[TIVIAN]

Technische und Organisatorische Maßnahmen

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: Dörthe Minde
Dokumentversion: 2.0
Vertraulichkeitsklassifizierung: Öffentlich
Veröffentlichungsdatum: Januar 2024

[TIVIAN]

Inhaltsverzeichnis

1. EINFÜHRUNG

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

Personenbezogene Daten der Kunden von Tivian und der Befragten, die im Rahmen des Feedback-Prozesses erhoben und verarbeitet werden, werden in Übereinstimmung mit dem Kundenvertrag, der jeweils abgeschlossenen Auftragsverarbeitungsvereinbarung, und den Beschreibungen in diesem Dokument verarbeitet.

1.1 Software as a Service

Tivian stellt seinen Kunden seine Softwareplattformen für das Feedbackmanagement als Software as a Service (SaaS) zur Verfügung, wie in diesem Dokument beschrieben.

In diesem Dokument erläutern die Unterabschnitte "**Softwareplattformen**" im jeweiligen Abschnitt, wie der Schutz personenbezogener Daten softwareseitig von Tivian gewährleistet wird.

1.2 Tivian Rechenzentren

Tivian stellt seinen Kunden seine Softwareplattformen über externe Rechenzentren zur Verfügung. Hierfür kommen Rechenzentren in Deutschland, der EU und/oder den USA zum Einsatz. Der konkrete Standort des eingesetzten Rechenzentrums richtet sich nach der Vereinbarung in dem individuellen Vertrag zwischen dem Kunden und Tivian.

In diesem Dokument erläutern die Unterabschnitte "**Rechenzentren**", wie der Schutz personenbezogener Daten in der Software von Tivian in Übereinstimmung mit den in den Rechenzentren implementierten Standards gewährleistet wird.

1.2.1 Datagroup

Verarbeitung in Softwareplattformen im Rechenzentrum in Frankfurt am Main/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 in Frankfurt am Main/Deutschland gehostet. Die DATAGROUP wurde wie folgt zertifiziert:

- gemäß ISO/IEC 27001:2017 (Zertifikat-ID: DSC.1369.02.2024, https://www.datenschutz-cert.de/fileadmin/uploads/tx_dscertcertlist/Datagroup_ISO27001_Urkunde_20240228_digital.pdf)
- gemäß ISO/IEC 20000-1:2018 (Zertifikat-ID: 12 410 44148/01 TMS, dieses Zertifikat ist auf Anfrage erhältlich)

1.2.2 Amazon Web Services (AWS)

Verarbeitung in Softwareplattformen in Rechenzentren in Frankfurt am Main, Deutschland/EU - 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 AWS kontrollierten Rechenzentrum grundsätzlich in Frankfurt am Main, sowie - nach Vereinbarung mit dem Kunden - in anderen Standorten in der Europäischen Union gehostet.

Verarbeitung in Softwareplattformen in Rechenzentren in den USA - Falls mit dem Kunden vertraglich vereinbart, werden personenbezogene Daten der Kunden von Tivian und der Befragten, die im Rahmen des Feedback- und Kommunikationsprozesses gesammelt und verarbeitet werden, auf externen Servern im von AWS kontrollierten Rechenzentrum grundsätzlich in North Virginia, sowie in anderen Standorten in den USA gehostet.

AWS ist im Besitz diverser Zertifikate und Testate.

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

1.2.3 Microsoft

Verarbeitung in Softwareplattformen in Rechenzentren in der EU – Wenn dies vertraglich vereinbart ist, werden personenbezogene Daten der Kunden von Tivian und der Befragten, die im Rahmen des Feedback-Prozesses gesammelt und verarbeitet werden, auf externen Servern in von Microsoft verwalteten Rechenzentren innerhalb der EU 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://servicetrust.microsoft.com/viewpage/ISOIEC abrufen.

