Data Processing Agreement for Software and Cloud Services

1. DEFINITIONS

1.1. "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to Taulia be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

1.2. "**Data Protection Law**" means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement.

1.3. "**Data Subject**" means an identified or identifiable natural person as defined by Data Protection Law.

1.4. "**EEA**" means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.

1.5. "**EU Standard Contractual Clauses**" means the unchanged standard contractual clauses, published by the European Commission, reference 2021/914 or any subsequent final version thereof which shall automatically apply. To avoid doubt Modules 2 and 3 shall apply as set out in Section 8.

1.6. "**GDPR**" means the General Data Protection Regulation 2016/679.

1.7. "**SCC Relevant Transfer**" means a transfer (or an onward transfer) to a Third Country of Personal Data that is either subject to GDPR or to applicable Data Protection Law and where any required adequacy means under GDPR or applicable Data Protection Law can be met by entering into the EU Standard Contractual Clauses.

1.8. "**Personal Data**" means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is:

a) entered by Customer or its authorized users into or derived from their use of the Software and Cloud Services; or

b) supplied to or accessed by Taulia or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).

1.9. "**Personal Data Breach**" means a confirmed:

a) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data; or

b) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

1.10. "**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller, be it directly as processor of a Controller or indirectly as subprocessor of a processor which processes personal data on behalf of the Controller.

1.11. "**Schedule**" means the numbered Annex with respect to the EU Standard Contractual Clauses.

1.12. **"Software and Cloud Services"** means the Software and Cloud Services as defined in the Agreement.

1.13. "**Subprocessor**" or "**sub-processor**" means Taulia Affiliates, SAP SE, SAP SE Affiliates and third parties engaged by Taulia, SAP SE or SAP SE's Affiliates in connection with the Software and Cloud Services and which process Personal Data in accordance with this DPA.

1.14. "**Technical and Organizational Measures**" means the technical and organizational measures identified under Schedule 2.

1.15. "**Third Country**" means any country, organization or territory not acknowledged by the European Union under Article 45 of GDPR as a safe country with an adequate level of data protection.

2. BACKGROUND

2.1. Purpose and Application

This document ("**DPA**") is incorporated into the framework terms and conditions under which Taulia supplies Software and Cloud Services to Customer (the "**Agreement**"). This DPA applies to Personal Data processed by Taulia and its Subprocessors in connection with its provision of the Software and Cloud Services. This DPA does not apply to non-production environments of the Software and Cloud Services if such environments are made available by Taulia. Customer shall not store Personal Data in such environments.

2.2. Structure

Schedules 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of Data Subjects (Schedule 1) and the applicable Technical and Organizational Measures (Schedule 2).

2.3. Governance

Taulia acts as a Processor and Customer and those entities that it permits to use the Software and Cloud Services act as Controllers under the DPA.

Customer acts as a single point of contact and shall obtain any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use Taulia as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Software and Cloud Services. Where Taulia informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Software and Cloud Services. Customer shall forward such information and notices to the relevant Controllers.

3. SECURITY OF PROCESSING

Taulia has implemented and will apply the Technical and Organizational Measures. Taulia may change the Technical and Organizational Measures at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

4. TAULIA OBLIGATIONS

4.1. Instructions from Customer

Taulia will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Software and Cloud Services then constitutes further instructions. Taulia will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Software and Cloud Services. If any of the before-mentioned exceptions apply, or Taulia otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, Taulia will immediately notify Customer (email permitted).

4.2. Processing on Legal Requirement

Taulia may also process Personal Data where required to do so by applicable law. In such a case, Taulia shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

4.3. Personnel

To process Personal Data, Taulia and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. Taulia and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

4.4. Cooperation

4.4.1. At Customer's request, to the extent that Customer does not have access to the relevant information in its use of the Software and Cloud Services, Taulia will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding Taulia's processing of Personal Data or any Personal Data Breach. For the avoidance of doubt, Customer shall be -subject to Section 4.4.2 below- solely responsible for communicating with Data Subjects.

4.4.2. If Taulia receives a request from a Data Subject in relation to the Personal Data processing hereunder, Taulia will promptly notify Customer (where the Data Subject has provided information to identify the Customer) via e-mail and shall not respond to such request itself but instead ask the Data Subject to redirect its request to Customer.

4.4.3. In the event of a dispute with a Data Subject as it relates to Taulia's processing of Personal Data under this DPA, the Parties shall keep each other informed and, where appropriate, reasonably cooperate with the aim of resolving the dispute amicably with the Data Subject.

