[TIVIAN]

TECHNISCHE & ORGANISATORISCHE MASSNAHMEN FÜR DEN DATENSCHUTZ

Ziel dieses Dokuments ist es, einen Überblick über die technischen und organisatorischen Maßnahmen von Tivian zum Schutz der in der Tivian Group (im Folgenden: Tivian) verarbeiteten personenbezogenen Daten zu geben.

Dokumentbesitzer: Eric M. Roßner
Dokumentversion: 1.72
Vertraulichkeitsklassifizierung: Öffentlich
Veröffentlichungsdatum: 03. August 2021

[TIVIAN]

Inhalt

1. EINFÜHRUNG

1.1 Software as a Service

Tivian bietet seinen Kunden Software as a Service an.

Tivian ist ein weltweit führender Anbieter im Bereich Enterprise Feedback Management mit Kunden weltweit, die seine Lösungen für die Datenerfassung und -analyse sowie für geschäftskritische Informationen einsetzen.

Tivian stellt seinen Kunden seine Softwareplattformen für das Feedbackmanagement als Software as a Service (SaaS) aus externen Rechenzentren zur Verfügung, wie in den Tivian Binding Corporate Rules für Prozessoren und in diesem Dokument beschrieben.

Personenbezogene Daten der Kunden von Tivian und der Befragten, die im Rahmen des Feedback-Prozesses erhoben und verarbeitet werden, werden in Übereinstimmung mit dem Tivian Group Code of Privacy, den Tivian Binding Corporate Rules und den Beschreibungen in diesem Dokument verarbeitet.

In diesem Dokument zeigen die Abschnitte "**Software**", wie der Schutz personenbezogener Daten in der Software von Tivian gewährleistet wird.

1.2 Tivian Rechenzentren

Tivian stellt seinen Kunden seine Softwareplattformen für das Feedbackmanagement als Software as a Service (SaaS) aus Rechenzentren in Deutschland und/oder den USA zur Verfügung, je nach individuellem Vertrag zwischen Kunde und Tivian.

In diesem Dokument zeigen die Abschnitte "**Rechenzentrum**", wie der Schutz personenbezogener Daten in der Software von Tivian in Übereinstimmung mit diesen in den **Datagroup**-, **Amazon**- und **Microsoft**-Rechenzentren implementierten Standards gewährleistet wird.

1.2.1 Datagroup

Verarbeitung in Softwareplattformen im Rechenzentrum in Frankfurt, Deutschland - personenbezogene Daten der Kunden von Tivian sowie im Rahmen des Feedbackprozesses gesammelte und verarbeitete Daten der Befragten werden auf externen Servern im Rechenzentrum der DATAGROUP Bremen GmbH an Standorten der DATAGROUP Data Center GmbH, Frankfurt am Main, gehostet. Die DATAGROUP wurde wie folgt zertifiziert:

- gemäß ISO/IEC 27001:2017 (Zertifikat-ID: DSC.936.02.2021, dieses Zertifikat ist auf Anfrage erhältlich)
- gemäß ISO/IEC 20000-1:2011 (Zertifikat-ID: 12 410 44148 TMS, dieses Zertifikat ist auf Anfrage erhältlich)

1.2.2 Amazon

Verarbeitung in Softwareplattformen im Rechenzentrum in Frankfurt, Deutschland - personenbezogene Daten der Kunden von Tivian in Europa sowie im Rahmen des Feedbackprozesses gesammelte und verarbeitete Daten der Befragten werden auf externen Servern im von Amazon kontrollierten Rechenzentrum in Frankfurt gehostet.

Verarbeitung in Softwareplattformen im Rechenzentrum in North Virginia, USA - falls mit dem Kunden vertraglich vereinbart, werden personenbezogene Daten der Kunden von Tivian und der Befragten, die im Rahmen des Feedback-Prozesses gesammelt und verarbeitet werden, auf externen Servern im von Amazon kontrollierten Rechenzentrum in USA gehostet.

Amazon ist im Besitz diverser Zertifikate und Testate.

- Genaue Details über bestehende Zertifikate lassen sich auf der von Amazon bereitgestellten Informations-Seiten unter https://aws.amazon.com/compliance/programs/ abrufen.

1.2.3 Microsoft

Verarbeitung in Softwareplattformen im Rechenzentrum in den Niederlanden und Irland – bei der Nutzung von QUBIE für MS Teams vertraglich vereinbart, werden personenbezogene Daten der Kunden von Tivian und der Befragten, die im Rahmen des Feedback-Prozesses gesammelt und verarbeitet werden, auf externen Servern im von Microsoft kontrollierten Rechenzentrum gehostet.

Microsoft ist im Besitz diverser Zertifikate und Testate.

- Genaue Details über bestehende Zertifikate lassen sich auf der von Microsoft bereitgestellten Informations-Seiten unter https://gallery.technet.microsoft.com/Overview-of-Azure-c1be3942 abrufen.

[TIVIAN]

1.2.4 Betreiber der Rechenzentren

Firma	Adresse	Land
DATAGROUP Bremen GmbH	Mary-Somerville-Straße 8 28359 Bremen	Deutschland
DATAGROUP Data Center GmbH	Hanauer Landstraße 310 60314 Frankfurt am Main	Deutschland
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 Geschäftsstellen

Verarbeitung in den Büros und Systemen von Tivian - Persönliche Daten von Mitarbeitern, Kunden, Besuchern und Lieferanten von Tivian werden gemäß den Tivian Binding Corporate Rules verarbeitet.

In diesem Dokument zeigen die Abschnitte "**Geschäftsstellen**", wie der Schutz personenbezogener Daten in den Büros und Systemen von Tivian gewährleistet wird.

Weitere Informationen zur Struktur des Datenspeicherungsprozesses sowie Kontaktinformationen zu den Datenschutzbeauftragten der Tivian Gruppe finden Sie in den Tivian Binding Corporate Rules und auf Tivian.com.

Name der Tivian Organisation	Adressen der Geschäftsstellen	Land
Tivian GmbH	Gustav-Heinemann-Ufer 72a 50968 Köln	Germany
Tivian Limited	7th Floor, 110 Cannon Street London EC4N 6EU	United Kingdom
Tivian, Inc.	575 Lexington Avenue, 14th floor / WeWorks, New York, NY 10022	New York, USA

1.4 Erfüllung der Datenschutzgrundverordnung (DSGVO)

Dieses Dokument beschreibt, wie Tivian seinen Verpflichtungen zur Verarbeitung personenbezogener Daten im Namen seiner Kunden gemäß den Anforderungen der DSGVO für technische und organisatorische Maßnahmen nachkommt. Die entsprechenden Anforderungen finden sich in den Artikeln 5, 17, 19, 24, 25, 28, 29, 32, 33, 35 und 39 der DSGVO.

Die in diesem Dokument beschriebenen technischen und organisatorischen Maßnahmen werden von Tivian unter Berücksichtigung des Stands der Technik, der Kosten der Umsetzung und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie des Risikos für die Rechte und Freiheiten natürlicher Personen dargelegt. Referenz Artikel 32 DSGVO.

Die Rechenzentren selbst stellen weiterführende Informationen in diversen Formaten zur Verfügung.

1.4.1 Datagroup

Alle Stellen, die personenbezogene Daten verarbeiten, sind gemäß Art.32 Abs.1 EU Datenschutzgrundverordnung (DSGVO) verpflichtet, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau für die Rechte und Freiheiten natürlicher Personen zu gewährleisten.

Datagroup setzt gemäß Art.32 Abs.1 DSGVO hierzu die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten um.

Datagroup überprüft die getroffenen technischen und organisatorischen Maßnahmen regelmäßig daraufhin, ob sie dem Stand der Technik und den organisatorischen Möglichkeiten entsprechen. Insoweit ist es Datagroup gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei ist gewährleistet, dass das Sicherheitsniveau der in diesem Dokument festgelegten Maßnahmen nicht unterschritten wird.

Datagroup ermöglicht auf Anfrage Einsicht in Dokumentationen zu Datenschutz- und Informationssicherheitsprozessen.

1.4.2 Amazon

Amazon stellt weitreichende Informationen zur Verfügung über die AWS Webseite.

https://aws.amazon.com/de/compliance/gdpr-center/

1.4.3 Microsoft

Microsoft Azure unterhält ein Informationssicherheitsprogramm (einschließlich der Annahme und Durchsetzung interner Richtlinien und Verfahren), das dem Kunden helfen soll, Kundendaten gegen versehentlichen oder unrechtmäßigen Verlust, Zugriff oder Offenlegung zu schützen, vernünftigerweise vorhersehbare und interne Sicherheitsrisiken und unbefugten Zugriff auf das Azure Netzwerk zu identifizieren und Sicherheitsrisiken zu minimieren, einschließlich durch Risikobewertung und regelmäßige Tests. Microsoft wird einen oder mehrere Mitarbeiter benennen, die das Informationssicherheitsprogramm koordinieren und dafür verantwortlich sind.

