Data Processing Agreement

This Data Processing Agreement ("**DPA**") is made and entered into by and between

(1) Tempo Software Inc., a company incorporated under the laws of the Commonwealth of Massachusetts, having its principal place of business at 10 Mall Road Suite 301, Burlington, MA 01803, USA, and its Affiliates (as defined below) (hereinafter "**Tempo**"), and

(2) The Company (hereinafter "**Customer**") identified in the signature block and/or in the Customer License Agreement (CLA) and/or the End User License Agreement ("**EULA**") (each is a "**Service Agreement**").

Together the "**Parties**" and each a "**Party**".

The Parties agree as follows:

1. Subject matter of this DPA

1.1. This DPA applies to the Processing by Tempo of Customer's Personal Data under Data Protection Law (as defined below).

1.2. If relevant, this DPA is incorporated into and forms part of the Service Agreement, under which Tempo provides certain services ("**Services**").

1.3. The Parties agree that this DPA shall replace any existing DPA the Parties may have previously entered into in connection with the Services.

1.4. In the event of a conflict between this DPA and the Service Agreement, this DPA shall control in respect of data protection.

2. Definitions

2.1. All capitalized terms not defined in this DPA shall have the meanings set forth in the Service Agreement.

2.2. **"Data Protection Law"** means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data, including without limitation (i) 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, and repealing Directive

95/46/EC (General Data Protection Regulation) ("**GDPR**" or "**EU GDPR**") and any applicable national implementations of the GDPR; (ii) the Privacy and Electronic Communications (EC Directive) Regulations 2003; (iii) the Swiss Federal Act on Data Protection of 19 June 1992 ("**FADP**"); (iv) the California Consumer Privacy Act of 2018 ("**CCPA**"); and (v) the GDPR as amended and incorporated into UK Law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act ("**UK GDPR**") and the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

2.3. The terms "**Processing**", "**Personal Data**", "**Controller**", "**Processor**", "**Personal Data Breach**" and "**Supervisory Authority**", "**Commission**", "**Member State**" (or equivalent terms used in applicable Data Protection Law) shall have the meanings given to them under applicable Data Protection Law and shall be interpreted accordingly.

2.4. "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

2.5. "**Standard Contractual Clauses**" mean the EU SCCs and the UK SCCs.

2.6. "**EU SCCs**" mean the standard contractual clauses approved by the European Commission in Commission Decision 2021/914, dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).

2.7. "**UK SCCs**" mean the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner (as amended and updated from time to time).

2.8. "**Revised FADP**" means the FADP revised as of 25 September 2020.

3. Roles and Responsibilities

3.1. Customer

3.1.1. Customer is a Controller. Customer will comply with any applicable Data Protection Law obligations with respect to the processing of Personal Data. Customer will not instruct Tempo to process any Personal Data in a manner that would constitute a breach of the Data Protection Law.

3.1.2. Customer warrants that Customer has all the necessary rights to provide the Personal Data to Tempo for the Processing to be performed in relation to the Services. To the extent required by the Data Protection Law, Customer is responsible for ensuring that any necessary data subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Should a consent be revoked by the data subject, Customer is responsible for communicating the fact of such revocation to Tempo, and Tempo remains responsible for implementing any Customer instruction with respect to the further processing of that Personal Data.

3.2. Tempo

3.2.1. Tempo is a Processor. Tempo will comply with any applicable Data Protection Law obligations with respect to the processing of Personal Data.

3.2.2. Tempo shall process Personal Data as described in Exhibit 1 to this DPA. Tempo shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements of this DPA.

3.3. Instructions

3.3.1. Tempo will process Customer's Personal Data:

(a) as described in Customer's written instructions as set forth in the Service Agreement and in this DPA,
(b) as agreed upon in writing by the Parties and to the extent that the processing is appropriate for the provision of the Services, or
(c) if required to comply with a legal obligation to which Tempo is subject. In such a case, Tempo shall notify Customer of that legal obligation before processing unless that legal obligation explicitly prohibits the furnishing of such information to Customer.

4. Confidentiality

Tempo personnel authorized to process Personal Data shall be subject to appropriate obligations of confidentiality. Tempo shall take reasonable steps to: (a) ensure that access is limited to those individuals who need to know and/or access the relevant Personal Data for the purposes of the Services; and (b) ensure that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality and have received appropriate training regarding the Processing of Personal Data.

