

Data Processing Addendum

to the Tungsten End User License
Agreement and/or Subscription Terms of
Service for Tungsten Power PDF Cloud

This data processing addendum (the “**Data Processing Addendum**”) is entered into between **Tungsten** and **Customer** and forms part of the **Tungsten End User License Agreement and/or Subscription Terms of Service** between Tungsten and Customer (the “**Agreement**”) pursuant to which Tungsten provides Customer with Tungsten Power PDF Cloud.

The Parties agree that this Data Processing Addendum supplements the Agreement and applies only where in the course of providing the Services to the Customer, Tungsten is Processing Personal Data on behalf of the Customer within the meaning of Art. 4 No. 2 and Art. 28 GDPR.

This Data Processing Addendum serves as a data processing agreement between Tungsten and each Data Controller providing Personal Data in connection with the Services. It further defines the applicable technical and organizational measures Tungsten implements and maintains to protect Personal Data when providing the Service.

By accepting this Agreement and/or availing of the Service, You acknowledge and agree to be bound by the terms and conditions set forth herein. If You do not agree to these terms, You must not use the Service.

Unless otherwise defined herein, all capitalised terms shall have the meaning given to them in the Agreement.

1. DEFINITIONS

The following terms shall have the following meanings in this Data Processing Addendum.

- “**Affiliate**” shall mean any entity controlled by, under common control with or controlling a Party.
- “**Customer**” shall mean the entity that has entered into and accepted the terms and conditions of this Agreement.
- The terms “**Controller**” (also “**Data Controller**”), “**Processor**” (also “**Data Processor**”), “**Personal Data**”, “**Processing**” and “**Subprocessor**” shall have the same meaning as defined in the Standard Contractual Clauses and Article 4 GDPR;
- “**Data Protection Laws**” means any applicable legislation protecting the fundamental rights and freedoms of individuals, and in particular the right to privacy with respect to the Processing of Personal Data, including, but not restricted to the GDPR and the Swiss DPA;
- “**GDPR**” shall mean, as applicable the EU GDPR or the UK GDPR.
- “**EEA**” shall mean the European Economic Area, consisting of the Member States of the European Union and Iceland, Liechtenstein and Norway.
- “**EU GDPR**” shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
- “**EU Standard Contractual Clauses**” shall mean the contractual clauses issued by the European Commission by implementing decision 2021/914 of 4th of June 2021 on

standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

- **“FDPIC”** shall mean the Swiss Federal Data Protection and Information Commissioner.
- **“Parties”** shall mean Tungsten and the Customer.
- **“Security Breach”** shall mean any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

“Services” shall mean solely with respect to the Power PDF Cloud product offering, the Software Maintenance and Support, Subscription Services, Subscription Services Support and Professional Services as further defined in the Agreement.

- **“Standard Contractual Clauses”** shall mean, as applicable the EU Standard Contractual Clauses or the UK Standard Contractual Clauses.
- **“Swiss DPA”** shall mean the Swiss Federal Act on Data Protection and the Swiss Ordinance on the Federal Data Protection Act, as amended from time to time.
- **“Third Country”** shall mean a country outside of the EEA, the UK or Switzerland, as the case may be.
- **“Tungsten”** means Tungsten Automation Ireland Limited or any other Tungsten group entity which is a party to the Agreement.
- **“UK GDPR”** shall mean EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended), and applicable secondary legislation made under that Act.
- **“UK Standard Contractual Clauses”** has the meaning given in Annex 4.

2. PROCESSING OF PERSONAL DATA

- 2.1 The Parties acknowledge and agree that with regard to the Processing of Personal Data, the Customer is the Data Controller (or acts in the capacity of the Data Controller on behalf of its Affiliates and/or third parties in accordance with Section 2.3) and Tungsten is the Data Processor within the meaning of Article 4 no. 7 and no. 8 GDPR.
- 2.2 Within the scope of this Data Processing Addendum, Customer shall be solely responsible for compliance with applicable Data Protection Laws, including, but not limited to, the lawfulness of disclosing Personal Data to Tungsten and the lawfulness of having Personal Data processed on behalf of Customer.
- 2.3 In case it is expressly agreed under the Agreement that Affiliates of the Customer or any other third parties shall also benefit from the Services and the Customer acts in this respect on behalf of and in the name of its Affiliates and/or third parties in their capacity as Data Controllers, Customer shall enter into data processing agreements

with its Data Controllers required to allow Tungsten and its Subprocessors to process any Personal Data as described in this Data Processing Addendum. Customer shall serve as a single point of contact for Tungsten and shall be solely responsible for the internal coordination, review and submission of instructions or requests of other Data Controllers to Tungsten and Tungsten shall be entitled to refuse any requests or instructions provided directly by a Data Controller that is not the Customer. Tungsten shall further have no obligation to inform or notify a Data Controller when it has provided such information or notice to Customer.

