritten signature) or in text form (email, provided the sender's identity can be verified) to be valid. Qualified electronic signatures (QES) are equivalent to a handwritten signature (Art. 14(2)^(bis) of the Swiss Code of Obligations (CO)).

2. Definitions

- 2.1 'Software' refers to the software solutions provided by the Contractor in accordance with the quotation, including associated documentation, irrespective of the delivery model.
- 2.2 'Customer's data' refers to all content, configurations and data entered into the software by the Customer that is not machine-generated operational data (in particular master data, configuration parameters and any personal data). Machine-generated operational data is defined separately in Clause 2.6.
- 2.3 'Users' means the natural persons authorised by the Customer who are entitled to use the Software in accordance with these terms and conditions.
- 2.4 'Contract Term' means the period of software use agreed in the quotation or in the written acceptance of the quotation.
- 2.5 'Further Developments' means new versions, releases, updates and upgrades of the software provided by the Contractor at its own discretion. The Customer shall have no entitlement to the provision of specific Further Developments unless expressly agreed in writing.
- 2.6 'Machine data' refers to the raw measurement values and process signals (in particular sensor data, operating parameters, status data and error codes) automatically generated by the Customer's machines and plant during operation, insofar as these are recorded or transmitted by the software. Machine data is non-personal and remains the property of the Customer. Insofar as machine data can, in exceptional cases, be attributed to a specific natural person (in particular through linkage with operator or shift identifiers), the provisions of Clause 13 (Data Protection) shall also apply to this part of the data.
- 2.7 'Processed data' refers to analysis results, evaluations, models, benchmarks, key performance indicators and other information products which the Contractor creates by processing, aggregating or enriching machine data or other sources using its own algorithms, know-how or reference data. Processed data is the intellectual property of the Contractor and may be used by the Contractor as it sees fit.

3. Conclusion of the Contract and Scope of Services

- 3.1 The contract for the use of the software is concluded upon receipt by the Contractor of the written acceptance of the offer. Offers without a deadline for acceptance are non-binding.
- 3.2 The scope of services is exhaustively set out in the offer and the written acceptance of the offer, as well as, where agreed, the applicable Service Level Agreement (SLA). The Contractor has no further obligations to provide services.
- 3.3 The Contractor is entitled to further develop the software, provided that the agreed scope of services is not significantly reduced. Technical changes shall be announced with reasonable notice.
- 3.4 Clause 2.5 of these terms and conditions applies to further developments.
- 3.5 The Contractor may engage qualified third parties to provide the software services. The Contractor remains responsible to the Customer for the provision of services in accordance with the contract.
- 3.6 Maintenance and support services, as well as further developments, are included in the agreed scope of services. Any services going beyond this, in particular customer-specific adaptations or extensions, require a separate written agreement.

4. Delivery Models

4.1 Software as a Service (SaaS)

- 4.1.1 In SaaS models, the Contractor makes the software available as a service via a data network. The Contractor is responsible for operating the infrastructure.
- 4.1.2 Where a Service Level Agreement (SLA) has been agreed, it forms an integral part of these terms and conditions and defines availability targets, response times and service credits. Where no SLA has been agreed, the Contractor shall perform the service in accordance with the standard of care customary in the industry; there is no entitlement to a specific level of availability or to service credits.
- 4.1.3 Planned maintenance windows shall be notified to the Customer in good time and shall not be regarded as downtime.
- 4.1.4 Faults must be reported to the Contractor immediately in text form via the agreed support channel.
- 4.1.5 Where the Customer relies on the service for critical operational processes, it is the Customer's responsibility to put in place suitable redundancy and fallback measures.

4.2 On-premises licence

- 4.2.1 In the case of on-premises models, the Contractor shall provide the software for installation on the Customer's own infrastructure. The operation, maintenance and backup of the infrastructure are the sole responsibility of the Customer.
- 4.2.2 Delivery is deemed to have been completed upon handover of the installation medium or activation of the download link.
- 4.2.3 Updates and patches are provided within the agreed scope of support. The Customer is responsible for ensuring they are installed in a timely manner.
- 4.2.4 The Customer shall operate the software exclusively on systems that meet the minimum requirements defined by the Contractor.

4.3 Hybrid model

- 4.3.1 In the case of hybrid models, the provisions of Clauses 4.1 and 4.2 apply mutatis mutandis to the respective SaaS and on-premises components of the solution. The offer specifies which components are provided as SaaS and which as on-premises.

