[TIVIAN]

Technical and Organizational Measures

The purpose of this document is to provide an overview of the technical and organizational measures taken by Tivian to protect the personal data processed within the Tivian Group (hereinafter: Tivian).

Document owner: Dörthe Minde
Document version: 2.0
Confidentiality classification: Public
Publication date: January 2024

[TIVIAN]

Inhalt

1. INTRODUCTION

Tivian is an enterprise feedback management provider with customers worldwide who use Tivian's software products for data collection, analysis and business-critical information.

Personal data of Tivian's customers and respondents collected and processed as part of the feedback process will be processed in accordance with the customer contract, the respective data processing agreement concluded and the descriptions in this document.

1.1 Software as a service

Tivian makes its feedback management software platforms available to its customers as Software as a Service (SaaS), as described in this document.

In this document, the subsections "**Software platforms**" in the respective section explain how the protection of personal data is ensured by Tivian on the software side.

1.2 Tivian data centers

Tivian makes its software platforms available to its customers via external data centers. Data centers in Germany, the EU and/or the USA are deployed for this purpose. The specific location of the deployed data center depends on the agreement in the individual contract between the customer and Tivian.

In this document, the subsections "**Data Centers"** explain how the protection of personal data in Tivian's software is ensured in accordance with the standards implemented in the data centers.

1.2.1 Datagroup

Processing in software platforms in the data center in Frankfurt am Main/Germany - personal data of Tivian's customers as well as data of respondents collected and processed as part of the feedback process are hosted on external servers in the data center of DATAGROUP Bremen GmbH in Frankfurt am Main/Germany. DATAGROUP has been certified as follows:

- ISO/IEC 27001:2017 (certificate ID: DSC.936.02.2021, https://www.datagroup.de/wp-content/uploads/2023/03/Urkunde_ISO27001_DATAGROUP_20210226.pdf)
- ISO/IEC 20000-1:2018 (certificate ID: 12 410 44148/01 TMS, this certificate is available on request)

1.2.2 Amazon Web Services (AWS)

Processing in software platforms in data centers in Frankfurt am Main, Germany/EU - Personal data of Tivian's customers in Europe as well as respondent data collected and processed as part of the feedback process are hosted on external servers in the data center managed by AWS, basically in Frankfurt am Main, as well as - by agreement with the customer - in other locations in the European Union.

Processing in software platforms in data centers in the USA - If contractually agreed with the customer, personal data of Tivian's customers and respondents collected and processed as part of the feedback and communication process is hosted on external servers in the data center managed by AWS, basically in North Virginia, as well as in other locations in the USA.

AWS is in possession of various certificates and attestations.

- Precise details about existing certificates can be found in the information provided by AWS at https://aws.amazon.com/compliance/programs/.

1.2.3 Microsoft

Processing in software platforms in data centers in the EU - If contractually agreed, personal data of Tivian's customers and respondents collected and processed as part of the feedback process will be hosted on external servers in Microsoft-managed data centers within the EU.

Microsoft is in possession of various certificates and attestations.

- Precise details about existing certificates can be found in the information provided by Microsoft at https://servicetrust.microsoft.com/viewpage/ISOIEC.

- Microsoft Azure has security mechanisms to help manage and monitor Azure cloud services and Azure virtual machines. Microsoft provides up-to-date information online: https://docs.microsoft.com/azure/security/security-management-and-monitoring-overview

1.2.4 Operator of the data centers

The company	Address	Country

DATAGROUP Bremen GmbH	Mary-Somerville-Strasse 8 28359 Bremen	Germany
DATAGROUP Data Center GmbH	Hanauer Landstrasse 310 60314 Frankfurt am Main	Germany
Amazon Web Services, Inc.	410 Terry Avenue North Seattle WA 98109	USA
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855	Luxembourg
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521	Ireland

1.3 Tivian offices

Processing in Tivian's offices and systems - Personal data of Tivian employees, customers, visitors and suppliers is processed in accordance with Tivian's internal privacy policy.

In this document, the subsections "**Offices**" in the respective section show how the protection of personal data is ensured in Tivian's offices and systems.

Further information on the structure of the data storage process and contact information for the Tivian Group's data protection officer can be found in the Tivian Trust Center at https://www.tivian.com/de/trust-center

Name of the Tivian organization	**Addresses of the offices**	**Country**
Tivian XI GmbH	Christophstr. 15-17 50670 Cologne	Germany
Tivian Limited	2 Minster Court London EC3R 7BB	United Kingdom
Tivian, Inc.	31 Hudson Yards 11th Floor New York, NY 10001	USA
Tivian AS	Haakon VII's gate 2 0161 Oslo	Norway

1.4 Compliance with the General Data Protection Regulation (GDPR)

All entities that process personal data are obliged under Art. 32(1) of the EU General Data Protection Regulation (GDPR) to implement appropriate technical and organizational measures in order to ensure a level of protection of the rights and freedoms of natural persons adequate to the risk, 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.

This document describes how Tivian complies with its obligations to process personal data on behalf of its customers in accordance with the requirements of the GDPR for technical and organizational measures. The relevant requirements can be found in Art. 5, 17, 19, 24, 25, 28, 29, 32, 33, 35 and 39 of the GDPR.

The data centers themselves provide further information in various ways and formats.

1.4.1 Datagroup

Datagroup has implemented technical and organizational measures for the protection of personal data in accordance with Art. 32 (1) GDPR. Datagroup regularly reviews the technical and organizational measures in place to ensure that they correspond to the state of the art and the organizational capabilities. In this respect, Datagroup is permitted to implement alternative adequate measures. In doing so, it shall be ensured that the security level of the measures specified in this document is not undercut.

Datagroup provides access to documentation on data protection and information security processes on request.

1.4.2 AWS

AWS provides extensive information via the AWS website: https://aws.amazon.com/de/compliance/gdpr-center/

1.4.3 Microsoft

Microsoft Azure maintains an information security program (including the adoption and enforcement of internal policies and procedures) designed to help customers protect customer data against accidental or unlawful loss, access or disclosure. Furthermore, the implemented security program purposes identifying reasonably foreseeable and internal security risks and unauthorized access to the Azure network, and mitigating security risks, including through risk assessment and periodic testing. Microsoft provides extensive information via the Microsoft website: https://www.microsoft.com/trustcenter/privacy/privacy-overview

2. PHYSICAL ACCESS CONTROL

This section describes the measures taken by Tivian to prevent unauthorized persons from physically accessing the data processing systems used to process or use personal data.