- 2.4 The objective of the Personal Data Processing under this Data Protection Addendum is to ensure that the performance of the Services and the Processing will be carried out as further defined in the Agreement. The persons affected by the Processing, the nature of Personal Data to be used as well as the scope, nature and purpose of the Processing by Tungsten are set out in Annex 1 to this Data Processing Addendum.
- 2.5 Each Party shall notify to the other the point of contact for any issues related to data protection arising out of or in connection with the Agreement.
- 2.6 Tungsten shall:
 - 2.6.1 be responsible for complying with all Data Protection Laws applicable to its provision of the Services in its role as Data Processor. However, Tungsten is not responsible for compliance with any laws applicable to the Customer or the Customer's industry that are not generally applicable to information technology service providers;
 - 2.6.2 process the Personal Data only in accordance with the written instructions from the Customer (on its own behalf or on behalf of Data Controllers covered by this Data Processing Addendum that are not the Customer) as set out exclusively in the Agreement and this Data Processing Addendum and Tungsten will not use or disclose the Personal Data for its own purposes except where expressly permitted by Article 28 (3)(a) GDPR. Customer's instructions for the Processing of Personal Data shall comply with the Data Protection Laws and the Customer shall have sole responsibility for the accuracy, quality and legality of the Personal Data and the means by which the Customer acquired the Personal Data. Without any obligation to perform a legal examination, Tungsten shall notify Customer without undue delay in case it believes that an instruction would be in breach of the Data Protection Laws (Art. 28 para. 3 sentence 3 GDPR). Tungsten shall be entitled to suspending performance on such instruction until Customer confirms or modifies such instruction. In any instance where the GDPR applies and Customer is a Data Processor Customer warrants to Tungsten that Customer's instructions, including appointment of Tungsten as a Data Processor or Sub-processor, have been authorized by the relevant Data Controller;
 - 2.6.3 follow and comply with additional instructions relating to the Services received from Customer provided that they are (i) legally required, (ii) legally not prohibited, (iii) technically reasonably feasible and (iv) do not require any material modifications of the Service. In case of additional instructions of the Customer (i.e. instructions that are not covered by the Services as agreed in the Agreement), Customer shall compensate Tungsten based on time and material to then current standard rates of Tungsten. If and to the extent Tungsten is

unable to comply with an additional instruction it shall promptly notify Customer hereof (per email or by any further means allowed under the Agreement);

- 2.6.4 process the Personal Data only to the extent, and in such manner, as it is necessary for the provision of the Services;
- 2.6.5 implement and maintain appropriate technical and organisational measures to protect the Personal Data. Those measures are set out in Annex 2 to this Data Processing Addendum. Customer understands and agrees that these measures are subject to technical progress and development and Tungsten is therefore expressly allowed to implement adequate alternative measures as long as the general security level described in Annex 2 of this Data Processing Addendum is maintained;
- 2.6.6 ensure that access to the Personal Data is limited to those personnel who require such access to provide Services under the Agreement;
- 2.6.7 ensure that all Tungsten personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, and are subject to respective confidentiality obligations. Tungsten shall ensure that such confidentiality obligations survive the termination of their engagement;
- 2.6.8 without any undue delay notify Customer of any Security Breach if it becomes aware of it within the scope of its responsibility, investigate the Security Breach and take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach. Customer is solely responsible for complying with any Security Breach notification obligations applicable to Customer and fulfilling any third-party notification obligations related to any Security Breach. Tungsten shall make reasonable efforts to assist Customer in fulfilling Customer's obligations under Article 33 GDPR or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Breach. Tungsten's obligation to report or respond to a Security Breach under this section is not an acknowledgement by Tungsten of any fault or liability with regard to the Security Breach;
- 2.6.9 Tungsten shall support Customer (in a manner consistent with the functionality of the Services and Tungsten's role as a Processor and to the extent reasonably possible for Tungsten and only where Customer cannot do so without Tungsten's assistance) (i) in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR or corresponding provision in applicable Data Protection Laws, and (ii) in fulfilling the obligations set out in Articles 32 to 36 GDPR or corresponding provision in applicable Data Protection Laws (provided that this support does not result in any breach of Tungsten's confidentiality obligations towards third parties). Where a data subject asserts claims for rectification, erasure or access against Tungsten, and where Tungsten is able to correlate the data subject to Customer, based on the information provided by the data subject, Tungsten shall refer such data subject to Customer. Tungsten shall forward the data subject's claim to Customer without undue delay and support Customer, where reasonably possible. Tungsten shall not be liable in cases where Customer fails to respond to the data subject's request in total, correctly, or in a timely manner.