- Microsoft Azure verfügt über Sicherheitsmechanismen, die als Hilfe bei der Verwaltung und Überwachung von Azure-Clouddiensten und virtuellen Azure-Computern dienen. Microsoft stellt aktuelle Informationen online zur Verfügung: https://docs.microsoft.com/azure/security/security-management-and-monitoring-overview

1.2.4 Betreiber der Rechenzentren

Unternehmen	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 - Personenbezogene Daten von Mitarbeitern, Kunden, Besuchern und Lieferanten von Tivian werden gemäß Tivians internen Richtlinien zum Datenschutz verarbeitet.

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

Weitere Informationen zur Struktur des Datenspeicherungsprozesses sowie Kontaktinformationen zu dem Datenschutzbeauftragten der Tivian Gruppe finden Sie im Tivian Trust Center unter https://www.tivian.com/de/trust-center .

Name der Tivian Organisation	Adressen der Geschäftsstellen	Land
Tivian XI GmbH	Christophstr. 15-17 50670 Köln	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 VIIs gate 2 0161 Oslo	Norway

1.4 Compliance mit der Datenschutzgrundverordnung (DSGVO)

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.

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 Art. 5, 17, 19, 24, 25, 28, 29, 32, 33, 35 und 39 der DSGVO.

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

1.4.1 Datagroup

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 Kapazitäten 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 AWS

AWS 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 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/ EU – AWS

2.1.1.1 Einführung

Für das Gebäude des Rechenzentrums gelten die Standards der BSI / ISO 27001 Zertifizierung, entsprechend verfügt es über ein physisches Zugangsberechtigungskonzept, das vor Ort einsehbar ist. Zur Steuerung des physischen Zugangs zu den Hochsicherheitsbereichen des Rechenzentrums wurde ein zweistufiges Zutrittssystem installiert.

2.1.1.2 Mitarbeiterzugang zum Rechenzentrum

Der physische Zugang erfolgt auf Antrag des Teamleiters und die Gegenkontrolle durch die Geschäftsführung des jeweiligen Cloud Providers. 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.

2.1.1.3 Zugang von Dritten zum Rechenzentrum

Der Zugang von Dritten muss von autorisierten Cloud Provider Mitarbeitern angefragt werden, die auch eine gültige geschäftliche Legitimation für diesen Zugang vorweisen müssen. Diese Anfrage wird basierend auf dem Prinzip geringstmöglicher Berechtigungen stattgegeben, 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 Frankfurt, Deutschland – Datagroup

Für das Gebäude des Rechenzentrums gelten die Standards der BSI / ISO 27001 Zertifizierung, entsprechend verfügt es über ein physisches Zugangsberechtigungskonzept, das vor Ort einsehbar ist. Zur Steuerung des physischen Zugangs zu den Hochsicherheitsbereichen des Rechenzentrums wurde ein zweistufiges Zutrittssystem installiert.

2.1.3 Rechenzentren in den USA (grundsätzlich in North Virginia, USA) – AWS

2.1.3.1 Einführung

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

Die Alarme sind direkt mit den örtlichen Feuerwehr- und Polizeibehörden verbunden. AWS-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/Ausweis 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.

2.1.3.2 Mitarbeiterzugang zum Rechenzentrum

Nur autorisiertes AWS-Personal erhält Zugang zu den physischen Rechenzentren. Alle Mitarbeiter, die Zugang zu einem Rechenzentrum benötigen, müssen zunächst eine Anfrage auf Zugang stellen und eine gültige geschäftliche Legitimation vorlegen. Dieser Anfrage wird basierend auf dem Prinzip geringstmöglicher Berechtigungen stattgegeben, 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.

2.1.3.3 Zugang von Dritten zum Rechenzentrum

Der Zugang von Dritten muss von autorisierten AWS-Mitarbeitern angefragt werden, die auch eine gültige geschäftliche Legitimation für diesen Zugang vorlegen müssen. Dieser Anfrage wird basierend auf dem Prinzip geringstmöglicher Berechtigungen stattgegeben, d. h. die Besucher 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.