2.1 Data centers

2.1.1 Data center in Frankfurt, Germany/ EU - AWS

2.1.1.1 Introduction

The BSI / ISO 27001 certification standards apply to the data center building. In addition a physical access authorization concept is implemented that can be viewed on site. A two-stage access system has been installed to control physical access to the high-security areas of the data center.

2.1.1.2 Employee access to the data center

Physical access may be granted at the request of the team leader and is subject to cross-checking by the management of the respective cloud provider. This physical access is set up on a corresponding transponder for the respective employee. According to the second stage of the data center's physical access concept, code locks shall be added for the data center administrator group "Knowledge". The physical access authorization lists are repeatedly reviewed during internal and external ISO27001 audits and updated if there are any changes to the physical access authorizations.

2.1.1.3 Third-party access to the data center

Third-party access must be requested by authorized cloud provider employees, who must also present valid business credentials for this access. This request is granted based on the principle of “least privilege”, i.e. employees must specify in the request to which level of the data center and for how long they require access. These requests are approved by authorized personnel. Access is withdrawn after the requested period has expired. Persons with a visitor badge must present it on arrival at the site and will be registered and accompanied by authorized personnel.

2.1.2 Data center in Frankfurt, Germany - Datagroup

The BSI / ISO 27001 certification standards apply to the data center building. A physical access authorization concept has been implement and can be viewed on site. In addition, a two-stage access system has been set up to control physical access to the high-security areas of the data center.

2.1.3 Data centers in the USA (generally in North Virginia) - AWS

2.1.3.1 Introduction

The ISO 27001 certification standards apply to the respective data center building.

Alarms are linked directly to local fire and police authorities. AWS data centers maintain 24x7x365 monitored CCTV coverage, with CCTV/DVRs supporting data retention for 90 days in accordance with PCI requirements. Sensitive equipment such as information processing equipment, including customer servers, are housed in secure sub-areas within the secure perimeter of each data center and are subject to additional controls. Two-factor authentication is required for access to all data center facilities. Electromechanical locks are controlled by biometric authentication (hand geometry or fingerprint scanner) and key card/ID card. Termination and role change control procedures are in place so that all physical or logical access rights are removed in a timely manner when access is no longer required or appropriate.

2.1.3.2 Employee access to the data center

Only authorized AWS personnel are granted access to the physical data centers. All employees who require access to a data center must first submit a request for access and provide valid business credentials. This request is granted based on the principle of “least privilege”, i.e. employees must specify in the request to which level of the data center and for how long they require

access. The request is checked and approved by authorized personnel. Access is withdrawn after the requested period has expired. Employees with access to a data center are restricted to certain areas by their authorizations.

2.1.3.3 Third-party access to the data center

Third-party access must be requested by authorized AWS employees, who must also provide valid business credentials for this access. This request is granted based on the principle of “least privilege”, i.e. visitors must specify in the request to which level of the data center and for how long they require access. These requests are approved by authorized personnel. Access is withdrawn after the requested period has expired. Persons with a visitor badge must present it on arrival at the site and will be registered and accompanied by authorized personnel.

2.1.4 Data centers in the EU (generally in the Netherlands and Ireland) - Microsoft

Microsoft designs, builds, and operates data centers to strictly control physical access to the areas where personal data is stored. Microsoft also designs, builds and operates the facilities that support Azure and strives to maintain up-to-date physical security.

Microsoft takes a layered approach to physical security to reduce the risk of unauthorized users gaining physical access to data and data center resources. Microsoft-managed data centers have comprehensive layers of protection: Access authorization at the facility perimeter, at the building perimeter, in the building and on the data center floor. Microsoft provides up-to-date information online under: https://docs.microsoft.com/azure/security/azure-physical-security#physical-security

2.2 Tivian offices

All Tivian offices adhere to the requirements of the IT governance guidelines, including the definition of security zones. No local servers are operated in any of the offices. The following sections describe specific elements for each office:

- Visitors must report to reception or to a member of staff with whom they have an appointment and will be accompanied by a member of staff in the building.
- The entrance doors are equipped with a digital locking system that can only be opened using employee key cards. The Office Manager has the list of activated keys that are used by the employees.

3. DATA ACCESS CONTROL

This section describes Tivian's measures, including identification and authentication, that are in place to prevent unauthorized persons from accessing and using data processing systems and removable media.

3.1 Data centers

3.1.1 Data center in Frankfurt, Germany/EU - AWS

The AWS network is electronically regulated and controlled access for employees, contractors and any other person required to provide the Services. AWS maintains access controls and policies to manage access to the AWS network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS maintains corrective actions and incident response plans to respond to potential security threats.

3.1.2 Data center in Frankfurt, Germany - Datagroup

User administration is realized via VPN. DATAGROUP has implemented a comprehensive authorization concept to grant authorized users access only to the systems and applications relevant to them. Access authorizations are assigned according to the need-to-know principle. This means that employees only have access to the data they need to know for their assigned tasks. Users are only provided with those applications that they need to complete the tasks entrusted to them. The applications are also only assigned the rights required to perform the task. Only the user rights required for the specific task are used on all IT systems. Access to system software is blocked for persons who are not administrators. The use of private data carriers is prohibited by the S2 security policy for employees and administrators. The disposal of data carriers (backup media and hard disks) is always carried out by qualified service providers as part of order processing in accordance with Art. 28 GDPR.

3.1.3 Data center in the USA (generally in North Virginia, USA) - AWS

AWS has placed a limited number of access points to the cloud in strategic locations to enable more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API endpoints and are used for secure access (HTTPS) that allows you to have a secure communication session with your storage or data processing instances within AWS. To support customers with FIPS140-2 requirements, the AWS Virtual Private Cloud (VPN) endpoints and TLS1.3 terminating load balancers are deployed in the AWS GovCloud (USA) using FIPS 140-2 Level 2 validated hardware.