5. Right of Use

- 5.1 The Contractor grants the Customer a non-exclusive, non-transferable, non-sublicensable right to use the software to the agreed extent for the agreed term of the contract. In the case of licence agreements of indefinite duration, the right of use shall apply for the duration of the contractual relationship.
- 5.2 The right of use entitles the Customer to grant authorised users access to the software for their own operational purposes. Disclosure to third parties outside the Customer's organisation is not permitted.
- 5.3 All intellectual property rights in the software, the underlying infrastructure, algorithms, concepts and documentation remain with the Contractor or the authorised rights holders. These terms and conditions do not constitute a transfer of ownership rights.

- 5.4** The Customer's data as set out in Clause 2.2 and the machine data as set out in Clause 2.6 are the property of the Customer. The Contractor shall process the Customer's data as set out in Clause 2.2 solely for the purpose of providing the services in accordance with the contract; Clause 6.4 applies to machine data.
- 5.5** The Customer is not authorised to decompile, disassemble or otherwise reverse engineer the software, unless this is expressly permitted by mandatory law. Findings from an interoperability analysis permitted under mandatory law must not be used to develop a competing product.
- 5.6** The Customer shall ensure that the use of the software by its users complies with the provisions of these Terms and Conditions. It shall be liable for any breaches committed by its users in the same way as for its own breaches.

6. Obligations and responsibilities of the Contractor

- 6.1** The Contractor shall provide the agreed software services with the diligence of a competent software provider and in accordance with the state of the art.
- 6.2** The Contractor is responsible in particular for:
- The security of the software layer and infrastructure operated by the Contractor (in the case of SaaS and hybrid models)
 - Regular security updates and patches for the software components falling within the Contractor's area of responsibility
 - Encryption of data transmission between the Contractor's infrastructure and the Customer's access points
 - Physical security of the data centres and cloud infrastructure used by the Contractor
 - Reporting of security incidents affecting the Customer's data within 72 hours of becoming aware of them
 - Provision of an overview of the technical security measures upon written request ('Security Summary')
- 6.3** Where the software contains third-party components or open-source software, the Contractor shall, upon request, provide an overview of the third-party components used, including their key licence terms.
- 6.4** The Contractor is entitled to use machine data in accordance with Clause 2.6 for the following purposes of its own: (a) quality assurance and functional testing of the software; (b) further development of the software and the Contractor's products; (c) creation of processed data in accordance with Clause 2.7 (in particular benchmarks, process optimisation models); (d) anonymised, aggregated industry benchmarking, provided that no conclusions can be drawn regarding the Customer. The identification of the Customer by name or the disclosure of non-anonymised machine data to third parties without the Customer's prior written consent is prohibited, unless this is necessary for the provision of the agreed services (see Clause 3.5).
- 6.5** Insofar as the software additionally collects non-personal software diagnostic data (in particular performance metrics, error logs, system statuses of the software itself – not machine data as defined in Clause 2.6), this serves exclusively for quality assurance, functional verification and the further development of the software. The nature and scope of the diagnostic data collected are set out in the product documentation. Clause 6.4 and, where applicable, Clause 14 apply to machine data. Where diagnostic data should contain personal data within the meaning of the FADP, Clause 13 applies exclusively.

7. Obligations and Responsibilities of the Customer

- 7.1** The Customer shall, at its own expense and under its own responsibility, provide the IT infrastructure required for the use of the software in accordance with the Contractor's technical requirements.
- 7.2** The Customer shall appoint a designated contact person ('System Administrator') who is authorised to issue binding decisions and instructions in connection with the use of the software.
- 7.3** The Customer shall, no later than upon conclusion of the contract, draw the Contractor's attention to any site-specific safety regulations, regulatory requirements and standards relevant to the operation of the software.
- 7.4** If the Customer breaches its obligations to cooperate, the Contractor shall be released from any obligation to meet agreed performance targets and deadlines. Any additional costs shall be borne by the Customer.
- 7.5** The Customer is prohibited from using the software in any way that contravenes applicable laws, is inconsistent with the purpose of the software, or places an excessive burden on the Contractor's infrastructure.
- 7.6** The Customer shall keep the number of active users within the agreed quota. If usage exceeds the quota, the Customer shall notify the Contractor immediately. The Contractor is entitled to charge for the excess usage after giving prior notice, provided that the Customer does not rectify the excess within 30 days.
- 7.7** The Customer is responsible in particular for:
- Protecting its own network infrastructure through appropriate measures, in particular firewalls, network segmentation (OT/IT separation) and access controls

