# GTT (General Terms of Trade) of IT-HAUS GmbH on order processing in accordance with Art. 28 GDPR including a description of the technical and organisational measures taken

## Introduction

IT-HAUS GmbH (abbreviated below to “ITH” or the “Contractor” or “we”) is one of the top system engineering and trading houses in Germany. As a provider of domestic and international IT solutions and services, ITH offers comprehensive, full-service concepts from one source. A powerful network with blanket coverage across the world, 25 locations in Germany, an international site in Luxembourg and over 260 employees ensure that ITH is one of the leading providers in the B2B sphere. The company’s experts advise and serve customers in all questions involving IT and develop innovative, intelligent and forward-looking concepts - from a simple application through to a complete, all-encompassing solution.

## 1. General, sphere of validity

(1) These GTT apply to all activities, which are owed under the individual contract with the Client (referred to below as the “main contract”) or are connected to the main contract, and under which we, our employees or agents working on our behalf process the Client’s personal data (referred to below as “order processing”). These GTT therefore contain the contractually agreed regulations on order processing pursuant to Art. 28 GDPR by ITH for its respective customer. Insofar as the services to be provided by ITH involve or require the processing of personal data to order, these GTT especially concern ITH services such as

- outsourcing the processing of personal data in the course of Cloud computing, without ITH being required to access the content of data as the Cloud operator;
- stock removal of security back-ups and other archives;
- disposing of data carriers;
- inspecting or maintaining (e.g. remote maintenance, external support) automatic procedures or data processing systems, if access to personal data cannot be excluded during these activities;
- inspecting or maintaining (e.g. remote maintenance, on-site maintenance, external support) devices with integrated storage media, if access to personal data cannot be excluded during these activities;

(2) These GTT only apply if the Client is an undertaking (§ 14 BGB), a legal entity under public law or a public law special trust.

(3) Unless something different has been agreed, these GTT apply as a framework agreement in the version valid at the date of the Client’s order or in any case notified to it in text form, including the same types of contract in future, without us having to refer to them again in each single case.

(4) These GTT apply exclusively. The Client’s general conditions of business that deviate, contradict or supplement these GTT do not become components of the order processing contract unless we have specifically approved their validity. This requirement of approval applies in every case, even



IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel. +49 6502 9208-0 | Fax +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

if, for example, we execute the service without reservation in the knowledge of the Client's business conditions.

(5) Individual agreements made with the Client in a stand-alone case (including auxiliary accords, supplements and changes) have priority over these GTT in all cases. The processing details are defined by the individual main contract.

(6) References to the validity of legal regulations only have a clarifying meaning. Legal regulations therefore apply even without such a clarification, unless they are directly changed or specifically excluded in these GTT.

**2. Object and duration**

(1) The Contractor provides deliveries and services for the IT sphere of the Client. For the rest, the regulations of the main contract apply.

(2) The Contractor thereby processes personal data for the Client in the sense of Art. 4 No. 2 and Art. 28 GDPR on the basis of this order processing contract.

(3) The service agreed in the order processing contract is solely provided in a Member State of the European Union or in state subject to the treaty concerning the European Economic Area. Any relocation of a service or parts of the same to a third country requires prior approval from the Client. This may not happen unless the special prerequisites of Art. 44 ff. GDPR are fulfilled (e.g. resolution of reasonableness by the Commission, standard clauses of data protection, authorised rules of conduct).

(4) This order processing contract is concluded for an indefinite time. It can be terminated by either party by serving notice of one month to the end of a month. If a main contract exists, it is not possible to terminate this agreement separately without terminating the main contract at the same time; the periods and dates of notice in the main contract then apply here in uniform fashion.

(5) The Client can immediately terminate the order processing contract at any time without serving notice in the following cases; the Contractor is culpable of a serious violation of data protection regulations or of the provisions of this order processing contract; the Contractor cannot or will not execute an instruction issued by the Client; the Contractor refuses the Client's rights of control contrary to the contract. In particular, non-compliance with the duties agreed in this order processing contract and derived from Art. 28 GDPR represent a serious violation.