In addition, AWS has implemented network devices to manage interface communications with Internet Service Providers (ISPs). AWS uses a redundant connection to more than one communication service at each Internet-connected point on the AWS network. Each of these connections has its own network devices. Further information can be found on the AWS website https://aws.amazon.com/de/security/.

3.1.4 Data centers in the EU (generally in the Netherlands and Ireland) - Microsoft

Microsoft's Azure Security has defined specific requirements for active monitoring. Service teams configure the tools for active monitoring in accordance with these requirements. Active monitoring tools include the Microsoft Monitoring Agent (MMA) and System Center Operations Manager. These tools are configured to provide real-time alerts to Azure security personnel in situations that require immediate action.

Microsoft provides up-to-date information under: https://docs.microsoft.com/azure/security/azure-infrastructure-monitoring

3.2 Tivian offices

All Tivian offices adhere to the requirements of the IT governance guideline.

3.2.1 Device encryption

All portable storage devices are fully encrypted (notebook hard disk and USB sticks).

3.2.2 Authentication

Authentication for the operating system and applications is carried out via individual user IDs and passwords. A separate password must be entered to access the hardware decryption. Employees are obliged to lock the workstation client when they leave the room ("clear screen"). They are also obliged to keep their passwords secret and not to pass them on to third parties, not even for support purposes. There are password regulations that are implemented technically (system configuration) and organizationally (password policy). According to these regulations, all passwords must meet the defined minimum requirements.

3.3 Software platforms

3.3.1 Password

The default setting is as follows: The password must be changed after the first login. After that, it expires every 90 days. The licensed software requires users to change their passwords when they log in after the expiration date. Account names are not case sensitive. In contrast, passwords are case sensitive.

DXI offers a wide range of password complexity settings:

- Password lengths are variable and are determined by the customer.
- Passwords must have at least 6 characters, but no more than 12 characters.
- Passwords must contain characters from at least two of the following four groups: Lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9) and other printable ASCII characters. Passwords must not contain spaces.
- Password expiry date, can be set from "one day" to "never expire" (forced password update, password validity check in days).
- Password repetition count, can be set from "do not count" to "the password must never be used again" (check the last x passwords to see if the password has already been used once).

Users are not allowed to use the same password if they have to change passwords when they first log in or after one month. To protect against brute force attacks, the system temporarily blocks access for 30 minutes after six incorrect entries. Passwords are not stored in plain text. Customers can only access the licensed software and authenticate themselves via user-specific accounts.

3.3.2 Rights and roles concept

Power users or administrator accounts are grouped into teams in the software platforms, which control access to functional rights (ACL) and content rights (objects). If rights/role concepts are to be adopted from external platforms, the concept must first be replicated in the software platforms. The rights situation can then be automatically mirrored via an API-controlled assignment to the teams in the software platforms.

3.3.3 Vulnerability management

Vulnerability scans are performed once a month for each server using the Nessus network and vulnerability scanner. The Nessus standard test set is used for these scans. A RIPS code analysis scan is used to check the vulnerability of the source code. Security controls can be implemented as follows:

- Tivian system administrators (the normal case).
- customer (at the customer's request and expense).
- external security companies (on behalf of a customer who also bears the costs).
- BSI/ISO auditors (during the certification process and when renewing certificates).

Any critical errors that occur are rectified immediately after the logs have been checked. Data carriers and confidential documents are stored by certified service providers and destroyed in compliance with data protection regulations once the respective purpose no longer applies. The application software records administrative access in logs. These logs contain information about the account, time, module, action and other parameters. A separate right is required to view the administration protocols. This right is assigned to specific roles. The standard storage period is 90 days.

4. LOGGING OF THE PROCESSING OF PERSONAL DATA

This section describes Tivian's measures for recording and documenting access to and processing of personal data on behalf of its customers.

4.1 Data centers

4.1.1 Data center in Frankfurt, Germany/EU - AWS

The data transfer is logged and the logs are continuously evaluated. Every removal of data carriers is also logged and the logs are evaluated. The logging and evaluation of the logs are carried out as part of the technical and organizational measures described here.

Scope of the Internet protocols: Metadata of the Internet traffic (IP address of the connected client, the domain accessed, the date, time and time zone from which the connection originated, the specific request from the client in plain text, the method used, the data requested, the protocol used, the URL accessed, the referrer, the HTTP status code returned with the request, the size of the data transferred, measured in bytes, operating system and version, client type, browser and version).

4.1.2 Data center in Frankfurt, Germany - Datagroup

There is a defined and documented change management process. This process ensures that necessary or desired changes to the IT infrastructure are carried out using a standardized and controlled procedure.

- The administrator's activities on a server are logged. The traceability of input processes is achieved through the restrictive assignment of access rights. By observing the minimum principle when assigning access rights, the number of people with access rights is kept as small as possible. It is ensured that users can only enter, change or delete data in accordance with the authorizations valid for them.
- DATAGROUP generally only enters personal data for a customer as part of user registration in the Active Directory. In addition, personal data may be accessed in the course of general administrative activities. Therefore, all activities performed are documented using an ITSM tool and corresponding tickets and can be traced.
- In principle, customer orders are received via defined interfaces and recorded by a ticket system. Further processing is documented for each individual ticket.
- In some cases, access to particularly sensitive data is logged. Depending on the type of protocol, the user ID, origin of the request (IP address), computer name, date and time are recorded
- In some cases, anonymized logs are evaluated on a random basis. If the evaluation gives rise to suspicions of data misuse, further appropriate steps are taken in consultation with the works council - if present - and the data protection officer.
- System activity is recorded via the event log of the operating system used. Log files are always saved in protected system directories and backed up in accordance with the applicable data backup concept.

4.1.3 Data centers in the USA (generally in North Virginia) - AWS

The same measures are applied here as in Frankfurt am Main Germany/EU - AWS.

4.1.4 Data center in the EU (generally in the Netherlands and Ireland) - Microsoft

The Azure and Azure SQL Database operations teams are jointly responsible for managing and operating the Azure production network. The teams use several tools to monitor system and application performance in the environment. They also use appropriate tools to monitor network devices, servers, services and application processes. To ensure the secure execution of services in the Azure environment, the operations teams implement multiple levels of monitoring, logging and reporting.