5. Security

5.1. Tempo will take any security measures required by Data Protection Law.

5.2. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, without prejudice to any other security standards agreed upon by the Parties, Tempo shall maintain at least the following technical and organizational measures in Exhibit 1 to this DPA.

5.3. In assessing the appropriate level of security, Tempo shall take into account the particular risks that are presented by processing, for example, from accidental or unlawful destruction, loss, alteration, unauthorized or unlawful storage, processing, or access or disclosure of Personal Data (i.e. Personal Data Breach).

6. Subprocessing

6.1. Customer authorizes the engagement of Tempo's Affiliates as subprocessors. Customer also authorizes the continued use of those subprocessors already engaged by Tempo as of the date of this DPA.

6.2. Information about subprocessors, including their functions and locations, is available upon request to legal@tempo.io.

6.3. Customer generally authorizes the engagement of subprocessors in connection with the provision of the Services. Tempo will enter into a written agreement with all subprocessors containing obligations that are equivalent to those applicable to Tempo in this DPA.

6.3.1. Tempo shall provide at least 30 calendar days prior notice to Customer of any change to its subprocessors and provide Customer with an opportunity to object to the change. Customer shall notify Tempo within 15 calendar days of receipt of the notice if it has reasonable concerns that the subprocessor will not meet the requirements of the Data Protection Law and the grounds for such concerns in order to permit Tempo to re-evaluate any such subprocessors based on the applicable concerns and Tempo may choose to:

(a) not engage the subprocessor, or

(b) if Customer objects to a subprocessor, the Parties shall come together in good faith to discuss a resolution to the objection. If the Parties cannot resolve the objection within 15 days, then Customer may terminate those Services which cannot be provided by Tempo without the use of the objected-to new subprocessor by providing written notice to Tempo.

6.4. In case an authorized subprocessor fails to fulfill its data protection obligations under such written agreement with Tempo, Tempo will remain fully liable to Customer for the performance of the authorized subprocessor's obligations under such agreement.

7. International Data Transfers

7.1. Customer agrees that Tempo may transfer Personal Data processed under this DPA outside the European Economic Area (the "EEA"), the UK, or Switzerland as necessary to provide the Services. This includes locations where Tempo or any of its subprocessors maintain facilities. Customer acknowledges that Tempo's primary processing facilities are located in the United States, however Customer is able pin the data residency of the utilized application to the EU (Germany) at any time. Additionally, some of the Customer's Personal Data may be transferred to the United States for minor processing activities essential to the Services, such as notification delivery, customer support, etc. Such transfers will be conducted in compliance with applicable Data Protection Law to ensure an adequate level of data protection.

7.2. To the extent Customer transfers to Tempo any Personal Data that is subject to Data Protection Law, and the transfer is to a country that is deemed to not provide an adequate level of protection, Customer and Tempo hereby agree to the Standard Contractual Clauses as set forth below:

7.2.1. Transfers of Personal Data subject to the EU GDPR. The Parties agree that transfers of Personal Data subject to the EU GDPR are made pursuant to the EU SCCs and choose Module 2 of the EU SCC with the following specifications:

(a) Annexes I and II are located at Exhibit 1 of this DPA;

(b) the "data exporter" and the "data importer" are the Parties identified in Annex I.A;

(c) Clause 7, the optional docking clause will not apply;

(d) with respect to Clause 9, Option 2 will apply, and the time period for the above-mentioned option shall be as set out in Section 6.3.1. of this DPA. Annex III shall not apply;

(e) in Clause 11, the optional clause will not apply;

(f) in Clause 17, the Parties agree on the laws of Iceland; and

(g) in Clause 18 (b), the Parties agree that any dispute arising from the EU SCCs shall be resolved by the courts of Iceland.

If the EU SCCs are applicable to the Parties, each party is deemed to have executed the EU SCCs by executing this DPA.