2.1.4 Rechenzentren in der EU (grundsätzlich in den Niederlanden und Irland) – Microsoft

Microsoft entwickelt, erstellt und betreibt Rechenzentren so, dass der physische Zugriff auf die Bereiche, in denen personenbezogene Daten gespeichert sind, streng kontrolliert wird. Microsoft befasst sich mit der Entwicklung, der Erstellung und dem Betrieb der Einrichtungen, die Azure unterstützen, und bemüht sich stets 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 Anlagengrenze, 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 - Alle Büros

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

- 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/EU – AWS

Das 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 Frankfurt, Deutschland – Datagroup

Die Benutzerverwaltung wird über VPN 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.

3.1.3 Rechenzentrum in den USA (grundsätzlich in North Virginia, USA) – AWS

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 AWS 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 eingesetzt.

Zusätzlich hat AWS Netzwerkgeräte für die Verwaltung der Schnittstellenkommunikation mit Internet Service Providern (ISPs, Internetdienstanbietern) implementiert. 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.

3.1.4 Rechenzentren in der EU (grundsätzlich in den Niederlanden und Irland) – Microsoft

Microsofts Azure Security hat konkrete Anforderungen für die aktive Überwachung festgesetzt. 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 - Alle Büros

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

3.2.1 Geräteverschlüsselung

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

3.2.2 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"). Sie sind außerdem verpflichtet, ihre Passwörter geheim zu halten und nicht an Dritte weiterzugeben, auch nicht zu Supportzwecken. Es gibt Passwortvorschriften, die technisch (Systemkonfiguration) und organisatorisch (Passwortrichtlinie) umgesetzt sind. Nach diesen Vorschriften müssen alle Passwörter die definierten Mindestanforderungen erfüllen.

3.3 Softwareplattformen

3.3.1 Passwort

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. Im Gegensatz dazu wird bei Passwörtern zwischen Groß- und Kleinschreibung unterschieden.

DXI 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.

3.3.2 Rechte- und Rollenkonzept

Power-User oder Administratoren-Accounts werden in den Softwareplattformen in 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 den Softwareplattformen repliziert werden. Über eine API gesteuerte Zuweisung zu den Teams in den Softwareplattformen kann dann die Rechtesituation automatisiert gespiegelt werden.

3.3.3 Schwachstellenmanagement

Schwachstellen-Scans werden mit dem Netzwerk- und Schwachstellen-Scanner Nessus 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 umgesetzt 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 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.

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/EU – AWS

Die Datenübertragung wird protokolliert und die Protokolle werden kontinuierlich ausgewertet. Jede Entfernung von Datenträgern wird ebenfalls protokolliert und die Protokolle werden ausgewertet. Die Protokollierung und 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)

4.1.2 Rechenzentrum in Frankfurt, Deutschland – Datagroup

Es besteht ein definierter und dokumentierter Change-Management Prozess. Dieser Prozess stellt sicher, dass notwendige oder gewünschte Änderungen an der IT-Infrastruktur anhand eines standardisierten und kontrollierten Verfahrens erfolgen.

- Die Aktivitäten des Administrators auf einem Server werden protokolliert. Die Nachvollziehbarkeit von Eingabevorgängen wird über die restriktive Vergabe von Zugriffsrechten erreicht. Durch Beachtung des Minimalprinzips bei der Vergabe von Zugriffsrechten wird der Kreis zugriffsberechtigter Personen so klein wie möglich gehalten. Es ist gewährleistet, dass den Benutzern das Eingeben, Ändern oder Löschen von Daten nur entsprechend den für sie gültigen Berechtigungen möglich ist.
- Die Eingabe von personenbezogenen Daten für einen Kunden erfolgt durch DATAGROUP in der Regel nur im Rahmen der Benutzerregistrierung im Active Directory. Darüber hinaus kann es im Rahmen der allgemeinen administrativen