The Microsoft Monitoring Agent (MMA) primarily collects monitoring and diagnostic log information from many sources, including the Fabric Controller (FC) and the root operating system (OS), and writes it to log files. The agent then transfers a subset of the information in digest form to a preconfigured Azure Storage account. The standalone monitoring and diagnostic service reads various monitoring and diagnostic log data and summarizes the information. The monitoring and diagnostics service writes the information to an integrated log. Azure uses Azure Custom Security Monitoring, an extension of the Azure monitoring system. This has components that monitor, analyze and report security-related events at various points in the platform.

Microsoft provides up-to-date information under**:** https://learn.microsoft.com/de-de/azure/security/fundamentals/infrastructure-operations

4.2 Software platforms

Customer and Tivian activities are logged in the system. When processing personal data, the software keeps a login log and an admin log. The login log provides information about which user has logged in and when, including rejected attempts.

- Content of the login log: Account, IP address, access/error, error message, date.

The admin log provides a detailed log of the actions performed by users in the system.

- Content of the admin log: Entry ID, account, entry date, module name, action, execution time, functions.

These logs can be viewed directly in the software. A search and filter function is also provided. A description of the functionalities can be found in the corresponding chapters of the software manual.

5. TRANSMISSION CONTROL

This section describes the measures taken by Tivian to ensure that personal data cannot be read, copied, modified or deleted during electronic transmission, transportation or storage on data carriers and that the locations at which personal data is to be transmitted using data transmission devices are checked and specified.

5.1 Data centers

5.1.1 Data center in Frankfurt am Main, Germany/EU - AWS

5.1.1.1 Encryption of data during transmission ("encryption in transit")

Access to the databases at AWS is encrypted via SSH (Secure Shell) and VPN tunnels. All data lines to the Internet are redundant and designed as BGP (Border Gateway Protocol). The entire network infrastructure (firewalls, switches, etc.) is fully redundant. Firewalls and DMZ settings are defined by BSI/ISO standards. Any access by Tivian employees (especially from support or development) to customer data hosted by the data center for the purpose of administering the DXI surveys is done using TLS1.3 encryption (PCI compliance).

5.1.1.2 Encryption for data at rest ("encryption at rest")

All data in the Frankfurt data center at AWS is stored encrypted at rest.

AWS has written provisions on the use of data carriers, including the creation of copies of data carriers for use as backups. These are e.g:

- Only administrators are granted such access rights.
- Every removal of data carriers is logged.
- All data transmissions are logged and the logs are continuously analyzed.

5.1.2 Data center in Frankfurt am Main, Germany - Datagroup

DATAGROUP is ISO-27001-certified with its Frankfurt am Main location (data center) and thus also complies with the provisions of the GDPR. Further information can be found at https://www.datagroup.de/zertifizierungen-datagroup-stuttgart.

5.1.3 Data centers in the USA (generally in North Virginia) - AWS

The measures correspond to the measures in the data center Frankfurt am Main/Germany/EU - AWS.

5.1.4 Data centers in the EU (generally in the Netherlands and Ireland) - Microsoft

5.1.4.1 Encryption of data during transmission ("encryption in transit")

Microsoft Azure offers various procedures to protect data when transferring it between different storage locations.

Microsoft uses the Transport Layer Security protocol (TLS1.3) to protect data during transmission between the cloud services and customers. The Microsoft data centers use a TLS connection with client systems that connect to Azure services. TLS provides strong authentication, message privacy and integrity (enables detection of message tampering, interception and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

Perfect Forward Secrecy (PFS) protects connections between customers' client systems and Microsoft's cloud services using unique keys. The connections also use RSA-based encryption key lengths of 2,048 bits. This combination makes it more difficult to intercept and access data during transmission.

Microsoft provides up-to-date information under: https://docs.microsoft.com/azure/security/security-azure-encryption-overview.

5.1.4.2 Encryption for data at rest ("encryption at rest")

Data at rest includes information stored in any digital format in permanent storage on physical media. Media includes files on magnetic or optical media, archived data and backups. Microsoft also offers encryption to protect Azure SQL Database, Azure Cosmos DB and Azure Data Lake. For a detailed description of the encryption of data at rest in Azure, please refer to Azure data encryption of data at rest.

5.2 Software platforms

Data access to all software components of the software platforms is carried out using TLS1.3 encryption. The transfer of personal data is secured through the use of HTTPS/TLS1.3 encryption. For this purpose, Tivian offers a data transfer platform in projects. The type and scope of the transferred data (metadata) are logged. The logs resulting from this are evaluated regularly.

5.3 Tivian offices

The use of external mobile data carriers (e.g. USB sticks) is prohibited. The use of mobile storage media is only permitted for certain data with prior written consent. However, personal or security-relevant data does not belong to this category. All mobile workstations are fully encrypted. In addition, e-mail communication and access to documents is also always encrypted.

6. INPUT CONTROL

This section describes the measures taken by Tivian to ensure that it is always possible to check and determine whether and by whom personal data has been entered, changed or deleted in the data processing systems:

6.1 Data centers

6.1.1 Data center in Frankfurt, Germany/EU - AWS

The employees of the AWS data center who are responsible for remote maintenance measures can neither enter data into the data processing systems nor view, change or delete personal data of Tivian customers. Remote maintenance measures are logged by a firewall. The logs resulting from this are checked on a random basis (spot checks) and whenever this is justified by incidents.

6.1.2 Data center in Frankfurt, Germany - Datagroup

The employees of DATAGROUP's data center who are responsible for remote maintenance measures can neither enter data into the data processing systems nor view, change or delete personal data of Tivian customers. Remote maintenance measures are logged by a firewall. The following measures are taken:

- The traceability of input processes is achieved through the restrictive assignment of access rights. By adhering to the minimum principle when assigning access rights, the number of people with access rights is kept as small as possible. It is therefore ensured that users can only enter, change or delete data in accordance with the authorizations that apply to them.
- The administrator's activities on a server are always logged.
- DATAGROUP generally only enters personal data for a customer as part of user registration in the Active Directory. In addition, personal data may be accessed in the course of general administrative activities. Therefore, all activities carried out are documented using an ITSM tool and corresponding tickets and can be traced.
- In principle, customer orders are received via defined interfaces and recorded by a ticket system. Further processing is documented for each individual ticket.
- In some cases, access to particularly sensitive data is logged. Depending on the type of protocol, the user ID, origin of the request (IP address), computer name, date and time are recorded.
- In some cases, anonymized logs are evaluated on a random basis. If the evaluation gives rise to suspicions of data misuse, further appropriate steps shall be taken in consultation with the works council - if present - and the data protection officer.
- The system activity is recorded via the event log of the operating system used.
- Log files are always stored in protected system directories and backed up in accordance with the applicable data backup concept.