Microsoft stellt weitreichende Informationen zur Verfügung über die Microsoft Webseite.

https://www.microsoft.com/trustcenter/privacy/privacy-overview

2. ZUGANGSKONTROLLE

Dieser Abschnitt beschreibt die Maßnahmen von Tivian, mit denen verhindert werden soll, dass unbefugte Personen physisch auf die Datenverarbeitungssysteme zugreifen können, die zur Verarbeitung oder Nutzung personenbezogener Daten eingesetzt werden:

2.1 Rechenzentren

2.1.1 Rechenzentrum in Frankfurt, Deutschland

Für das Gebäude des Rechenzentrums gelten die Standards der BSI / ISO 27001 Zertifizierung:

Eine Alarmanlage, die mit der Polizei verbunden ist. Das Rechenzentrum befindet sich im zweiten Stock und verfügt über zwei separate Zugangskontrollmechanismen. Eine Videoüberwachung dient der Überwachung des Computerraums. Die Cloud Provider Amazon und DATAGROUP verfügen gemäß ISO27001 über ein physisches Zugangsberechtigungskonzept, das vor Ort einsehbar ist. Zur Steuerung des physischen Zugangs zu den Hochsicherheitsbereichen des Rechenzentrums wurde ein zweistufiges Zutrittssystem installiert.

Mitarbeiterzugang zum Rechenzentrum

Der physische Zugang erfolgt auf Antrag des Teamleiters und die Gegenkontrolle durch die Geschäftsführung der jeweiligen Cloud Provider. Dieser physische Zugang wird auf einem entsprechenden Transponder für den jeweiligen Mitarbeiter eingerichtet. In der zweiten Stufe des physischen Zugangskonzepts des Rechenzentrums werden Codeschlösser für die Rechenzentrumsadministratorengruppe "Wissen" hinzugefügt. Die physischen Zugriffsberechtigungslisten werden bei internen und externen ISO27001-Audits immer wieder überprüft und aktualisiert, wenn sich Änderungen an den physischen Zugriffsberechtigungen ergeben.

Zugang von Dritten zu Rechenzentren

Der Zugang von Dritten muss von autorisierten Cloud Provider Mitarbeitern beantragt werden, die auch eine gültige geschäftliche Begründung für diesen Zugang vorlegen müssen. Dieser Antrag wird basierend auf dem Prinzip geringstmöglicher Berechtigungen gewährt, d. h. Mitarbeiter müssen in der Anfrage angeben, auf welche Ebene des Rechenzentrums und für welchen Zeitraum sie Zugang benötigen. Diese Anfragen werden von autorisiertem Personal genehmigt. Der Zugang wird nach Ablauf des beantragten Zeitraums wieder entzogen. Personen mit einem Besucherausweis müssen diesen bei Ankunft am Standort vorlegen und werden von autorisiertem Personal angemeldet und begleitet.

2.1.2 Rechenzentrum in North Virginia, USA

Für das Gebäude des Rechenzentrums gelten die Standards der ISO 27001-Zertifizierung:

Die Alarme sind direkt mit den örtlichen Feuerwehr- und Polizeibehörden verbunden. Amazon-Rechenzentren unterhalten eine 24x7x365 überwachte CCTV-Abdeckung, wobei CCTV/DVRs die Datenaufbewahrung für 90 Tage gemäß den PCI-Anforderungen unterstützen. Sensible Geräte wie z.B. Informationsverarbeitungsanlagen, einschließlich Kundenserver, sind in sicheren Teilbereichen innerhalb des sicheren Perimeters jedes Rechenzentrums untergebracht und unterliegen zusätzlichen Kontrollen. Für den Zugriff auf alle Rechenzentrumseinrichtungen ist eine Zwei-Faktor-Authentifizierung erforderlich. Elektromechanische Schlösser werden durch biometrische Authentifizierung (Handgeometrie oder Fingerabdruckscanner) und Schlüsselkarte/Abzeichen gesteuert. Kündigungs- und Rollenwechsel-Kontrollverfahren sind vorhanden, so dass alle physischen oder logischen Zugriffsrechte rechtzeitig entfernt werden, wenn der Zugriff nicht mehr erforderlich oder angemessen ist.

Mitarbeiterzugang zu Rechenzentren

Nur autorisiertes Amazon-Personal erhält Zugang zu den physischen Rechenzentren. Alle Mitarbeiter, die Zugang zu einem Rechenzentrum benötigen, müssen zunächst einen Antrag auf Zugang stellen und eine gültige geschäftliche Begründung vorlegen. Dieser Antrag wird basierend auf dem Prinzip geringstmöglicher Berechtigungen gewährt, d. h. Mitarbeiter müssen in der Anfrage angeben, auf welche Ebene des Rechenzentrums und für welchen Zeitraum sie Zugang benötigen. Die Anfrage wird geprüft und von autorisiertem Personal genehmigt. Der Zugang wird nach Ablauf des beantragten Zeitraums wieder entzogen. Mitarbeiter mit Zugang zu einem Rechenzentrum sind durch ihre Berechtigungen auf bestimmte Bereiche beschränkt.

Zugang von Dritten zu Rechenzentren

Der Zugang von Dritten muss von autorisierten Amazon-Mitarbeitern beantragt werden, die auch eine gültige geschäftliche Begründung für diesen Zugang vorlegen müssen. Dieser Antrag wird basierend auf dem Prinzip geringstmöglicher Berechtigungen gewährt, d. h. Mitarbeiter müssen in der Anfrage angeben, auf welche Ebene des Rechenzentrums und für welchen Zeitraum sie Zugang benötigen. Diese Anfragen werden von autorisiertem Personal genehmigt. Der Zugang wird nach Ablauf des beantragten Zeitraums wieder entzogen. Mitarbeiter mit Zugang zu einem Rechenzentrum sind durch ihre Berechtigungen auf bestimmte Bereiche beschränkt. Personen mit einem Besucherausweis müssen diesen bei Ankunft am Standort vorlegen und werden von autorisiertem Personal angemeldet und begleitet.

2.1.3 Rechenzentrum in den Niederlanden bzw. Irland

Microsoft entwickelt, erstellt und betreibt Rechenzentren so, dass der physische Zugriff auf die Bereiche, in denen Ihre Daten gespeichert sind, streng kontrolliert wird. Microsoft weiß genau, wie wichtig der Schutz Ihrer Daten ist, und hat sich den Schutz der Rechenzentren, die Ihre Daten enthalten, auf die Fahnen geschrieben. Eine komplette Abteilung befasst sich bei Microsoft mit der Entwicklung, der Erstellung und dem Betrieb der Einrichtungen, die Azure unterstützen. Dieses Team hat die Aufgabe, die physische Sicherheit auf dem neuesten Stand zu halten.

Microsoft verfolgt einen mehrstufigen Ansatz bei der physischen Sicherheit, um das Risiko zu verringern, dass nicht autorisierte Benutzer physischen Zugriff auf Daten und Rechenzentrumsressourcen erhalten. Von Microsoft verwaltete Rechenzentren haben umfassende Schutzebenen: Zugriffsgenehmigung an der Einrichtungsgrenze, an der Gebäudegrenze, im Gebäude und in der Rechenzentrumsetage.

Microsoft stellt aktuelle Informationen online zur Verfügung:

https://docs.microsoft.com/azure/security/azure-physical-security#physical-security

2.2 Geschäftsstellen

2.2.1 Alle Büros

Alle Tivian-Büros halten sich an die Anforderungen der IT-Governance-Richtlinie, hierunter Definition von Sicherheitszonen. Die folgenden Abschnitte beschreiben spezifische Elemente für jedes Büro.

2.2.2 Köln, Deutschland

Das Gebäude und das Gelände werden durch Bewegungsmelder, ein Videoüberwachungssystem und eine vernetzte Gebäudealarmanlage überwacht. An allen Eingängen des Gebäudes ist ein physisches Zutrittskontrollsystem installiert. Alle Eingangstüren des Gebäudes sind zusätzlich mit einer Zentralverriegelung ausgestattet. Innerhalb des Gebäudes dient ein digitales Schließsystem mit Transpondern und PC-Aufzeichnung als Zugangskontrolle zu den Büros. Separate Codeschlösser sichern Büros/Bürobereiche, die eine besonders hohe Sicherheit erfordern. Besucher müssen sich an der Rezeption anmelden. Besucher werden immer von einem Mitarbeiter begleitet, solange sie sich in den Geschäftsräumen aufhalten.

2.2.3 London, United Kingdom

- Besucher müssen sich an der Rezeption oder bei einem Mitarbeiter melden, mit dem sie einen Termin haben, und werden im Gebäude von einem Mitarbeiter begleitet.
- Die Eingangstüren sind mit einem digitalen Schließsystem ausgestattet, das nur durch Mitarbeiter-Key-Cards geöffnet werden kann. Der Office Manager verfügt über die Liste der aktivierten Schlüssel, die von den Mitarbeitern verwendet werden.

2.2.4 New York, USA

- Besucher müssen sich an der Rezeption oder bei einem Mitarbeiter melden, mit dem sie einen Termin haben, und werden im Gebäude von einem Mitarbeiter begleitet.
- Die Eingangstüren sind mit einem digitalen Schließsystem ausgestattet, das nur durch Mitarbeiter-Key-Cards geöffnet werden kann. Der Office Manager verfügt über die Liste der aktivierten Schlüssel, die von den Mitarbeitern verwendet werden.

3. ZUGRIFFSKONTROLLE

Dieser Abschnitt beschreibt die Maßnahmen von Tivian, einschließlich der Identifizierung und Authentifizierung, die vorhanden sind, um Unbefugte daran zu hindern, auf Datenverarbeitungssysteme zuzugreifen und diese zu nutzen sowie auf Wechselmedien zuzugreifen und diese zu verwenden.