Tätigkeiten zu einer Kenntnisnahme von personenbezogenen Daten kommen. Daher werden alle ausgeführten Tätigkeiten mit Hilfe eines ITSM-Werkzeugs und über korrespondierende Tickets dokumentiert und können nachvollzogen werden.
- Grundsätzlich werden Aufträge eines Kunden über definierte Schnittstellen entgegengenommen und durch ein Ticket-System erfasst. Die weitere Bearbeitung wird zu jedem einzelnen Ticket dokumentiert.
- Teilweise werden Zugriffe auf besonders schützenswerte Daten protokolliert. Je nach Art des Protokolls werden Benutzerkennung, Ursprung der Anfrage (IP-Adresse), Rechnername, Datum und Uhrzeit aufgezeichnet
- Teilweise werden erstellte Protokolle in anonymisierter Form stichprobenartig ausgewertet. Sofern sich aufgrund der Auswertung der Verdacht eines Datenmissbrauchs ergibt, werden in Abstimmung mit dem Betriebsrat – soweit vorhanden – und dem Datenschutzbeauftragten weitere geeignete Schritte eingeleitet.
- Die Systemaktivität wird über das Ereignisprotokoll des verwendeten Betriebssystems aufgezeichnet. Protokolldateien werden grundsätzlich in geschützten Systemverzeichnissen gespeichert und entsprechend dem geltenden Datensicherungskonzept gesichert.

4.1.3 Rechenzentren in den USA (grundsätzlich in North Virginia, USA) – AWS

Hier werden die gleichen Maßnahmen angewendet wie in Frankfurt am Main Deutschland/EU - AWS.

4.1.4 Rechenzentrum in der EU (grundsätzlich in den Niederlanden und Irland) – Microsoft

Für die Verwaltung und den Betrieb des Azure-Produktionsnetzwerks sind die Betriebsteams von Azure und Azure SQL-Datenbank gemeinsam zuständig. Die Teams verwenden mehrere Tools zur Überwachung der System- und Anwendungsleistung in der Umgebung. Darüber hinaus verwenden Sie entsprechende Tools, um Netzwerkgeräte, Server, Dienste und Anwendungsprozesse zu überwachen. Um die sichere Ausführung der Dienste in der Azure-Umgebung zu gewährleisten, implementieren die Betriebsteams mehrere Ebenen der Überwachung, Protokollierung und Berichterstellung.

Der Microsoft Monitoring Agent (MMA) erfasst in erster Linie Überwachungs- und Diagnoseprotokollinformationen aus vielen Quellen, einschließlich des Fabric Controller (FC) und des Stammbetriebssystems (BS), und schreibt sie in Protokolldateien. Der Agent überträgt schließlich eine Teilmenge der Informationen in Digestform in ein vorkonfiguriertes Azure Storage-Konto. Der eigenständige Überwachungs- und Diagnosedienst liest verschiedene Überwachungs- und Diagnoseprotokolldaten und fasst die Informationen zusammen. Der Überwachungs- und Diagnosedienst schreibt die Informationen in ein integriertes Protokoll. Azure verwendet das benutzerdefinierte Azure Security Monitoring, eine Erweiterung des Azure-Überwachungssystems. Es verfügt über Komponenten, die sicherheitsrelevante Ereignisse an verschiedenen Stellen in der Plattform beobachten, analysieren und melden.

Microsoft stellt aktuelle Informationen online zur Verfügung**:** https://learn.microsoft.com/de-de/azure/security/fundamentals/infrastructure-operations

4.2 Softwareplattformen

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.

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. Zusätzlich kann es dadurch geprüft und festgelegt werden, an welchen Stellen personenbezogene Daten mit Hilfe von Datenübertragungsgeräten übertragen werden sollen.

5.1 Rechenzentren

5.1.1 Rechenzentrum in Frankfurt am Main, Deutschland/EU – AWS

5.1.1.1 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 DXI-Umfragen gehostet werden, erfolgt mittels TLS1.3-Verschlüsselung (PCI-Compliance).