4.4.4. Taulia shall provide functionality to support Customer's ability to access, correct, or delete Personal Data from the Software and Cloud Services, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, Taulia will provide access, correct, or delete any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

4.5. Personal Data Breach Notification

Taulia will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. Taulia may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by Taulia.

4.6. Data Protection Impact Assessment

If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, to the extent that Customer does not have access to the relevant information, Taulia will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, Audit Reports and Certifications). Any additional assistance shall be mutually agreed between the Parties.

5. DATA EXPORT AND DELETION

5.1. Export and Retrieval by Customer

During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case Taulia and Customer will find a reasonable method to allow Customer access to Personal Data.

5.2. Deletion

Before the Subscription Term expires, at Customer's request, and to the extent that any Personal Data has not been synched to the Connected ERP System, as defined under the Agreement, Taulia shall provide Customer with relevant Customer Personal Data from the Software and Cloud Services in standard format. Such shall constitute a "return" of Personal Data. At the end of the Subscription Term, Customer hereby instructs Taulia to delete the Personal Data remaining on servers hosting the Software and Cloud Services within a reasonable time period in line with Data Protection Law (not to exceed 6 months) unless applicable law requires retention.

6. CERTIFICATIONS AND AUDITS

6.1. Customer Audit

Customer or its independent third party auditor reasonably acceptable to Taulia (which shall not include any third party auditors who are either a competitor of Taulia or not suitably qualified or independent) may audit Taulia's control environment and security practices relevant to Personal Data processed by Taulia only if

a) Taulia has -on Customer's request- not provided sufficient evidence of its compliance with the Technical and Organizational Measures that protect the production systems of the Cloud Service through providing a copy of its most current SSAE18 SOC2 audit report;

b) a Personal Data Breach has occurred; or

c) such audit is provided under mandatory Data Protection Law conferring Customer a direct audit right and provided that Customer shall only audit once in any 12 months period unless mandatory Data Protection Law requires more frequent audits.

6.2. Other Controller Audit

Any other Controller may assume Customer's rights under Section 6.1 only if it applies directly to the Controller and such audit is permitted and coordinated by Customer. Customer shall use all reasonable means to combine audits of multiple other Controllers to avoid multiple audits unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by Taulia on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

6.3. Scope of Audit

Customer shall provide at least 60 days advance written notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of 3 business days. Beyond such restrictions, the parties will use current audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to Taulia.

6.4. Cost of Audits

Customer shall bear the costs of any audit unless such audit reveals a material breach by Taulia of this DPA, then Taulia shall bear its own expenses of an audit. If an audit determines that Taulia has breached its obligations under the DPA, Taulia will promptly remedy the breach at its own cost.

7. SUBPROCESSORS

7.1. Permitted Use

Taulia is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

a) Taulia or SAP SE as Taulia's ultimate holding company on Taulia's behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. Taulia shall be liable for any breaches by the Subprocessor in accordance with the terms of this DPA;

b) Taulia will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

c) Taulia's list of Subprocessors in place on the effective date of the Agreement is published at: https://taulia.com/taulia-sub-processors/.

7.2. New Subprocessors

Taulia's use of Subprocessors is at its discretion, provided that:

a) Taulia will inform Customer in advance by email of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and

b) Customer may object to such changes as set out in Section 7.3.

7.3. Objections to New Subprocessors

7.3.1. If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may do so. In the event the Customer objects to a new Subprocessor, Taulia will use reasonable efforts to make available to Customer a change in the Software and Cloud Services or recommend a commercially reasonable change to the Customer`s configuration or use of the Software and Cloud Services to avoid processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening Customer. If Taulia is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those Software and Cloud Services which cannot be provided by Taulia without the use of the objected-to new Subprocessor by providing written notice to Taulia. Taulia will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Software and Cloud Services. Any termination under this Section 7.3 shall be deemed to be without fault by either party

7.4. Emergency Replacement

Taulia may replace a Subprocessor without advance notice where the reason for the change is outside of Taulia's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, Taulia will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 7.3 applies accordingly.

8. INTERNATIONAL PROCESSING

8.1. Conditions for International Processing

Taulia shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

8.2. Applicability of EU Standard Contractual Clauses

8.2.1. The following applies in respect of SCC Relevant Transfers:

8.2.1.1. Where Taulia is not located in a Third Country and acts as a data exporter, Taulia (or SAP SE as Taulia's ultimate holding company on Taulia's behalf) has entered into the EU Standard Contractual Clauses with each Subprocessor as the data importer. Module 3 (Processor to Processor) of the EU Standard Contractual Clauses shall apply to such SCC Relevant Transfers.