3.1 Rechenzentren

3.1.1 Rechenzentrum in Frankfurt, Deutschland

Datagroup

Die Benutzerverwaltung wird über das Active Directory realisiert. Um berechtigten Benutzern ausschließlich den Zugriff auf die für sie relevanten Systeme und Anwendungen zu gewähren, hat DATAGROUP ein umfassendes Berechtigungskonzept umgesetzt. Die Vergabe von Zugriffsberechtigungen erfolgt nach dem Need-to-know-Prinzip. Beschäftigte erhalten damit nur Zugriff auf diejenigen Daten, deren Kenntnis im Rahmen der ihnen übertragenen Aufgaben notwendig ist. Benutzern werden nur diejenigen Anwendungen zur Verfügung gestellt, die diese für die Erledigung der ihnen übertragenen Aufgaben benötigen. Den Anwendungen werden dabei ebenfalls nur die für die Erfüllung der Aufgabe notwendigen Rechte zugewiesen. Auf allen IT-Systemen wird nur mit den für die konkrete Aufgabe erforderlichen Benutzerrechten gearbeitet. Der Zugriff auf Systemsoftware ist für Personen, die nicht Administratoren sind, gesperrt. Die Nutzung von privaten Datenträgern ist durch die S2 Sicherheitsrichtlinie für Mitarbeiter und Administratoren untersagt. Die Entsorgung von Datenträgern (Sicherungsmedien und Festplatten) erfolgt grundsätzlich durch qualifizierte Dienstleister im Rahmen einer Auftragsverarbeitung nach Art.28 DSGVO.

Amazon

Das Amazon AWS Netzwerk ist für Mitarbeiter, Auftragnehmer und jede andere Person, die für die Erbringung der Dienstleistungen erforderlich ist, elektronisch reguliert und kontrolliert zugänglich. AWS hält Zugangskontrollen und Richtlinien aufrecht, um den Zugang zum AWS Netzwerk von jedem Netzwerkanschluss und Benutzer aus zu verwalten, einschließlich der Verwendung von Firewalls oder funktional gleichwertiger Technologie und Authentifizierungskontrollen. AWS hält Korrekturmaßnahmen und Reaktionspläne für Vorfälle aufrecht, um auf potenzielle Sicherheitsbedrohungen zu reagieren.

3.1.2 Rechenzentrum in North Virginia, USA

Amazon AWS hat eine beschränkte Anzahl von Zugriffspunkten zur Cloud an strategisch geeigneten Stellen platziert, damit eine umfassendere Überwachung der ein- und ausgehenden Kommunikation sowie des Netzwerkdatenverkehrs ermöglicht wird. Diese Kundenzugriffspunkte heißen API-Endpunkte und dienen dem sicheren Zugriff (HTTPS), der Ihnen eine sichere Kommunikationssitzung mit Ihren Speicher- oder Datenverarbeitungs-Instanzen innerhalb von AWS ermöglicht. Um Kunden mit FIPS140-2-Anforderungen zu unterstützen, werden die Amazon Virtual Private Cloud (VPN)-Endpunkte und die TLS1.3-terminierenden Lastverteiler in der AWS GovCloud (USA) mithilfe von nach FIPS 140-2 Level 2 validierter Hardware betrieben.

Zusätzlich hat AWS Netzwerkgeräte implementiert, die für die Verwaltung der Schnittstellenkommunikation mit Internet Service Providern (ISPs, Internetdienstanbietern) vorgesehen sind. AWS verwendet eine redundante Verbindung zu mehr als einem Kommunikationsdienst an jeder mit dem Internet verbundene Stelle des AWS-Netzwerks. Jede dieser Verbindungen verfügt über eigene Netzwerkgeräte.

Weitere Informationen können Sie der AWS Webseite https://aws.amazon.com/de/security/ entnehmen.

3.1.3 Rechenzentrum in den Niederlanden bzw. Irland

Microsofts Azure Security weist definierte Anforderungen für die aktive Überwachung auf. Dienstteams konfigurieren die Tools für die aktive Überwachung in Übereinstimmung mit diesen Anforderungen. Zu den aktiven Überwachungstools zählen der Microsoft Monitoring Agent (MMA) und System Center Operations Manager. Diese Tools werden für die Bereitstellung von Echtzeitwarnungen für Azure-Sicherheitspersonal in Situationen konfiguriert, die ein sofortiges Handeln erfordern.

Microsoft stellt aktuelle Informationen online zur Verfügung:

https://docs.microsoft.com/azure/security/azure-infrastructure-monitoring

3.2 Geschäftsstellen

3.2.1 Alle Büros

Alle Tivian-Büros halten sich an die Anforderungen der IT-Governance-Richtlinie.

Geräteverschlüsselung

Alle tragbaren Speichergeräte sind vollständig verschlüsselt. (Notebook-Festplatte, USB-Sticks)

Authentifizierung

Die Authentifizierung gegenüber dem Betriebssystem und den Anwendungen erfolgt über individuelle Benutzerkennungen und Passwörter. Für den Zugriff auf die Hardware-Entschlüsselung muss ein separates Passwort eingegeben werden. Die Mitarbeiter sind verpflichtet, den Arbeitsplatz-Client zu sperren, wenn sie den Raum verlassen ("Clear Screen"). Die Mitarbeiter sind außerdem verpflichtet, ihre Passwörter geheim zu halten und nicht an Dritte weiterzugeben, auch nicht zu Supportzwecken. Es gibt Passwortkonventionen, die technisch (Systemkonfiguration) und organisatorisch (Passwortrichtlinie) umgesetzt sind. Nach diesen Konventionen müssen alle Passwörter die definierten Mindestanforderungen erfüllen.

3.3 Software

3.3.1 Enterprise Feedback Suite (EFS)

Die Standardeinstellung ist folgende: Das Passwort muss nach der ersten Anmeldung geändert werden. Danach verfällt es alle 90 Tage. Die lizenzierte Software erfordert, dass Benutzer ihre Passwörter ändern, wenn sie sich nach dem Ablaufdatum einloggen. Bei den Kontonamen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden.

EFS bietet eine breite Palette von Passwort-Komplexitätseinstellungen an:

- Passwortlängen sind variabel und werden vom Kunden festgelegt.
- Passwörter müssen mindestens 6 Zeichen, aber nicht mehr als 12 Zeichen haben.
- Passwörter müssen Zeichen aus mindestens zwei der folgenden vier Gruppen enthalten: Kleinbuchstaben (a-z), Großbuchstaben (A-Z), Zahlen (0-9) und andere druckbare ASCII-Zeichen. Passwörter dürfen keine Leerzeichen enthalten.
- Passwort-Verfallsdatum, kann von "einem Tag" auf "nie verfallen" eingestellt werden.
  (Erzwungene Passwort-Aktualisierung, Gültigkeitsprüfung der Passwörter in Tagen)
- Passwort-Wiederholungszahl, kann von "nicht zählen" bis "das Kennwort darf nie wieder verwendet werden" eingestellt werden.
  (Überprüfung der letzten x Passwörter, ob das Passwort schon einmal verwendet wurde)

Benutzer dürfen nicht das gleiche Passwort verwenden, wenn sie bei der ersten Anmeldung oder nach Ablauf eines Monats Passwörter ändern müssen. Um sich vor Brute-Force-Angriffen zu schützen, sperrt das System nach sechs Fehleingaben vorübergehend den Zugriff für 30 Minuten. Passwörter werden nicht im Klartext gespeichert. Kunden können nur über benutzerspezifische Konten auf die lizenzierte Software zugreifen und sich authentifizieren.

Rechte- und Rollenkonzept der EFS-Plattform

Power-User oder Administratoren-Accounts werden in der Tivian Plattform in EFS Teams gruppiert, die die Zugriffe auf funktionale Rechte (ACL), als auch auf inhaltliche Rechte (Objekte) steuern. Wenn Rechte- / Rollenkonzepte aus externen Plattformen übernommen werden sollen, muss zunächst das Konzept in Tivian EFS repliziert werden. Über eine API gesteuerte Zuweisung zu den Teams in EFS kann dann die Rechtesituation automatisiert gespiegelt werden.

Schwachstellenmanagement

Schwachstellen-Scans werden mit dem Netzwerk- und Schwachstellen-Scanner Nessus durchgeführt. Diese Scans werden für jeden Server einmal im Monat durchgeführt. Für diese Scans wird das Nessus Standard-Testset verwendet. Ein RIPS Code Analysis Scan wird verwendet, um die Verwundbarkeit des Quellcodes zu überprüfen. Sicherheitskontrollen können wie folgt durchgeführt werden:

- Tivian-Systemadministratoren (der Normalfall).
- Kunden (auf Wunsch und auf Kosten des Kunden).
- Externe Sicherheitsunternehmen (im Auftrag eines Kunden, der auch die Kosten trägt).
- BSI/ISO-Auditoren (während des Zertifizierungsprozesses und bei der Verlängerung von Zertifikaten).

Auftretende kritische Fehler werden sofort nach der Prüfung der Protokolle behoben. Datenträger und vertrauliche Dokumente werden von zertifizierten Dienstleistern aufbewahrt und nach Wegfall des jeweiligen Zwecks datenschutzkonform vernichtet. Die Anwendungssoftware EFS protokolliert Verwaltungszugriffe in Protokollen. Diese Protokolle enthalten Informationen über das Konto, die Zeit, das Modul, die Aktion und andere Parameter. Für die Einsicht in das Administrationsprotokoll ist ein gesondertes Recht erforderlich. Dieses Recht ist bestimmten Rollen zugeordnet. Die Standardlagerzeit beträgt 90 Tage.