7.2.2. Transfers of Personal Data subject to Swiss FADP or Revised FADP. The Parties agree that transfers of Personal Data subject to the Swiss FADP or Revised FADP are made pursuant to the EU SCCs with the following modifications:

(a) the terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted as references to the Swiss FADP with respect to data transfers subject to the FADP;

(b) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss FADP;

(c) references to Regulation (EU) 2018/1725 shall be removed;

(d) references to "EU", "Union" and "Member State" shall be replaced with references to "Switzerland";

(e) Clause 13(a) and Part C of Annex II are not used, and the "competent supervisory authority" shall be the Swiss Federal Data Protection Information Commissioner;

(f) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland";

(g) in Clause 17, the Standard Contractual Clauses shall be governed by the laws of Switzerland;

(h) to the extent the Swiss FADP applies to the processing, Clause 18 shall be replaced to state: "Any dispute arising from these Clauses shall be resolved by the competent courts of Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts"; and

(i) the terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

If the Swiss FADP or Revised FADP is applicable to the Parties, each party is deemed to have executed the EU SCCs by executing this DPA.

7.2.3. Transfers of Personal Data subject to the UK GDPR and UK Data Protection Act 2018. The Parties agree that transfers of Personal Data subject to the UK GDPR and UK Data Protection Act 2018 are made pursuant to the UK SCCs with the following modifications:

(a) in Table 1 of the UK SCCs, the parties' details and key contact information is in Annex I.A to the EU SCCs in Exhibit 1 to this DPA;

(b) in Table 2 of the UK SCCs, information about the version of the Approved EU SCCs, modules, and selected clauses which these UK SCCs are appended to is in 7.2.1 of this DPA;

(c) in Table 3 of the UK SCCs:

(i) the list of Parties is in Annex I.A to the EU SCCs in Exhibit 1 to this DPA;

(ii) the description of the transfer is set forth in Annex I.B to the EU SCCs in Exhibit 1 to this DPA;

(iii) Annex II is in Annex II to the EU SCCs in Exhibit 1 to this DPA;

(iv) the list of subprocessors, including their functions and locations, is available upon request to legal@tempo.io.

(d) in Table 4 of the UK SCCs, both the importer and the exporter may end the UK SCCs in accordance with the terms of the UK SCCs.

7.3. To the extent that a Party relies on a basis for international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Parties agree to cooperate in good faith to promptly terminate the transfer and to pursue an alternate mechanism that can lawfully support the transfer.

7.4. Nothing in this DPA is intended to alter or have any adverse effect on the Standard Contractual Clauses. In the event of a contradiction between the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

8. Data Subject Rights

8.1. Taking into account the nature of the processing, Tempo shall use reasonable efforts to assist Customer by appropriate technical and organizational measures, insofar as this is possible, so that Customer can respond to data subject requests. Tempo shall provide reasonable and timely assistance to Customer in responding to Data Subjects requests. If otherwise is not provided under the Data Protection Law, the performance and cost of such requests shall be in accordance with the Service Agreement and Tempo's then-current price list.

8.2. If Tempo receives a data subject request, Tempo will forward it to Customer without undue delay. Responsibility for responding to a data subject request shall remain with Customer. Contact details associated with the SEN are considered as a Customer's primary contact.

9. Cooperation

9.1. If requested and to the extent required under applicable Data Protection Law, Tempo will (considering the nature of processing and the information available to Tempo) provide reasonable assistance to Customer so Customer can comply with its obligations under the Data Protection Law, in particular, to carry out data protection impact assessments or prior consultations with a Supervisory Authority as required by Data Protection Law.

9.2. Tempo shall make available to Customer upon request any reasonable information to demonstrate compliance with Tempo's obligations under Data Protection Law to the extent Customer does not otherwise have access to the relevant information and such information is available to Tempo.

9.3. If Tempo believes that the request under this section exceeds what would be reasonable, Tempo may charge Customer based on Tempo's then-current price list at any given time.

10. Audit

10.1. Where requested, Tempo will permit Customer to audit Tempo solely to the extent required to demonstrate compliance with its obligations under this DPA provided that (unless expressly required by any competent authority or a Personal Data Breach):

10.1.1. To the extent the audit scope is covered in any audit carried out for Tempo by an independent third-party auditor or Tempo's own internal audit function within 12 months prior to Customer's audit request and there have been no material changes to the controls audited, Tempo may share the report to the extent relevant to Customer and the disclosure of the report shall be deemed to satisfy the audit request made by Customer.

10.1.2. Where, after review of Tempo's earlier audit report and acting reasonably, a specific audit request is requested by Customer, the Parties shall agree on the date, location and scope of any such audit, and such audit shall be conducted during regular business hours, subject to Tempo's policies and may not unreasonably interfere with Tempo's business activities. Customer will reimburse date, location and scope of any such audit for reasonable costs and expenses undertaken by Tempo in assisting with the audit;

10.1.3. The audit, any audit materials and the audit report shall be confidential, and Customer will share a copy of the audit report with Tempo; and

10.1.4. Customer may not conduct an audit more than once in any calendar year unless there has been a Personal Data breach or a request by a data protection supervisory authority.