5.1.1.2 Verschlüsselung für ruhende Daten („encryption at rest“)

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

AWS verfügt über schriftliche Bestimmungen über die Verwendung von Datenträgern, einschließlich der Erstellung von Kopien von Datenträgern zur Verwendung als Backup. Diese sind z.B.:

- Derartige Zugriffsrechte werden nur Administratoren gewährt.
- Jede Entfernung von Datenträgern wird protokolliert.
- Alle Datenübertragungen werden protokolliert und die Protokolle andauernd ausgewertet.

5.1.2 Rechenzentrum in Frankfurt am Main/Deutschland – Datagroup

DATAGROUP ist mit ihrem Standort Frankfurt am Main (Rechenzentrum) ISO-27001-zertifiziert und erfüllt hierdurch auch die Bestimmungen der DSGVO. Weitere Informationen können Sie unter https://www.datagroup.de/zertifizierungen-datagroup-stuttgart entnehmen.

5.1.3 Rechenzentren in den USA (grundsätzlich in North Virginia, USA) – AWS

Die Maßnahmen entsprechen den Maßnahmen im Rechenzentrum Frankfurt am Main/Deutschland/EU – AWS.

5.1.4 Rechenzentren in der EU (grundsätzlich in den Niederlanden und Irland) – Microsoft

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

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

Microsoft verwendet das Transport Layer Security-Protokoll (TLS1.3) zum Schutz von Daten bei der Übertragung zwischen den Clouddiensten und Kunden. Die Microsoft-Rechenzentren verwenden 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.

5.1.4.2 Verschlüsselung für ruhende Daten („encryption at rest“)

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 bietet zudem eine Verschlüsselung zum Schutz von Azure SQL-Datenbank, Azure Cosmos DB und Azure Data Lake. Eine ausführliche Erörterung zur Verschlüsselung ruhender Daten in Azure finden Sie unter Azure-Datenverschlüsselung ruhender Daten.

5.2 Softwareplattformen

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

5.3 Geschäftsstellen – Alle Büros

Der Einsatz von betriebsfremden mobilen externen Datenträgern (z.B. USB-Sticks) ist untersagt. Die Verwendung von mobilen Speichermedien ist nur nach vorheriger schriftlicher Zustimmung zulässig für bestimmte Daten. Personenbezogene oder sicherheitsrelevante Daten gehören jedoch nicht zu dieser Kategorie. Alle mobilen Arbeitsplatzrechner sind vollständig verschlüsselt. Zudem ist die E-Mail-Kommunikation und der Zugriff auf Dokumente ebenfalls stets verschlüsselt.

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/EU – AWS

Die Mitarbeiter des Rechenzentrums von AWS, 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 Frankfurt, Deutschland – Datagroup

Die Mitarbeiter des Rechenzentrums von DATAGROUP, 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 folgenden Maßnahmen werden getroffen:

