



Data Processing Terms and Conditions

These Data Processing Terms and Conditions ("Data T&Cs") are established pursuant to Article 28(3) of the General Data Protection Regulation (GDPR) and applies to any FFT Production Systems, Inc. (hereinafter "FFT") contractor or processor of FFT data (hereinafter "Contractor").

1. Introduction, scope of application

These Data T&Cs govern the data protection obligations of the parties arising in connection with the provision of services by the Contractor to FFT under any purchase order, statement of work and/or other underlying agreement (hereinafter referred to as the "Main Contract"). These Data T&Cs apply to all activities in connection with any Main Contract in which employees of the Contractor or persons commissioned by Contractor process personal data ("data") of FFT. The Contractor agrees to be bound by these Data T&Cs when accepting a Main Contract with FFT.

2. Definitions

The terms of these Data T&Cs shall be construed in accordance with the EU-General Data Protection Regulation. Insofar as statements in the following are to be made "in writing", this refers to the written form in accordance with § 126 BGB (German Civil Code). Otherwise, statements may be made in any other form, provided that adequate evidence is provided.

3. Object and duration of data processing

Object

In the context of the performance of the Main Contract, the processing of personal data by the Contractor is possible and may be necessary.

These Data T&Cs shall apply mutatis mutandis to the (remote) testing and maintenance of automated processes, data processing systems or the use of shared databases on the servers of FFT or FFT's customer, if access to personal data cannot be excluded.

Duration

Data processing begins with the first provision of access to data within the scope of the Main Contract and continues indefinitely until the Main Contract is terminated by one of the parties.

4. Type and purpose of data collection, processing or use:

Type of data

In the course of its activities, the Contractor may or may need to collect, record, organize, sort, store, adapt or modify, read, consult, use, disclose by transmission, dissemination or any other form of provision, compare or link data (hereinafter referred to as "data processing") relating to an identified or identifiable natural person (hereinafter referred to as "data subject"). **The typical categories of information that may be disclosed on a data subject include, but are not limited to, the following categories:**

- a) Personnel master data (names, age, marital status, date of birth, certificates, etc.)
- b) Communication data (e.g. telephone, e-mail)
- c) Project/organization charts

- d) Identity card numbers, social security number
- e) IP addresses
- f) Vehicle numbers, license plates (with personal reference)
- g) Account and credit card numbers
- h) Genetic data and disease data
- i) Criminal record/certificates of good conduct

5. Categories of Data Subjects

Typical data subjects include, but are not limited to:

- a) Employees of the client
- b) Employees of contractual partners of the client (customers, suppliers, etc.)
- c) Applicants

6. Obligations of the Contractor

- (1) The Contractor shall process personal data exclusively in accordance with these Data T&Cs, the Main Contract, any further instructions of FFT and FFT's customer and any further specific processing requirements under the law. To the extent that any additional obligations exist for the Contractor, the Contractor shall inform FFT thereof prior to data processing, unless such notification is prohibited by law. The Contractor shall not use the data provided for processing for other purposes; in particular, not for Contractor's own purposes or benefits.
- (2) The Contractor confirms that it is aware of and fully abides by all relevant general data protection regulations.
- (3) The Contractor undertakes to maintain strict confidentiality during processing. Persons engaged by Contractor, including any employees, officers and contractors, must be bound by the same written confidentiality obligations.
- (4) The Contractor warrants that all of its employees, officers and contractors who may obtain access to the data processed in the Main Contract must be subject to a separate contractual requirement to fully maintain confidentiality, unless they are already subject to a relevant confidentiality obligation by law.
- (5) The Contractor warrants that the persons employed by it for data processing have been familiarized with the relevant provisions of data protection and these Data T&Cs prior to the start of data processing. Appropriate training and awareness-raising measures shall be repeated at regular intervals. The Contractor shall ensure that persons employed for commissioned data processing are appropriately instructed and monitored on an ongoing basis with regard to compliance with data protection requirements.
- (6) In connection with the commissioned data processing, the Contractor shall support FFT in the preparation and updating the record of data processing activities and in the implementation of the data protection impact assessment. All necessary

Information and documentation must be kept available and forwarded to FFT immediately upon request.