6.1.3 Data center in the USA (generally in North Virginia) - AWS

The employees of the AWS data center who are responsible for maintenance measures can neither enter data into the data processing systems nor view, change or delete personal data of Tivian customers. Remote maintenance measures are logged. The resulting logs are reviewed on a random basis (spot checks) and whenever justified by events.

6.1.4 Data centers in the EU (generally in the Netherlands and Ireland) - Microsoft

The employees of the Microsoft data center who are responsible for maintenance measures can neither enter data into the data processing systems nor view, change or delete personal data of Tivian customers. Remote maintenance measures are logged. The resulting logs are reviewed on a random basis (spot checks) and whenever justified by events.

Microsoft also employs a combination of preventive, defensive, and reactive controls, including the following mechanisms, to protect against unauthorized developer and administrative activity:

- strict access controls for sensitive data, including a requirement for multi-factor authentication
- combinations of controls that enhance independent detection of malicious activity
- multiple levels of monitoring, logging and reporting and

- just-in-time access to minimize the number of individuals who have persistent or ongoing administrative privileges.

6.2 Tivian offices

All Tivian offices adhere to the requirements of the IT governance guideline, including the definition of security zones.

All employees sign a confidentiality clause as an integral part of their employment contracts and thus undertake to maintain data secrecy, which protects customers even after termination or expiry of the employees' employment contracts. A ticket system in the support and administration area ensures that all tasks are completed correctly and on time. Tivian employees are supported by a directory service and may only access the data that is required for their work within the scope of their respective tasks and activities.

6.3 Software platforms

All changes to the version are documented. Usage is documented in relation to the respective account; the corresponding data is stored for a maximum of 90 days. When using the software platforms, files with personal data are stored version by version. The corresponding date, time and user are logged. User comments can be entered in a comment field that is not included in the document. Documents cannot be changed. Documents entered into the system can be password protected separately to restrict access.

7. ORDER CONTROL

7.1 Introduction

This section describes the measures taken by Tivian to ensure that personal data processed on behalf of a customer can only be processed in accordance with the customer's instructions.

The following measures have been implemented and are aimed at the efficient realization of the aforementioned purpose:

Organizational measures

- Prior inspection of the safety measures taken by the subcontractor and their documentation
- Checking and ensuring that the confidentiality, data protection and data security requirements agreed with customers are met by subcontractors.
- Conclusion of the necessary agreement on order processing (e.g. data processing agreement acc. to rt. 28 GDPR) or EU standard contractual clauses
- Instructions to subcontractors are documented in the form of e-mails or other electronic systems that offer an appropriate level of protection
- Selection of the service provider from a due diligence perspective
- Checking and documenting the security measures taken by the service provider
- Agreement of effective control rights vis-à-vis the subcontractor
- Clear contract design

Further technical measures

- Documented deletion of customer data, at the customer's request in accordance with BSI specifications
- Regular installation of updates for all operating systems and applications
- Operating system updates weekly
- Updates for internal Tivian applications monthly when available
- Regular installation of updates for customer-operated applications, unscheduled in the event of known security vulnerabilities
- Detailed monitoring of all server systems to detect faults

7.2 Data centers

Tivian has reviewed the respective security concepts of all data centers and concluded order processing contracts with all data center providers. Written data processing agreements in accordance with Art. 28 GDPR are in place with the data centers to ensure data protection.

At no time do the cloud providers Datagroup, Microsoft or AWS process any personal data other than hosting services without an explicit order. All employees are subject to non-disclosure agreements (NDAs).

7.3 Tivian offices

All Tivian employees are bound by Tivian's internal policies and receive regular training on the protection of personal data. The evaluation of content in order processing contracts or the customer's instructions for data processing are part of such training.

Tivian managers and Tivian employees who are in dialog with customers are obliged to ensure that instructions are given to the relevant personnel and followed.

7.4 Software platforms

If a customer's contractual relationship with one of Tivian's services is terminated or expired, their account will be deactivated immediately and will no longer be accessible to them. The information collected via the website will be deleted immediately.

8. CONFIDENTIALITY CONTROL

8.1 Data centers

The data centers responsible for the storage and technical operation of Tivian's data do not have access to the data. In addition, the operators of data centers do not have an account on Tivian's servers. Exceptions to this rule only apply to the creation of backups so that the backup software can save the data. The backups are securely stored and documented in encrypted form and are subject to strict access rules.

8.2 Tivian offices

Tivian offices ensure confidentiality through a variety of measures. These include visitor management, a room locking system, strong account management, clear workplace rules, encrypted devices, confidentiality agreements, sealed backup media and certified destruction of data carriers.

8.3 Software platforms

Tivian's software ensures confidentiality through a variety of measures. These include access through strong account management, the use of certified data centers, access control via a second factor, data backup and encrypted transport via the Internet.

9. INTEGRITY CONTROL

According to Art. 32(1) lit. b GDPR, appropriate technical and organizational measures must be taken to ensure the integrity of the systems and services and thus the integrity of the data.

9.1 Data centers

The data centers commissioned by Tivian guarantee integrity through a variety of measures. These include various national and international certifications, such as ISO 27001 or SOC, which maintain the integrity of all information processing systems and data as well as encrypted backup tapes and encrypted transport via the Internet.

9.2 Tivian offices

The Tivian offices ensure integrity through a variety of measures. These include the encryption of media, strong access controls and the use of encrypted communication: communication between end devices and the office cloud environment is generally encrypted, and the transmission path (WLAN of the office landlord) is also encrypted.

9.3 Software platforms

The integrity of Tivian's software is ensured by a variety of measures. This includes ensuring the integrity of the program modules themselves through (cryptographic) checksums/comparisons with reference lists, URL manipulation mechanisms, secure cookies, specific web service rights and logging, secure sandbox program extension LUA, continuous improvement of the current code base, file integrity checks, change audit log and input validation checks.