2.7 Customer shall:

- 2.7.1 notify Tungsten, without undue delay, and comprehensively, of any defect or irregularity in terms of data protection compliance when providing the Services;
- 2.7.2 support Tungsten in defending claims asserted by data subjects against Tungsten in accordance with Article 82 GDPR (if and to the extent reasonably possible).

3. USE OF SUBPROCESSORS

- 3.1 Tungsten may use Affiliates and third parties to provide certain parts of the Services (as Subprocessors) on Customer's behalf. Customer hereby authorizes Tungsten (also on behalf of its Data Controllers and, if applicable under this Data Processing Addendum, also for the relevant clauses of the Standard Contractual Clauses) to engage these Affiliates and third parties for the processing of Personal Data as Subprocessors. This authorisation will constitute the Customer's prior written consent to the subcontracting by Tungsten of the Processing of Personal Data if such consent is required under the Standard Contractual Clauses or the Data Protection Laws.
- 3.2 Any such Subprocessor will be permitted to process Personal Data only to deliver the Services Tungsten has retained them to provide, and they are prohibited from using Personal Data for any other purpose. Tungsten remains responsible for its Affiliates' and other Subprocessors' compliance with the obligations of this Data Processing Addendum.
- 3.3 Any Subprocessors that are engaged by Tungsten for the provision of the Services shall be subject to written Subprocessor terms with Tungsten requiring that the Subprocessor abides by terms no less protective than this Data Processing Addendum (including, if applicable under this Data Processing Addendum, the relevant obligations in the Standard Contractual Clauses). Before selecting a third party as Subprocessor, Tungsten will (if available based on respective certifications) evaluate the security, privacy and confidentiality practices of this party as relevant for its respective data handling.
- 3.4 For the avoidance of doubt, the approval requirements for Subprocessors under the Data Processing Addendum and the Standard Contractual Clauses shall not apply in cases where Tungsten or Subprocessors subcontract ancillary services/deliverables from third parties which are not specific to the provision of the Services. Such ancillary services/deliverables shall, for example, include (but not be limited to) general infrastructure services like telecommunications services or facility management services. Tungsten and Subprocessors shall nevertheless conclude, with such third parties, agreements necessary to ensure applicable data protection standards.
- 3.5 Tungsten currently uses the Subprocessors listed in Annex 3 to this Data Processing Addendum to provide the Services. Tungsten may remove or appoint suitable and reliable other Subprocessors at its own discretion in accordance with this Section 3. Tungsten will inform Customer by email with at least thirty (30) days prior notice of any changes to the list of Subprocessors ("New Subprocessor Notice").

- 3.6 If Customer objects to the use of a Subprocessor for legitimate and reasonable reasons, Customer has the right to terminate the Agreement by written notice within thirty (30) days upon receipt of Tungsten's New Subprocessor Notice. If Customer does not terminate the Agreement within this timeframe, Customer is deemed to accept the respective Subprocessor.
- 3.7 Customer accepts that a replacement of a Subprocessor may be required in cases where the reason for the change is outside of Tungsten's reasonable control (so-called emergency replacement). Tungsten will notify the Customer respectively. If Customer objects to the use of this Subprocessor for legitimate and reasonable reasons, Customer may exercise its right to terminate the Agreement as described in Section 3.6 above.

4. THIRD COUNTRY TRANSFERS

- 4.1 The Parties understand and agree that Tungsten uses Affiliates and third party Subprocessors who are located in, process or have access to Personal Data from Third Countries.
- 4.2 Customer hereby authorizes Tungsten (also on behalf of its Data Controllers and, if applicable under this Data Processing Addendum) to transfer Personal Data to its Subprocessors in Third Countries for Tungsten's provision of the Services. This authorisation will constitute the Customer's prior written approval to the transfer by Tungsten required under Data Protection Laws provided that the specific conditions of Article 44 et seq. GDPR or corresponding provisions in Data Protection Laws, as applicable, have been fulfilled (e.g. Adequacy Decision, Standard Contractual Clauses, Binding Corporate Rules). Tungsten currently transfers Personal Data to Third Countries as specified in Annex 3.
- 4.3 In case of a transfer to a Third Country where no adequate level of data protection exists according to an adequacy decision of the European Commission, the Secretary of State in the UK or the FDPIC or the Swiss Federal Council (as applicable) Tungsten and its Affiliates and third party Subprocessors shall execute and adhere to (i) the EU Standard Contractual Clauses, Module Three (Transfer EU Processor to Processor) for the transfer of any such Personal Data to which the EU GDPR was applicable prior to transfer; and (ii) any applicable country-specific amendments, additions or appendices to the EU Standard Contractual Clauses provided for in Annex 4 for the transfer of any such Personal Data to which the UK GDPR or the Swiss DPA (as the case may be) was applicable prior to transfer.

