GDPR order processing agreement

The following contract is concluded between the ITEXIA customer (client) and ITEXIA GmbH (contractor).

Preamble

(1) This agreement sets out in concrete terms the data protection obligations of the contracting parties arising from the order processing described. This applies to all activities which are connected to the use and where employees or representatives of the contractor may come into contact with personal data of the client.

(2) The term of this agreement corresponds to that of the contract. Termination of the contract will automatically lead to termination of this agreement. Isolated termination of this agreement is excluded.

§ 1 Subject matter, duration and specification of the engagement

(1) The use of the ITEXIA software takes place as SaaS solutions (cloud) on the servers of the contractor. The subject matter and term of this agreement are defined in the contract. The client is solely responsible for assessing the lawfulness of the data gathering / processing / use, as well as for safeguarding the rights of the data subjects. This agreement sets out the data protection obligations of the contracting parties in concrete terms which are connected to the order data processing of the use of the ITEXIA software. The gathering, processing or use of personal data by the contractor for the client following an engagement by the latter and in accordance with the instructions of the client in connection with the provision of services for the ITEXIA software.

(2) Product description:
We assist companies in eliminating the high costs of manual inventory taking of furniture, IT equipment, machines, etc by digitising and automating inventory administration. The inventory is provided with machine-readable labels (barcode, QR code or RFID tag). During the inventory, the labels are scanned with a mobile data recording device (smartphone, industrial scanner or RFID reader) in connection with the ITEXIA MDT app or ITEXIA Smartphone app and added to the data inventory. By doing so, we are able to create a simple overview of all items (inventories) at the company. The inventory data which has been verified can then be transferred from the ITEXIA software directly into existing third-party systems. The inventory manager receives an up-to-date target/actual comparison via his or her access and can process any deviations that arise by himself or herself in the ITEXIA software. Change and retirement protocols are no longer necessary.

(3) The group of data subjects can be the following amongst others:

☒ Personnel including voluntary persons, representatives, temporary workers and casual employees,
☒ university students and school pupils.

(4) This agreement regulates the measures relating to the protection of personal data between the client and the contractor which are required in accordance with Article 28 GDPR.

Type of client data	Types of processing	Purpose of the data gathering, processing or use	Group of data subjects
First name, surname Technical data relating to devices with possible personal reference, email address	Assignment to the respective inventory / object	The contractor shall carry out inspection work for the client, where the possibility of access to personal data can not be excluded. For authentication and entitlement	Client / employees

§ 2 Area of applicability and responsibility

(1) The contractor shall process any personal data on behalf of the client in accordance with the contract and its service description and as set out in concrete terms in this agreement. Within the framework of this agreement, the client is solely responsible for compliance with the statutory provisions set out in the data protection laws, in particular for the lawfulness of the data disclosure to the contractor, as well as for the lawfulness of the data processing.

(2) The instructions will be initially set by means of this agreement and can then be altered, added to or replaced by the client in written or text form (individual instruction). Instructions which go beyond the contractually agreed service will be treated as a service change request. The justified costs shall be borne by the client.

The recipients of instructions on the part of the contractor are the following:

- The specialist department or individual persons placing the order:
  Customer Success Management (CSM)
- (or separately appointed deputy / successor)
  Steffen Prasse

§ 3 Obligations of the contractor

(1) The contractor may only process personal data of data subjects within the framework of the engagement, which is set out in more detail in the contract and this agreement and in accordance with the documented instructions of the client, unless an exceptional case as set out in Article 28 Paragraph 3 Letter a) GDPR is present. In such an exceptional case, the contractor shall inform the client of its legal obligation, provided that it is not prevented from doing so in accordance with the law.

(2) The contractor shall set up the internal organisation in its area of responsibility in such a way that it meets the special requirements relating to data protection. It shall take technical and organisational measures for the reasonable protection of the data of the client which meet the requirements set out in Article 32 GDPR. The contractor must take technical and organisational measures which ensure the confidentiality, integrity, availability and durability of the systems and services in connection with the processing on a permanent basis. Furthermore, measures must be taken in order to immediately restore the availability of personal data and access to it following a physical or technical incident and a procedure must be implemented in order to regularly review the effectiveness of the technical and organisational measures to ensure the security of the processing. The measures to be taken also include the pseudonymisation and encryption of personal data, should this be necessary to guarantee a reasonable level of protection.

(3) The technical and organisational measures are subject to technical progress and further development. To this extent, the contractor is permitted to implement alternative, adequate measures. During this process, the security level of the determined measures may not be fallen below. Essential changes must be documented and communicated to the client immediately.

1. Confidentiality (Article 32 Paragraph 1 Letter b) GDPR)

1.1. Entry control
Deutsche Telekom AG's computer centre buildings are secured by security locks, barred windows and roller blinds. Access via the designated access routes is only possible for authorised persons with a magnetic card and key. In addition, the access routes are secured by security guards, video monitoring and alarm systems. Employees with access authorisation are defined organisationally, magnetic cards and keys are only issued in accordance with the organisational instructions. Attendance lists are kept in relation to access, regulations for external staff and guidelines for escorting guests are in place. Access to the offices of the contractor is controlled by means of various keys. Keys have been documented and allocated. Visitor control and pick-up and escort by staff members are in place. Persons from outside the company are accompanied whilst on the contractor's premises.