10. TRANSFER CONTROL

It is ensured that personal data cannot be read, copied, changed or removed without authorization during transmission, forwarding or storage on data carriers. Furthermore, it is always possible to check which persons or bodies have received personal data. The following measures have been implemented to ensure this:

- **Encryption of e-mail and e-mail attachments**

  E-mails are transmitted exclusively via an encrypted transport route (SSL/TLS 1.3).

- **Encryption of the storage medium of notebooks**

  The hard disks of Tivian employees' notebooks are encrypted with Microsoft Windows Bitlocker (256-bit Advanced Encryption Standard - AES 256) as standard.

- **Secure file transfer**

  If no other transfer method is available, files are transferred exclusively via SFTP (Secured File Transfer Protocol).

- **Secure data transport**

  Data transport within the corporate environment (Azure Active Directory) is exclusively encrypted (SSL).

- **Electronic signature**

  An electronic signature is data linked to electronic information that can be used to identify the signatory or signature creator and verify the integrity of the signed electronic information. Tivian uses DocuSign and Adobe Acrobat solutions for this purpose.

- **Secured WLAN (at least WPA2)**

  The protection systems of Tivian employees' notebooks do not allow unsecured connections. This also includes the WEP encryption method.

- **"Data loss prevention (DLP) system"**

  Tivian uses DLP for SharePoint, OneDrive and Exchange Online in its Microsoft cloud environment.

- **Regulation on handling mobile storage media (e.g. external hard disk, USB stick, SD card)**

  The internal company guidelines prohibit the transportation of data using any form of mobile storage media.

- **Logging of data transmission or data transport**

  Every TIVIAN employee who has access to customer data in production has their own user for VPN and user for the respective bastion host / SSH. This means that every access to customer data via the VPN service, the OS and the file system is logged. The responsible employees have their own account or certificate and user.

  AWS IAM or AAD SSO is used for cloud services. This means that access is also logged here. Every change in AWS is also monitored and logged using AWS Config.

  In our DXI software, every login/login attempt is also logged in the database. In addition, every interaction with the system is also stored in the database.

  Monitoring / logging allows you to see which endpoints have been accessed and how, and what data volumes are being transported.

- **Logging of read accesses**

  Every TIVIAN employee who has access to customer data has their own user for VPN and user for the respective bastion host / SSH. This means that every access via the VPN service, the OS and the file system is logged. AWS IAM or AAD SSO is used for cloud services. These accesses are logged too. In our DXI software, every login or login attempt is also logged in the database.

- **Logging the copying, modification or removal of data**

  Every TIVIAN employee who has access to customer data has their own user for VPN and user for the respective bastion host / SSH. Hense every access via the VPN service, the OS and the file system is logged.

- **Tunneled remote data connections (VPN = virtual private network)**

  Datagroup Datacenter Frankfurt: There is a VPN here too, which allows administrative access to legacy services that are currently still in the Datagroup and are used productively as well (Exasol, Tableau, Hurricane, Datavoyager Reporting).

  Administration of the cloud environments (Microsoft Azure and AWS): Administrative access to the AWS cloud environments is provided by special access servers ("bastion hosts") and/or via SSH tunnels.

11. AVAILABILITY

Art. 32 GDPR defines availability as a requirement to ensure the security of processing. This section describes the measures taken by Tivian to ensure that personal data is available and at the same time prevent it from being accidentally destroyed or lost.

11.1 Data centers

11.1.1 Data centers in Frankfurt, Germany/EU - AWS

AWS performs complete backups of the data on a daily basis. Thanks to this backup, operations can be resumed immediately in the event of an emergency. The data is copied in parallel to a separate backup system in a separate fire compartment. In addition, the data is copied to magnetic tapes, which are stored separately and securely. The data on these magnetic tapes is encrypted on a case-by-case basis. The data backup log files are checked daily.

AWS operations personnel provide continuous staffing around the clock, seven days a week, 365 days a year to detect incidents and manage their impact and resolution. The stability plans of the AWS services are reviewed regularly. AWS checks the availability of the customer solution from the perspective of network and hardware availability as well as the availability of support services. Regular checks are carried out. Processes and architectures are inspected regularly. AWS manages incidents using industry-standard diagnostic procedures to drive the resolution of business-critical incidents.

The following standards are guaranteed in the data centers:

- Air conditioning: Four independently operating air conditioning systems are installed.
- Fire protection: The computer rooms are equipped with a fire alarm system connected to the fire department and an argon fire extinguishing system.
- Power supply: An emergency power system (uninterruptible power supply) is installed.
- Redundancy is available for all systems.

The AWS Backup Process is a fully managed backup service that centralizes and automates data protection across AWS services using AWS Storage Gateways. Backup policies are centrally configured and resources for backup activity are constantly monitored. The AWS Backup is automated and consolidates backup tasks. The default schedule contains weekly full and daily differential backups with retention rates of eight weeks. This means that backups can be restored precisely for every day of the last eight weeks. Regular data recovery and data readability training is conducted as part of emergency drills. Every week, all backups are stored in a secure storage cabinet.

AWS Backup protects backups by encrypting data at rest and during transmission. AWS Backup is PCI, ISO and HIPAA compliant. Backup activity logs are available for compliance audits.

11.1.2 Data centers in Frankfurt, Germany - Datagroup

Datagroup carries out complete backups of the data on a daily basis. Thanks to this safety feature, operations can be restarted immediately in the event of an emergency. The data is copied in parallel to a separate backup system in a separate fire compartment. In addition, the data is copied to magnetic tapes, which are stored separately and securely. The data on these magnetic tapes is encrypted on a case-by-case basis. The data backup log files are checked daily.

Every week, all backups are stored in a secure storage cabinet. The backups for each day of the last eight weeks can be restored precisely. Regular training on data recovery and data readability is carried out as part of emergency drills.

The following standards are guaranteed in the data centers:

- Air conditioning: Four independently operating air conditioning systems are installed.
- Fire protection: The computer rooms are equipped with a fire alarm system connected to the fire department and an argon fire extinguishing system.
- Power supply: An emergency power system (uninterruptible power supply) is installed.
- Redundancy is available for all systems.
- Current written guidelines and/or work instructions are available.