- Die Nachvollziehbarkeit von Eingabevorgängen wird über die restriktive Vergabe von Zugriffsrechten erreicht. Durch Beachtung des Minimalprinzips bei der Vergabe von Zugriffsrechten wird der Kreis zugriffsberechtigter Personen so klein wie möglich gehalten. Es ist gewährleistet, dass den Benutzern das Eingeben, Ändern oder Löschen von Daten nur entsprechend den für sie gültigen Berechtigungen möglich ist.
- Die Aktivitäten des Administrators auf einem Server werden grundsätzlich protokolliert.
- Die Eingabe von personenbezogenen Daten für einen Kunden erfolgt durch DATAGROUP in der Regel nur im Rahmen der Benutzerregistrierung im Active Directory. Darüber hinaus kann es im Rahmen der allgemeinen administrativen Tätigkeiten zu einer Kenntnisnahme von personenbezogenen Daten kommen. Daher werden alle ausgeführten Tätigkeiten mit Hilfe eines ITSM-Werkzeugs und über korrespondierende Tickets dokumentiert und können nachvollzogen werden.
- Grundsätzlich werden Aufträge eines Kunden über definierte Schnittstellen entgegengenommen und durch ein Ticket-System erfasst. Die weitere Bearbeitung wird zu jedem einzelnen Ticket dokumentiert.
- Teilweise werden Zugriffe auf besonders schützenswerte Daten protokolliert. Je nach Art des Protokolls werden Benutzerkennung, Ursprung der Anfrage (IP-Adresse), Rechnername, Datum und Uhrzeit aufgezeichnet.
- Teilweise werden erstellte Protokolle in anonymisierter Form stichprobenartig ausgewertet. Sofern sich aufgrund der Auswertung der Verdacht eines Datenmissbrauchs ergibt, werden in Abstimmung mit dem Betriebsrat – soweit vorhanden – und dem Datenschutzbeauftragten weitere geeignete Schritte eingeleitet.
- Die Systemaktivität wird über das Ereignisprotokoll des verwendeten Betriebssystems aufgezeichnet.
- Protokolldateien werden grundsätzlich in geschützten Systemverzeichnissen gespeichert und entsprechend dem geltenden Datensicherungskonzept gesichert.

6.1.3 Rechenzentrum in den USA (grundsätzlich in North Virginia, USA) – AWS

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

6.1.4 Rechenzentren in der EU (grundsätzlich in den Niederlanden und Irland) – Microsoft

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 protokolliert. Die daraus resultierenden Protokolle werden stichprobenartig (Stichproben) und immer dann, wenn dies durch Ereignisse gerechtfertigt ist, überprüft.

Außerdem setzt Microsoft eine Kombination aus präventiven, defensiven und reaktiven Kontrollen ein, einschließlich der folgenden Mechanismen, um sich vor nicht autorisierten Entwickler- und Verwaltungsaktivitäten zu schützen: Strenge Zugriffskontrollen für sensible Daten, einschließlich der Anforderung einer mehrstufigen Authentifizierung, Kombinationen von Kontrollen, die die unabhängige Erkennung bösartiger Aktivitäten verbessern, mehrere Ebenen der Überwachung, Protokollierung und Berichterstattung, Just-in-Time-Zugriff, um die Anzahl der Personen zu minimieren, die dauerhaft oder fortlaufend über administrative Berechtigungen verfügen.

6.2 Geschäftsstellen – Alle Büros

Alle Tivian-Büros halten sich an die Anforderungen der IT-Governance-Richtlinie, hierunter Definition von Sicherheitszonen.

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 von Tivian 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 Softwareplattformen

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 Softwareplattformen 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.

7. AUFTRAGSKONTROLLE

7.1 Einführung

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.

Die folgenden Maßnahmen sind implementiert und zielen auf die effiziente Realisierung des vorgenannten Zwecks:

Organisatorische Maßnahmen

- Vorherige Prüfung der vom Subunternehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Prüfung und Sicherstellung der mit den Kunden vereinbarten Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit bei beauftragten Subunternehmen.
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
- Weisungen an Subunternehmen werden in Form von E-Mails oder anderen elektronischen Systemen, die ein angemessenes Schutzniveau bieten, dokumentiert
- Auswahl des Dienstleisters unter Sorgfaltsgesichtspunkten
- Prüfung und Dokumentation der beim Dienstleister getroffenen Sicherheitsmaßnahmen
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Subunternehmer
- Eindeutige Vertragsgestaltung

Weitere technische Maßnahmen

- Dokumentierte Löschung von Kundendaten, auf Wunsch des Kunden nach BSI-Vorgaben
- Regelmäßiges Einspielen von Updates für alle Betriebssysteme und Anwendungen
- Betriebssystem-Updates wöchentlich
- Updates für interne Anwendungen von Tivian monatlich bei Verfügbarkeit
- Regelmäßiges Einspielen von Updates für Kunden betriebene Anwendungen, außerplanmäßig bei bekannten Sicherheitslücken
- Detailliertes Monitoring aller Serversysteme zur Erkennung von Störungen

7.2 Rechenzentren

Tivian hat die jeweiligen Sicherheitskonzepte aller Rechenzentren geprüft und Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO mit allen Rechenzentrenprovidern geschlossen. Zur Sicherstellung des Datenschutzes bestehen schriftliche Verträge mit den Rechenzentren.