**3. Type and purpose of processing, nature of personal data and categories of data subjects:**

(1) Type and purpose of processing:
Processing data to ensure deliveries and services to the Client's IT sphere. For the rest, the type and purpose of processing are governed by the main contract and the scope of the individual agreements made with the Client.



IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel. +49 6502 9208-0 | Fax +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

(2) Nature of personal data:
The nature of personal data processed in the course of data processing is determined by the Client itself. The following are examples of processed data: surname, first name, address, telephone number, e-Mail address, date of birth, settlement data.

(3) Categories of data subjects:
The data subjects (affected persons) affected by processing consist of employees, suppliers/manufacturers and/or customers. For the rest, the categories of data subjects are governed by the main contract and the Client's actual data processing procedures.

**4. Rights and duties of the client and its authority to issue instructions**

(1) The Client alone is responsible for assessing the reliability of processing pursuant to Art. 6 Para. 1 GDPR and for safeguarding the rights of data subjects in accordance with Art. 12 to 22 GDPR. Regardless of this, the Contractor is obliged to forward all such inquiries to the Client without delay, insofar as these are recognisably solely directed at the Client.

(2) Changes to the object of processing and revisions to procedures shall be agreed jointly between the Client and the Contractor and determined in writing or in a documented electronic format.

(3) The Client will not issue any orders, part orders or instructions verbally, but shall only do so in writing or in a documented electronic format. All instructions issued shall be documented both by the Client and the Contractor.

(4) The Client is entitled to verify – as determined under No. 6 – compliance with the technical and organisational measures taken by the Contractor and with the obligations determined in this order processing contract.

(5) The Client shall inform the Contractor without delay if it establishes errors or irregularities when checking the results of the order.

(6) The Client is obliged to treat in confidence all knowledge of business secrets obtained during the order processing relationship and of the data protection measures implemented by the Contractor. This obligation continues to exist even after this order processing contract has ended.

**5. Parties of the Client entitled to issue instructions; parties of the Contractor authorised to receive instructions**

(1) The Client shall inform the Contractor of its parties entitled to issue instructions in the course of this order processing contract (name, function, telephone number, e-Mail address). Parties of the Contractor authorised to receive instructions are the individual contact persons there.

(2) In case of a change of contact person or if a contact person is hindered over the long term, the opposite order processing party shall be informed without delay and, as a matter of principle, the successor or the deputy shall be nominated in writing or electronically. Instructions shall be retained for the duration of their validity and subsequently for a further three full calendar years.



IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel. +49 6502 9208-0 | Fax +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

**6. The Contractor's duties**

(1) The Contractor shall process personal data solely within the scope of the agreements made and on the instructions issued by the Client, insofar as it is not obliged to undertake some other processing by the law of the Union or of the Member States to which the Contractor is subject (e.g. investigations by criminal prosecution or state protection authorities); in such a case, the Contractor shall inform the controller of these legal requirements before processing, insofar as such notification is not forbidden under the applicable law due to an important public interest (Art. 28 Para. 3 Clause 2 Letter a GDPR).

(2) The Contractor shall not use the personal data provided for processing for any other purposes, especially not for its own purposes. Copies or duplicates of personal data shall not be produced without the knowledge of the Client.

(3) The Contractor assures that all the measures agreed conform to the order processing contract will be implemented for processing personal data according to the order. It assures that the data processed for the Client will be kept strictly separate from other data inventories. The data carriers originating from the Client or used for the Client shall be specifically labelled. Their receipt, departure and on-going use are documented.

(4) In particular, the Contractor shall perform the following inspections in its sphere throughout the entire processing of the service for the Client:
- Security inspections at the levels of infrastructure and applications;
- Availability controls of the data through regular data back-ups.

The results of controls shall be documented.