Tungsten shall make information on the transfer, and where applicable, Standard Contractual Clauses and supplementary measures, available without undue delay to Customer.

- 4.4 **Tungsten shall have the right to amend this Section 4 of this Data Processing Addendum in case Standard Contractual Clauses are amended, revoked or held in a court of competent jurisdiction to be invalid.**

5. AUDIT

- 5.1 Tungsten will on a regular basis audit the security of the computers and computing environment that it uses in processing Customer's Personal Data when providing the Services.
- 5.2 If the Customer requests in writing, Tungsten will provide the Customer with a confidential summary of the results of this audit ("**Summary Report**") so that Customer can reasonably verify Tungsten's compliance with the security obligations under this Data Processing Addendum. The Summary Report is Tungsten's Confidential Information. If the Agreement does not include a provision protecting Tungsten's Confidential Information, then a Summary Report will be made available to Customer subject to a mutually agreed upon non-disclosure agreement covering the Summary Report.
- 5.3 The Customer agrees to exercise its audit right by instructing Tungsten to execute the audit as described in sections 5.1-5.2 of this Data Processing Addendum. If the Customer reasonably concludes that an onsite audit at Tungsten's premises is necessary to monitor the compliance with the technical and organisational measures in an individual case, the Customer shall also have the right to carry out respective onsite inspections in individual cases or to have them carried out by an auditor (that is no competitor of Tungsten) provided that such audits and inspections will be conducted (i) during regular business hours, and (ii) without interfering with Tungsten's business operations, (iii) upon prior notice (observing an appropriate notice period) and further consultation with Tungsten, (iv) all subject to (if not covered already by the Agreement) the execution of a confidentiality undertaking, in particular to protect the confidentiality of the technical and organisational measures and safeguards implemented. Customer will bear its own expenses and compensate Tungsten the cost for its internal resources required to conduct the onsite audit (based on time and material according to the then current price list), the latter only if the audit does not reveal that Tungsten has in fact breached its obligations under the Agreement (in that case Tungsten will promptly remedy the breach at its own cost).
- 5.4 Nothing in this section 5 of this Data Processing Addendum varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

6. DELETION AND RETURN OF DATA

After termination of the Agreement, Tungsten will have no further obligation to provide the Services, and Customer will have no further rights to use or access the Services. After termination of the Agreement, or earlier upon the request of the Customer, Tungsten shall provide Customer either with the ability to correct, delete, or block Personal Data or make such corrections, deletions, or blockages on Customer's behalf. With regard to Subscription Services Tungsten shall under the conditions set out in Article 3.4 of the Agreement for Subscription Services, extract the Personal Data from the Services and deliver the Personal Data to the Customer within 90 days after the termination, or delete

all Personal Data, including back-ups, unless prohibited from doing so by any applicable law. The Services may not support retention or extraction of Personal Data after termination of the Agreement. Tungsten has no liability or further obligation to Customer with respect to the deletion of Personal Data as described in this section.

7. MISCELLANEOUS

- 7.1 This Data Processing Addendum shall automatically terminate upon any termination or expiration of the Agreement.
- 7.2 If there is any conflict between any provision of this Data Processing Addendum and any provision of the Agreement, this Data Processing Addendum shall prevail. If there is a conflict between this Data Processing Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.
- 7.3 Except for changes made by this Data Processing Addendum, the Agreement remains unchanged and in full force and effect.

Annex 1 to Data Processing Addendum (Description of Data Processing)

This Annex 1 provides a description of processing under this Data Processing Addendum

1. Categories of data, special categories of data (if applicable) and data subjects

Personal Data may concern different categories of Personal Data and sensitive data depending on the Customer's use of Services as defined in the Agreement. This data may relate to different data subjects such as employees, its affiliates or its customers or its suppliers and partners.

2. Processing operations

Personal Data will be processed by Tungsten (and its Subprocessors) in order to provide the Services as agreed in the Agreement (please see there for further details). The basic processing activities involve Subscription Services, Subscription Services Support, Processional Services or Software Maintenance and Support (as applicable).

The processing activities includes storage, structuring, and access to Personal Data in the context of technical support as well as other processing activities initiated by the Customer, depending on which Services the Customer has chosen to order from time to time.

3. Duration

Personal Data will be processed until expiration or termination of the Agreement.

4. List of Subprocessors

Current list of Tungsten's Subprocessors is provided in Annex 3 to the Data Processing Addendum.

Annex 2 to Data Processing Addendum (Technical and Organisational Measures)

Description of the technical and organisational measures implemented (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The following appropriate technical and organisational measures and safeguards are implemented and maintained to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. These measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected, taking into account the state of the art and the cost of implementation.