- Setting up and operating a secure communication channel (e.g. VPN or TLS) for data exchange with the software in accordance with the Contractor's technical requirements
- Restricting network connections to the ports and protocols necessary for the operation of the software
- Managing and protecting all access credentials and user accounts; using appropriate authentication mechanisms (e.g. multi-factor authentication, where supported)
- Ensuring the security and up-to-date status of the end devices used to access the software (operating system updates, antivirus protection)
- Protection of the Customer's own OT environment (production network, machines, control systems) against unauthorised access, including via the software
- Immediate reporting of security incidents within one's own area of responsibility that could affect the Contractor's service or data
- Ensuring that the machine data collections and exports configured by the Customer in accordance with Clause 2.6 do not contain any direct links to identifiable individuals (in particular, operator or login IDs), unless this has been expressly agreed upon for technical reasons; if such a link does nevertheless occur, the Customer shall inform the Contractor immediately so that the provisions of Clause 13 can be applied.

8. Information security – delimitation and shared responsibility

- 8.1** The areas of responsibility for information security are bindingly defined in Clause 6.2 (Contractor) and Clause 7.7 (Customer). Both parties are obliged to implement the security measures incumbent upon them on an ongoing basis and in accordance with the state of the art.
- 8.2** Security incidents originating within the Customer's area of responsibility (in particular compromised access credentials, malware on end devices, unsecured OT networks or inadequate network segmentation) shall be borne by the Customer. The Contractor shall not be liable for any damage arising from such incidents, even if they result in the software being impaired.
- 8.3** The Customer undertakes to comply with the technical security guidelines provided by the Contractor. Any significant deviations require the Contractor's prior written consent.
- 8.4** In the event of a security-related incident affecting the other party, both parties shall coordinate immediately and cooperate in the investigation and resolution of the incident.

9. Remuneration and Terms of Payment

- 9.1** The remuneration is set out in the quotation and is expressed in the currency specified therein, exclusive of VAT, without any cash discount or other deductions.
- 9.2** Recurring fees (e.g. annual fees) are payable in advance. One-off fees are due within 30 days of the invoice date.
- 9.3** If the payment deadline is exceeded, default interest is payable without the need for a reminder. The default interest rate is at least 5 per cent per annum. If the contractually agreed interest rate is higher, that rate shall apply.
- 9.4** The Customer may neither withhold nor reduce payments on the grounds of complaints or counter-claims, unless the counter-claim has been acknowledged in writing by the Contractor or has been finally and conclusively established.
- 9.5** In the event of a payment delay of more than 30 days, the Contractor is entitled, following a written reminder, to block access to the software until payment has been made in full. The obligation to pay remains unaffected. Even in the event of access being blocked, the Contractor is entitled to terminate the contract extraordinarily in accordance with Clause 10.2.
- 9.6** The Contractor is entitled to adjust the remuneration for recurring services upon renewal of the contract term. The Customer shall be notified in writing of the price adjustment at least 60 days before the expiry of the current contract term. If the Customer does not accept the price adjustment, they are entitled to terminate the contract extraordinarily with effect from the date on which the price adjustment comes into force. The notice of termination must be submitted to the Contractor in writing within 20 days of the notice of price adjustment being served.

10. Contract Term and Termination

- 10.1** The contract term is set out in the quotation. In the case of recurring usage models, the contract is automatically extended for a further year at a time, unless it is terminated in writing by either party with 60 days' notice prior to the expiry of the current term. Following termination, the software remains fully usable until the end of the current contract term. No refund will be made for fees already paid.
- 10.2** Either party may terminate the contract extraordinarily and without notice for good cause. Good cause shall be deemed to exist in particular in the event of: (a) a material breach of contract by the other party, provided that this

is not remedied within 30 days of a written notice of default; (b) a delay in payment of more than 60 days; (c) insolvency, composition moratorium or liquidation of the other party; (d) serious and repeated breaches of data protection, confidentiality or information security obligations.