3.3.2 QUBIE

Qubie für MS Teams

Anwender von QUBIE für MS TEAMS können nur über eigene MS TEAMS Konten auf die lizenzierte Software zugreifen und sich authentifizieren. Es gelten die jeweils lokalen Authentifizierungsbedingungen der Anwender von MS TEAMS.

Beim Chatten mit QUBIE Bot erfolgt die Authentifizierung durch das Bot-Framework / Microsoft Teams und die Anmeldung für Microsoft Teams wird verwendet.

Wenn der Benutzer zur neuen Registerkarte "Ergebnisse" navigiert, wird der OAuth 2-Endpunkt von Azure Active Directory verwendet (https://docs.microsoft.com/azure/active-directory/develop/active-directory-v2-protocols). Der Nutzer muss zustimmen, dass der Kontoname für die Anmeldung freigegeben wird.

Qubie für Web

Hier gelten die gleichen Bedingungen wie für die Enterprise Feedback Suite (EFS).

4. PROTOKOLLIERUNG DER VERARBEITUNG PERSONENBEZOGENER DATEN

Dieser Abschnitt beschreibt die Maßnahmen von Tivian zur Erfassung und Dokumentation des Zugriffs auf und der Verarbeitung personenbezogener Daten, die im Auftrag seiner Kunden verarbeitet werden.

4.1 Rechenzentren

4.1.1 Rechenzentrum in Frankfurt, Deutschland

Die Datenübertragung wird protokolliert und die Protokolle werden kontinuierlich ausgewertet. Jede Entfernung von Datenträgern wird protokolliert und die Protokolle werden ausgewertet. Die Protokollierung und Auswertung der Protokolle erfolgt im Rahmen der hier beschriebenen technischen und organisatorischen Maßnahmen. Umfang der Internetprotokolle: Metadaten des Internetverkehrs. (IP-Adresse des verbundenen Clients, die aufgerufene Domain, Datum, Uhrzeit und Zeitzone, aus der die Verbindung kam, die konkrete Anfrage des Clients im Klartext, die verwendete Methode, die angeforderten Daten, das verwendete Protokoll, die aufgerufene URL, der Referrer, der bei der Anfrage zurückgegebene HTTP-Statuscode, die Größe der übertragenen Daten, gemessen in Bytes, Betriebssystem und Version, Clienttyp, Browser und Version)

4.1.2 Rechenzentrum in North Virginia, USA

Die Datenübertragung wird protokolliert und die Protokolle werden kontinuierlich ausgewertet. Jede Entfernung von Datenträgern wird protokolliert und die Protokolle werden ausgewertet. Die Protokolle und die Auswertung der Protokolle erfolgen im Rahmen der hier beschriebenen technischen und organisatorischen Maßnahmen. Umfang der Internetprotokolle: Metadaten des Internetverkehrs. (IP-Adresse des verbundenen Clients, die aufgerufene Domain, Datum, Uhrzeit und Zeitzone, aus der die Verbindung kam, die konkrete Anfrage des Clients im Klartext, die verwendete Methode, die angeforderten Daten, das verwendete Protokoll, die aufgerufene URL, der Referrer, der bei der Anfrage zurückgegebene HTTP-Statuscode, die Größe der übertragenen Daten, gemessen in Bytes, Betriebssystem und Version, Clienttyp, Browser und Version)

4.1.3 Rechenzentrum in den Niederlanden bzw. Irland

Microsoft Azure verfügt über Sicherheitsmechanismen, die als Hilfe bei der Verwaltung und Überwachung von Azure-Clouddiensten und virtuellen Azure-Computern dienen.

Microsoft ist für die Azure-Plattform und die physische Sicherheit seiner Rechenzentren verantwortlich (durch den Einsatz von Sicherheitsmaßnahmen wie Türen mit elektronischer Zugangskontrolle, Zäunen und Wachpersonal). Microsoft Azure bietet eine umfassende Cloudsicherheit auf Softwareebene, die die Anforderungen seiner Kunden an Sicherheit, Datenschutz und Compliance erfüllt.

Microsoft stellt Sicherheitskontrollen und -funktionen bereit, die Tivian zum Schützen Ihrer Daten und Anwendungen unterstützen.

Microsoft stellt aktuelle Informationen online zur Verfügung:

https://docs.microsoft.com/azure/security/security-management-and-monitoring-overview

4.2 Software

4.2.1 EFS

Aktivitäten von Kunden und Tivian werden im System protokolliert. Bei der Verarbeitung personenbezogener Daten führt die Software ein Login-Log und ein Admin-Log durch. Das Login-Log informiert darüber, welcher Benutzer sich wann eingeloggt hat, einschließlich abgewiesener Versuche. Inhalt des Login-Logs: Konto, IP-Adresse, Zugriff/Fehler, Fehlermeldung, Datum. Das Admin-Log bietet ein detailliertes Protokoll der von den Benutzern im System ausgeführten Aktionen. Inhalt des Admin Log: Eintrags-ID, Konto, Eintragsdatum, Modulname, Aktion, Ausführungszeit, Funktionen. Diese Protokolle können direkt in der Software eingesehen werden. Eine Such- und Filterfunktion wird ebenfalls angeboten. Eine Beschreibung der Funktionalitäten finden Sie in den entsprechenden Kapiteln des Software-Handbuchs.

4.2.2 QUBIE

Qubie für MS Teams

MS Teams Analytics - Applicationinsights wird verwendet, um die verschiedenen Ereignisse zu protokollieren, die in QUBIE auftreten können. In QUBIE für MS TEAMS werden Aktivitäten von Benutzern protokolliert. Dazu gehören Ereignisse wie Error Events, Question Events, Role Events, Feedback Events, User Events, Help Events, Bug Events. Die Software bietet kein UI dieser Aktivitätsprotokolle an.

Qubie für Web

Hier gelten die gleichen Bedingungen wie für EFS.

5. ÜBERTRAGUNGSKONTROLLE

Dieser Abschnitt beschreibt die Maßnahmen von Tivian, die sicherstellen, dass personenbezogene Daten während der elektronischen Übermittlung, des Transports oder der Speicherung auf Datenträgern nicht gelesen, kopiert, geändert oder gelöscht werden können und dass geprüft und festgelegt wird, an welchen Stellen personenbezogene Daten mit Hilfe von Datenübertragungsgeräten übertragen werden sollen:

5.1 Rechenzentren

5.1.1 Rechenzentrum in Frankfurt, Deutschland

Verschlüsselung von Daten während der Übertragung („encryption in transit“)

Der Zugriff auf die Datenbanken bei **AWS** erfolgt verschlüsselt über SSH (Secure Shell) und VPN-Tunnel. Alle Datenleitungen zum Internet sind redundant ausgelegt und als BGP (Border Gateway Protocol) ausgeführt. Die gesamte Netzwerkinfrastruktur (Firewalls, Switches etc.) ist vollständig redundant ausgelegt. Firewalls und DMZ-Einstellungen werden durch BSI/ISO-Standards definiert. Jeder Zugriff von Tivian-Mitarbeitern (insbesondere vom Support oder der Entwicklung) auf Kundendaten, die vom Rechenzentrum zum Zwecke der Verwaltung der EFS-Umfragen gehostet werden, erfolgt mittels TLS1.3-Verschlüsselung (PCI-Compliance). Protokollierung der Datenübertragungen und laufende Auswertung der Protokolle.

Verschlüsselung für ruhende Daten („encryption at rest“)

Sämtliche Daten im Frankfurter Rechenzentrum bei **AWS** werden im Ruhezustand verschlüsselt gespeichert.

Schriftliche Bestimmungen über die Verwendung von Datenträgern, einschließlich der Erstellung von Kopien von Datenträgern zur Verwendung als Backup:

- Solche Zugriffsrechte werden nur Administratoren gewährt.
- Jede Entfernung von Datenträgern wird protokolliert.
- Die Protokolle werden ausgewertet

5.1.2 Rechenzentrum in North Virginia, USA

Amazon ermöglicht den Fernzugriff von Mitarbeitern über eine Verbindung mit einem AWS-Zugriffspunkt über HTTPS mit Transport Layer Security (TLS1.3), einem Verschlüsselungsprotokoll, das entwickelt wurde, um vor Abhörangriffen, Datenmanipulation oder Fälschung von Nachrichten zu schützen. Zusätzliche Ebenen an Netzwerksicherheit bieten die Amazon Virtual Private Cloud (VPC), die ein privates Subnetz innerhalb der AWS-Cloud bereitstellt, und die Verwendung eines IPsec Virtual Private Network (VPN)-Geräts ermöglicht, das einen verschlüsselten Tunnel zwischen dem Amazon-VPC und unserem Netzwerk herstellen kann. Ein direkter Zugriff auf Kundenlösungen über eine Fernverbindung ist nicht erlaubt. Es gibt eine Richtlinie zur Aufrechterhaltung der Sicherheit während des gesamten Fernzugriffsbereitstellungsprozesses und zur Bewältigung von Sicherheitsproblemen während der Telearbeit. Der Prozess beinhaltet eine Zwei-Faktor-Authentifizierung (RSA+PIN und SSO) und einen Bastion-Server. Der Zugriff auf die Datenbanken erfolgt verschlüsselt über SSH (Secure Shell) und VPN-Tunnel. Alle Datenleitungen zum Internet sind redundant ausgelegt und als BGP (Border Gateway Protocol) ausgeführt. Die gesamte Netzwerkinfrastruktur (Firewalls, Switches etc.) ist vollständig redundant ausgelegt. Firewalls und DMZ-Einstellungen sind durch ISO-Normen definiert. Alle Datenexporte werden in der lizenzierten Software protokolliert. Jeder Zugriff von Tivian-Mitarbeitern (insbesondere vom Support oder der Entwicklung) auf Kundendaten, die vom Rechenzentrum zum Zwecke der Verwaltung der EFS-Umfragen gehostet werden, erfolgt mittels TLS1.3-Verschlüsselung (PCI-Compliance). Protokollierung der Datenübertragungen und laufende Auswertung der Protokolle. Schriftliche Bestimmungen über die Verwendung von Datenträgern, einschließlich der Erstellung von Kopien von Datenträgern zur Verwendung als Backup.