8.2.1.2. Where Taulia is located in a Third Country:

Taulia and Customer hereby enter into the EU Standard Contractual Clauses with Customer as the data exporter and Taulia as the data importer which shall apply as follows:

a) Module 2 (Controller to Processor) shall apply where Customer is a Controller; and

b) Module 3 (Processor to Processor) shall apply where Customer is a Processor. Where Customer acts as Processor under Module 3 (Processor to Processor) of the EU Standard Contractual Clauses, Taulia acknowledges that Customer acts as Processor under the instructions of its Controller(s).

8.2.2. Other Controllers or Processors whose use of the Software and Cloud Services has been authorized by Customer under the Agreement may also enter into the New Standard Contractual Clauses with Taulia in the same manner as Customer in accordance with Section 8.2.1.2 above. In such case, Customer enters into the New Standard Contractual Clauses on behalf of the other Controllers or Processors.

8.2.3. With respect to an SCC Relevant Transfer, on request from a Data Subject to the Customer, Customer may make a copy of Module 2 or 3 of the EU Standard Contractual Clauses entered into between Customer and Taulia (including the relevant Schedules), available to Data Subjects, provided that Customer shall ensure to redact any part of the EU Standard Contractual Clauses prior to sharing a copy in order to protect business secrets or other confidential information, including the Technical and Organisational Measures described in Schedule 2.

8.3. Relation of the EU Standard Contractual Clauses to the Agreement

Nothing in the Agreement shall be construed to prevail over any conflicting clause of the EU Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and Subprocessor rules, such specifications also apply in relation to the EU Standard Contractual Clauses.

8.4. Third Party Beneficiary Right under the EU Standard Contractual Clauses

8.4.1. Where Customer is located in a Third Country and acting as a data importer under Module 2 or Module 3 of the EU Standard Contractual Clauses and Taulia is acting as Customer's sub-processor under the applicable Module, the respective data exporter shall have the following third party beneficiary right:

8.4.2. In the event that Customer has factually disappeared, ceased to exist in law or has become insolvent (in all cases without a successor entity that has assumed the legal obligations of the Customer by contract or by operation of law), the respective data exporter shall have the right to terminate the affected Software and Cloud Services solely to the extent that the data exporter's Personal Data is processed. In such event, the respective data exporter also instructs Taulia to erase or return the Personal Data.

8.5. Applicability of EU Standard Contractual Clauses where applicable Data Protection Law requires a variation to the EU Standard Contractual Clauses

8.5.1. Subject to Sections 8.2.1.1. to 8.2.1.2., in relation to Personal Data that is protected by the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR") the EU Standard Contractual Clauses are interpreted as follows:

8.5.1.1.1. "Third Country" shall be interpreted as any country, organization or territory which is not acknowledged as providing an adequate level of protection of personal data pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and

8.5.1.1.2. the "EU Standard Contractual Clauses" shall be interpreted as the "International Data Transfer Addendum to the EU Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("UK Addendum") and shall apply completed as follows:

i. the EU Standard Contractual Clauses, completed as set out above in Sections 8.2.1.1 and 8.2.1.2 (as applicable), shall also apply to transfers of such Personal Data, subject to (ii) below;

ii. Tables 1 to 3 of the UK Addendum shall be deemed completed with the relevant information from the EU Standard Contractual Clauses, completed as set out above at Sections 8.2.1.1 and 8.2.1.2 (as applicable), and the options "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this DPA.

9. DOCUMENTATION; RECORDS OF PROCESSING

9.1. Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

10. LIABILITY

The total combined liability of the data exporter on the one hand, and of the data importer on the other hand, under or in connection with this DPA, the EU Standard Contractual Clauses, and the Agreement, subject to the remaining terms of the Agreement relating to liability (including specific exclusions from any limitation of liability), will be limited to the maximum monetary liability amount set out under such Agreement.

11. GOVERNING LAW AND VENUE

This DPA shall be governed by the laws of Germany, and any action or proceeding related to this DPA (including those arising from non-contractual disputes or claims) will be brought in Dusseldorf, Germany.

However, where a dispute arises regarding the processing of UK Personal Data under this DPA, such dispute shall be governed by the laws of England and Wales.