- 10.3** In the event of termination by the Customer without good cause before the expiry of the minimum term, the obligation to pay for the remaining term of the contract shall remain in force.
- 10.4** Upon termination of the contract, the Contractor shall, in the case of SaaS models, provide the Customer with read-only access to the software for 30 days to enable the export of the Customer's data. Thereafter, the data shall be irrevocably deleted, provided that this does not conflict with any statutory retention obligations. In the case of on-premises models, the Customer must uninstall the software upon termination of the contract and destroy all copies.

11. Warranty

- 11.1** The Contractor warrants that, during the term of the contract, the software will substantially conform to the agreed specifications and that it holds the rights necessary to grant the rights of use.
- 11.2** Defects must be reported in writing immediately upon discovery or from the time at which the defect could have been discovered had the software been used with due care, and at the latest within 14 days. The Contractor shall rectify confirmed defects within a reasonable period. If rectification fails twice, the Customer may demand a reasonable reduction in the remuneration.
- 11.3** No warranty is provided for impairments attributable to causes beyond the Contractor's control, in particular insufficient infrastructure on the part of the Customer, unauthorised interference by the Customer or third parties, or force majeure.
- 11.4** Any further claims for defects are excluded to the extent permitted by law. Liability for wilful misconduct or gross negligence in accordance with Art. 100 of the Swiss Code of Obligations (CO) remains unaffected. For the limitation period for claims for defects, see Clause 11.5.
- 11.5** Claims for defects by the Customer shall become time-barred 12 months after delivery of the software or after the date on which the defect could have been discovered had the software been used with due care, insofar as permitted by law. This is subject to the statutory limitation period in the event of fraudulent concealment of defects.

12. Liability

- 12.1** The Contractor shall only be liable to the Customer for damage culpably caused by the Contractor, its organs, its staff or its vicarious agents in the provision of the software services. Liability for property damage is limited in total to CHF 5,000,000 (five million Swiss francs) per incident. With regard to personal injury, statutory liability applies.
- 12.2** Subject to cases of wilful misconduct or gross negligence, the Contractor's liability to the Customer for production downtime, loss of profit, loss of use, financial losses and losses resulting from a delay or interruption in the provision of services, as well as for loss of revenue, data loss or consequential damages, is excluded insofar as these are attributable to ordinary negligence. Likewise, any further claims by the Customer for compensation for damages of any kind – irrespective of the legal basis – are excluded insofar as these are based on ordinary negligence and are permitted by law.
- 12.3** The Customer shall be liable for any damage caused by its staff or users. This shall also apply where the Contractor's staff supervise or oversee the work, unless it can be proven that gross negligence in instructions, omissions or supervision caused the damage. The Customer shall also be liable for any damage caused by defects in the IT infrastructure, systems and means of access provided by the Customer. This shall also apply where the Contractor's staff have used these without raising any objections, unless they could have identified the defects had they exercised reasonable care.
- 12.4** If a third party asserts claims against the Contractor on the grounds of an infringement of intellectual property rights arising from the use of the software initiated by the Customer, the Customer shall indemnify the Contractor against such claims and compensate the Contractor for the proven loss.

13. Data Protection

- 13.1** Insofar as the Contractor processes personal data of the Customer or its employees in connection with the use of the software, this is carried out in its capacity as a data processor within the meaning of the Swiss Data Protection Act (FADP). Details are governed by the separate Data Processing Agreement (AVV / Data Protection Annex), which forms an integral part of these terms and conditions insofar as personal data is processed.

- 13.2** The Customer is responsible for the lawfulness of the personal data processed by them in the software. They shall ensure that the legal requirements for data processing on behalf of a data controller are met and that any data subjects have been informed in an appropriate manner.
- 13.3** The Contractor may process the Customer's data within the meaning of Clause 2.2 exclusively for the purpose of providing the agreed services. Use for the Contractor's own purposes or those of third parties is prohibited. Machine data as defined in Clause 2.6 is not covered by this provision; Clause 6.4 and, where applicable, Clause 14 apply to such data.
- 13.4** For customers with their registered office or branch in the European Economic Area, the General Data Protection Regulation (GDPR) applies in addition. In this case, the data processing agreement shall be amended accordingly. Machine data as defined in Clause 2.6 do not constitute personal data and are not subject to data protection law; they are governed by Clause 6.4 and, where applicable, Clause 14.

