Team improver

GDPR – Data Processing Agreement

TEAMIMPROVER: STRICTLY CONFIDENTAIL

Contents

Overview

This Data Processing Agreement ("DPA") forms part of the Terms of Service available at https://teamorgchart.com/termsofservice or any other agreement between TeamImprover Ltd ("Processor") and the Customer ("Controller").

TeamImprover acts as the **Data Processor** for personal data processed through the TeamOrgChart service, while the Customer retains the role of the **Data Controller**.

This DPA is executed in compliance with applicable Data Protection Legislation, including the EU General Data Protection Regulation (EU GDPR) and the UK General Data Protection Regulation (UK GDPR).

Binding Nature and Execution of Agreement

1. This DPA constitutes a legally binding agreement between the Customer and TeamImprover Ltd.
2. The DPA is considered enforced when a Customer commences a subscription to the TeamOrgChart application.
3. This DPA can be executed as a standalone agreement or incorporated into another agreement, such as the Terms of Service.

Subject Matter and Duration of Processing

1. Subject Matter:

This DPA governs the processing of personal data necessary to provide the TeamOrgChart service.

2. Duration of Processing:

The processing will continue for the duration of the Controller's subscription to the TeamOrgChart service and will cease upon termination unless otherwise required by law.

3. Termination Conditions:

The agreement may be terminated if:

- The Customer ceases to use the TeamOrgChart service.
- Data processing obligations are no longer required under applicable laws.
- Either party breaches the terms outlined in this DPA.

Nature and Purpose of Data Processing

Nature of Processing:

Personal data is processed to provide organizational charting services, including but not limited to importing, displaying, and managing organizational data.

Purpose of Processing:

- To deliver the TeamOrgChart application service to the Customer.
- To improve the functionality of the TeamOrgChart application.

Categories of Data Subjects

The personal data processed relates to the following categories of data subjects:

- Users of the TeamOrgChart application (both web and mobile).

- Individuals represented in the organizational chart (e.g., employees, contractors).

Types of Personal Data

The types of personal data processed may include:

- Name
- Email address
- Job title
- Department
- Managerial relationships
- Location (e.g., country, city, or office)
- Other organizational metadata

Responsibilities of the Customer

As data controller, the customer shall:

1. Ensure that personal data shared with the Processor is collected and transferred lawfully.
2. Limit personal data to what is necessary for the agreed purposes.
3. Handle data subject rights requests unless explicitly delegated to the Processor.
4. Notify the TeamImprover of any changes to personal data or processing instructions.

Obligations of TeamImprover as the Data Processor

1. TeamImprover shall only use data provided to provide the TeamOrgChart application service

2. Use this DPA as part of the TeamOrgChart terms of service.

3. TeamImprover may engage sub-processors without requiring the Controller's prior written approval.

TeamImprover will only use GDPR-compliant sub-processors and commits to ensuring that each sub-processor is bound by terms that offer an equivalent level of data protection.

TeamImprover remains liable for the actions of its sub-processors and will notify the Customer of significant changes related to sub-processors.

4.TeamImprover Implements and maintains appropriate technical and organizational measures to ensure the security of personal data, including protecting against accidental or unlawful destruction or loss, alteration, unauthorized disclosure, or access. Measures include encryption, secure transmission, access controls, and backup/recovery procedures.

5. TeamImprover shall notify the Customer without undue delay upon becoming aware of a personal data breach. Assist the Customer in complying with obligations regarding data breaches, including reporting to the supervisory authority.

6. TeamImprover shall Inform the Controller immediately if any of the Controller’s instructions would lead to a breach of the UK GDPR or local data protection laws.

7. TeamImprover will comply with relevant UK GDPR accountability obligations, such as maintaining processing records and appointing a Data Protection Officer where necessary and cooperate with supervisory authorities (such as the ICO) to assist in the performance of their

duties.

8.TeamImprover will assist the Customer in meeting obligations under Articles 32-36 of the GDPR and UK GDPR and allow the Customer or its authorized representatives to conduct audits or inspections upon reasonable notice.

Audit shall be conducted during TeamImprover's business hours, shall not disrupt TeamImprover's operations and shall ensure the protection of the Customers', TeamImprover's and other Data Subjects' Personal Data.

TeamImprover and Customer shall mutually agree in advance on the date, scope, duration and security and confidentiality controls applicable to the audit. Customer acknowledges that the signing of a non-disclosure agreement may be required by the Customer prior to the conduction of the audit.

The Customer is not entitled to get access to data or information about the TeamImprover's other customers, cost information, quality control and contract management reports, or any other confidential data of TeamImprover that is not directly relevant for the agreed audit purposes.

International Data Transfers

TeamImprover shall ensure that any transfer of personal data outside the UK or EU complies with the UK GDPR and EU GDPR transfer provisions. Specifically:

Transfers will rely on Standard Contractual Clauses (SCCs) approved by the European Commission or the UK ICO, where applicable.

For UK transfers, the UK International Data Transfer Addendum to the EU SCCs will be utilized.