5.1.3 Rechenzentrum in den Niederlanden bzw. Irland

Verschlüsselung für ruhende Daten

Ruhende Daten umfassen Informationen, die in einem beliebigen digitalen Format im dauerhaften Speicher auf physischen Medien gespeichert sind. Zu den Medien gehören Dateien auf Magnet- oder optischen Datenträgern, archivierte Daten und Datensicherungen. **Microsoft Azure** bietet eine Reihe von Datenspeicherlösungen für verschiedene Anforderungen, darunter Datei-, Daten-, Blob- und Tabellenspeicher. Microsoft bietet zudem eine Verschlüsselung zum Schutz von Azure SQL-Datenbank, Azure Cosmos DB und Azure Data Lake.

Die Verschlüsselung ruhender Daten ist für Dienste in allen Software-as-a-Service- (SaaS), Platform-as-a-Service- (PaaS) und Infrastructure-as-a-Service-Cloudmodellen (IaaS) verfügbar. In diesem Artikel werden Ressourcen zusammenfassend beschrieben und bereitgestellt, mit denen Sie die Verschlüsselungsoptionen von Azure nutzen können.

Eine ausführliche Erörterung zur Verschlüsselung ruhender Daten in Azure finden Sie unter Azure-Datenverschlüsselung ruhender Daten.

Verschlüsselung von Daten während der Übertragung

Microsoft Azure bietet viele Verfahren zum Schutz von Daten beim Übertragen zwischen verschiedenen Speicherorten.

TLS-Verschlüsselung in Azure

Microsoft verwendet das Transport Layer Security-Protokoll (TLS1.3) zum Schutz von Daten bei der Übertragung zwischen den Clouddiensten und Kunden. Die Microsoft-Rechenzentren verhandeln eine TLS-Verbindung mit Clientsystemen, die eine Verbindung mit Azure-Diensten herstellen. TLS bietet strenge Authentifizierung, Datenschutz von Nachrichten und Integrität (ermöglicht die Erkennung von Manipulation, Abfangen und Fälschung von Nachrichten), Interoperabilität, Algorithmus Flexibilität sowie einfache Bereitstellung und Verwendung.

Perfect Forward Secrecy (PFS) schützt Verbindungen zwischen den Clientsystemen von Kunden und den Clouddiensten von Microsoft durch eindeutige Schlüssel. Die Verbindungen verwenden zudem RSA-basierte Verschlüsselungsschlüssellängen von 2.048 Bit. Diese Kombination erschwert das Abfangen von Daten während der Übertragung und den Zugriff darauf.

Microsoft stellt aktuelle Informationen online zur Verfügung:

https://docs.microsoft.com/azure/security/security-azure-encryption-overview

5.2 Büros und Software

Der Datenzugriff auf alle Softwarekomponenten der Befragungsplattform wird mittels TLS1.3-Verschlüsselung erfolgen. Die Übertragung personenbezogener Daten wird durch die Verwendung von HTTPS/TLS1.3-Verschlüsselung gesichert. Zu diesem Zweck bietet Tivian eine Datentransferplattform in Projekten an. Art und Umfang der übertragenen Daten (Metadaten) werden

protokolliert. Diese Protokolle werden regelmäßig ausgewertet. Der Einsatz von mobilen Datenträgern ist grundsätzlich untersagt. Die Verwendung von mobilen Speichermedien ist für bestimmte Daten nur nach vorheriger schriftlicher Zustimmung zulässig. Persönliche oder sicherheitsrelevante Informationen gehören jedoch nicht zu dieser Kategorie. Alle mobilen Arbeitsplatzrechner sind vollständig verschlüsselt. Die E-Mail-Kommunikation und der Zugriff auf die Dokumente der Mitarbeiter des Auftragnehmers sind durch Verschlüsselung, VPNs und Firewalls geschützt.

6. EINGABEKONTROLLE

Dieser Abschnitt beschreibt die Maßnahmen von Tivian, die sicherstellen, dass überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in den Datenverarbeitungssystemen eingegeben, geändert oder gelöscht wurden:

6.1 Rechenzentren

6.1.1 Rechenzentrum in Frankfurt, Deutschland

Die Mitarbeiter des Rechenzentrums der **DATAGROUP** und **Amazon** Frankfurt, die für Fernwartungsmaßnahmen zuständig sind, können weder Daten in die Datenverarbeitungssysteme eingeben noch persönliche Daten von Tivian-Kunden einsehen, ändern oder löschen. Fernwartungsmaßnahmen werden durch eine Firewall protokolliert. Die daraus resultierenden Protokolle werden stichprobenartig (Stichproben) und immer dann, wenn dies durch Ereignisse gerechtfertigt ist, überprüft.

6.1.2 Rechenzentrum in North Virginia, USA

Die Mitarbeiter des Rechenzentrums von **Amazon**, die für Wartungsmaßnahmen zuständig sind, können weder Daten in die Datenverarbeitungssysteme eingeben noch persönliche Daten von Tivian-Kunden einsehen, ändern oder löschen. Fernwartungsmaßnahmen werden durch eine Firewall protokolliert. Die daraus resultierenden Protokolle werden stichprobenartig (Stichproben) und immer dann, wenn dies durch Ereignisse gerechtfertigt ist, überprüft.

6.1.3 Rechenzentrum in den Niederlanden bzw. Irland

Die Mitarbeiter des Rechenzentrums von **Microsoft**, die für Wartungsmaßnahmen zuständig sind, können weder Daten in die Datenverarbeitungssysteme eingeben noch persönliche Daten von Tivian-Kunden einsehen, ändern oder löschen. Fernwartungsmaßnahmen werden durch eine Firewall protokolliert. Die daraus resultierenden Protokolle werden stichprobenartig (Stichproben) und immer dann, wenn dies durch Ereignisse gerechtfertigt ist, überprüft.

6.2 Geschäftsstellen

Alle Tivian-Büros halten sich an die Anforderungen der IT-Governance-Richtlinie, hierunter Definition von Sicherheitszonen. Die folgenden Abschnitte beschreiben spezifische Elemente für jedes Büro.

Alle Mitarbeiter unterzeichnen eine Vertraulichkeitsklausel als integralen Bestandteil ihrer Arbeitsverträge und verpflichten sich damit zur Wahrung des Datengeheimnisses, das die Kunden auch nach Beendigung oder Ablauf der Arbeitsverträge der Mitarbeiter schützt. Ein Ticketsystem im Support- und Administrationsbereich sorgt dafür, dass alle Aufgaben korrekt und pünktlich erledigt werden. Die Mitarbeiter des Auftragnehmers werden durch einen Verzeichnisdienst unterstützt und dürfen nur auf die Daten zugreifen, die für ihre Arbeit im Rahmen des jeweiligen Aufgaben- und Tätigkeitsbereiches benötigt werden.

6.3 Software

6.3.1 EFS

Alle Änderungen der Versionsstände werden dokumentiert. Die Nutzung wird in Bezug auf das jeweilige Konto dokumentiert; die zugehörigen Daten werden maximal 90 Tage gespeichert. Bei der Nutzung der Austauschplattform werden Dateien mit personenbezogenen Daten versionsweise gespeichert. Das zugehörige Datum, die Uhrzeit und der Benutzer werden protokolliert. Benutzeranmerkungen können in ein Kommentarfeld eingegeben werden, das nicht im Dokument enthalten ist. Dokumente können nicht geändert werden. Dokumente, die in das System eingegeben werden, können mit einem separaten Passwortschutz versehen werden, um den Zugriff zu beschränken.

6.3.2 QUBIE

Qubie für MS Teams

In QUBIE für MS TEAMS werden die Ereignisse, die ein Benutzer auslösen kann, in Application Insights protokolliert. Weitere Details siehe 4.2.3.

Qubie für Web

Hier gelten die gleichen Bedingungen wie für EFS.

7. AUFTRAGSKONTROLLE

Dieser Abschnitt beschreibt die Maßnahmen von Tivian, die sicherstellen, dass personenbezogene Daten, die im Auftrag eines Kunden verarbeitet werden, nur gemäß den Anweisungen des Kunden verarbeitet werden können.

7.1 Rechenzentren

Tivian prüft die jeweiligen Sicherheitskonzepte und die Räumlichkeiten des Rechenzentrums werden regelmäßig inspiziert. Zur Sicherstellung des Datenschutzes bestehen schriftliche Verträge mit den Rechenzentren.