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

(1a) Measures to **ensure ongoing confidentiality** Article 32 Paragraph 1 Point b GDPR:

Tungsten is committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout organization in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with Tungsten' goals and our policy is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained and are supported by specific documented policies and procedures.

Tungsten has defined specific information security objectives, which are developed in accordance with the business objectives and the context of the organization.

(1b) Measures to **deny unauthorised individuals access to data processing facilities** (admission control through physical security measures) Article 32 Paragraph 1 Point b GDPR:

Tungsten has implemented measures to prevent the unauthorized access to data processing systems where personal data is processed. These measures include, but are not limited to:

- | | |
|--|--|
| ☒ Alarm system | ☒ CCTV at entry points (office and data centers) |
| ☒ Automatic access control system | ☒ Security locks |
| ☒ Photoelectric sensors / Movement detectors | ☒ Visitor management at reception desks |
| ☒ Key Management (Issuance of keys, etc.) | ☒ Careful selection of cleaning staff |
| ☒ Logging of visitors | ☒ Visible wearing of access badges mandatory |
| ☒ Careful selection of security guards | ☒ A separate, specific and documented access control for data centers and server rooms for authorized persons is implemented. Access by authorized persons is documented by name and card or token number. For the data centers, separate access control systems are implemented |
| ☒ Protection of building shafts | |
| ☒ Chip card / Transponder locking system | |
| ☒ Manual locking system (Limited usage for key employees to be used in the event of a failure in the access control systems) | |

(1c) Measures to prevent unauthorised individuals from using data processing systems (controlling access to data processing systems):

- 1 Tungsten controls access to information based on business and security requirements.
- 2 Access control rules and rights to applications, expressed in standard user profiles, for each user / group of users are clearly stated, together with the business requirements met by the controls.
- 3 The security requirements of each business application are determined by an identification of all information related to the application and the risks to that information.
- 4 The access rights to each application take into account:
 - a. Premises access control – unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems are located.
 - b. System access control – access to data processing systems is prevented from being used without authorization.
 - c. Data access control – Persons entitled to use a data processing system gain access only to the data to which they have a right of access.
 - d. Personal data cannot be read, copied, modified or removed without authorization.
 - e. The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements.
 - f. Data protection and privacy, legislation and contractual commitments regarding access to data or services.
 - g. The 'need to know' principle (i.e. access is granted at the minimum level necessary for the role).

- h. Rules that must always be enforced and those that are only guidelines
 - i. Prohibit user initiated changes to information classification labels
 - j. Prohibit user initiated changes to user permissions.
 - k. Enforcing rules that require specific permission before enactment.
 - l. Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.
- 5 Tungsten has standard user access profiles for common roles.
 - 6 Management of access rights across the network(s) is done electronically
 - 7 User access requests, authorization and administration are segregated as described in our policy
 - 8 User access requests are subject to formal authorization, to periodic review and to removal.

(1d) Measures to prevent access to personal data by unauthorised individuals (access control by authorisation management):

Tungsten provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of Tungsten or its affiliates.

All users/user groups that need to access organizational information have specific, pre-determined access rights to information, operating systems and applications that conform to and are restricted by the Access Control Policy.

Users are also classified in terms of the level of access they need to information and systems. These classification levels, which are to be recorded in user agreements, are set out below:

Classification of data users		
Classification	Access rights	Example
Guest	Able to see and read public data. Full create and edit rights to a Private data space.	Clients
Trustee	Full rights to a shared directory or sub system. Able to see and use basic business templates and core information sources and systems.	Partner organizations Software maintenance Data input staff Anyone who has signed a non-disclosure agreement
Individual	Premises access – persons are permitted to gain physical access to premises, buildings or rooms	name@organisation.co.uk

	where data processing systems are located. System access – access to data processing systems is permitted with prior authorization. Data access – persons are entitled to use data processing systems in order to gain access to the data to which they have a right of access for their work only. Personal data cannot be read, copied, modified or removed without prior authorization. Able to create files in a user group and delete owned files in that user group. Able to grant access rights to 'Private' files or directories to others. Access rights to restricted and confidential information dependent on role requirements.	
Supervisor	Full unrestricted rights to create new users and configure PCs and create user groups and manage the network.	IT staff
Administrator	Full unrestricted rights to defined systems and the ability to create and remove system supervisors.	IT Department / Senior Responsible Manager

(1e) Measures to **encrypt** personal data Article 32 Paragraph 1 Point a GDPR:

Server-side encryption

Service-managed keys provide a combination of control and convenience with low overhead.

Encryption at rest: Storage service encryption for Cloud services

Data at rest in storage (both Blob and File) is encrypted.

