DATA PROCESSING AGREEMENT (DPA)

TECHNIA SaaS Agreement

(version: 2023.1.1)

This DPA supersedes and replaces any and all previous agreements between the Parties in regard to the Processing of Company Personal Data for TECHNIA SaaS solutions. In the event of contradictions between the terms and conditions of this DPA and the Agreement, the Parties shall primarily apply the terms and conditions of this DPA for the processing of Company Personal Data. It governs the rights and obligations of the parties concerning the requirements of Article 28 of the General Data Protection Regulation (GDPR) during the commissioned processing of data.

In the course of providing the Services to the Controller pursuant to this DPA, Processor may process Personal Data on behalf of the Controller. Processor agrees to comply with the following provisions with respect to any Personal Data Processed for the Controller in connection with the provision of the Services. In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall have the meaning set forth in this DPA.

The provisions of this DPA shall apply as long as Processor processes personal data on behalf of Controller.

1. Purpose of this data processing agreement

a. This Data Processing Agreement is based on General Data Protection Regulation (GDPR) – Official Legal Text (gdpr-info.eu). The purpose of the Data Processing Agreement is to ensure that the Parties comply with the Applicable Data Protection Legislation.

b. In the event of conflict between the terms of the Agreement and the Data Processing Agreement, the terms of the Data Processing Agreement will take precedence regarding matters specifically related to the processing of personal data. In the event of any conflict between the Data Processing Agreement and its Appendices, the Appendices will take precedence.

2. Appendices

a. **APPENDIX A** of the Data Processing Agreement includes a detailed description of the processing that is to take place, as well as the purpose of processing, categories of personal data and data subjects. The Parties' designated privacy contact channels are specified in this appendix.

b. **APPENDIX B** of the Data Processing Agreement includes conditions for the use of Subprocessors, as well as a list of approved Subprocessors.

c. **APPENDIX C** of the Data Processing Agreement contains specific instructions for the processing of personal data under the Agreement, including security measures and the Data Controller's right of access to and audit of the Data Processor and any Subprocessors, as well as sector-specific provisions concerning the processing of personal data.

3. Definitions

a. **Applicable Data Protection Legislation.** The applicable versions of the EU's General Data Protection Regulation (2016/679) ("GDPR"), The Swedish Data Protection Act (2018:218) and other member states implementation of the GDPR with related regulations etc., and any other relevant legislation concerning the processing and protection of personal data, as specified in APPENDIX C.

b. **Agreement.** One or more agreements between the Data Controller and the Data Processor concerning the provision of services which entail the processing of personal data, as specified in section APPENDIX C. The Data Processing Agreement may apply to several underlying agreements.
c. **Subprocessor.** A company or person used by the Data Processor as a subcontractor for the processing of personal data under the Agreement.
d. **Affiliate** means an entity that directly or indirectly controls, is controlled by or is or under common control with the subject entity.
e. **TECHNIA** means TECHNIA AB, a Swedish company and any Affiliate thereof entering into an Agreement or Order Form with Company/Controller or otherwise provided services hereunder.

Article 4 of GDPR will apply to privacy policy terms not defined in this agreement.

4. Rights and obligations of the data controller

a. The Data Controller is responsible for the processing of personal data in accordance with the Applicable Data Protection Legislation. The Data Controller must specifically ensure that:

(i) the processing of personal data is for a specified and explicit purpose and is based on valid legal grounds
(ii) the data subjects have received the necessary information concerning the processing of the personal data
(iii) the Data Controller has carried out adequate risk assessments; and
(iv) the Data Processor has at all times, adequate instructions and information to fulfill its obligations under the Data Processing Agreement and the Applicable Data Protection Legislation.

5. Instructions from the data controller to the data processor

a. The Data Processor shall process the personal data in accordance with the Applicable Data Protection Legislation and the Data Controller’s documented instructions. If other processing is necessary to fulfill obligations to which the Data Processor is subject under applicable law, the Data Processor must notify the Data Controller to the extent this is permitted by law, cf. Article 28 (3) (a) of GDPR.
b. The Data Controller's instructions are stated in the Data Processing Agreement with Appendices. The Data Processor must notify the Data Controller immediately if the Data Processor believes the instructions conflict with the Applicable Data Protection Legislation, cf. Article 28 (3) (h) of GDPR.
c. The Data Processor must be notified in writing of any requested changes to the instructions in the Data Processing Agreement, and changes must be implemented by the Data Processor by the date agreed between the Parties. The Data Processor may require the Data Controller to pay documented costs accrued in connection with the implementation of such changes, or the proportional adjustment of the remuneration under the Agreement if the amended instructions entail additional costs for the Data Processor. The same applies to additional costs that accrue due to changes in the Applicable Data Protection Legislation which concern the activities of the Data Controller.