Zu keiner Zeit verarbeiten die Cloudprovider Datagroup, Microsoft oder Amazon personenbezogene Daten ohne Auftrag. Alle Mitarbeiter unterliegen Verschwiegenheitserklärungen (NDAs).

7.2 Geschäftsstellen

Alle Mitarbeiter von Tivian sind an die Regeln von Tivian Binding Corporate gebunden und erhalten regelmäßige Schulungen zum Schutz personenbezogener Daten. Die Bewertung von Inhalten in einem Datenverarbeitungsvertrag oder in Anweisungen des Kunden sind Teil einer solchen Schulung.

Tivian-Manager und Tivian-Mitarbeiter, die im Dialog mit Kunden stehen, sind verpflichtet, dafür zu sorgen, dass Anweisungen an das entsprechende Personal gegeben und befolgt werden.

7.3 Software

Wenn das Vertragsverhältnis eines Kunden zu einem der Dienste von Tivian beendet oder abgelaufen ist, wird das Konto deaktiviert und ist nicht mehr zugänglich. Die über die Website gesammelten Informationen werden gelöscht.

8. VERTRAULICHKEITSKONTROLLE

Der DSGVO Abschnitt 32 definiert die Vertraulichkeitskontrolle als Voraussetzung für die Sicherheit der Verarbeitung. Dieser Abschnitt beschreibt die Maßnahmen von Tivian zur Gewährleistung der Vertraulichkeitskontrolle.

8.1 Rechenzentren

Die Rechenzentren von Tivian, die für die Speicherung und den technischen Betrieb der Daten zuständig sind, haben keinen Zugriff auf die Daten. Die Betreiber von Rechenzentren haben kein Konto auf den Servern von Tivian. Ausnahmen von dieser Regel gelten nur für die Erstellung von Sicherungen, damit die Sicherungssoftware die Daten sichern kann. Die Backups werden sicher und dokumentiert gespeichert und unterliegen strengen Zugriffsregeln. Backups werden in verschlüsselter Form gespeichert.

8.2 Geschäftsstellen

Tivian-Büros sichern die Vertraulichkeit durch eine Vielzahl von Maßnahmen. Dazu gehören Besucherverwaltung, Raumschließsystem, starke Kontoverwaltung, klare Arbeitsplatzregeln, verschlüsselte Geräte, Vertraulichkeitsvereinbarungen, versiegelte Backup-Medien und zertifizierte Vernichtung von Datenträgern.

8.3 Software

Die Software von Tivian gewährleistet Vertraulichkeit durch eine Vielzahl von Maßnahmen. Dazu gehören der Zugriff durch ein starkes Account Management, die Nutzung eines zertifizierten Rechenzentrums, die Zugriffskontrolle über einen 2. Faktor, die Datensicherung und der verschlüsselte Transport über das Internet.

9. INTEGRITÄTSKONTROLLE

Der DSGVO Abschnitt 32 definiert die Integritätskontrolle als Voraussetzung für die Sicherheit der Verarbeitung. Dieser Abschnitt beschreibt die Maßnahmen von Tivian zur Gewährleistung der Integritätskontrolle.

9.1 Rechenzentren

Die Rechenzentren von Tivian gewährleisten die Integrität durch eine Vielzahl von Maßnahmen. Dazu gehören diverse nationale und internationale Zertifizierungen, wie z.B. ISO27001 oder SOC, die in der Ausprägung die Integrität aller Informationsverarbeitenden-Systeme und Daten aufrechterhalten ebenso wie verschlüsselte Backup-Bänder und verschlüsselter Transport über das Internet.

9.2 Geschäftsstellen

Die Tivian-Büros gewährleisten Integrität durch eine Vielzahl von Maßnahmen. Dazu gehören die Verschlüsselung von Medien, starke Zugriffskontrollen, die Verwendung von verschlüsselter Kommunikation und gekapselte Netzwerksegmente.

9.3 Software

Die Software von Tivian stellt die Integrität durch eine Vielzahl von Maßnahmen sicher. Dies beinhaltet die Sicherstellung der Integrität der Programmmodule durch (kryptografische) Prüfsummen/Vergleiche mit Referenzlisten, URL-Manipulationsmechanismen, sichere Cookies, spezifische Webservice-Rechte und Protokollierung, sichere Sandbox-Programmerweiterung LUA, kontinuierliche Verbesserung der aktuellen Codebasis, Dateiintegritätsprüfungen, Änderungs-Audit-Log und Eingabevalidierungskontrollen.

10. VERFÜGBARKEITSKONTROLLE

Der DSGVO Abschnitt 32 definiert die Verfügbarkeitskontrolle als Anforderung zur Gewährleistung der Verarbeitungssicherheit. Dieser Abschnitt beschreibt die Maßnahmen von Tivian, die sicherstellen, dass persönliche Daten verfügbar sind und gleichzeitig verhindern, dass sie versehentlich zerstört oder verloren gehen.

10.1 Rechenzentren

10.1.1 Rechenzentrum in Frankfurt, Deutschland

Jeder unserer Cloudprovider (Datagroup, Amazon und Microsoft) führen tägliche komplette Backups der Daten durch. Dank dieser Sicherung kann der Auftragnehmer im Notfall sofort wieder den Betrieb aufnehmen. Die Daten werden parallel auf ein separates Backup-System in einem separaten Brandabschnitt kopiert. Die Daten werden zusätzlich auf Magnetbänder kopiert, die separat sicher aufbewahrt werden. Die Daten auf den Magnetbändern sind fallabhängig verschlüsselt. Die Protokolldateien der Datensicherung werden täglich überprüft.

Jede Woche werden alle Backups in einem sicheren Lagerschrank aufbewahrt. Die Backups für jeden Tag der letzten acht Wochen können präzise wiederhergestellt werden. Im Rahmen von Notfallübungen werden regelmäßige Schulungen zur Datenrettung und Datenlesbarkeit durchgeführt.

- Klimatisierung: Vier unabhängig voneinander arbeitende Klimaanlagen sind installiert.
- Brandschutz: Die Computerräume sind mit einer an die Feuerwehr angeschlossenen Brandmeldeanlage und einer Argon-Feuerlöschanlage ausgestattet.
- Stromversorgung: Eine Notstromanlage (unterbrechungsfreie Stromversorgung) ist installiert.
- Redundanz ist für alle Systeme vorhanden.
- Es liegen aktuelle schriftliche Richtlinien und/oder Arbeitsanweisungen vor.

10.1.2 Rechenzentrum in North Virginia, USA

Verfügbarkeit

Die Amazon AWS Rechenzentren werden in Clustern in verschiedenen Regionen der Welt errichtet. Bei einem Ausfall verschieben automatische Prozesse den Kundendatenverkehr weg von den betroffenen Bereichen. Die Kernanwendungen werden in einer N+1-Konfiguration bereitgestellt, sodass im Falle eines Rechenzentrumsausfalls ausreichend Kapazität vorhanden ist, um den Datenverkehr lastverteilt an die verbleibenden Standorte zu verteilen. AWS platziert Instanzen und speichert Daten innerhalb mehrerer geografischer Regionen sowie über mehrere Availability Zones innerhalb der einzelnen Regionen. Jede Availability Zone ist als unabhängige Ausfallszone entwickelt. Dies bedeutet, dass Availability Zones innerhalb einer typischen Stadtregion physisch verteilt sind und sich z.B. in Gebieten mit niedrigerem Überschwemmungsrisiko befinden (je nach Region gibt es unterschiedliche Überschwemmungszonenkategorisierungen). Zusätzlich zu einer eigenständigen unterbrechungsfreien Stromversorgung und Notstromgeneratoren vor Ort werden alle Availability Zones über unterschiedliche Stromnetze von unabhängigen Stromversorgern gespeist, um Einzelfehlerstellen zu minimieren. Sämtliche Availability Zones sind redundant mit mehreren Tier-1-Transit-Providern verbunden. Amazon verwaltet Vorfällen über branchenübliche diagnostische Verfahren, um die Behebung unternehmenskritischer Vorfälle voranzutreiben.

Das AWS Betriebspersonal bietet eine kontinuierliche Besetzung rund um die Uhr, sieben Tage die Woche und an 365 Tagen im Jahr, um Störfälle zu erkennen und deren Auswirkungen und Behebung zu verwalten. Die Mitglieder der Geschäftsführung und des Prüfungsausschusses des Firmenvorstands überprüfen regelmäßig die Stabilitätspläne der AWS-Services. Amazon betrachtet dabei die Verfügbarkeit der Kundenlösung aus der Sicht der Netzwerk- und Hardwareverfügbarkeit sowie die Verfügbarkeit der Support-Services und überprüft regelmäßig Kontrollen, Prozesse und Architekturen, um die bestmögliche Verfügbarkeit zu gewährleisten.

Dazu gehören dokumentierte Richtlinien, die den Empfehlungen der Normen (wie z.B. ISO27001) entsprechen (einschließlich einer Richtlinie zur Informationssicherheit); ein formaler Kapazitätsmanagement-Prozess zur Sicherstellung der Verfügbarkeit aller vom Unternehmen benötigten Ressourcen, einschließlich Bandbreite, Rechenzentrumskapazität und Versorgungseinrichtungen, Inventar und Arbeitskräfte und Fähigkeiten der Mitarbeiter; unterbrechungsfreie Stromversorgungen (USV), um das Risiko kurzfristiger Stromausfälle und -schwankungen zu minimieren; Dieselgeneratoren, um das Risiko von langfristigen Stromausfällen und -schwankungen zu minimieren; Auslegung der Dächer und Außenwände des Rechenzentrums für hohe Beanspruchung und extremen Witterungseinflüssen inkl. Lichtschutz; Temperatur- und Feuchtigkeitsklimasysteme im Lagerbereich sowie die Ausstattung mit Brandmelde- und Löschanlagen, Feuerlöschern.