11. Incident Management

11.1. Tempo shall notify Customer without undue delay (but no later than 72 hours) upon Tempo becoming aware of a Personal Data Breach affecting Customer's Personal Data under its control. Any notification made to Customer shall be addressed to the Customer contact details provided in Exhibit 1 to this DPA and shall be accompanied by all relevant information and documentation required under the Data Protection Law.

11.2. Tempo shall make reasonable efforts to identify the cause of the Personal Data Breach and take reasonable steps in order to remediate the cause of such a Personal Data Breach to the extent remediation is within Tempo's control. If Customer requests additional information or reasonable action/cooperation, then Tempo will reasonably provide it. If Customer requests additional remedial action, then Tempo will, at Customer's cost and expense, reasonably try to provide such action.

12. Deletion or Return of Personal Data

12.1. Upon termination of this DPA, upon Customer's written request, or upon fulfillment of all purposes agreed in the context of the Services whereby no further processing is required, Tempo shall, at the discretion of Customer, either delete or return Customer's Personal Data.

12.2. Tempo and its subprocessors may retain Personal Data to the extent required by a legal obligation and only to the extent and for such period as required by the legal obligation, or as part of their backups until those backups are deleted. After the termination of the Service Agreement Tempo and its subprocessors may retain Personal Data for up to three (3) months, except for Tempo Cost Tracker, for which Tempo stores it for one (1) year to provide Customer with an opportunity to access Personal Data within this period, if required. Personal Data, stored at the backups, will be deleted within the specified above period from the date of deletion of Personal Data from the production database. Personal Data stored after the Service Agreement expiration or termination is subject to compliance with the terms of the data protection and confidentiality obligations within the Service Agreement.

12.3. Any Personal Data archived on Tempo's backup systems will be securely isolated and protected from any further processing, except as otherwise required by applicable law or regulation.

13. CCPA Specific Terms

To the extent Tempo processes Personal Data protected by the California Consumer Privacy Act (CCPA), the following terms shall apply in addition to the terms of this DPA. In the event of any conflict between the CCPA Specific Terms and any other terms of this DPA, the applicable CCPA Specific Terms will take precedence, but only to the extent of the CCPA Specific Terms' applicability to Tempo.

13.1. Except as described otherwise, the definitions of: "controller" includes "Business"; "processor" includes "Service Provider"; "data subject" includes "Consumer"; "personal data" includes "Personal Information"; in each case as defined under CCPA.

13.2. For this section only, "Services" means the services and/or products provided by Tempo to Customer under the Service Agreement, including activities that are required, usual, or appropriate in performing the Services, including to (a) carry out the Services or the business of which the Services are a part, (b) carry out the benefits, rights and obligations relating to the Services, (c) maintain records relating to the Services, or (d) comply with any legal or self-regulatory obligations relating to the Services.

13.3. For this section only, "Permitted Purposes" shall include processing personal data only for the purposes described in this DPA and in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, as otherwise agreed in writing, including, without limitation, in the Service Agreement, or as otherwise may be permitted for "service providers" under the CCPA.

13.4. Tempo's obligations regarding data subject requests, as described in Section 8 (Data Subject Rights) of this DPA, apply to Consumer's rights under the CCPA. Tempo shall promptly notify Customer of any verified request received by the Tempo from a data subject or authorized representative enforcing available rights in respect of the personal data of the data subject. Tempo shall direct such data subject or authorized representative to contact Customer.

13.5. Notwithstanding any use restriction contained elsewhere in this DPA, Tempo shall process personal data only to perform the Services, for the Permitted Purposes and/or in accordance with Customer's documented lawful instructions, except where otherwise required by applicable law.

13.6. Tempo shall not sell any personal data to another business or third party without the prior written consent of Customer.

13.7. Where subprocessors process Customer's personal data, Tempo takes steps to ensure that such subprocessors are Service Providers under the CCPA with whom Tempo has entered into a written contract that includes terms substantially similar to this DPA or are otherwise exempt from the CCPA's definition of "sale".