(5) The Contractor shall cooperate to the necessary extent in the Client's fulfilment of the rights of data subjects pursuant to Art. 12 to 22 GDPR, in the compilation of the directories of processing activities and in the Client's necessary data protection impact assessments. Insofar as possible, the Contractor shall support the Client to a reasonable extent (Art. 28 Para. 3 Clause 2 Letters e and f GDPR). Unless something different has been agreed (e.g. in the main contract or order), the Client shall bear the costs incurred by the Contractor in this context.

(6) The Contractor shall notify the Client without delay if it believes that an instruction issued by the Client violates the legal regulations (Art. 28 Para. 3 Clause 3 GDPR). The Contractor is entitled to postpone the execution of such an instruction until it has been confirmed or altered by the Client's controller after examination.

(7) The Contractor shall correct, delete or restrict the processing of personal data under the order relationship if this is demanded by the Client by means of an instruction and providing this does not contradict the Contractor's justified interests.

(8) The Contractor may only give information about personal data under the order relationship to a third party or to the data subject after receiving a prior instruction or approval from the Client.

(9) The Contractor agrees that the Client – after making an appointment as a matter of principle – is entitled to check compliance with the provisions of data protection, data security and with the



IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel. +49 6502 9208-0 | Fax +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

agreements made in the order processing contract in a reasonable and necessary scope, either itself or through third parties acting on behalf of the Client. In particular, this can be done by obtaining information, inspecting the stored data and the data processing programs and by on-site examinations and inspections (Art. 28 Para. 3 Clause 2 Letter h GDPR).

(10) The Contractor assures that it will cooperate in these controls, if required. The following is agreed in this context until further notice: a third party acting on behalf of the Client may not be in a competitive relationship with the Contractor. The Client shall only perform controls in the necessary scope and shall thereby not disturb the Contractor's operations to an unreasonable extent. Unless agreed differently (in the main contract, order etc.), the Client shall bear the costs incurred by the Contractor for on-site controls.

(11) Processing of data in private residences (telework or work-from-home by the Contractor's employees) is only allowed with the approval of the Client. If data are processed in a private residence, access to the employee's residence must be ensured beforehand for the employer's purposes of control conform to the order processing contract. The measures pursuant to Art. 32 GDPR must also be ensured in this case.

(12) The Contractor confirms that it is aware of the legal provisions of data protection under the GDPR relevant to order processing. It is obliged to observe the rules of confidentiality relevant to the order to which the Client is subject.

(13) The Contractor is obliged to maintain confidentiality in processing the Client's personal data conform to order. This duty continues to exist, even after the order processing contract has ended.

(14) The Contractor assures that it has made its workforce deployed to execute the work aware of the provisions of data protection decisive for them before they commence their work and has obliged them to maintain secrecy in a suitable manner for the duration of their work as well as after the employment relationship has ended (Art. 28 Para. 3 Clause 2 Letter b and Art. 29 GDPR). The Contractor shall monitor compliance with the provisions of data protection law on its premises.

(15) Ms Sarah Müller, IT-HAUS GmbH, 06502-9208-549, datenschutz@it-haus.com, has been appointed by the Contractor as the controller for data protection. The Client must be informed of a change in the data protection controller without delay.

## 7. The Contractor's duties of notification in case of disturbances to processing and in case of violations against the protection of personal data

The Contractor shall inform the Client without delay about disturbances, about violations against the laws of data protection or the stipulations of the order committed by the Contractor or by the people it employs and about the suspicion of data protection infringements or irregularities in the processing of personal data. This particularly applies with regard to any of the Client's duties of reporting and notification pursuant to Art. 33 and Art. 34 GDPR. The Contractor assures that it will support the Client, if necessary, in its duties pursuant to Art. 33 and 34 GDPR in a reasonable manner (Art. 28 Para. 3 Clause 2 Letter f GDPR). The Contractor may only make reports for the Client pursuant to Art. 33 or 34 GDPR after receiving a prior instruction in accordance with Item 5 of this order processing contract.



IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel. +49 6502 9208-0 | Fax +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

## 8. Sub-order relationships with subcontractors (Art. 28 Para. 3 Clause 2 Letter d GDPR)

(1) The Contractor is only allowed to commission subcontractors to process the Client's data with the approval of the Client, Art. 28 Para. 2 GDPR, which must be given through one of the aforesaid communication channels (Item 5). Approval cannot be given unless the Contractor provides the Client with the name and address of the subcontractor and the activity foreseen for it. In addition to this, the Contractor must ensure that it carefully selects the subcontractors, taking particular consideration of the suitability of the technical and organisational measures taken by the subcontractor in the sense of Art. 32 GDPR. The relevant inspection documents in this context shall be provided to the Client upon request.

(2) Subcontractors in third countries may not be commissioned unless the special prerequisites pursuant to Art. 44 ff. GDPR are fulfilled (e.g. resolution of reasonableness by the Commission, standard clauses of data protection, authorised rules of conduct).

(3) The Contractor must ensure by contract that the regulations agreed between the Client and the Contractor also apply to subcontractors. The contract with the subcontractor must be drawn up in such a way that the responsibilities of the Contractor and of the subcontractor are clearly demarked from each other. If several subcontractors are deployed, this also applies to the responsibilities between these subcontractors. In particular, the Client must be entitled to undertake reasonable examinations and inspections of subcontractors as and when necessary, including on-site, or to have these conducted by third parties working on its behalf.

(4) The contract with the subcontractor must be concluded in writing, which can also be done in an electronic format (Art. 28 Para. 4 and Para. 9 GDPR).

(5) Data may not be forwarded to a subcontractor unless this subcontractor has fulfilled the obligations pursuant to Art. 29 and Art. 32 Para. 4 GDPR with regard to its workforce.

(6) The Contractor must regularly inspect compliance with the duties of the subcontractor(s).

(7) The Contractor is liable to the Client for ensuring that the subcontractor fulfils the duties of data protection, which have been contractually imposed upon it by the Contractor in accordance with the foregoing section of the contract.

(8) The subcontractor deployed by IT-HAUS to process personal data can make inquiries to the Client's personal contact person or at info@it-haus.com. The Client declares its agreement with the commissioning of this subcontractor within the framework of the provisions of the main contract and the services owed by the Contractor under this.

(9) The order processor shall always inform the controller of each intended change regarding the deployment of new subcontractors or the replacement of old ones, whereby the Client shall be given the opportunity to object to such changes (Art. 28 Para. 2 Clause 2 GDPR).

(10) A subcontracting relationship in the sense of these provisions does not apply if the Contractor commissions services from a third party that can be regarded as purely auxiliary services. Examples of these are post services, transport services and dispatch services, cleaning work,



IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel. +49 6502 9208-0 | Fax +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

telecommunications services without a tanAgible acquisition of services that the Contractor provides for the Client and guard services. Maintenance and inspection services represent a subcontracting relationship requiring approval, insofar as these are provided for IT systems, which are also used in the context of providing services for the Client.

## 9. Technical and Organisational Measures pursuant to Art. 32 GDPR (Art. 28(3) Sentence 2 (c) GDPR)

(1) An adequate level of protection must be guaranteed to mitigate the risks posed to the rights and freedoms of the natural persons subject to the commissioned data processing. The data protection goals specified in Art. 32(1) GDPR – including the confidentiality, integrity, availability and resilience of systems and services – shall be considered in relation to the nature, scope, context and purposes of processing, in order to permanently mitigate risks by adopting the appropriate technical and organisational measures.

(2) An appropriate and comprehensible risk assessment method shall be used to process personal data in accordance with the contract, taking into account the likelihood and severity of the risks posed to the rights and freedoms of data subjects.

(3) The data protection policy described below includes a detailed description of the technical and organisational measures adopted to contain the identified risks, taking into account the data protection goals, the current state of the art, and especially the IT systems and processing methods used by the Contractor. The procedure used to regularly review, assess and evaluate the effectiveness of these technical and organisational measures, thus ensuring that processing is carried out in accordance with data protection regulations, is outlined **below** and established as binding.