14. Access to data (EU Data Act)

- 14.1** Clauses 14.2 to 14.6 constitute the core substantive provisions governing data access for all customers, regardless of their place of business. For customers with their registered office or branch in the European Economic Area (EEA), only those additional obligations arising directly and mandatorily from the EU Data Act (Regulation (EU) 2023/2854 on data access) shall apply, insofar as it is applicable to the contractual relationship. For customers with their registered office or branch outside the EEA, Clauses 14.2 to 14.6 shall apply mutatis mutandis, without these additional obligations specifically arising from the EU Data Act.
- 14.2** The Customer shall have the right to access and export the machine data generated by its machines via a programming interface (API) provided by the Contractor. The scope, format and technical requirements of the API are set out in the quotation or in the technical documentation. The Contractor is obliged to make the API available for the duration of the contract and to ensure that it remains state-of-the-art.
- 14.3** The right of access to data under Clause 14.2 covers exclusively machine data as defined in Clause 2.6. The Customer has no entitlement to access to Processed Data as defined in Clause 2.7 (in particular, analysis results, process optimisation models, benchmarks and other information products created by the Contractor). Processed Data is the intellectual property of the Contractor.
- 14.4** The Contractor is entitled to use the Customer's machine data for the purposes set out in Clause 6.4. Use for the purpose of disclosure to the Customer's competitors is prohibited. Upon conclusion of the contract, the Customer expressly consents to the Contractor's use of its machine data in accordance with Clause 6.4.
- 14.5** Where the Contractor discloses the Customer's machine data to third parties, this is only permitted: (a) for the provision of the agreed services by qualified third parties in accordance with Clause 3.5, provided that such third parties are bound by confidentiality obligations at least equivalent to those of the Contractor under Clause 17; or (b) upon the Customer's express written instruction. Disclosure to companies that are in direct competition with the Customer is prohibited without the Customer's express written consent.
- 14.6** Access to data under this Clause 14 is subject to compliance with Clause 18 (Export Controls). The Contractor is entitled to refuse or restrict access to the extent necessary to comply with applicable export control or sanctions regulations.

15. Cybersecurity (EU Cyber Resilience Act)

- 15.1** The EU Cyber Resilience Act (Regulation (EU) 2024/2847, 'CRA') applies to manufacturers placing products containing digital elements on the EU market, irrespective of the manufacturer's or the Customer's place of business. Insofar as the software is subject to this regulation, the Contractor shall fulfil the obligations incumbent upon it as a manufacturer in accordance with the CRA; the following provisions of this Clause 15 apply in addition and irrespective of the Customer's place of business. The obligations include, in particular: (a) state-of-the-art software security ('security by design' and 'security by default'); (b) provision of security updates for the support period prescribed by law; (c) documentation of the software components (Software Bill of Materials, SBOM) upon request.
- 15.2** The Contractor shall actively report exploited vulnerabilities and serious security incidents to the competent authority in accordance with the requirements of the CRA from the date of its applicability (September 2026). Vulnerabilities that could affect the Customer's systems or machine data shall be notified to the Customer without delay, at the latest within 24 hours of becoming known.
- 15.3** The Customer is obliged to install updates classified by the Contractor as security-related within 30 days of receiving a written request to do so. If the Customer fails to install the update within this period, the Contractor shall not be liable for security-related damage attributable to the failure to install the update; this is subject to the

Contractor's liability for wilful misconduct or gross negligence in accordance with Clause 12.2. At the same time, the Contractor is entitled to restrict access to the software until the update has been fully installed.

- 15.4** These provisions apply subject to the phased implementation of the CRA (full implementation from December 2027). The Contractor is entitled to amend these terms and conditions in accordance with Clause 21 as soon as new CRA requirements become binding at the time of the amendment. The amendment shall be deemed material within the meaning of Clause 21.2 if it results in an increase in the Customer's obligations. This also applies insofar as such an increase in obligations is related to an update to Annex 3 (Clause 16.1); the exemption from the procedure set out in Clause 21 contained therein applies exclusively to the mere categorisation of an application, but not to any associated increase in the Customer's obligations arising from new CRA requirements that become binding at the time of the update.