13.8. Customer is responsible for complying with the CCPA in connection with the collection, use and storage of personal data and will ensure that it obtains all necessary consents, and provides all necessary notices, for the lawful processing of personal data by the Tempo in accordance with the Service Agreement.

14. Limitation of Liability

14.1. This DPA does not affect either party's liability to data subjects under applicable Data Protection Law.

14.2. Tempo's liability to Customer for any kind of loss or damage arising out of or in connection with this DPA shall be subject to the limitation of liability provisions in the Service Agreement. Any liability incurred under this DPA, such as regulatory fines, will be included in the calculation of Tempo's liability in the Service Agreement.

15. Termination

This DPA will remain in effect until the later of: (a) the termination or expiry of the Service Agreement, or (b) Tempo ceases to process Customer's Personal Data.

16. General Terms

16.1. The terms of the Service Agreement shall apply to this DPA.

16.2. This DPA has been pre-signed on behalf of Tempo. To enter into this DPA, Customer must: (a) be a customer of the Services; (b) complete the signature block below by signing and providing all relevant information, as well as contact information in Annex I.A to the EU SCCs in Exhibit 1 to this DPA; and (c) submit the completed and signed DPA to Tempo.

16.3. If Customer makes any deletions or other revisions to this DPA, this DPA will be deemed null and void.

16.4. Customer signatory represents to Tempo that he or she has the legal authority to bind Customer and is lawfully able to enter into this DPA.

The Parties' authorized signatories have duly executed this DPA below:

Customer: __________________	**Tempo Software Inc.**
Signature:	Signature: Gregg Clevenger
Name:	Name: Gregg Clevenger
Title:	Title: Chief Financial Officer
Date:	Date: 06/04/2024
Address:	Address: 10 Mall Road Suite 301, Burlington, MA 01803, USA

Exhibit 1

Annex I to the EU SCCs

A. List of Parties

Data exporter:

The data exporter is the legal entity specified as “Customer” in the DPA.

Activities relevant to the data transferred under these Clauses: Please see Annex I.B below, which describes the processing operations.

Role (controller/processor): Controller

Contact information for the data protection officer/compliance officer of Customer:

____

____

____

____

Data importer:

Name: Tempo Software Inc.

Activities relevant to the data transferred under these Clauses: Please see Annex I.B below, which describes the processing operations.

Role (controller/processor): Processor

Contact information for the data protection officer/compliance officer of Tempo:

Data Protection Officer
Tempo Software Inc.
10 Mall Road Suite 301, Burlington, MA 01803, USA
legal@tempo.io

B. Description of Transfer

Categories of data subjects whose personal data is transferred

Employees, contractors, and agents of Customer.

Categories of personal data transferred

- Anonymized User ID;
- Jira authentication token;
- Worklogs (work schedule/hours worked/sick leaves);
- Any other Personal Data submitted by, sent to, or received by employees, contractors, and agents of Customer through the Services, including but not limited to, in:
  - open text field for comments;
  - Jira issue information (project/issue ID, key, name, issue type, URL to an issue, description, summary, etc.);
  - support request/case.

Sensitive data transferred and applied restrictions or safeguards

The parties do not anticipate the transfer of sensitive data.

The frequency of the transfer

Ongoing basis for cloud products and services, one-off basis for support requests and other bespoke customer submissions.

Nature of the processing

Tempo will process the Personal Data submitted to, stored on, or sent through the products and services.

Purpose(s) of the data transfer and further processing

Tempo’s provision of Services to Customer, and related technical support.

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

The Personal Data will be processed in connection with the Services for the duration of the Service Agreement, or such shorter period where the processing is no longer authorized, and in respect of any post-termination processing activities permitted by the Customer. Subject to the "Deletion or Return of Personal Data" section of this DPA, Tempo and its subprocessors may retain Personal Data to the extent required by a legal obligation and only to the extent and for such period as required by the legal obligation, or as part of their backups until those backups are deleted. Tempo may retain Personal Data for up to three (3) months, except for Tempo Cost Tracker, for which Tempo stores it for one (1) year after the Service Agreement termination to provide Customer with an opportunity to access Personal Data within this period, if required. Personal Data, stored at the backups, will be deleted within the specified above period from the date of deletion of Personal Data from the production database. Personal Data stored after the Service Agreement expiration or termination is subject to compliance with the terms of the data protection and confidentiality obligations within the Service Agreement. Any Personal Data archived on Tempo's backup systems will be securely isolated and protected from any further processing, except as otherwise required by applicable law or regulation.