6. Confidentiality & duty of secrecy

a. The Data Processor must ensure that employees and other parties who have access to personal data are authorized to process personal data on behalf of the Data Processor. If such authorization expires or is withdrawn, access to the personal data must cease without undue delay.

b. The Data Processor shall only authorize persons who need access to the personal data in order to fulfill their obligations under the Agreement, the Data Processing Agreement and any other processing that is necessary to fulfill obligations to which the Data Processor is subject, in accordance with applicable law.
c. The Data Processor must ensure that persons authorized to process personal data on behalf of the Data Controller are subject to obligations of confidentiality either by agreement or applicable law. The obligations of confidentiality shall survive the duration of the Data Processing Agreement and/or employment relationship.
d. At the request of the Data Controller, the Data Processor shall document that the relevant persons are subject to said obligations of confidentiality.
e. Upon the expiry of the Data Processing Agreement, the Data Processor is required to discontinue all access to personal data that is processed under the agreement.

7. Assistance to the data controller

a. When requested, the Data Processor shall as reasonably requested assist the Data Controller with the fulfillment of the rights of the data subjects under Chapter III of the GDPR through appropriate technical or organizational measures. The obligation to assist the Data Controller solely applies insofar as this is possible and appropriate, taking into consideration the nature and extent of the processing of personal data under the Agreement.
b. Without undue delay, the Data Processor shall forward all inquiries that the Data Processor may receive from the data subject concerning the rights of said data subject under the Applicable Data Protection Legislation to the Data Controller. Such inquiries may only be answered by the Data Processor when this has been approved in writing by the Data Controller.
c. The Data Processor must assist the Data Controller as reasonably requested in ensuring compliance with the obligations pursuant to Articles 32-36 of GDPR, including providing assistance with personal data impact assessments and prior consultations with the Data Protection Authorities, in view of the nature and extent of the processing of personal data under the Agreement.
d. If the Data Processor, at the reasonable request of the Data Controller, provides assistance as described in above, and the assistance goes beyond what is necessary for the Data Processor to fulfill its own obligations under the Applicable Data Protection Legislation, the Data Processor will be reimbursed in accordance with the price provisions of the Agreement.

8. Security of processing

a. The Data Processor shall take all measures necessary under Article 32 of the Regulation, including planned, systematic, organizational and technical measures, ensuring adequate confidentiality, integrity, and availability of information in the processing of Personal Data. The technical and organizational measures ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Data Processor must, as a minimum, apply the measures specified in APPENDIX C.
b. The Data Processor shall carry out risk assessments to ensure that an appropriate security level is maintained at all times. The Data Processor must ensure regular testing, analysis and assessment of the security measures, in particular with regard to ensuring sustained confidentiality, integrity, availability and robustness in processing systems and services, and the ability to quickly restore the availability of personal data in the event of an incident.

c. The Data Processor must document the risk assessment and security measures, and make them available to the Data Controller on request, and also allow for the audits agreed between the Parties.

9. Notification of breach of personal data security

a. In case of a personal data breach, the Data Processor shall without undue delay, notify the Data Controller in writing of the breach, and in addition provide the assistance and information necessary for the Data Controller to be able to report the breach to the supervisory authorities in line with the Applicable Data Protection Legislation.
b. Notification must be given to the Data Controller's point of contact specified in the Data Processing Agreement, and must:

   (i) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories of and approximate number of personal data records concerned
   (ii) state the name and contact details of the data protection officer or other contact point from where more information can be obtained
   (iii) describe the likely consequences of the personal data breach; and
   (iv) describe the measures taken or proposed by the Data Processor to address the breach, including where appropriate, measures to mitigate possible adverse effects.

   If necessary, information may be given in phases without any further undue delay.

c. The Data Processor shall implement all necessary measures that may reasonably be required to rectify and avoid similar personal data breaches. As far as possible, the Data Processor must consult the Data Controller concerning the measures to be taken, including assessment of any measures proposed by the Data Controller.
d. The Data Controller is responsible for notifying the Data Protection Authority and the data subjects affected by the personal data breach. The Data Processor may not inform third parties of any breach of personal data security unless otherwise required under applicable law or in accordance with the express written instructions of the Data Controller.