- (7) If FFT is subject to an inspection by supervisory or governmental authorities or if data subjects assert rights against it, the Contractor undertakes to support FFT in fulfilling the requests and claims of data subjects in accordance with Chapter III of the GDPR and in complying with the obligations set out in Art. 33 to 36 GDPR.
- (8) The Contractor may only provide information to third parties or the data subject with the prior consent of FFT. The Contractor shall forward any requests addressed directly to it to FFT without delay.
- (9) In the event of a claim against FFT by a data subject with regard to any claims under Art. 82 GDPR, the Contractor undertakes to support FFT in the defence of the claim.
- (10) Where required by law, the Contractor shall appoint a competent and reliable person as data protection officer. It must be ensured that there are no conflicts of interest for the data protection officer. In cases of doubt, FFT may contact the data protection officer directly. The Contractor shall inform FFT immediately of any changes in the person or internal tasks of the officer.
- (11) The data processing shall generally take place within the EU or the EEA. Any relocation to a third country may only take place with the consent of FFT and under the conditions contained in Chapter V of the General Data Protection Regulation and in compliance with the provisions of these Data T&Cs.
- (12) If the Contractor is not established in the European Union, it shall appoint a responsible contact person in the European Union in accordance with Art. 27 of the General Data Protection Regulation. The contact details of the contact person as well as any changes in the contact person must be communicated to FFT without delay.

7. Technical and organizational measures

- (1) The data security measures described in Annex 1 are binding. They define the minimum security standards required by the Contractor. If the Contractor must describe the measures that must be taken to a third party, the description of the measures must be so detailed that a knowledgeable third party can recognize beyond doubt at any time what the minimum security standards are. Reference to information that cannot be taken directly from these Data T&Cs or its annexes is not permitted.
- (2) The data security measures can be adapted in line with further technical and organizational developments, as long as they do not fall below the level agreed here. The Contractor shall implement any changes required to maintain information security without delay. FFT must be informed of any changes without delay. Significant changes must be agreed between the parties.
- (3) If the security measures taken do not or no longer meet the FFT's requirements, the Contractor shall notify FFT immediately.
- (4) Copies or duplicates of personal information shall not be made without the knowledge of FFT, except for technically necessary temporary copies provided that said copies remain at the level of protection required in these Data T&Cs.

- (5) The processing of data in private residences is excluded.
- (6) Dedicated data carriers that originate from FFT or are used for FFT shall be specially marked and are subject to ongoing administration. Data carriers must be stored appropriately at all times and must not be accessible to unauthorized persons. Inputs and outputs must be documented.

The Contractor shall provide regular evidence of the fulfilment of its obligations, in particular the complete implementation of the agreed technical and organizational measures and their effectiveness. The proof must be provided to FFT every 12 months at the latest without being asked and otherwise at any time on request. The proof can be provided, for example, by implementation of a self-audit, internal company rules of conduct including external proof of compliance with them, certificate for data protection and/or information security (e.g. ISO 27001, TISAX),

- (7) approved code of conduct in accordance with Art. 40 GDPR, certificates according to Art. 42 GDPR, Should inspections by FFT or an auditor commissioned by FFT be necessary in individual cases, these shall be implemented during normal business hours without disrupting operations after notification, taking into account a reasonable lead time. The Contractor may make this dependent on prior notification with a reasonable lead time and on the signing of a confidentiality agreement regarding the data of other customers and the technical and organizational measures in place. If the auditor commissioned by FFT is in a competitive relationship with the Contractor, the Contractor shall have the right to object to the auditor and request a new auditor.
- (8) Should a data protection supervisory authority or another sovereign supervisory authority of FFT carry out an inspection, paragraph (7) shall apply accordingly. It is not necessary to sign a confidentiality agreement if this supervisory authority is subject to professional or statutory confidentiality, where a breach is punishable under the German Criminal Code.