16. Machinery Regulation (EU) 2023/1230

- 16.1** The software consists of individual applications which are categorised according to their function in Annex 3 ('Categorisation of Unity Applications'). Where an application is classified as 'information/analysis support' in accordance with Annex 3, it is designed as a stand-alone product and is used in such a way that it performs exclusively information and analysis support functions (in particular monitoring, dashboards, visualisation, analyses, diagnostics) and does not perform any safety-related control functions for machinery or plant within the meaning of Art. 3(3) of Regulation (EU) 2023/1230 ('Machinery Regulation'); it therefore does not constitute a safety component within the meaning of the Machinery Regulation. Where an application is classified as 'control-related' in accordance with Annex 3, it is regarded as a safety component within the meaning of Art. 3(3) of the Machinery Regulation; Clause 16.3 applies to it. The Contractor shall update Annex 3 upon the introduction of new or substantially modified applications. The mere updating of Annex 3 as such (i.e. the technical classification of an application into one of the two categories and the legal consequences already set out in this Clause 16.1 and Clause 16.3) does not constitute an amendment to these terms and conditions within the meaning of Clause 21 and does not require the procedure set out therein; however, Clause 15.4 remains reserved and unaffected insofar as the introduction or upgrading of an application simultaneously leads to an increase in the Customer's obligations due to new CRA requirements that become binding at the time of the update. The Contractor shall in any event inform the Customer of any update to Annex 3, insofar as this results in a change in the classification of an application already in use by the Customer from 'information/analysis support' to 'control'. Clause 1.5 remains reserved.
- 16.2** The Contractor's remote access to the Customer's machinery and plant within the scope of the software is limited to diagnosis, observation and the provision of analyses. Active intervention in safety-relevant control parameters of machinery or plant (in particular grinding height, feed rate or comparable process parameters, the incorrect setting of which may endanger the safety of persons) via the software is excluded, unless the parties expressly agree to this in writing on a case-by-case basis. Any such agreement requires a prior assessment as to whether it would result in a substantial modification within the meaning of Art. 3(16) of the Machinery Regulation; in such a case, the provisions of Clause 16.3 shall apply.
- 16.3** Insofar as the software is, exceptionally, classified as a safety component within the meaning of Art. 3(3) of the Machinery Regulation, or the Contractor is deemed, by virtue of a digital modification agreed on a case-by-case basis in accordance with Clause 16.2, to be a manufacturer within the meaning of Art. 18 of the Machinery Regulation, the Contractor shall fulfil the manufacturer's obligations incumbent upon it under Art. 10 of the Machinery Regulation, in particular regarding conformity assessment, CE marking, technical documentation and the retention of such documentation for at least 10 years. Upon a reasoned request, the Contractor shall make the source code or the programming logic available to the competent market surveillance authority, insofar as this is necessary to verify compliance with the essential health and safety requirements. The confidentiality obligations under Clause 17 shall not apply in this respect; the Contractor shall inform the Customer of any such disclosure, insofar as this is legally permitted.
- 16.4** For control software that qualifies as a safety component in accordance with Clause 16.3, the Customer may agree with the Contractor to enter into a separate source code escrow agreement with an escrow agent (e.g. a notary or specialised trustee) nominated by the Contractor or jointly designated by both parties. Such an agreement shall, in particular, govern the scope of the software deposited, the conditions for its release to the Customer and the allocation of costs, and must be in writing. In the absence of such a separate agreement, the Customer shall have no claim to the handover or deposit of the source code. The Contractor's obligation to disclose the source code to the competent market surveillance authority in accordance with Clause 16.3 remains unaffected.
- 16.5** The Customer shall inform the Contractor without delay if it uses or intends to use the software in a manner that goes beyond the information and analysis support functions described in Clause 16.1 or that could affect safety-

related machine functions. If the software is integrated into machine lines comprising components from other manufacturers (third-party machines), the Customer shall be responsible for the overall conformity of the system, unless the software itself qualifies as a safety component in accordance with Clause 16.3.

- 16.6** These provisions shall apply irrespective of the Customer's place of business, provided that the Machinery Regulation applies to the machine or plant in question. The Machinery Regulation shall apply in full from 20 January 2027; certain provisions, in particular those relating to market surveillance, shall apply earlier. With regard to the interaction with the EU Cyber Resilience Act as set out in Clause 15, the following applies: both sets of regulations shall apply in parallel, provided that the software qualifies both as a product with digital elements within the meaning of the CRA and as a safety component within the meaning of the Machinery Regulation.