10. Use of Subprocessor

a. The Data Processor may only use Subprocessors with the prior general or specific written authorization of the Data Controller. For an overview of approved Subprocessors, see APPENDIX B of the Data Processing Agreement. The Data Controller hereby grants the Data Processor with a general authorization to engage Subprocessors defined in APPENDIX B.
b. If a Data Processor engages a Subprocessor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in this Data Processing Agreement shall be imposed on the Subprocessor by way of written agreement.
c. The Data Processor may only engage Subprocessors who provide appropriate technical and organizational measures to ensure that the processing fulfills the requirements in accordance with the Applicable Data Protection Legislation. The Data Processor must use reasonable efforts to assess and verify that satisfactory measures have been taken by the Subprocessors. Upon request, the Data Processor must be able to submit reports from such assessments to the Data Controller.
d. The Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of Subprocessors, thereby giving the Data Controller the opportunity to object to such changes. Such objection shall be made in writing and within thirty (30) calendar days after the Data Processor has informed the Data Controller about the intended changes. If the Data Controller objects to changes in the use of

Subprocessors, the Data Controller may, as a sole remedy, terminate the Agreement (and therefore this Data Processing Agreement) pursuant to the SaaS SUBSCRIPTION AGREEMENT.

e. The Data Processor is obligated, on request, to disclose agreements with Subprocessors to the Data Controller. This solely applies to the parts of the agreement that are relevant to the processing of personal data, and subject to any statutory or regulatory limitations. Commercial terms and conditions are not required to be submitted.
f. Data Processor shall remain liable to the Data Controller for the performance of the Subprocessor's obligations aligned with section 10 in the SaaS SUBSCRIPTION AGREEMENT.

11. Transfer of personal data to countries outside of the EEA

a. Personal data may only be transferred to a country outside the EEA ('Third country') or to an international organization if the Data Controller has approved such transfer in writing and the terms in section below are fulfilled. Transfer includes, but is not limited to:

   (i) processing of personal data in data centers, etc. located in a Third Country, or by personnel located in a Third Country (by remote access)
   (ii) assigning the processing of personal data to a Subprocessor in a Third State; or
   (iii) disclosing the personal data to a Data Controller in a Third Country, or in an international organization.

b. The Data Processor may nonetheless transfer personal data if this is required by applicable law in the EEA area. In such cases, the Data Processor must notify the Data Controller, to the extent permitted by law.
c. Transfer to Third Countries or international organizations may only take place if there are the necessary guarantees of an adequate level of data protection in accordance with the Applicable Data Protection Legislation. Unless otherwise agreed between the Parties, such transfer may only take place on the following grounds:

   (i) a decision of the European Commission concerning an adequate level of protection in accordance with Article 45 of GDPR; or
   (ii) a Data Processing Agreement which incorporates standard personal data protection provisions as specified in Article 46 (2) (c) or (d) of the GDPR (EU model clauses); or
   (iii) binding corporate rules in accordance with Article 47 of GDPR.

d. Any approval by the Data Controller for the transfer of personal data to a Third Country or international organization must be stated in Section APPENDIX B of the Data Processing Agreement.

12. Audit

a. Upon reasonable request, the Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and this Data Processing Agreement.
b. The Data Processor shall upon prior reasonable notice allow and contribute to annual inspections and audits carried out by or on behalf of the Data Controller one time per calendar year. The Data Processor shall also allow and contribute to inspections conducted by relevant supervisory authorities.
c. If an audit reveals a breach in the obligations in the Applicable Data Protection Legislation or the Data Processing Agreement, the Data Processor must rectify the breach as soon as possible. The Data Controller may require the Data Processor to temporarily stop all or part of the processing activities until the breach has been rectified and approved by the Data Controller.

d. Each Party shall pay its own costs associated with an annual audit. If an audit reveals significant breaches of the obligations under the Applicable Data Protection Legislation or the Data Processing Agreement, the Data Processor shall pay for the Data Controller's reasonable costs accrued from the audit.

13. Erasure & return of information

a. Upon the expiry of this Data Processing Agreement, the Data Processor is obligated to return and erase all personal data processed on behalf of the Data Controller under the Data Processing Agreement, in accordance with the provisions of section APPENDIX C. This also applies to any back-up copies.
b. The Data Controller will determine how any return of personal data is to take place. The Data Controller may require return to take place in a structured and commonly used machine-readable format. The Data Controller will pay the Data Processor's documented costs associated with the return unless this is included in the remuneration under the Agreement.
c. If a shared infrastructure or back-up is used and direct erasure is not technically possible, the Data Processor must ensure that the personal data is made inaccessible until it has been overwritten.
d. The Data Processor must confirm in writing to the Data Controller that the data has been erased or made inaccessible, and shall, upon request document how this has taken place.
e. Further provisions concerning erasure and return are stated in APPENDIX C.