8. Regulations on the rectification, erasure and blocking of data

- (1) The Contractor shall only correct, delete or block data processed within the scope of the Main Contract or in accordance with FFT's written instructions.
- (2) The Contractor shall comply with the corresponding instructions of FFT at all times and also beyond the termination of these Data T&Cs.

9. Subcontracting relationships/subcontractors

- (1) The commissioning of subcontractors is only permitted with the written consent of FFT in individual cases.
- (2) Consent is only possible if the subcontractor has been contractually subject to data protection obligations that are at least comparable to those agreed in these Data T&Cs. Upon request, FFT shall be given access to the relevant contracts between the Contractor and subcontractor.
- (3) The comprehensive rights of FFT must also be able to be exercised by FFT against the subcontractor. In particular, FFT must be entitled to carry out inspections of subcontractors or have them carried out by third parties at any time to the extent specified here.

- (4) The Contractor must assure that the responsibilities of the Subcontractor be clearly delineated.
- (5) The Contractor shall carefully select the Subcontractor, paying particular attention to the suitability of the technical and organizational measures taken by the Subcontractor.
- (6) The forwarding of data processed in the Main Contract to the Subcontractor is only permitted if the Contractor has documented that the Subcontractor has completely fulfilled its obligations. The Contractor must submit the documentation to FFT without first being requested to do so.
- (7) The commissioning of Subcontractors who do not perform data processing on behalf of FFT exclusively from the territory of the EU or the EEA is only possible if the conditions specified in Chapter (5) (10) and (11) of these Data T&Cs are observed. In particular, it is only permitted if and as long as the Subcontractor offers appropriate data protection guarantees. The Contractor shall inform FFT of the specific data protection guarantees offered by the Subcontractor and how proof of this can be obtained.
- (8) The Contractor shall carry out an appropriate review of the Subcontractor's compliance with its obligations on a regular basis, at least every 12 months. The inspection and its results must be documented in such a meaningful way that they are comprehensible to a competent third party. The documentation must be submitted to FFT without being first requested to do so.
- (9) If the Subcontractor fails to comply with its data protection obligations, the Contractor shall be responsible and liable to FFT for any and all costs, losses damages and claims resulting from this failure.
- (10) Subcontracting relationships within the meaning of these Data T&Cs are only those services that are directly related to the provision of the Main Contract. Ancillary services such as transportation, maintenance and cleaning as well as the use of telecommunications services or user services are not covered. The Contractor's obligation to ensure compliance with data protection and data security in these cases remains unaffected.

10. Rights and obligations of FFT

- (1) Within the scope of these Data T&Cs, FFT is solely responsible for its own compliance with the statutory provisions of the data protection laws, in particular for the lawfulness of data transfer to the Contractor and for the lawfulness of data processing ("Controller" within the meaning of Art. 4 No. 7 GDPR).
- (2) FFT shall issue all orders, partial orders or instructions in writing. In urgent cases, instructions may be issued verbally and FFT shall confirm such oral instructions in writing without delay.
- (3) FFT shall inform the Contractor immediately if it discovers errors or irregularities in the inspection of the order results.

11. Notification obligations

- (1) The Contractor shall notify FFT immediately of any breaches of personal data protection. Reasonable suspicions of this must also be reported. The notification must be sent to an address specified by FFT within 24 hours of the Contractor

becoming aware of the relevant event. It must contain at least the following information:

- a. A description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, the categories concerned and the approximate number of personal data records concerned
 - b. The name and contact details of the data protection officer or other contact point for further information
 - c. A description of the likely consequences of the personal data breach
 - d. A description of the measures taken or proposed to be taken by the Contractor to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects
- (2) Significant disruptions in the execution of any demands/instructions made by FFT as well as violations of data protection regulations or the provisions of these Data T&Cs by the Contractor, Contractor's employees and/or subcontractors must also be reported immediately.
- (3) The Contractor shall inform FFT immediately of any inspections or measures by supervisory authorities or other third parties insofar as these relate to data processing.
- (4) The Contractor shall support FFT in its obligations under Art. 33 and 34 of the General Data Protection Regulation to the extent necessary.
- (5) Should FFT's data at the Contractor be jeopardized by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform FFT thereof without delay. The Contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lie exclusively with FFT as the "controller" within the meaning of the General Data Protection Regulation.