Transfers will occur to countries with an adequacy decision by the European Commission or the UK government.

Where it is stored at all, customer data is exclusively stored in the Microsoft Azure Cloud, Western Europe Region.

Data Retention and Deletion

1. TeamImprover will retain personal data only as long as necessary to fulfil the purposes outlined in this DPA.
2. Upon termination of the agreement, TeamImprover shall securely delete or return all personal data.

Data Breach Notification and Reporting

The TeamImprover shall notify the Customer of any personal data breach without undue delay, including:

1. A description of the breach.
2. The likely consequences of the breach.
3. Measures taken or proposed to address the breach.

Data Subject Access Requests

1. If a data subject contacts the TeamImprover directly with a request to exercise their rights (e.g., right to be forgotten, data correction), the TeamImprover shall promptly inform the Customer.
2. TeamImprover shall not respond to such requests without the prior written consent of the Customer, except to confirm receipt of the request.
3. TeamImprover will assist the Customer in responding to such requests in compliance with applicable data protection laws.

Termination Conditions

This DPA may be terminated by:

1. Agreement of both parties.
2. Breach of the terms by either party.
3. Expiration or termination of the Customer subscription to TeamOrgChart.

Annex 1 – Details of the Data Processing

Processing Details	Information
Subject Matter	Organizational charting services
Duration	Duration of service subscription
Nature	Importing, managing, and displaying organizational data
Purpose	Providing the TeamOrgChart service
Data Subjects	Users of TeamOrgChart and individuals represented within the organisational charts
Data Types	Name, job title, department, location, manager relationships

Annex 2 – Details of 3rd Party Subcontractors

Sub-Processor	Purpose	GDPR Compliance
Microsoft Azure	Cloud hosting, application, security services and storage	Microsoft GPDR Overview
Campaign Monitor	Trial and customer emails	Campaign Monitor GDPR FAQs
2CheckOut	Payment processing	2CheckOut GDPR Commitment
FreshDesk	Ticketing and support system	GDPR Statement

Appendix 1 – Technical and Organizational Measures

Access Control

Physical and Electronic Access Control

All data processing required for the TeamOrgChart application occurs within Microsoft Azure Data Centres. Microsoft is responsible for the management and control of physical access to the data centres, as detailed here: Microsoft Physical Security.

Access to the production resources is limited to a small set of administrative accounts with 2FA enabled. Access reviews are conducted periodically to ensure elevated privileges are only available where necessary, and all access activities are logged and monitored for auditing purposes.

Internal Access Control

No TeamImprover staff member, other than members of the support team, has access to any client data, including the meta-data defining the organizational chart or the people data representing individuals within an organizational chart. TeamImprover staff do not have access to the client's Azure Active Directory or SharePoint Online system.

The TeamOrgChart application is granted "Read-Only" access to the client's Azure Active Directory, ensuring that neither TeamImprover staff nor the application can change or delete data held within the client's Active Directory.

Isolation Control

TeamImprover provides several hosting options for clients:

- **Client Hosted**: TeamOrgChart installed on the client's Azure Subscription.
- **Private Managed**: TeamOrgChart installed on dedicated infrastructure but managed by TeamImprover.
- **Shared Infrastructure**: Client uses shared infrastructure managed by TeamImprover.

Regardless of the hosting option, TeamOrgChart partitions all client data on a unique ID ("Tenant ID") and segregates data throughout the system.

Pseudonymisation

Pseudonymisation strategies are used whenever possible.

For example Personal data is read from the client's Active Directory but is not stored within the TeamOrgChart application. The data can only be read by an individual with a valid account within the client's Active Directory. It is processed and transformed into the organizational chart, which is sent to the client user's web browser but is not stored in the TeamOrgChart application database.

Integrity

Data Transfer Control

TeamImprover does not transfer any organization chart data to any other third-party systems.

TeamImprover uses the official Microsoft libraries and Software Development Kits (SDK's) to authenticate and interact with Customer data.

Data processed and transmitted to a Customer is secured using SSL.

All data is encrypted at rest.

Data Entry Control

TeamOrgChart does not have the required permission to change personal data stored within the client's Active Directory (Entra ID).

Data modifications must be carried out at the "source," with changes flowing into TeamOrgChart. Only users with administrative privileges granted by the client can modify organizational chart meta-data.

Availability and Resilience

Availability Control

TeamOrgChart does not have the required permissions to change personal data within the client's Active Directory, ensuring that accidental or wilful destruction of data is not possible.

TeamImprover's Servers have anti-malware and virus protection installed and are located behind a firewall.

The TeamOrgChart application is monitored using Microsoft Azure security tools, providing real-

time information about availability, performance, and security.

Rapid Recovery

TeamImprover utilises the high-availability features within Microsoft Azure to provide TeamOrgChart.
Disaster Recovery (DR) plans are tested periodically to ensure minimal downtime during incidents.

info@teamimprover.com
+4420 3290 1133
teamimprover.com

company number: 77770066
VAT: GB 120 3384 58
Sanderum House, Oakley Road, Chinnor, Oxfordshire, OX39 4TW