14. Breach & suspension order

a. In the event of breach of the Data Processing Agreement and/or Applicable Data Protection Legislation, the Data Controller and relevant supervisory authorities may order the Data Processor to cease all or part of the processing of the data effective immediately.
b. If the Data Processor fails to comply with its obligations pursuant to this Data Processing Agreement and/or Applicable Data Protection Legislation, this shall be deemed a breach of the Agreement, and the obligations, deadlines, sanctions and limitations of liability in the Agreement's regulation of the Supplier's breach will be applied.

15. Duration & expiry

a. The Data Processing Agreement will come into effect from the date it is signed by both Parties. The Data Processing Agreement shall apply for as long as the Data Processor processes personal data on behalf of the Data Controller. It shall also apply to any personal data held by the Data Processor or any of its Subprocessors after the expiry of the Agreement.
b. The rules concerning termination specified in the Agreement/s shall also apply to the Data Processing Agreement, to the extent this is applicable. The Data Processing Agreement may not be terminated if the Agreement/s is/are in effect, unless it is replaced by a new Data Processing Agreement.

16. Notifications

a. Notification under this Data Processing Agreement shall be submitted in writing to:

    (i) For Customer as Data Controller: As per contact details provided under the Agreement.
    (ii) For TECHNIA as Data Processor: Email to privacy@technia.com

17. Governing law & legal venue

a. The Data Processing Agreement is governed by Swedish law. Disputes will be resolved in accordance with the provisions of the Agreement, including any provisions concerning legal venue.

APPENDIX A

PROCESSING ACTIVITIES and DATA CLASSIFICATION

TECHNIA SaaS Agreement

1. Purpose & instructions

a. The Data Processor shall not process Personal Data beyond the requirements necessary for the Service to comply with the obligations under the Agreement without prior written agreement or written instructions from the Data Controller.

b. Categories of data subject whos personal data is processed in the Services:

(i) Customer’s authorized users, which may include Customer’s employees, contractors, collaborators, partners, stakeholders and/or customers of the Customer.

2. Data Stored & Processed

a. “Light My Way”

(i) The data stored and processed in the solution is:

a. Training Content (user guides)

i. instruction text (e.g. “click here”)
ii. html element selectors (e.g xpath “//div[contains(@class,'menu')]”)
iii. html element identifiers (e.g “li_ENCEBOMPowerViewCommand”)

b. Configurations (makes it possible to tie training content to app state)

i. html element selectors (e.g. xpath & css selectors)

c. Usage Data

i. Data generated in connection with client's access, use and configuration of the Services and data derived from it

(ii) Personal Data

a. User email (licensing/access)
b. User last use

b. "Widget Box”

(i) The data stored and processed in the solution is:

a. Widget definition

i. Configuration of UI components (e.g. table definitions, column headers and payload data keys to populate in cells)
ii. Plugin code used for custom logic such as calculated values of rendering

b. Usage data

i. Platform data passed in connection with client, used to identify the specific platform (e.g. tennant id, widget id)

(ii) Personal data

a. User email
b. User name (3DEXPERIENCE 3DPassport)
c. IP address
d. Last use date

c. “**TIF Cloud Integration**”

(i) The data stored and processed in the solution is:

a. Jobs Content

i. Jobs logs
ii. Inbound / Outbound REST request

b. Configurations

i. List of services
ii. Parameterizations of services
iii. Information to connect to the integrated applications

c. Usage Data

i. Data generated in connection with client's access

(ii) Personal Data

a. User email
b. User First Name / Last Name

d. “TIF Cloud SAP Connector”

(i) Same as “TIF Cloud Integration”

e. “3DXJira Connector”

(i) The data stored and processed in the solution is:

a. Configurations
b. Application configurations stored and processed in encrypted database.
c. Usage Data

i. Data generated in connection with client's access, use and configuration of the Services and data derived from it

d. Content

i. Data generated by end user events being processed and transferred to integrating system.
ii. Storing for audit purposes with purge policy to delete data after certain time.

(ii) Personal Data

a. User email (licensing/access)

Complimentary user information for support and security purposes

a. IP Address

3. Data Security Classification

a. “Light My Way”

(i) The nature of the data that is stored & processed in the services is considered low in sensitivity.
(ii) The data consists of user documentation holding configurations related to how the application works tied to training instructions.
(iii) There is also limited personal data stored such as email address, last login data and what part of the application is often used.

(iv) The overall effects of a breach would be minimal. Considering four standard type of data (public, personal, internal, confidential, and restricted), the data stored and processed by Services is defined as “internal”.

b. "Widget Box”

(i) The nature of the data that is stored and processed in the services is considered low in sensitivity

(ii) The data consists of widget/UI definitions (configurations)

(iii) There is also limited personal data stored such as email address, last login, and application domain is often used.