1.2. Admission control
Access to ITEXIA systems takes place with authentication by means of an individual user ID and password. Entitlements are issued according to an access authorisation concept. Continuously updated systems against malware (for example anti-virus protection) for servers and workstations are in place.
The systems are secured against unauthorised access by means of a firewall. Password-protected screen savers protect against unauthorised viewing, also when an employee of the contractor is temporarily absent. Data backup carriers are only stored in secured rooms. A controlled destruction of data carriers and electronic data of the client takes place.

1.3. Access control
Authorisations are defined in the ITEXIA software, differentiated accesses and differentiated entitlements are set. Organisational and technical entitlements are separate. Access according to entitlement is also maintained during procedures for restoring data from backups. Remote maintenance takes place with a clear user ID. All users of the contractor have clear user ID's. Regulations concerning the use of passwords are in place and are known. A regular change of password is mandatory and employees who leave the company are immediately blocked.

1.4. Separation control (principle of separation)
There is a separation of the client's data from one's own data / other order data, at least by means of separation in the course of entitlement management (clients). Separation of the test and productive system takes place at the premises of the client.

1.5. Pseudonymisation
There are no anonymised or pseudonymised forms of data.

2. Integrity (Article 32 Paragraph 1 Letter b) GDPR)

2.1. Disclosure control
All employees of the contractor are informed about data secrecy. Where necessary, the data is protected against access on a network level, data is encrypted and interfaces are protected against unauthorised data export.

2.2. Input control
Following a request by the client, it is ensured by means of individual access accounts of the contractor at the premises of the client within the framework of the data backup of the client systems that it can be checked whether and by whom personal data has been entered, altered or removed on the part of the contractor.

3. Availability and durability (Article 32 Paragraph 1 Letter b) GDPR)

3.1. Availability control
Regular backups of the systems of the contractor are tested. The client is responsible itself for the backup of the data on its systems, however it can obtain support from the contractor for the technical implementation. Sufficient anti-virus and firewall protections are implemented at the premises of the contractor. The storing of the data backup carrier with data of the client takes place in a different fire compartment than the operation of the systems which are to be backed up. The hosting for the SaaS solution takes place on the servers of T-Systems International GmbH. Current security updates are used on the systems of the contractor.

3.2. Speedy restoration capability (Article 32 Paragraph 1 Letter c) GDPR)
The contractor ensures availability of the personal data and access to it in case of a physical or technical incident.

4. Procedures for regular review, assessment and evaluation (Article 32 Paragraph 1 Letter d) GDPR; Article 25 Paragraph 1 GDPR)

4.1. Data protection management
- Data protection officer has been appointed
- Regular audits by the data protection officer
- Employees are obliged to handle personal data confidentially

4.2. Data protection friendly default settings
The client reserves the right to take measures to ensure that by default, only such personal data whose processing is necessary for the respective specific processing purpose is processed.

4.3. Incident response management
No incident response plan is in place.

(4) The contractor guarantees that the employees and other persons who work for the contractor and who are involved in the processing of the data of the client are prohibited by means of an obligation which has been entered into from gathering, processing or using the data in an unauthorised manner.

(5) The contractor shall immediately inform the client in case of serious breaches by the contractor or persons working for the contractor within the framework of the engagement of regulations concerning the protection of the personal data of the client or the stipulations concluded in the agreement. The contractor shall take the necessary measures to secure the data and to mitigate possible detrimental consequences for the data subjects and shall co-ordinate with the client immediately for this purpose.

(6) Following a request, the contractor shall nominate a contact person to the client for data protection queries which may arise in the course of this agreement.

(7) The contractor hereby confirms that it is aware of the applicable regulations under data protection laws, for example its obligation to appoint a data protection officer where mandated by law.

(8) The contractor shall not use the data which has been handed over for any purposes other than fulfilment of the contract.

(9) The contractor shall correct, delete or block the contractual data if instructed to do so by the client. The contractor shall carry out the destruction of data carriers and other materials in accordance with data protection requirements following an individual engagement by the client, unless already agreed in the service contract. In special cases to be determined by the client, these will be retained or handed over.

(10) Data, data carriers and all other materials must be either surrendered or deleted after completion of the engagement, following a request by the client. Should additional costs arise due to deviating specifications at the time of handover or deletion of the data, these shall be borne by the client.

§ 4 Rights and obligations of the client

(1) Within the framework of this agreement, the client is responsible for compliance with the applicable data protection laws, in particular relating to the obligations of the client for the lawfulness of issuing the order to the contractor for the processing of personal data, as well as for the lawfulness of the processing of the personal data.