Backup und Restore

Der Amazon AWS Backup Prozess ist ein vollständig verwalteter Backup-Service, der die Datensicherung über AWS-Services hinweg unter Verwendung von AWS Storage Gateways zentralisiert und automatisiert. Die Backup-Richtlinien sind zentral konfiguriert und die Ressourcen für die Backup-Aktivität werden permanent überwacht. Das AWS Backup ist automatisiert und konsolidiert Sicherungsaufgaben, zur Vermeidung benutzerdefinierter Skripts und manueller Prozesse. Sicherungsrichtlinien definieren die Automatisierung der Sicherungszeitpläne und Aufbewahrung der Sicherungen. Der Backup-Prozess ist so strukturiert, dass er den Bedürfnissen und Anforderungen des Unternehmens entspricht. Der Standardzeitplan ist wöchentlich volle und tägliche differentielle Backups mit Aufbewahrungsraten von acht Wochen.

AWS Backup schützt die Sicherungen durch Verschlüsselung der Daten im Ruhezustand und während der Übertragung. Die Protokolle zu Sicherungsaktivitäten stehen für Compliance-Überprüfungen zur Verfügung. Das AWS Backup ist PCI-, ISO- und HIPAA-konform.

10.1.3 Rechenzentrum in den Niederlanden bzw. Irland

Microsoft Azure bietet zuverlässige Verfügbarkeit auf Grundlage umfassender Redundanz mithilfe von Virtualisierungstechnologie. Microsoft Azure bietet zahlreiche Redundanzebenen zur Gewährleistung maximaler Verfügbarkeit von Kundendaten.

Das Microsoft Cloud Infrastructure and Operations-Team entwirft, erstellt, betreibt und verbessert den Schutz der Cloudinfrastruktur. Dieses Team stellt für die Azure-Infrastruktur Hochverfügbarkeit und Zuverlässigkeit, hohe Effizienz, intelligente Skalierbarkeit sicher. Das Team bietet eine sicherere, private und vertrauenswürdige Cloud.

Unterbrechungsfreie Stromversorgungen und riesige Batteriebänke gewährleisten eine fortgesetzte Energieversorgung bei kurzfristigen Stromausfällen. Notstromaggregate sorgen bei längeren Ausfallzeiten und geplanter Wartung für Reservestrom. Im Falle einer Naturkatastrophe kann das Rechenzentrum die vor Ort befindlichen Brennstoffreserven verwenden.

Stabile Glasfasernetze für hohe Geschwindigkeit verbinden die Rechenzentren mit anderen wichtigen Hubs und Internetbenutzern. Serverknoten hosten Workloads näher am Benutzer, um die Latenz zu verringern, Georedundanz bereitzustellen und die Resilienz von Diensten insgesamt zu steigern. Ein Technikerteam arbeitet rund um die Uhr, um sicherzustellen, dass die Dienste ständig zur Verfügung stehen.

Microsoft gewährleistet Hochverfügbarkeit durch erweiterte Überwachung und Reaktion auf Vorfälle, Dienstunterstützung sowie Sicherungs- und Failoverfunktion. Geografisch verteilte Microsoft-Betriebszentren sind 24 Stunden am Tag, 7 Tage die Woche und 365 Tage im Jahr in Betrieb. Das Azure-Netzwerk ist eines der größten der Welt. Das Glasfasernetz für die Inhaltsverteilung verbindet Rechenzentren und Edge-Knoten, um hohe Leistung und Zuverlässigkeit sicherzustellen.

Azure SQL Server-Datenbanken werden automatisch gesichert (https://docs.microsoft.com/azure/sql-database/sql-database-automated-backups) Vollständige Datenbank-Backups werden alle 12 Stunden erstellt, transaktionale Backups werden alle 5-10 Minuten erstellt.

Microsoft stellt aktuelle Informationen online zur Verfügung:

https://docs.microsoft.com/azure/security/azure-infrastructure-availability

10.2 Geschäftsstellen

Sicherungsstrategie:

- Jede Nacht wird ein vollständiges Backup der Daten auf einem unabhängigen Backup-System durchgeführt. Dank dieser Sicherung kann der Auftragnehmer im Notfall sofort wieder den Betrieb aufnehmen.
- Jede Woche werden alle Backups des zentralen Servers in einem Safe aufbewahrt.

- Backups können für jeden der letzten sieben bis 30 Tage präzise wiederhergestellt werden, je nachdem, wie kritisch das System ist.

Zusätzliche Maßnahmen

- Die Computerräume sind mit einer Klimaanlage ausgestattet.
- Stromversorgung: Eine Notstromanlage (unterbrechungsfreie Stromversorgung) ist installiert.
- Zertifizierte Feuerlöscher sind erhältlich.
- Virenschutz, Spamfilter und Firewalls werden verwendet.

10.3 Software

Sicherungsstrategie:

- Jede Nacht wird ein vollständiges Backup der Daten auf einem unabhängigen Backup-System durchgeführt. Dank dieser Sicherung kann der Auftragnehmer im Notfall sofort wieder den Betrieb aufnehmen.
- Jede Woche werden alle Backups des zentralen Servers in einem Safe aufbewahrt.
- Backups können für jeden der letzten sieben bis 60 Tage präzise wiederhergestellt werden, je nachdem, wie kritisch das System ist.

11. BELASTBARKEIT VON VERARBEITUNGSSYSTEMEN UND -DIENSTEN

Der DSGVO Abschnitt 32 definiert die Belastbarkeit von Verarbeitungssystemen und -diensten als Voraussetzung für die Gewährleistung der Verarbeitungssicherheit. Dieser Abschnitt beschreibt die Maßnahmen von Tivian zur Sicherstellung der Ausfallsicherheit von Verarbeitungssystemen und -diensten.

11.1 Rechenzentren

Die Rechenzentren von Tivian gewährleisten die Ausfallsicherheit durch eine Vielzahl von Maßnahmen. Dazu gehören der Einsatz skalierbarer Netzwerkkomponenten, on the fly anschließbare Ressourcen, fehlertolerante Hardwarekomponenten, modernste Netzwerkinfrastruktur, Bereitstellung von ausreichend Personal und permanente Überwachung des Betriebszustandes.

11.2 Geschäftsstellen

Die Büros von Tivian sichern die Belastbarkeit durch eine Vielzahl von Maßnahmen. Dazu gehören der Einsatz skalierbarer Netzwerkkomponenten, eine vorausschauende Bedarfsplanung, die Bereitstellung von ausreichend Personal und die permanente Überwachung des Betriebszustandes.

11.3 Software

Die Software von Tivian stellt die Ausfallsicherheit durch eine Vielzahl von Maßnahmen sicher. Dazu gehören der Einsatz skalierbarer Datenbanken, modernes Coding, agile Entwicklung, Einsatz leistungsfähiger Softwarekomponenten.

12. TRENNUNGSGEBOT

Dieser Abschnitt beschreibt die Maßnahmen von Tivian, die sicherstellen, dass Daten, die für verschiedene Zwecke gesammelt wurden, getrennt verarbeitet werden.

12.1 Software

12.1.1 EFS

Trennung der personenbezogenen Daten an verschiedenen Speicherorten durch organisatorische und räumliche Trennung (Mandantenfähigkeit). Die Datenverarbeitungssysteme für besonders sensible Daten sind physisch und organisatorisch getrennt. Testcomputer sind physisch von Live-Systemen getrennt und unterliegen separaten Sicherheitseinschränkungen. Spiegel des Live-Systems werden zu Testzwecken bei jeder Änderung der Installationen erstellt. Alle personenbezogenen Daten werden vor der Durchführung der Tests anonymisiert.

12.1.2 QUBIE

QUBIE FÜR MS TEAMS

IN QUBIE für MS TEAMS erfolgt die Trennung der personenbezogenen Daten logisch durch ID-Filterung (Mandantenfähigkeit). Daten unterschiedlicher Mandaten werden logisch in den Datenbanken getrennt. Testinstanzen sind von Live-Systemen getrennt und unterliegen separaten Sicherheitseinschränkungen. Für Testzwecke stehen separate Instanzen für Staging und Penetrationstests zur Verfügung. Alle personenbezogenen Daten werden vor der Durchführung der Tests anonymisiert.

Qubie für Web

Hier gelten die gleichen Bedingungen wie für EFS.

13. PSEUDONYMISIERUNG UND VERSCHLÜSSELUNG PERSONENBEZOGENER DATEN

Der Abschnitt 32 der DSGVO definiert die Pseudonymisierung und Verschlüsselung von Daten als Voraussetzung für die Sicherheit der Verarbeitung. Dieser Abschnitt beschreibt die Maßnahmen von Tivian zur Pseudonymisierung und Verschlüsselung von Daten.

13.1 Rechenzentren

Die Tivian Rechenzentren kommunizieren verschlüsselt mit den Kunden unter Verwendung moderner Transportverschlüsselung. Backups werden verschlüsselt gespeichert.