C. Competent Supervisory Authority

The competent supervisory authority, in accordance with Clause 13 of the EU SCCs, must be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to the processing of personal data to which the UK GDPR applies, the competent supervisory authority is the UK Information Commissioner's Office. With respect to the processing of personal data to which the Swiss law applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

Annex II to the EU SCCs

Technical and Organisational Measures

TEMPO shall implement appropriate technical and organizational measures to protect against the unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. These measures are to be maintained and reviewed regularly by TEMPO as necessary to keep such measures up-to-date, efficient, and appropriate with respect to the sensitivity of the Personal Data for all our customers.

Access control to premises and facilities

Measures must be taken to prevent unauthorized physical access to premises and facilities holding personal data. Measures shall include:

- Access control system with access cards.
- Video surveillance.
- Intrusion detection alarms.
- Fire alarms system.
- Logging of facility exits/entries.

Access control to systems

Measures must be taken to prevent unauthorized access to IT systems. The following technical and organizational measures for user identification and authentication must include:

- Password policy implemented.
- No access for guest users or anonymous access.
- Central management of system access.
- Access to IT systems subject to approval from HR management and IT system owner.

Access control to data

Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights and the unauthorized modification or disclosure data. These measures shall include:

- Differentiated access rights.
- Access rights defined according to duties.
- Automated log of user access to IT systems.
- Number of administrators kept to the minimum necessary.
- Measures to prevent the use of automated data-processing systems by unauthorized persons using data communication equipment (incl. encryption data “in-transit”, “at rest”, encrypted backups, private networks, network segregation, networking rules, privileged access management).
- Confidential or highly confidential paper documents are locked away securely or disposed of properly.

Input control

Measures must be put in place to ensure all data management and maintenance is logged, and audit trail of whether data have been entered, changed or removed and by whom must be maintained.

Disclosure control

In order to prevent unauthorized access, alteration, or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures must include:

- Encryption using a VPN for remote access, transport and communication data.
- The electronic transfer of data and transmission of personal data is carried out with state-of-the-art encryption methods.
- Transmission of data in anonymized or pseudonymized form.
- Logging of access and retrieval.

Separate processing control

Data collected for different purposes shall be processed separately. Different customers' data shall not be processed together. These measures shall include:

- Separation between server operation and application development.
- Multi-client applications used where relevant: different customers' data is stored in different databases;
- Control via user permissions model.
- Specification of database rights.

Pseudonymization

Where personal data is pseudonymized, it is processed in such a way that no data may be matched to a specific data subject without additional information. Where pseudonymization is used, additional information for attributing the personal data to a specific data subject is kept separately in separate and secure systems. There is an internal requirement to anonymize/pseudonymize personal data as far as possible where the data is to be transmitted or the statutory time limit for deletion of data expires.

Availability control

Measures should be put in place to ensure that data are protected against accidental destruction or loss. These measures must include:

- Ensuring that installed systems may, in case of interruption, be restored.
- Ensuring systems are functioning, and that faults are reported.
- Ensure stored personal data cannot be corrupted by means of a malfunctioning of the system.
- Remote storage.
- An emergency plan is in place, including backup processes and decentralized data storage. There are defined availability periods.
- Backups are regularly available as agreed; a backup and recovery plan are in place.
- Monitoring of the backup process.

- Business continuity procedures.

Risk Management

Tempo will assess risks related to processing of Personal Data and create an action plan to mitigate identified risks.

Human Resources Security

Tempo informs its personnel about relevant security procedures and their respective roles. Tempo also informs its personnel of possible consequences of breaching the security rules and procedures. Tempo will only use anonymous data in training.

Workstation protection

Tempo will implement protections on end-user devices and monitor those devices to be in compliance with the security standard requiring hard drive passwords, screen saver, antivirus software, firewall software, unauthenticated file sharing, hard disk encryption and appropriate patch levels. Controls are implemented to detect and remediate workstation compliance deviations.

Tempo will securely sanitize physical media intended for reuse prior to such reuse and will destroy physical media not intended for reuse.

Information Security Incident Management

Tempo will maintain an incident response plan and follow documented incident response policies including data breach notification to Data Controller without undue delay where a breach is known or reasonably suspected to affect Client Personal Data.