12. Instructions

- (1) FFT reserves a detailed right to issue instructions regarding information processing.
- (2) FFT and the Contractor shall name the persons exclusively authorized to issue and accept instructions in writing.
- (3) In the event of a change or a longer-term absence of the named persons, the other party must be informed immediately of any successors or representatives.
- (4) The Contractor shall notify FFT immediately if, in its opinion, an instruction issued by FFT violates statutory provisions. The Contractor shall be entitled to suspend the implementation of the corresponding instruction until it is confirmed or amended by the person responsible at FFT.
- (5) The Contractor shall document any instructions issued to it and their implementation.

13. Termination of the Main Contract

- (1) Upon termination of the contractual relationship or at any time at the request of FFT, the Contractor shall either destroy the data processed related to the Main Contract or hand it over to FFT at FFT's discretion. All existing copies of the data shall also

be destroyed. The destruction must be carried out in such a way that it is no longer possible to restore even residual information with reasonable effort. Physical destruction shall be carried out in accordance with DIN 66399, whereby at least protection class 1 shall apply.

- (2) The Contractor is obliged to ensure the immediate return or deletion of data sent to subcontractors as well.
- (3) The Contractor shall provide proof of proper destruction and submit it to FFT without delay.
- (4) Documentation that serves as proof of proper data processing shall be retained by the Contractor in accordance with the respective retention periods, even beyond the end of the Main Contract. The Contractor may hand them over to FFT at the end of the Main Contract in order to discharge FFT.

14. Remuneration

The Contractor's remuneration is conclusively determined in the Main Contract. There is no separate remuneration or reimbursement of costs by FFT under these Data T&Cs.

15. Liability

- (1) FFT and Contractor are liable to data subjects in accordance with the provisions of Art. 82 GDPR.
- (2) The Contractor shall bear the burden of proof that damage is not the result of a circumstance for which it is responsible, insofar as the relevant data was processed by it under these Data T&Cs. Unless this proof has been provided that the Contractor was not, in part, responsible for the damage, the Contractor shall indemnify FFT on first demand against all claims asserted against FFT in connection with the commissioned data processing. Under these conditions, the Contractor shall also reimburse FFT for all legal defense costs incurred.
- (3) The Contractor shall be liable to FFT for any damage resulting from the acts or omissions of the Contractor, its employees or the subcontractors engaged by it to perform the Main Contract.

16. Special right of termination

- (1) FFT may terminate the Main Contract at any time without notice in the event of a serious breach by the Contractor of data protection regulations or the provisions of these Data T&Cs, if the Contractor is unable or unwilling to carry out a lawful instruction from FFT or if the Contractor refuses to comply with FFT's control rights in breach of these Data T&Cs.
- (2) A serious breach exists in particular if the Contractor does not or has not fulfilled the obligations specified in these Data T&Cs, in particular the agreed technical and organizational measures, to a significant extent.
- (3) In the event FFT deems the violation insignificant, FFT shall set the Contractor a reasonable deadline for remedial action. If the remedy is not completed by Contractor in the time specified by FFT, FFT shall be entitled to terminate the Main Contract as described in this section.
- (4) In addition, the Contractor shall reimburse FFT for all costs incurred by FFT due to the termination of the Main Contracts.

17. Miscellaneous

- (1) Both parties are obliged to treat all knowledge of business secrets and data security measures of the other party obtained within the framework of the contractual relationship as confidential, even after the termination of the Main Contract. If there is any doubt as to whether information is subject to the confidentiality obligation, it shall be treated as confidential until written release by the other party.
- (2) Amendments and supplements to these Data T&Cs may be unilaterally made by FFT at any time.
- (3) The defense of the right of retention within the meaning of § 273 BGB is excluded with regard to the data processed in the order and the associated data carriers.
- (4) Should individual parts of these Data T&Cs be invalid, this shall not affect the validity of the remainder of the agreement.
- (5) German law shall apply to these Data T&Cs.