### a) Physical Access Control

The following technical and organisational measures are taken to control access to buildings and verify authorised persons:

- ⇨ Site security, gatekeepers;
- ⇨ Access control system,
  Registration system for authorised persons, identity checks;
- ⇨ Electronic door locking system;
- ⇨ Surveillance system
  Alarm system, video / TV monitor

### b) Password-Protected Access Control

The following technical (password protection) and organisational (user master records) measures are taken to identify and authenticate users:

- ⇨ Password requirements (e.g. special characters, minimum length, regular password change);
- ⇨ Automatic locking (password / pausing);
- ⇨ Creation of <u>one</u> master record per user;
- ⇨ Encryption of data storage devices.

**c) Digital Access Control**

A needs-based authorisation concept has been designed for access rights, monitoring and logging:

- ⇨ Differentiated rights (profiles, roles, transactions and objects);
- ⇨ Evaluations;
- ⇨ Perusal;
- ⇨ Modification;
- ⇨ Deletion.

**d) Data Transfer Control**

The following measures are taken when transporting, transferring, transmitting and storing data storage devices (manually or electronically) and when subsequently checking them:

- ⇨ Encryption / tunnelling connection (VPN = Virtual Private Network);
- ⇨ Logging;
- ⇨ Transport safety.

**e) Input control**

The following measures are taken to subsequently check whether and by whom data has been entered, altered or removed (deleted):

- ⇨ Logging and log evaluation systems.

**f) Order Control**

The following technical and organisational measures are taken to divide responsibilities between the Client and Contractor:

- ⇨ Contractual arrangements;
- ⇨ Formal placement of orders (order form / email / specific group of persons identified by the Client and Customer);
- ⇨ Monitoring of contract execution.

**g) Availability and Resilience**

The following physical and logical measures are taken to secure data:

- ⇨ Back-up to disk to tape (B2D2T);
- ⇨ Mirroring of hard disks, e.g. RAID procedure;
- ⇨ Uninterruptible power supply (UPS);
- ⇨ Anti-virus / firewall;
- ⇨ Emergency plan.

**h) Data Separation**

The following measures are taken to ensure the separate processing of data with different purposes:

- ⇨ Internal multi-client capability / purpose limitation;
- ⇨ Separation of functions / production / testing



IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel. +49 6502 9208-0 | Fax +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

**i) Pseudonymisation**
Personal data is processed in such a way that it can no longer be linked to a specific data subject without the need for additional information, provided this additional information is stored separately and subject to appropriate technical and organisational measures.

**j) Procedure for Regular Review, Assessment and Evaluation**

- Incident response management;
- Default settings for data protection (Art. 25(2) GDPR);
- Data protection management:

A procedure must be implemented to regularly review, assess and evaluate data protection and the effectiveness of technical and organisational measures.

The Contractor follows a process-oriented approach when implementing its data protection management system (DPMS), focusing on its processes and not its organisational structure. The general procedure used for the DPMS is the Deming Cycle, also known as the "PDCA Cycle" (Plan-Do-Check-Act), which is also used in quality management systems. This methodology makes it possible to adapt to changing events and improve the system.

- Plan: The planning phase is used to set goals, strategies, processes, budgets and timelines. This is done when establishing the DPMS and adapting the DPMS after the Act stage. E.g. Privacy policy / guidelines, involvement of the Data Protection Officer, record of processing activities, contract management, data secrecy obligations, data protection training, processes implemented to honour the rights of data subjects, reporting of data breaches, evidence of data security.

- Do: The DPMS plans are implemented in this phase. Requests for information and deletion are processed, and data breaches are reported, etc.

- Check: The monitoring and verification phase is used to measure and maintain the DPMS, providing information for improvements and adjustments. E.g. Regular DPMS evaluations are carried out. Risk assessments must also be reviewed on a regular basis to check for changes in organisational structures, processes and threats, etc.