Encryption of data at rest of SQL database

Encryption in-transit

Data encrypted in transit using the Transport Layer Security (TLS) protocol

(1f) Measures for **keeping processing of personal data collected for different purposes separate** (separation control by keeping clients separate and by authorisation management):

Tungsten has implemented measures, to ensure that data which is collected for different purposes can be processed separately.

- | | |
|--|---|
| ☒ Creation of an authorization concept | ☒ Logical client separation (in software) |
| ☒ Provision of records with purpose attributes / data fields | ☒ Approved and documented database rights |

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

(2a) Measures to **ensure ongoing integrity** Article 32 Paragraph 1 Point b GDPR:

Tungsten has implemented measures, to ensure that personal data which is processed by request of the data owner by a data processor, shall only be processed as instructed by the data owner.

- | | |
|---|--|
| ☒ Contractor selection via history review (in particular regarding data security) | ☒ Obligation of the contractor's employees to maintain data confidentiality (GDPR) |
| ☒ Written instructions to the contractor (for example, by Data Processing Agreement) (GDPR) | ☒ Continual review of contractors and their activities |
| ☒ Effective control rights over data processors have been agreed | |

(2b) Measures to **prevent unauthorised perusal and to ensure accountability and protection of data integrity during data transmission** (transfer control by safe transmission):

Tungsten has implemented measures, to ensure that personal data cannot be read, copied or modified during electronic transmission or during transportation or storage to disk. Additionally to control and determine to which bodies that the transfer of personal data provided by data communication equipment is allowed. These measures include, but are not limited to:

- | | |
|--|--|
| ☒ Creation of dedicated lines or VPN tunnels | ☒ Disk encryption (backup tapes for off-site storage) |
| ☒ During physical transport, careful selection of transport personnel and vehicles (tape off-site storage) | ☒ During physical transport, secure transport containers / packaging (tape off-site storage) |

☒ TLS encryption of communications

(2c) Measures for the **subsequent examination and accountability of input, changes and erasures** (input control by creating a protocol):

Tungsten has implemented measures, to ensure that it is possible to ensure, subsequently control, and determine if and by whom, personal data has been entered, changed or removed on data processing systems.

- | | |
|--|---|
| ☒ Granting of rights for the input, modification or the deletion of data based on an authorization concept | ☒ Creation of an overview of which applications are permitted to input, modify or delete which data |
| ☒ Storage of forms, through which data has been acquired during automated processing | |

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

(3a) Measures to **ensure ongoing availability** Article 32 Paragraph 1 Point b GDPR:

Tungsten has implemented measures, to ensure that personal data is protected against accidental destruction or loss. These measures include, but are not limited to:

- | | |
|---|---|
| ☒ Uninterruptible power supplies (UPS) | ☒ Air conditioning in server rooms |
| ☒ Devices for monitoring temperature and humidity in server rooms | ☒ Protection power strips in server rooms |
| ☒ Fire and smoke detection systems | ☒ Fire extinguishers in server rooms |
| ☒ Alarm when unauthorized entry to server rooms is detected | ☒ Creation of a backup & recovery concept |
| ☒ Testing of data recovery | ☒ Preparation of an emergency response plan |
| ☒ Secure off-site storage of data backups | ☒ Server rooms not located under sanitary installations |
| ☒ In flood areas, server rooms are above the water border | |

(3b) Measures to **ensure ongoing resilience of the systems and services** Article 32 Paragraph 1 Point b GDPR:

Tungsten has implemented measures by which Tungsten monitors, measures, analyses and evaluates the effectiveness of the data protection. Sources of information that can drive continual improvement include:

☒ Post-incident reports ☒ Audit and nonconformity reports ☒ Exercise reports	☒ Suggestions from staff, managers, and Suggestions from staff, managers, and interested parties such as customers, partners, suppliers, local community, emergency services, regulators
--	--

(3c) Measures for timely restoring availability in case of a physical or technical incident Article 32 Paragraph 1 Point c GDPR:

Tungsten has implemented measures for restoring availability in case of a physical or technical incident. These measures include, but are not limited to:

- | | |
|--|---|
| ☒ Information security events, weaknesses and personal data breaches are reported in line with Tungsten security procedure | ☒ Information security weaknesses and events are reported immediately after they are seen or experienced. |
|--|---|

(3d) Measures to restore personal data in case of failure (availability control by Business Continuity Management):

Tungsten has implemented measures, to ensure that personal data is protected against accidental destruction or loss. These measures include, but are not limited to:

- | | |
|--|--|
| ☒ Uninterruptible power supplies (UPS)
☒ Devices for monitoring temperature and humidity in server rooms
☒ Fire and smoke detection systems
☒ Alarm when unauthorized entry to server rooms is detected
☒ Testing of data recovery
☒ Secure off-site storage of data backups
☒ In flood areas, server rooms are above the water border | ☒ Air conditioning in server rooms
☒ Protection power strips in server rooms
☒ Fire extinguishers in server rooms
☒ Creation of a backup & recovery concept
☒ Preparation of an emergency response plan
☒ Server rooms not located under sanitary installations |
|--|--|