(2) Prior to the start of the data processing and then at regular intervals, the client must satisfy itself of compliance with the technical and organisational measures relating to data security taken by the contractor. The client shall document the results in a suitable manner. The client is responsible for ensuring that these provide a reasonable level of protection in relation to the risks of the data to be processed.

(3) The instructions will be initially set by means of the contract and this agreement and can then be altered, added to or replaced by the client in written or text form addressed to the location specified by the contractor by means of individual instructions (so-called individual instructions). Changes to the object of the processing or procedural changes must be agreed jointly and set by the client in writing or text form in accordance with Sentence 1. The final authority to take decisions rests with the client.

(4) The client has the right to issue additional instructions to the contractor, in particular to the following extent:

☒ In relation to fulfilment of the contract

☒ In relation to additional data backup measures

☒ In relation to the procedure in case of data protection breaches

(5) The client shall nominate persons who are authorised to issue instructions. The direct contact to the contractor shall take place via the person of the client or his or her nominated deputy.

(6) In case that the persons authorised to issue instructions or the primary contact persons on the part of the client change, the client shall notify the contractor of such in writing.

(7) The client must immediately and fully inform the contractor if it becomes aware of errors or irregularities in the results of the order in relation to the provisions under data protection laws.

(8) Should a claim be brought against one of the contracting parties by a data subject in relation to any claims under Article 82 GDPR concerning the data processing under or in connection with this agreement, the contracting party against whom the claim is being brought shall be obliged to inform the other contracting party immediately. The contracting parties shall mutually support each other in the defence of the claim.

§ 5 Queries from data subjects

(1) Should the client be obliged to provide an individual person with information concerning the gathering, processing or use of his or her data under applicable data protection laws, the contractor shall support the client in providing the said information. This is subject to the client having made a corresponding request to the contractor in writing or text form and the client reimbursing the contractor the costs which are incurred as a result of the provision of this support. The contractor will not respond to any requests for information and will refer the data subject on to the client.

(2) Should a data subject contact the contractor with requests for rectification, erasure or blocking, the contractor shall refer the data subject to the client.

§ 6 Monitoring obligations

Prior to commencing the data processing and then at regular intervals, the client shall satisfy itself of the technical and organisational measures of the contractor and shall document the results.

- For this purpose, the client can obtain information from the contractor as an example
- or carry out personal inspections or have these undertaken by a professional third-party who is not in competition with the contractor during normal business hours following timely agreement and without disturbing the operational processes of the contractor.
- Where necessary, the contractor is hereby providing an undertaking that it will co-operate in such inspections. Any additional expenses shall be borne by the client.

§ 7 Subcontractors

(1) At the time of conclusion of this agreement, the companies listed in Paragraph 3 are working as subcontractors for the contractor for partial services and also directly process and/or use the data of the client in this context. For these subcontractors, consent is deemed to have been issued in relation to their engagement.

(2) The client agrees that the contractor may engage its associated companies in order to fulfil its contractually agreed services and/or subengage companies in relation to the listed services. This requires the express agreement of the client (in text form as a minimum).

(3) The contractually agreed services and the partial services listed below will be carried out by engaging a subcontractor, namely:

Name and address of the subcontractor	Description of the partial services
Open Telekom Cloud der Deutschen Telekom AG T-Systems International GmbH, Hahnstraße 43d, 60528 Frankfurt am Main, Germany	Infrastructure-as-a-Service, Hosting
HubSpot Germany GmbH, Koppenstrasse 93, 10243 Berlin, Germany	CRM provider

(4) Should the contractor issue engagements to subcontractors, the contractor shall be obliged to assign its obligations under this agreement to the subcontractor. Sentence 1 shall apply in particular to the requirements concerning confidentiality, data protection and data security between the contracting partners to this agreement. Any inspection carried out by the client at the premises of the subcontractor shall only take place by agreement with the contractor.

(5) By means of a written request, the client is entitled to obtain information from the contractor concerning the obligations of the subcontractor which are relevant from a data protection point of view, if necessary also by viewing the relevant contractual documents.

(6) A subcontracting relationship which requires agreement shall not be deemed to be present if the contractor engages third-parties within the framework of an ancillary service connected to the principal service, for example in case of external personnel, postal and shipping services or maintenance.
The contractor shall conclude agreements with the said third-party to the necessary extent in order to guarantee reasonable data protection.

§ 8 Severability clause, written form clause, choice of law

(1) Should individual parts of this agreement be or become invalid in part, this shall not affect the validity of the remaining provisions of this agreement. In place of the invalid provisions, the contracting parties shall agree a reasonable clause which is lawful and which comes closest to the economic content of the original provision.

(2) Amendments and additions to this agreement and to all of its components, including any undertakings of the contractor, require a written agreement and an express notice that this concerns an amendment or addition to these conditions. The same also applies to any omission of this form requirement.

(3) In case of conflicts, the provisions of this agreement relating to data protection shall take priority over the clauses of the service contract. Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of this agreement.

(4) German law shall apply. Dresden (Germany) is hereby being agreed as the place of jurisdiction.

As of: October 2021 ITEXIA GmbH