Appendix 1 - Technical and organizational measures

The Contractor shall design its internal organization in its area of responsibility in such a way that it meets the special requirements of data protection. The Contractor shall take technical and organizational measures for the appropriate protection of FFT data that meet the requirements of the General Data Protection Regulation (Art. 32 GDPR). The Contractor shall take technical and organizational measures to ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the data processing in the long term.

In this Appendix, the technical and organizational measures to ensure data protection and data security are defined, which the Contractor must adhere to and continuously update. The aim is to ensure, in particular, the confidentiality, integrity and availability of the information processed on behalf of FFT and FFT's customer(s).

Contractor reserves the right to modify the security measures in place provided that the level of protection agreed upon herein is not diminished.

1. Certification and Destruction Standards

Contractor shall maintain industry standard security certifications relevant to the scope of processing (e.g. ISO 27001, TISAX, customer specification requirements or certification according to Art. 42 GDPR) and shall provide proof of certification to FFT upon request. Data destruction shall adhere, at a minimum, to Security Level 4 in accordance with DIN 66399 or an equivalent recognized standard.

2. Physical Access control

ContractorS shall prevent unauthorized physical access to facilities and data processing systems data by implementing:

- a) secured entry control systems (e.g. electronic badge, locking systems, alarm systems, video surveillance or security personnel);
- b) formal determination and tracking of authorized individuals, including visitor control regulations, authorization cards and logging of entry/exit;
- c) physical separation and division of safety zones

3. System Access control

Contractors shall prevent unauthorized utilization of data processing systems by implementing:

- a) documented authorization concepts for end devices, applications and core systems;
- b) identity and access management tools to enforce user identification, strong authentication procedures, including multi-factor authorization and strict password policy guidelines;
- c) perimeter and endpoint defense systems, including firewalls, anti-malware software, encrypted storage of passwords and secure VPNs;
- d) active monitoring of access attempts and incident response procedures.

4. Data Access control

Contractors shall enforce controls to ensure authorized users access only the data permitted under their access scope by implementing:

- a) role-based access controls following the principles of “need-to-know” and “least privilege”;
- b) mandatory encryption of FFT personal data;
- c) comprehensive audit logging with routine and incident driven evaluations
- d) clear rules on media handling, disposal, retention/deletion schedules and strict separation between development, testing and production environments.

5. Transfer control

Contractors shall safeguard FFT data during electronic transmission, transportation and storage on data carriers by implementing:

- a) strong end-to-end encryption for all electronic transmissions and storage media in transit;
- b) complete documentation of interfaces, data transfer channels, logging of transfers and receipt validation;
- c) technical and administrative measures to prevent data loss using USB port restrictions and strict permissions.

6. Input control

Contractors shall maintain measures to determine whether personal data has been entered, modified or deleted within data processing systems by implementing:

- a) system logging of data modification, entry and deletion operations;
- b) organizationally assigned responsibilities for data management and regular log review protocols.

7, Order control

Contractors shall process personal data solely in accordance with FFT's documented instructions and contract requirements. Contractors shall maintain internal control frameworks, including periodic self-assessments to monitor compliance across data processing activities.

8. Availability control

Contractors shall protect FFT data against accidental destruction or loss by maintaining:

- a) documented business continuity and disaster recovery plans, subject to regular testing;
- b) automated backup procedures, status monitoring and defined data archiving and recovery standards;
- c) system redundancies (e.g. servers, storage, etc.)

9. Separation requirement

Contractors shall ensure data collected for different purposes or clients can be processed separately.

10. Organizational security criteria

Contractors shall establish and maintain appropriate governance structure, including:

- a) documented information security management systems and data protection management systems with clearly designated governance;
- b) comprehensive security incident management and response plans;
- c) information classification schemes and mandatory security awareness training for all employees and management