17. Confidentiality

- 17.1** Both parties undertake to treat as confidential all confidential information received from the other party in the course of the contractual relationship and not to disclose it to third parties. In particular, technical documentation, configurations, business data and operational or production data shall be deemed confidential.
- 17.2** The duty of confidentiality shall apply even before the conclusion of the contract and shall continue for a period of 5 years following the termination of the contractual relationship. For information that qualifies as a trade secret (in particular technical algorithms, production processes and software architecture), the duty of confidentiality shall apply indefinitely.
- 17.3** The Contractor is entitled to name the Customer as a reference customer with the Customer's written consent.

18. Export controls

- 18.1** The software, as well as any associated information and technologies, may be subject to the export and import control regulations of Switzerland and other countries. The Customer is obliged to comply with all applicable export control regulations and, upon request, to inform the Contractor of the intended use and the location of use. This also applies to data access in accordance with Clause 14.
- 18.2** The Customer shall ensure that neither they nor their users disclose the software to persons, companies or countries that appear on sanctions lists or are subject to trade restrictions. For its part, the Contractor shall comply with the export and sanctions regulations applicable to it and shall not supply any services to persons, companies or countries for which a corresponding legal prohibition exists.

19. Force majeure

- 19.1** Neither party shall be liable for any failure to perform or delay in the performance of its contractual obligations to the extent that this is attributable to events beyond its control and which could not be averted despite the exercise of reasonable care (force majeure). These include, in particular: natural disasters, epidemics, acts of war, measures taken by public authorities and failures of the public telecommunications infrastructure.
- 19.2** The affected party must inform the other party without delay and take all reasonable measures to minimise the impact. If the force majeure event lasts for more than 60 days, both parties are entitled to terminate the contract without liability for damages.

20. Termination of the contract by the Contractor

- 20.1** If, after the conclusion of the contract, events occur which the Contractor could neither foresee nor avert (in particular force majeure or actual subsequent impossibility), and these significantly alter the economic significance or the content of the software service or render its provision impossible, the contract shall first be appropriately amended. Where such an adjustment is not economically justifiable, the Contractor shall be entitled to withdraw from the contract in whole or in part. Claims for damages by the Customer arising from such a withdrawal are excluded, provided that the Contractor is not at fault for the impossibility.

21. Amendments to these Terms and Conditions

- 21.1** The Contractor is entitled to amend these terms and conditions in text form (including by email) with at least 60 days' notice. The notice must clearly specify the material changes. Unless the Customer objects within 30 days of receipt, the new terms and conditions shall be deemed accepted. In the event of material changes, the Customer shall be entitled to the special right of termination in accordance with Clause 21.2.
- 21.2** Changes are deemed material within the meaning of Clause 21.1 if they place the Customer at a significant disadvantage. These include, in particular: (a) an increase in remuneration outside the scope of Clause 9.6; (b) a restriction on the agreed scope of use or the scope of services; (c) an extension of exclusions of liability or

limitations of warranty to the detriment of the Customer; (d) a shortening of the time limits available to the Customer for exercising their rights; (e) the introduction of new material obligations on the part of the Customer. In the event of a material amendment, the Customer shall be entitled to terminate the contract extraordinarily with effect from the date on which the amendments come into force. The notice of termination must be submitted to the Contractor in writing within 20 days of receipt of the notice of amendment.

22. Use of AI-supported functions

- 22.1** Where and to the extent that the software includes AI-supported functions (in particular machine learning, automated analyses or recommendation systems), these shall be specified in the quotation or in the product documentation. If AI-supported functions are only introduced after the conclusion of the contract as part of further developments in accordance with Clause 2.5, the Contractor shall inform the Customer in advance in an appropriate manner before the function becomes actively available for use. The following provisions of this Clause 22 shall apply from the time at which the relevant AI-supported functions are made available to the Customer. The Contractor reserves the right to adapt AI models and algorithms as part of further developments in accordance with Clause 2.5.
- 22.2** The results and recommendations of AI-supported functions are decision-making aids. The professional review and the final decision rest with the Customer. The Contractor shall not be liable for any damage arising from the unchecked adoption of AI results.
- 22.3** The Contractor may use aggregated, anonymised usage data to improve and train AI models, provided that no conclusions can be drawn about the Customer or individual users. The use of the Customer's non-anonymised data for AI training requires the Customer's express written consent.
- 22.4** The Customer shall ensure that they do not input any data into AI-supported functions that is subject to statutory confidentiality or data protection requirements, unless the Contractor has expressly confirmed such compliance in writing.