Zu keiner Zeit verarbeiten die Cloudprovider Datagroup, Microsoft oder AWS außer der Hosting-Dienstleistungen weiter personenbezogene Daten ohne einen expliziten Auftrag. Alle Mitarbeiter unterliegen Verschwiegenheitserklärungen (NDAs).

7.3 Geschäftsstellen – Alle Büros

Alle Mitarbeiter von Tivian sind an die internen Richtlinien von Tivian gebunden und erhalten regelmäßige Schulungen zum Schutz personenbezogener Daten. Die Bewertung von Inhalten in Auftragsverarbeitungsverträgen oder der Anweisungen des Kunden für die Datenverarbeitung 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.

7.4 Softwareplattformen

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

8. VERTRAULICHKEITSKONTROLLE

8.1 Rechenzentren

Die Rechenzentren, die für die Speicherung und den technischen Betrieb der Daten von Tivian zuständig sind, haben keinen Zugriff auf die Daten. Zudem verfügen die Betreiber von Rechenzentren über 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 in verschlüsselter Form sicher gespeichert und dokumentiert und unterliegen strengen Zugriffsregeln.

8.2 Geschäftsstellen – Alle Büros

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 Softwareplattformen

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

9. INTEGRITÄTSKONTROLLE

Nach Art.32 Abs.1 lit. b) DSGVO sind geeignete technische und organisatorische Maßnahmen zu treffen, um die Integrität der Systeme und Dienste und damit die Unversehrtheit der Daten zu gewährleisten.

9.1 Rechenzentren

Die von Tivian beauftragten Rechenzentren 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 – Alle Büros

Die Tivian-Büros gewährleisten Integrität durch eine Vielzahl von Maßnahmen. Dazu gehören die Verschlüsselung von Medien, starke Zugriffskontrollen sowie die Verwendung von verschlüsselter Kommunikation: Sowohl erfolgt die Kommunikation zwischen Endgeräten und Office-Cloudumgebung generell verschlüsselt, als auch ist der Übertragungsweg (WLAN des Bürovermieters) ebenfalls verschlüsselt.

9.3 Softwareplattformen

Die Integrität der Software von Tivian wird durch eine Vielzahl von Maßnahmen sichergestellt. Dies beinhaltet die Sicherstellung der Integrität der Programmmodule selbst 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. WEITERGABEKONTROLLE

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung, Weitergabe oder Speicherung auf Datenträgern nicht unbefugt während des Transportweges gelesen, kopiert, verändert oder entfernt werden können. Ferner kann es stets überprüft werden, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- **Verschlüsselung von E-Mail und E-Mail-Anhängen**

Die Übertragung von E-Mails erfolgt ausschließlich auf einem verschlüsselten Transportweg (SSL/TLS 1.3).

- **Verschlüsselung des Speichermediums von Notebooks**

Die Festplatten der Notebooks der Belegschaft von Tivian sind standardmäßig mit dem Microsoft-Windows Bitlocker (256 Bit Advanced Encryption Standard - AES 256) verschlüsselt.

- **Gesicherter Dateien-Transfer**

Sofern kein anderer Übertragungsweg verfügbar ist, erfolgen Dateien-Transfers ausschließlich über SFTP (Secured File Transfer Protocol).

- **Gesicherter Datentransport**

Der Datentransport innerhalb der Unternehmensumgebung (Azure Active Directory) erfolgt ausschließlich verschlüsselt (SSL).