(iv) The overall effects of a breach would be minimal. Considering the standard type of data (public, personal, internal, confidential and restricted), the data stored and processed by Services is defined as internal

c. “**TIF Cloud Integration**”

(i) The nature of the data that is stored & processed in the services is considered low to high in sensitivity. It highly depends on the use case and mapping configuration. The data consists of integration configuration related to how the application works and fields content in the scope of the integration. There is also some limited personal data (see Privacy Policy & Security Statement) stored such as email address.

d. “TIF Cloud SAP Connector”

(i) Same as “TIF Cloud Integration”

e. “3DXJira Connector”

(i) The nature of the data that is stored & processed in the services is considered low to high in sensitivity. It highly depends on the use case and mapping configuration. The data consists of integration configuration related to how the application works and fields content in the scope of the integration. There is also some limited personal data (see Privacy Policy & Security Statement) stored such as email address.

4. User identification

a. **“Light My Way”**

(i) Users may be identified by a unique subscription key or their email address. Administrators are identified by a valid combination of username and password.

b. “**Widget Box”**

(i) Users may be identified by their username or their email address. Administrators are identified by a valid combination of username and password.

c. “**TIF Cloud Integration**”

(i) Users and Administrators are identified by a valid combination of email and password.

d. “TIF Cloud SAP Connector”

(ii) Same as “TIF Cloud Integration”

e. “3DXJira Connector”

(iii) Users will be identified by a unique Atlassian account id and their email address.

APPENDIX B

LIST OF SUBPROCESSORS

TECHNIA SaaS Agreement

1. Subprocessors

The Data Processor engage following Subprocessors who provide appropriate technical and organizational measures to ensure that the processing fulfills the requirements in the data processing agreement.

Company	Location	Processing region	Purpose
AWS (Amazon Web Services)	Stockholm, Sweden	EU, Sweden, Stockholm (eu-north-1)	Operations platform
AWS (Amazon Web Services)	Frankfurt, Germany	EU, Germany, Frankfurt (eu-central-1)	Operations platform

APPENDIX C

SECURITY STATEMENT

TECHNIA SaaS Agreement

1. Overview

TECHNIA has long experience with handling business critical information and data security for clients. As a supplier we are dedicated to give you a reliable and secure solution. We take the task of providing you with a safe solution very seriously and place great emphasis on ensuring that your content is always available and secure.

2. Security & instructions

a. The Data Processor shall take all measures necessary under Article 32 of the Regulation, including planned, systematic, organizational and technical measures, ensuring adequate confidentiality, integrity, and availability of information in the processing of Personal Data. These measures include:

(i) Protection relating to physical access and logical access
(ii) Multi-factor authentication for admin purposes
(iii) Daily backup and process for secure restore
(iv) Log of access

3. Encryption of data

All data traffic and credentials are encrypted using TLS (Transport Layer Security) to ensure that no unauthorized access to data.

4. Safety tests & security

Independent safety tests are done by expert communities to ensure against attacks such as cross site request forgery (CSRF), cross-site scripting (XSS), SQL injections among other on technical level. Security is a continuous focus and includes organizational awareness, standard tools, and competence.

5. AWS Cloud Hosting

AWS Cloud Services offers a rich service catalog and a dynamic allocation of resources. AWS is utilized to provide a stable and future proof operating environment for our applications and data.

All data as defined in section “Data Stored & Processed” is stored and operated on Amazon Web Services (AWS) platform and safeguarded by Cloud Security – Amazon Web Services (AWS).

a. The Operating Environment

AWS is used to ensure that all customer data stay located in Europe (Frankfurt or Stockholm).

b. Backup & Restore

(i) Backup service for the Solution running on AWS uses reliable storage with in-built security and high availability features. If in rare case needed your data can be recovered to a previous snapshot. We have the following standard backup:

a. Backup is performed daily
b. Backup is available for 7 days

(ii) Backup is taken daily with guaranteed response to restore in the event of hardware failure or data loss. Backup services are online and do not imply downtime for backup Access to backups is restricted only to authorized Backup Admins.

(iii) All infrastructure is represented as code and can quickly be rebuilt from scratch in case of a disastrous loss of data. Infrastructure code is located in a secure git repository. Infrastructure as code makes it easy to move the entire deployment of services to a different datacenter should the need arise.

6. Conclusion

The safety, performance and reliability of client's data is our first priority. If you have any questions about the Services and its safety, performance or reliability, send us an email to support@technia.com.