Schedule 1 Description of the Processing

This Schedule 1 applies to describe the Processing of Personal Data for the purposes of the EU Standard Contractual Clauses and applicable Data Protection Law.

1. OPTIONAL CLAUSES OF THE EU STANDARD CONTRACTUAL CLAUSES

1.1. Except where applicable Data Protection Law requires a variation to the EU Standard Contractual Clauses, the governing law of the EU Standard Contractual Clauses shall be the laws of Germany and the German courts shall have jurisdiction for any disputes arising out of or in connection with them.

1.2. The optional Clause 7 and the option in Clause 11a of the EU Standard Contractual Clauses shall not apply.

1.3. Option 2, General Written Authorisation of Clause 9 shall apply in accordance with the notification periods set out in Section 7 of this DPA.

2. A. LIST OF PARTIES

2.1. Under the EU Standard Contractual Clauses

2.1.1. Module 2: Transfer Controller to Processor

Where Taulia is located in a Third Country, Customer is the Controller and Taulia is the Processor, then Customer is the data exporter and Taulia is the data importer.

2.1.2. Module 3: Transfer Processor to Processor

Where Taulia is located in a Third Country, Customer is a Processor and Taulia is a Processor, then Customer is the data exporter and Taulia is the data importer.

3. B. DESCRIPTION OF TRANSFER

3.1. Data Subjects

The Customer Personal Data relates to Customer's users of the Software and Cloud Services, individual suppliers of Customers or individual agents of Customer's suppliers and their respective employees.

3.2. Data Categories

The transferred Personal Data concerns the following categories of data:

The Customer Personal Data relates to names, email addresses, telephone numbers, job titles, addresses and bank details of Customer's suppliers and other Personal Data that may be contained in business related communications.

3.3. Special Data Categories (if agreed)

3.3.1. Not applicable.

3.4. Purposes of the data transfer and further processing; Nature of the processing

3.4.1. The transferred Personal Data includes the following basic processing activities:

a) use of Personal Data to set up, operate, monitor and provide the Software and Cloud Services (including operational and technical support);

b) continuous improvement of service features and functionalities provided as part of the Cloud Service including automation, transaction processing and machine learning;

c) provision of related Professional Services;

d) communication to authorized users of Customer;

e) storage of Personal Data in dedicated data centers (multi-tenant architecture);

f) release, development and upload of any fixes or upgrades to the Software and Cloud Services;

g) back up and restoration of Personal Data stored in the Software and Cloud Services;

h) computer processing of Personal Data, including data transmission, data retrieval, data access;

i) network access to allow Personal Data transfer;

j) monitoring, troubleshooting and administering the underlying Software and Cloud Services infrastructure and database;

k) security monitoring, network-based intrusion detection support, penetration testing; and

l) execution of instructions of Customer in accordance with the Agreement.

3.4.2. The purpose of the transfer is to provide and support the Software and Cloud Services. Taulia and its Subprocessors may support the Software and Cloud Services remotely.

3.5. Additional description in respect of the EU Standard Contractual Clauses:

3.5.1. Applicable Modules of the EU Standard Contractual Clauses

a) Module 2: Transfer Controller to Processor

b) Module 3: Transfer Processor to Processor

3.5.2. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

In respect of the EU Standard Contractual Clauses, transfers to Subprocessors shall be on the same basis as set out in the DPA.

3.5.3. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Transfers shall be made on a continuous basis i.e., each time the Customer or its suppliers access or uses the Software and Cloud Services.

3.5.4. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

Personal Data shall be retained for the duration of the Agreement and subject to Section 5.2 of the DPA.

4. C. COMPETENT SUPERVISORY AUTHORITY

4.1. In respect of the EU Standard Contractual Clauses:

4.1.1. Module 2: Transfer Controller to Processor

4.1.2. Module 3: Transfer Processor to Processor

4.2. Where Customer is the data exporter, the supervisory authority shall be the competent supervisory authority that has supervision over the Customer in accordance with Clause 13 of the EU Standard Contractual Clauses.

Schedule 2 Technical and Organizational Measures

This Schedule 2 applies to describe the applicable technical and organizational measures for the purposes of the EU Standard Contractual Clauses and applicable Data Protection Law.

To the extent that the provisioning of the Software and Cloud Services comprises SCC Relevant Transfers, the Technical and Organizational Measures set out in Schedule 2 describe the measures and safeguards which have been taken to fully take into consideration the nature of the personal data and the risks involved.

TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define 's current technical and organizational measures. Taulia may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1. PHYSICAL ACCESS CONTROL

Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

1. Taulia protects its assets and facilities using the appropriate means based on the Taulia IT Security Policy
2. In general, buildings are secured through access control systems (e.g., smart card access system).
3. As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
4. Depending on the security classification, buildings, individual areas and surrounding premises maybe further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
5. Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 2 and 3 below). This also applies to visitor access. Guests and visitors to Taulia buildings must register their names at reception and must be accompanied by authorized Taulia personnel.
6. Taulia employees and external personnel must wear their ID cards at all Taulia locations.
7. Additional measures for Data Centers:
    a. All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
    b. Taulia and all third-party Data Center providers log the names and times of authorized personnel entering Taulia's private areas within the Data Centers.

2. SYSTEM ACCESS CONTROL

Data processing systems used to provide the Taulia Service must be prevented from being used without authorization.

Measures:

1. Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the Taulia IT Security Policy
2. All personnel access Taulia's systems with a unique identifier (user ID).
3. Taulia has procedures in place to so that requested authorization changes are implemented only in accordance with the Taulia IT Security Policy (for example, no rights are granted without authorization).In case personnel leaves the company, their access rights are revoked.
4. Taulia has established a password policy that prohibits the sharing of passwords, governs responses to

password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password protected screensaver.
5. The company network is protected from the public network by firewalls.
6. Taulia uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
7. Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to Taulia's corporate network and critical infrastructure is protected by strong authentication.

3. DATA ACCESS CONTROL

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

Measures:

1. Personal Data requires at least the same protection level as "restricted" information according to the Taulia Information Classification standard.
2. Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. Taulia uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the Taulia IT Security Policy.
3. All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, Taulia conducts internal and external security checks and penetration tests on its IT systems.
4. Taulia does not allow the installation of software that has not been approved by Taulia.
5. A Taulia security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

4. DATA TRANSMISSION CONTROL

Except as necessary for the provision of the Taulia Services in accordance with the relevant Agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at Taulia to provide the agreed-upon service levels (for example, encryption and lead-lined containers).

Measures:

1. Personal Data in transfer over Taulia internal networks is protected according to Taulia IT Security Policy.
2. When data is transferred between Taulia and its customers, the protection measures required for data transfer are hereby mutually agreed upon between Taulia and its customer and included as a part of the Agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of Taulia-controlled systems (e.g. data being transmitted outside the firewall of the Taulia Data Center).

5. DATA INPUT CONTROL

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from Taulia data processing systems.

Measures:

1. Taulia only allows authorized personnel to access Personal Data as required in the course of their duty.
2. Taulia has implemented a logging system for input, modification and deletion, or blocking of Personal Data by Taulia or its Subprocessors within the Taulia Service to the extent technically possible.

6. JOB CONTROL

Job Control is required to ensure that personal data processed on behalf of others are processed strictly in compliance with the Customer's instructions

Measures:

1. Taulia uses controls and processes to monitor compliance with contracts between Taulia and its customers, Subprocessors or other service providers.
2. Personal Data requires at least the same protection level as "restricted" information according to the Taulia Information Classification standard.
3. All Taulia employees and contractual Subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of Taulia customers and partners.

For Support Services, Taulia customers have control over their remote support connections at all times. Taulia employees cannot access a customer system without the knowledge and consent of the customer. Taulia employees cannot access a customer on premise system without the knowledge and active participation of the customer.

7. AVAILABILITY CONTROL

Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

1. Taulia employs regular backup processes to provide restoration of business-critical systems as and when necessary.
2. Taulia uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
3. Taulia has defined business continuity plans for business-critical processes;
4. Emergency processes and systems are regularly tested.

8. DATA SEPARATION CONTROL

Personal Data collected for different purposes can be processed separately.

Measures:

1. Taulia uses appropriate technical controls to achieve Customer Data separation at all times.
2. Customer (including its approved Controllers) will have access only to their own Data based on secure authentication and authorization.
3. If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

9. DATA INTEGRITY CONTROL

Personal Data will remain intact, complete and current during processing activities.

Measures:

1. Taulia has implemented a multi-layered defense strategy as a protection against unauthorized modifications.
2. In particular, Taulia uses the following to implement the control and measure sections described above. In particular:
    a. Firewalls;
    b. Security Monitoring Center;
    c. Antivirus software;
    d. Backup and recovery;
    e. External and internal penetration testing;
    f. Regular external audits to prove security measures.