23. Applicable Law and Jurisdiction

- 23.1** The legal relationship is governed by the substantive law of Switzerland, to the exclusion of the UN Convention on Contracts for the International Sale of Goods (CISG).
- 23.2** The place of jurisdiction for both the Customer and the Contractor is the Contractor's registered office (St. Gallen). The Contractor reserves the right to bring proceedings against the Customer at the Customer's registered office.

24. Dispute Resolution

- 24.1** The parties undertake to resolve disputes arising out of or in connection with this contract by mutual agreement through direct negotiations at management level within 30 days before resorting to court proceedings. The obligation to seek interim relief immediately remains unaffected.

25. Final provisions

- 25.1** Any amendments or additions to these terms and conditions must be made in writing or in text form (email), unless these terms and conditions expressly provide otherwise (in particular Clause 21.1).
- 25.2** Should any individual provisions be wholly or partially invalid, the validity of the remaining provisions shall remain unaffected. The parties undertake to replace invalid provisions with new ones that come as close as possible to the economic purpose of the invalid provisions (severability clause).
- 25.3** The Customer is not entitled to assign any rights or obligations arising from this contract to third parties without the Contractor's written consent. The same applies to a transfer of the contractual relationship in the context of a business transfer (asset deal) and in the context of a merger, demerger or conversion under the Mergers Act (FusG). In such cases, the Contractor's prior written consent is required. The Contractor may refuse to give its consent on objective grounds.
- 25.4** The following annexes form an integral part of these terms and conditions, where agreed:
- Service Level Agreement (SLA) – for SaaS models
 - Data Protection / Data Processing Agreement (DPA) – where personal data is processed
 - Categorisation of Unity Applications (Appendix 3)
- 25.5** These Terms and Conditions replace the Contractor's previous terms and conditions governing the use of its software. For Customers who were already using the Contractor's software prior to these Terms and Conditions coming into force, the following applies: The Contractor shall give notice of the transition to these Terms and Conditions, applying Clause 21.1 mutatis mutandis, with at least 60 days' notice. If the Customer does not object within 30 days of notification, these terms and conditions shall be deemed to have been accepted. The Customer

is also entitled to terminate the contract extraordinarily with effect from the date on which these terms and conditions come into force, in accordance with the provisions of Clause 21.2.

Appendix 3: Categorisation of Unity Applications

The table below categorises the applications and components of the Steinemann Unity platform existing at the time these terms and conditions come into force, as well as the digital components integrated into the Satos TSQ grinding machines, according to their function as set out in Clause 16.1. The Contractor shall update this table upon the introduction of new or significantly modified applications, in particular in the course of increasing automation of production processes.

Application / Component	Category	Applicable provision / legal consequence
Remote Service	Information/analysis support	Clause 16.1, second sentence (not a safety component)
Sanding Dashboard	Information/analysis support	Clause 16.1, second sentence (not a safety component)
Performance Intelligence	Information/analysis support	Clause 16.1, second sentence (not a safety component)
Unified Name Space	Information/analysis support	Clause 16.1, second sentence (not a safety component)
BQC Machine Automation	Control	Clause 16.1, sentence 3 in conjunction with Clause 16.3 (safety component)
Integrated Siemens HMI	Control	Clause 16.1, sentence 3 in conjunction with Clause 16.3 (safety component)
Unity Hub (edge device)	Information/analysis support	Clause 16.1, second sentence (not a safety component)
Symmedia remote access	Information/analysis support	Clause 16.1, second sentence (not a safety component)
Unity SaaS / Azure Cloud	Information/analysis support	Clause 16.1, second sentence (not a safety component)
Octocore Master / Symmedia Hub VM (on-premises)	Information/analysis support	Clause 16.1, second sentence (not a safety component)
Vibration modules (condition monitoring)	Information/analysis support	Clause 16.1, second sentence (not a safety component)
Thickness measurement system	Information/analysis support	Clause 16.1, second sentence (not a safety component)
Chatter Rough Scanner (CRS)	Information/analysis support	Clause 16.1, second sentence (not a safety component)
Linux operating system (edge device)	Information/analysis support	Clause 16.1, second sentence (not a safety component)