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

(4a) Measures for regular testing, assessing and evaluating Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR:

Tungsten has implemented measures for regular testing, assessing and evaluating of the effectiveness of technical and organizational measures. Business owner identifies

processes that require monitoring and measurement, according to the following conditions:

- | | |
|---|--|
| ☒ The process produces results or by-products that can be quantitatively measured | ☒ The process generates error reports or other evidence of non-conformance |
| ☒ Regular review by implemented Data Protection Management and Incident Response Management | |

(4b) Order or Contract Control

Tungsten has implemented measures to prevent third party data processing other than upon instruction from the controller.

- | | |
|--|---|
| ☒ Clear and unambiguous contractual arrangements | ☒ Formalized order management |
| ☒ Third party sign confidentiality clauses | |

(4c) Measures for **safe software development** :

Tungsten's Secure Software Development Lifecycle process consists of a series of product activities designed to address various aspects of security as it relates to the software development process. These activities apply to all phases of the development process, from Planning through Design and Implementation phases, and finally through Quality Assurance, Release and Maintenance. The high level activities include:

- Training
- Threat Modelling
- Static Application Security Testing: use of Veracode or other tools
- Dynamic Application Security Testing: use of BurpSuite, Acunetix, Zap, etc.
- Penetration Testing: by an independent party

For Cloud Services, Tungsten has implemented measures, to ensure safe software development. Tungsten uses the SOC 2 attestation process in evaluating our systems. The SOC 2 framework includes five key sections, forming a set of criteria called the Trust Services Principles. These include:

- The security of the service provider's system
- The processing integrity of this system
- The availability of this system
- The privacy of personal information that the service provider collects, retains, uses, discloses and disposes of for user entities
- The confidentiality of the information that the service provider's system processes or maintains for user entities

The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost.

☒ Core Security Training

☒ Establish Security Requirements

☒ Implementation Practices

(4d) Results of a penetration test (Cloud services):

Security assessment is an important part of application development and deployment. Tungsten conducts regular penetration testing performed by independent third party to improve security controls and processes annually. Pentest test results are assessed for risk and are remediated accordingly.

Prior to penetration test, Tungsten needs to inform our hosting vendor. Per our hosting service provider's policy for customers to carry out authorized penetration testing on their applications hosted in Cloud server. Because such testing can be indistinguishable from a real attack, it is critical that customers conduct penetration testing only after obtaining approval in advance from our hosting service provider's Customer Support. Penetration testing must be conducted in accordance with the terms and conditions of our hosting server. Requests for penetration testing should be submitted with a minimum of 7-day advanced notice.

Annex 3 to Data Processing Addendum

List of Subprocessors

Tungsten (formerly Kofax) may use other Affiliates and third parties to provide certain parts of the Service on Customer's behalf. Any such Sub-processors will be permitted to process Personal Data only to deliver the services Tungsten has retained them to provide, and they are prohibited from using the Personal Data for any other purpose. These parties or their subsidiaries may provide services to one or more services offered under the Agreement.

1. 3rd party Sub-processors

1.1 3rd party Sub-processors for Subscription Services and related Services

Sub-processor	Location	Function
Microsoft (Azure)	Ireland	Hosting Service Provider for most Subscription Services
Google Cloud (formerly Actifio)	UK, USA	Cloud Data Management
Amazon (AWS)	USA	Hosting Service Provider for Subscription Services
Cloudfare, Inc.	USA	Content distribution, security, abuse prevention
Salesforce, Inc.	USA	Sales/Tech Support Communication
Zoho Corp.	USA	Sales/Tech Support Communication - limited data Processing

2. Tungsten Affiliates

Tungsten Entity*	Location	Function
Tungsten Automation Australia Pty Ltd	Australia	Technical or Management Support
Tungsten Automation Austria GmbH	Austria	Technical or Management Support
Tungsten Automation Benelux NV/SA	Belgium	Technical or Management Support
Kofax Produtos de Imagem DO Brasil Ltda.	Brazil	Technical or Management Support
Tungsten Automation EOOD	Bulgaria	Technical or Management Support
Tungsten Automation Development A/S	Denmark	Technical Support, R&D
Tungsten Automation Finland Oy	Finland	Technical or Management Support
Tungsten Automation France S.A.S.	France	Technical or Management Support
Tungsten Automation Deutschland GmbH	Germany	Technical Support, R&D (AP Essentials, SoftPro, AIA, TIS etc.)
Tungsten Automation Ten GmbH	Germany	Technical or Management Support
Tungsten Deutschland Technologies GmbH	Germany	Technical Support, R&D (AP Essentials, SoftPro, etc.)
Tungsten Development GmbH	Germany	Technical Support, R&D
Tungsten Development Private Limited	India	Technical Support, R&D
Tungsten Automation Ireland Ltd	Ireland	Technical Support
Top Image Systems Ltd	Israel	Technical or Management Support