11.1.3 Data centers in the USA (generally in North Virginia) - AWS

The AWS data centers are set up in clusters in different regions of the world. In the event of an outage, automatic processes move customer data traffic away from the affected areas. The core applications are provided in an N+1 configuration so that in the event of a data center failure, there is sufficient capacity to load balance the data traffic to the remaining locations.

In addition, AWS places instances and stores data within multiple geographic regions and across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically distributed within a typical city region and are located, for example, in areas with a lower risk of flooding (there are different flood zone categorizations depending on the region). In addition to a stand-alone uninterruptible power supply and on-site backup generators, all Availability Zones are fed via different power grids from independent power suppliers to minimize single points of failure. All Availability Zones are redundantly connected to multiple Tier 1 transit providers. AWS manages incidents using industry-standard diagnostic techniques to drive resolution of mission-critical incidents.

AWS operations personnel provide continuous staffing around the clock, seven days a week, 365 days a year to detect incidents and manage their impact and resolution. The stability plans of the AWS services are reviewed regularly. AWS considers the availability of the customer solution from the perspective of network and hardware availability as well as the availability of support services. Regular checks are carried out and processes and architectures are reviewed to ensure the best possible availability. This includes:

- documented policies that comply with the recommendations of standards such as ISO 27001 (including an information security policy);
- a formal capacity management process to ensure the availability of all resources required by the business, including bandwidth, data center capacity and utilities, inventory and labor, and employee skills;
- uninterruptible power supplies (UPS) to minimize the risk of short-term power failures and fluctuations;
- diesel generators to minimize the risk of long-term power outages and fluctuations;
- design of the roofs and exterior walls of the data center for high loads and extreme weather conditions, including light protection;
- temperature and humidity control systems in the storage area as well as fire detection and extinguishing systems and fire extinguishers.

The AWS Backup Process is a fully managed backup service that centralizes and automates data protection across AWS services using AWS Storage Gateways. Backup policies are centrally configured and resources for backup activity are constantly monitored. The AWS Backup is automated and consolidates backup tasks. The default schedule is weekly full and daily differential backups with retention rates of eight weeks.

AWS Backup protects backups by encrypting data at rest and during transmission. AWS Backup is PCI, ISO and HIPAA compliant. Backup activity logs are available for compliance audits.

11.1.4 Data centers in the EU (generally in the Netherlands and Ireland) - Microsoft

- Microsoft Azure offers reliable availability based on comprehensive redundancy using virtualization technologies. Microsoft Azure offers numerous levels of redundancy to ensure maximum availability of customer data.
- The Microsoft Cloud Infrastructure and Operations team ensures high availability and reliability, high efficiency and intelligent scalability for the Azure infrastructure, so that a more secure, private and trustworthy cloud can be guaranteed.
- Uninterruptible power supplies and huge battery banks ensure a continued energy supply in the event of short-term power failures. Emergency generators provide backup power during extended outages and planned maintenance. In the event of a natural disaster, the data center can use on-site fuel reserves.
- Stable, high-speed fiber networks connect data centers to other key hubs and Internet users. Server nodes host workloads closer to the user to reduce latency, provide geo-redundancy and increase the overall resilience of services. A team of technicians works around the clock to ensure that services are always available.
- Microsoft guarantees high availability through extended monitoring and response to incidents, service support as well as backup and fail-over functions. Geographically dispersed Microsoft operations centers operate 24 hours a day, 7 days a week, 365 days a year. The fiber network for content distribution connects data centers and edge nodes to ensure high performance and reliability.
- Azure SQL Server databases are backed up automatically (https://docs.microsoft.com/azure/sql-database/sql-database-automated-backups): Full database backups are created every 12 hours, transactional backups are created every 5-10 minutes.
- Microsoft provides up-to-date information online at: https://docs.microsoft.com/azure/security/azure-infrastructure-availability

11.2 Software platforms

The following backup strategy is used:

- A complete backup of the data is carried out daily on an independent backup system. This ensures that the contractor can resume operations immediately in the event of an emergency.
- The AWS service "AWS Backup" is used to secure backups.
- Backups can be restored precisely for each of the last 7 to 60 days, depending on how critical the system is.

12. RESILIENCE OF PROCESSING SYSTEMS AND SERVICES

Art. 32 GDPR defines the resilience of processing systems and services as a prerequisite for ensuring processing security. This section describes the measures taken by Tivian to ensure the resilience of processing systems and services.

12.1 Data centers

The data centers used by Tivian ensure reliability through a variety of measures (see section 11 above). These include:

- the use of scalable network components, resources that can be expanded without interrupting operations ("on the fly")
- fault-tolerant hardware components
- state-of-the-art network infrastructure
- provision of sufficiently qualified personnel and
- permanent monitoring of the operating status.

12.2 Tivian offices

The operational safety of Tivian's offices is ensured by a variety of measures. These include:

- the use of scalable technical components
- forward-looking demand planning
- the provision of sufficiently qualified personnel and
- permanent monitoring of the operating status.

12.3 Software platforms

Tivian's software platforms ensure reliability through a variety of measures. These include:

- the use of scalable databases
- modern programming technology

- agile development and
- the use of powerful software components.

13. SEPARATION

This section describes the measures taken by Tivian to ensure that data collected for different purposes is processed separately.

13.1 Software platforms

The following measures are taken, among others:

- Separation of personal data at different storage locations through organizational and spatial separation (multi-client capability)
- The data processing systems for particularly sensitive data are physically and organizationally separated
- Development, test and production systems are physically separated from each other and are subject to separate security restrictions
- Before personal data is transferred from productive to test environments, it is anonymized
- Separation of data by client / customer
- Creating an authorization concept

14. PSEUDONYMIZATION AND ENCRYPTION OF PERSONAL DATA

Art. 25(1) and Art. 32(1) lit. a GDPR require that personal data shall be processed pseudonymously and encrypted wherever possible. Art. 32 GDPR defines the pseudonymization and encryption of data as a prerequisite for the security of processing. This section describes the measures taken by Tivian to pseudonymize and encrypt data.

14.1 Data centers

Communication between the Tivian data centers and third parties takes place exclusively in encrypted form. In addition to customers, "third parties" also includes suppliers, processors and all other persons who process personal data when accessing all platforms. Technologies are used that meet the applicable legal requirements and correspond to the state of the art. All backups are stored in encrypted form.