13.2 Software

Tivians Software speichert Passwörter verschlüsselt (hashed). Die Daten werden im System mittels eines Skripts anonymisiert. Alle Datenfelder (z.B. E-Mail-Adresse, Vorname / Nachname) werden durch generische Informationen ersetzt. (Mittels Überschreiben durch ein Skript in der Datenbank).

14. AUFBEWAHRUNG UND LÖSCHUNG

Dieser Abschnitt beschreibt die Aufbewahrungszeit von Tivian für Daten, hierunter personenbezogene Daten, die von Tivian im Auftrag seiner Kunden verarbeitet werden. Weiterhin werden die Routinen zum Löschen von Daten definiert.

14.1 Rechenzentren

Die Rechenzentren bewahren die Daten für die Dauer eines bestehenden Vertragsverhältnisses, zwischen Tivian und seinen Kunden, auf. Nachdem ein Kundenvertrag endet, terminiert Tivian die Kundeninstallation und -datenbank.

14.2 Software

14.2.1 Standardeinstellung: Aufbewahrungszeit für persönliche Daten, die der Tivian-Kunde festgelegt hat.

Tivian Software wird den Kunden von Tivian zur Verfügung gestellt, damit sie Umfragen und Fragebögen erstellen können, die den Befragten zur Verfügung gestellt werden. Bei der Erstellung einer Umfrage oder eines Fragebogens legt der Kunde die Aufbewahrungszeit für die betreffenden Daten fest. Die Daten werden nach Ablauf der Aufbewahrungszeit automatisch anonymisiert. Die im Backup gespeicherten Daten werden spätestens 60 Tage nach der Löschung der Originaldaten gelöscht (überschrieben). Das Löschen erfolgt in Übereinstimmung mit den aktuellen Löschroutinen von Tivian.

14.2.2 Optionale Einstellung: Aufbewahrungsdauer nicht vom Kunden definiert

Sollte der Kunde keine Aufbewahrungsfrist festlegen, werden die betreffenden Daten bis zur manuellen Löschung oder bis zur Beendigung des Vertrages zwischen Tivian und dem Kunden aufbewahrt. Die im Backup gespeicherten Daten werden spätestens 60 Tage nach der Löschung der Originaldaten gelöscht (überschrieben). Das Löschen erfolgt in Übereinstimmung mit den aktuellen Löschroutinen von Tivian.

14.2.3 QUIBIE

Qubie für MS Teams

QUBIE für MS TEAMS speichert Daten für die Laufzeit der Nutzung der App. Eine unwiederbringliche Löschung der Daten erfolgt im Moment der Deinstallation der App.

Qubie für Web

Hier gelten die gleichen Bedingungen wie für die Tivian Software Standard- und Optionale Einstellung.

15. STÖRFALLMANAGEMENT

Die Meldung von Verstößen ist ein Pflichtthema zwischen Tivian und seinen Kunden. Ein Datenverstoß, der ein Risiko für die Rechte und Freiheiten des Einzelnen darstellt, wird nach geltendem Recht behandelt. Die Meldung eines Verstoßes muss innerhalb von 72 Stunden nach Bekanntwerden des Verstoßes erfolgen. Tivian wird seine Kunden, die Controller, "ohne unangemessene Verzögerung" benachrichtigen, nachdem Tivian von einem Datenverstoß erfahren hat.

Während die obige Erklärung nur die Anforderung einer Benachrichtigung innerhalb von 72 Stunden nach der Identifizierung eines Datenverstoßes angibt und nicht besagt, dass Tivian ein Incident Response Programm haben muss, ist es selbstverständlich, dass Tivian in der Lage ist, einen Verstoß innerhalb ihrer Netzwerke, Systeme oder Anwendungen schnell zu erkennen, um die 72-Stunden-Benachrichtigungsanforderung zu erfüllen.

15.1 Erkennung

Um einen Angriff oder ein sicherheitsrelevantes Ereignis erkennen zu können, hat Tivian verschiedene Überwachungs- und Kontrollmaßnahmen eingerichtet, die im Falle eines Angriffs alarmieren. Tivian geht dann sofort gegen einen Gegner im Netzwerk vor, insbesondere wenn eine Früherkennung die Möglichkeit eröffnet, den Angriff zu stoppen, bevor er Schaden anrichten kann.

Das Response-Framework von Tivian bietet die Möglichkeit, schnell zu analysieren, auf was die Angreifer zugegriffen oder kopiert haben. Dies trägt wesentlich dazu bei, die potenziellen Auswirkungen auf den Kunden und vor allem auf die betroffenen Personen zu minimieren.

15.2 Kommunikation

Neben den oben genannten Erkennungsanforderungen wurde auch die interne Kommunikation zwischen den betroffenen Abteilungen und Gruppen vereinbart, um eine reibungslose Reaktion auf einen Vorfall oder eine Verletzung zu gewährleisten. Ein Kommunikationsplan legt fest, wer berechtigt ist, mit externen Stellen und Kunden zu sprechen.

Tivian testet das Reaktionsprogramm routinemäßig, um die Effektivität und rechtzeitige Benachrichtigung sicherzustellen und die gesetzlichen Anforderungen und Fristen einzuhalten.

15.3 Benachrichtigung

Um das Risiko zu verringern, keine vollständige oder gründliche Rückmeldung zu erhalten, hat Tivian ein Incident Response Programm entwickelt, Richtlinien und Prozeduren erstellt und sichergestellt, dass jeder das Programm kennt.

Das Datenverzeichnis von Tivian hilft zu wissen, wo die Daten einer Person gespeichert sind, so dass das Incident Response Team schnell die möglichen Auswirkungen eines Sicherheitsereignisses auf ein System oder eine Anwendung kennt. Der genaue Datenbestand von Tivian ist entscheidend, um bei eventuellen individuellen Benachrichtigungen im Falle eines Verstoßes zu helfen, indem er darauf hinweist, welcher Kunde betroffen ist, und den Prozess zur Benachrichtigung des Kunden im Falle eines Verstoßes unterstützt. Die dann beginnende Kommunikation mit dem Kunden beschreibt die Art des Verstoßes und Empfehlungen zur Minderung möglicher negativer Auswirkungen.

16. INTERNE KONTROLLE

Dieser Abschnitt beschreibt die Maßnahmen von Tivian, die sicherstellen, dass seine Richtlinien, einschließlich der in diesem Dokument beschriebenen Richtlinien, durch die Organisation eingehalten werden, und den Prozess zur regelmäßigen Überprüfung, Bewertung und Bewertung der Wirksamkeit dieser technischen und organisatorischen Maßnahmen.

16.1 Überwachung

16.1.1 EFS

- Tivian überwacht mehr als 1000 Hosts und mehr als 4500 Dienste von dedizierten und gemeinsam genutzten Instanzen.
- Jede Minute werden ca. 1000 Prüfungen durchgeführt und gemeldet.
- Alarme werden rund um die Uhr ausgegeben.
- Alarme werden sofort von erfahrenen Systemadministratoren der Tivian aufgenommen.
- Das Überwachungssystem ist redundant ausgelegt und wird von einem externen Überwachungstool überwacht.
- Ein weiteres viertes Monitoring-System gibt Einblicke in die Performance der Plattformen aus aller Welt.

16.2 Sicherheitsaudits

Regelmäßige Audits der Hosting-Umgebung sind Teil der ISO 27001-Zertifizierungsanforderungen.

Neben den Audits für die Rechenzentren hat sich Tivian verschiedenen Ad-hoc-Audits unterzogen, die von einigen unserer Kunden durchgeführt wurden, die eine Verifizierung für höchste Sicherheitsstandards benötigen. Tivian führt auch regelmäßig Selbstaudits durch.

16.2.1 Sicherheitsüberprüfung

Um die hohen Anforderungen an Sicherheit der eigenen Software Plattformen zu erfüllen, beauftragt Tivian Sicherheitsexperten von Drittanbietern mit der Durchführung von Sicherheitstests für unsere Plattformen. Ziel ist es, kontinuierliche Sicherheit in Bezug auf aktuelle und kommende Technologien und ständige, inkrementelle Entwicklungsarbeit zu gewährleisten.

Die Tests werden als Anwendungspenetrationstests mit den folgenden Schwerpunkten durchgeführt:

- OWASP Top 10
- Cross-Site-Scripting (XSS)
- Session-Fixierung
- Schwache oder fehlende Authentifizierung
- Versteckte Parameter
- Durchsuchen von Verzeichnissen
- SQL-Injektion

16.2.2 Regelmäßige Sicherheitsprüfungen

- Ein bis zwei Anwendungstests des Dienstes werden jedes Jahr durchgeführt.
- Ein Infrastrukturtest unserer Hosting-Umgebung jedes Jahr - dies wird im Abschnitt Hosting näher erläutert.

16.2.3 Ergebnisse der Audits

- Ergebnisse von Applikations- und Infrastrukturtests werden dem Produktmanagement präsentiert.
- Jede kritische Schwachstelle wird zur Behebung an die Entwicklung geschickt.
- Die Betriebsabteilung kümmert sich um die Infrastruktur und die Serverumgebung.
- Probleme im Zusammenhang mit der Tivian-Serverumgebung werden durch den IT-Betrieb behoben.
- Schwachstellen in der kommerziellen Website www.tivian.com werden von Entwicklern behoben, die für das Design unserer Front-End-Webseiten verantwortlich sind.