Tungsten Automation Italia S.R.L.	Italy	Technical or Management Support
Tungsten Automation Japan Co., Ltd.	Japan	Technical or Management Support
Tungsten Automation Malaysia Sdn. Bhd.	Malaysia	Technical or Management Support
Tungsten Automation Ten Sdn Bhd	Malaysia	Technical or Management Support
Tungsten Automation SAPIde CV	Mexico	Technical or Management Support
Tungsten Montenegro d.o.o. Podgorica	Montenegro	Technical or Management Support etc.
Tungsten Automation Benelux NV/SA, Dutch branch	The Netherlands	Technical or Management Support
Tungsten Automation Netherlands BV	The Netherlands	Technical or Management Support
Tungsten Automation Norway AS	Norway	Technical or Management Support
TNGSTN Portugal, S.A.	Portugal	Technical or Management Support
Tungsten Automation Singapore Pte. Ltd.	Singapore	Technical or Management Support
Tungsten Automation South Africa Ltd.	South Africa	Technical or Management Support
Tungsten Automation Ibérica S.A.U.	Spain	Technical or Management Support)
Tungsten Automation Schweiz AG	Switzerland	Technical or Management Support
Tungsten Automation ME FZE Ltd	UAE	Technical or Management Support
Tungsten Automation England Limited	UK	Technical Support, R&D (Tungsten)
Tungsten Automation UK Ltd	UK	Technical or Management Support
Tungsten Automation Corporation	USA	Tungsten HQ, R&D
Tungsten Vietnam Development Co., Ltd.	Vietnam	Technical Support, R&D

*We are in the process of rebranding from Kofax to Tungsten Automation. Part of this process is a corresponding change of name of our Affiliates, so that further changes of name may take place in the near future. Such changes of name will not affect other company details or registrations.

Annex 4 to Data Processing Addendum

(Country-Specific Amendments to the EU Standard Contractual Clauses)

UK

In respect of any Personal Data to which UK GDPR was applicable prior to export, and which is exported to a Third Country where no adequate level of data protection exists according to an adequacy decision or regulation of the Secretary of State in the UK:

Tungsten and its Affiliates and third party Subprocessors shall execute and adhere to the UK Standard Contractual Clauses, with Module Three selected in table 2, as appended to the EU Standard Contractual Clauses.

"UK Standard Contractual Clauses" shall mean the International Data Transfer Addendum to the EU Standard Contractual Clauses, issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022.

Switzerland

Where a transfer to third countries is subject to the Swiss DPA, the EU Standard Contractual Clauses as applicable according to Section 4 shall apply with the following amendments (these amendments shall not affect the application of the EU Standard Contractual Clauses for the purposes of the GDPR or other Data Protection Laws):

- Clause 8.8(i) of Modules Two and Three is replaced with: "the onward transfer is to a country that has been the subject of an adequacy assessment by the Swiss Federal Data Protection and Information Commissioner ("FDPIC") or the Swiss Federal Council (as the case may be) that covers the onward transfer";
- References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are to be interpreted as references to the Swiss DPA to the extent applicable;
- References to "Regulation (EU) 2018/1725" are removed;
- References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" shall be interpreted to mean Switzerland;
- Clause 13 (a) and Part C of Annex I are not used;
- The "competent supervisory authority" and "supervisory authority" are both replaced with the FDPIC insofar as the relevant transfers are governed by the Swiss DPA;

- In Clause 16(e), subsection (i) is replaced with: "the FDPIC adopts its own standard contractual clauses pursuant to Article 16(2)(d) of the Swiss Federal Act on Data Protection and the Swiss Ordinance on the Federal Data Protection Act, as amended from time to time ("Swiss DPA"), applicable as of 1 September 2023, that cover the transfer of personal data to which these clauses apply";
- Clause 17 is replaced with: "These Clauses are governed by the laws of Switzerland insofar as the relevant transfers are governed by the Swiss DPA.";
- Clause 18 is replaced with: "Any dispute arising from these Clauses relating to the Swiss DPA shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The parties agree to submit themselves to the jurisdiction of such courts.";
- As long as the Swiss DPA of 19 June 1992 is in force, the EU Standard Contractual Clauses shall also protect Personal Data of legal entities and legal entities shall receive the same protection under the EU Standard Contractual Clauses as natural persons.