14.2 Software platforms

Tivian's software platforms store passwords in encrypted form (hashed). The data is anonymized in the system using a script. All data fields (e.g. e-mail address, first name/last name) are replaced by generic information by means of overwriting by a script in the database.

15. STORAGE AND DELETION

This section describes the retention period for data, including personal data, processed by Tivian on behalf of its customers. The routines for deleting data are also defined.

15.1 Data centers

The data centers store the data for the duration of an existing contractual relationship between Tivian and its customers. After a customer contract ends, Tivian immediately terminates the customer installation and database.

15.2 Software platforms

15.2.1 Default setting: retention period for personal data defined by the customer

The Tivian software is made available to customers by Tivian so that they can create surveys and questionnaires. When creating a survey or questionnaire, the customer specifies the retention period for the data concerned. The data is automatically anonymized after the retention period has expired. The backups are deleted (overwritten) no later than 60 days after deletion of the original data. Deletion is carried out in accordance with Tivian's current deletion routines.

15.2.1 Optional setting: Retention period not defined by the customer

If the customer does not specify a retention period, the relevant data will be retained until manual deletion or until the termination of the contract between Tivian and the customer. The backups will be deleted (overwritten) no later than 60 days after the original data has been deleted. The deletion is carried out in accordance with Tivian's current deletion routines.

16. INCIDENT RESPONSE MANAGEMENT

Breach notification is a mandatory topic between Tivian and its customers. A data breach that poses a risk to the rights and freedoms of individuals will be handled in accordance with the applicable law. Notification of a breach must be made within 72

hours of becoming aware of the breach. Tivian will notify its customers, the data controllers, "without undue delay" after Tivian becomes aware of a data breach.

16.1 Recognition

In order to be able to recognize an attack or a security-relevant event, Tivian has set up various monitoring and control measures that alert in the event of an attack. In such a case, Tivian immediately initiates countermeasures to stop the respective attack before it can cause damage that results in a data breach.

Tivian's response framework provides the ability to quickly analyze what the attackers have accessed or copied. This contributes significantly to minimizing the potential impact on the customer and, above all, on the people affected.

16.2 Communication

In addition to the above-mentioned detection requirements, internal communication between the departments and groups concerned has also been agreed to ensure a smooth response to an incident or breach. A communication plan defines who is authorized to speak to external bodies and customers.

Tivian routinely tests the response program to ensure effectiveness and timely notification and to comply with regulatory requirements and deadlines.

16.3 Notification

To reduce the risk of not receiving complete or thorough feedback, Tivian has developed an incident response program, created policies and procedures, and ensured that everyone is aware of the program.

Tivian's data processing directory helps to know where an individual's data is stored so that the incident response team can quickly understand the potential impact of a security event on a system or application. Tivian's accurate data inventory is critical to assist with any customized breach notifications by pointing out which customer is affected as well as supporting the process for notifying the customer in the event of a breach. The subsequent communication with the customer will describe the nature of the breach and recommendations to mitigate any potential negative impact.

17. INTERNAL CONTROL

This section describes the measures implemented to ensure that internal policies, including the policies described in this document, are complied with by the organization. In addition, the process for regularly reviewing, assessing and evaluating the effectiveness of these technical and organizational measures is defined below.

17.1 Monitoring of the software platforms

The following measures are examples of the monitoring measures used by our software platforms:

- Alarms are issued around the clock
- Alarms are recorded immediately by Tivian's qualified technical staff
- The monitoring system has a redundant design and is monitored by an external monitoring tool
- Another monitoring system provides insights into the performance of the platforms from locations around the world.

17.2 Safety audits

Regular audits of the hosting environment are part of the ISO 27001 certification requirements to which the data centers used by Tivian are subject.

In addition to the data center audits, Tivian has undergone various ad hoc audits conducted by some of our customers who require verification for the highest security standards. Tivian also conducts regular self-audits.

17.3 Security check

In order to meet the high security requirements of its own software platforms, Tivian engages third-party security experts to carry out security tests for our platforms. The aim is to ensure continuous security in relation to current and upcoming technologies and constant, incremental development work.

The tests are carried out as application penetration tests with the following focal points:

- OWASP Top 10
- Cross-site scripting (XSS)
- Session fixation
- Weak or missing authentication
- Hidden parameters
- Searching directories

- SQL injection

In order to ensure the confidentiality, integrity and availability of our software platform in accordance with Art. 32 (1) lit. c and d, appropriate technical measures are carried out once or twice a year.

An infrastructure test of our hosting environment takes place every year.

17.4 Penetration tests

Tivian's systems are examined for vulnerabilities at regular intervals by an external service provider. The results of the regular and automated vulnerability scans are reviewed and processed by the IT security officer.

17.5 Results of the audits

- The results of application and infrastructure tests are presented to product management.
- Every critical vulnerability is sent to development for rectification.
- The operations department takes care of the infrastructure and the server environment.
- Problems in connection with the Tivian server environment are resolved by IT operations.
- Vulnerabilities in the commercial website www.tivian.com are fixed by developers who are responsible for the design of our front-end websites.

17.6 Risk analysis

A risk analysis is carried out regularly by the IT information security officer together with the IT managers in order to assess the current threat situation and derive measures for implementation.

17.7 Information security officer

Tivian has appointed an internal information security officer whose main tasks include the development, establishment and monitoring of an information security management system (ISMS).

17.8 Data Protection Officer

Tivian has appointed both an external Data Protection Officer and an internal Privacy Counsel, whose main tasks include the regular monitoring of processing activities, the implementation of data protection measures and ensuring compliance with the applicable data protection laws.

18. DATA PROTECTION-FRIENDLY DEFAULT SETTINGS (ART. 25 GDPR)

18.1 "Privacy by default"

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 data subjects associated with the processing, appropriate technical and organizational measures are implemented to safeguard the rights of data subjects. The following measures are taken, among others:

- No more personal data is collected than is necessary for the respective purpose.
- The simple exercise of the data subject's right of withdrawal is complied with by technical measures

18.2 "Privacy by design"

The following measures are taken, among others:

- When developing our software, care is taken to ensure that only the personal data that is actually required to fulfill the respective purpose is collected.