- Act: During the improvement phase, the findings from the Check phase are processed to improve the DPMS. Identified improvements are implemented, corrective actions and precautionary measures are derived from security incidents, and improvements are checked against the set goals. After this phase, the process restarts at the planning stage.
  The aim is to constantly optimise and improve the DPMS. The DPMS is constantly exposed to new influences and threats, and the Contractor must respond to these.

Some of the measures implemented by the Contractor include:

- The deletion of data that is no longer required (e.g. outdated data, test environments);
- Secure disposal of defective / unneeded hardware;
- Secure disposal of documents (e.g. shredders)
- Secure storage of documents (e.g. lockable filing cabinets)

(4) The Contractor must review, assess and evaluate its technical and organisational measures when needed, but at least once a year, to ensure the security of processing (Art. 32(1) (d) GDPR). The Contractor must make the results available to the Client – alongside a complete audit report – at the latter's request.

(5) Significant security decisions for the organisation of data processing and the procedures used must be agreed between the Client and Contractor.

(6) The Contractor shall immediately inform the Client if its adopted measures do not meet the Client's requirements.

(7) The measures adopted by the Contractor may be adapted over the course of the contract to accommodate any technical and organisational developments, but they must not fall below the agreed standards.

(8) Significant changes must be agreed between the Client and Contractor in a documented format (in writing or electronically). Any costs subsequently incurred by the Client shall be reimbursed by the Contractor if corresponding provisions are stipulated in other agreements between the parties (e.g. main contract, order). Any such arrangements must be stored for the duration of this Agreement.

**10. Obligations of the Contractor after the order has ended, Art. 28 Para. 3 Clause 2 Letter g GDPR**

(1) After the contractual work has been concluded, the Contractor must return to the Client all the data, documents and the compiled results of processing or use in its possession and those that have reached subcontractors, which are connected to the order relationship, or, on the written (text form is sufficient) instruction of the Client, delete or destroy these conform to data protection law or have them destroyed. In this case, the Contractor is obliged to ensure organisationally that the Client's data can actually be deleted or destroyed; the Contractor must inform its entire workforce of this duty of deletion.

(2) Deletion or destruction must be confirmed to the Client with details of the date in writing or in a documented electronic format.



IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel. +49 6502 9208-0 | Fax +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

## 11. Liability

(1) Reference is made to Art. 82 GDPR

(2) In the internal relationship to the Contractor, the Client alone is responsible to the affected person for recompensing damages, which a data subject suffers due to inadmissible or incorrect data processing under data protection laws or use in the course of order processing.

## 12. Miscellaneous

(1) German law shall prevail over this agreement. The place of jurisdiction for all disputes arising from the order processing relationship between the Client and the Contractor is the Contractor's headquarters.

(2) Agreements on technical and organisational measures and on control and inspection documents (also involving subcontractors) shall be retained by both parties for their duration of validity and subsequently for a further three full calendar years.

(3) As a matter of principle, the written form or a documented electronic format is required for auxiliary accords.

(4) If ownership or the Client's personal data to be processed become endangered at the Contractor's premises by third party intervention (perhaps by attachment or seizure), by insolvency proceedings or a settlement process or by other events, the Contractor must inform the Client of this without delay.

(5) The objection of the right of retention in the sense of § 273 BGB is excluded with regard to the data processed for the Client and the associated data carriers.

(6) This agreement for order processing contains all details pursuant to Art. 30 GDPR for the directory of processing activities.

(7) Should individual parts of this agreement be unworkable, this shall not affect the workability of the remainder of the agreement.

General Managers
Ingo Burggraf, Stefan Sicken, Dr. Thomas Simon, Ulrich Simon

Commercial Register
Wittlich Magistrates' Court, HRB 3983 VAT ID No.: DE 192 270 896

Address
IT-HAUS GmbH • Europa-Allee 26/28 • 54343 Föhren • Deutschland / Germany