- **Elektronische Signatur**

Unter einer elektronischen Signatur versteht man mit elektronischen Informationen verknüpfte Daten, mit denen man den Unterzeichner bzw. Signaturersteller identifizieren und die Integrität der signierten elektronischen Informationen prüfen kann. Tivian verwendet hierfür die Lösungen von DocuSign und Adobe Acrobat.

- **Gesichertes WLAN (mindestens WPA2)**

Die Schutzsysteme der Notebooks der Belegschaft von Tivian erlauben keine ungesicherte Anbindung. Hierzu gehört auch die Verschlüsselungsmethode WEP.

- **„Data Loss Prevention (DLP)-System“**

Tivian verwendet in seiner Microsoft-Cloudumgebung DLP für SharePoint, OneDrive und Exchange Online.

- **Regelung zum Umgang mit mobilen Speichermedien (z.B. externe Festplatte, USB-Stick, SD-Karte)**

Es ist in den internen Unternehmensrichtlinien untersagt, einen Datentransport mit jeglicher Form von mobilen Speichermedien durchzuführen.

- **Protokollierung von Datenübertragung oder Datentransport**

Jeder TIVIAN Mitarbeiter, welcher Zugriff auf Kundendaten in der Produktion hat, hat einen eigenen User für VPN und User für die jeweiligen Bastion-Host / SSH. Somit ist jeder Zugriff auf Kundendaten über den VPN-Service, das OS und dem Filesystem protokolliert. Die zuständigen Mitarbeiter haben ihren eigenen Account bzw. ihr eigenes Zertifikat und Nutzer.

Bezüglich Cloud Services wird AWS IAM oder AAD SSO eingesetzt. Somit sind auch hier die Zugriffe protokolliert. Jede Änderung in AWS wird ebenfalls mit Hilfe AWS Config überwacht und protokolliert.

In unserer Software DXI wird ebenfalls jeder Login/Login-Versuch in der Datenbank protokolliert. Außerdem wird jede Interaktion mit dem System ebenfalls in der Datenbank abgelegt.

Über das Monitoring / Logging gibt es die Möglichkeit einzusehen, welche Endpunkte und wie aufgerufen wurden und welche Datenmengen transportiert werden.

- **Protokollierung von lesenden Zugriffen**

Jeder TIVIAN Mitarbeiter, welcher Zugriff auf Kundendaten hat, hat einen eigenen User für VPN und User für die jeweiligen Bastion-Host / SSH. Somit ist jeder Zugriff über den VPN-Service, das OS und dem Filesystem protokolliert. Für Cloud Services wird AWS IAM oder AAD SSO eingesetzt. Somit sind auch hier die Zugriffe protokolliert. In unserer Software DXI wird ebenfalls jeder Login/Login-Versuch in der Datenbank protokolliert.

- **Protokollierung des Kopierens, Veränderns oder Entfernens von Daten**

Jeder TIVIAN Mitarbeiter, welcher Zugriff auf Kundendaten hat, hat einen eigenen User für VPN und User für die jeweiligen Bastion-Host / SSH. Somit ist jeder Zugriff über den VPN-Service, das OS und dem Filesystem protokolliert.

- **Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)**

Datagroup Datacenter Frankfurt: Hier existiert ebenfalls ein VPN, welches den administrativen Zugriff auf Legacy-Services erlaubt, die aktuell noch in der Datagroup sind und auch produktiv genutzt werden (Exasol, Tableau, Hurricane, Datavoyager Reporting).

Administration der Cloud-Umgebungen (Microsoft Azure und AWS): Die administrativen Zugriffe auf die Cloud-Umgebungen von AWS erfolgen durch spezielle Zugriffsserver ("Bastion Hosts") und/oder über SSH-Tunnel.

11. VERFÜGBARKEITSKONTROLLE

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

11.1 Rechenzentren

11.1.1 Rechenzentren in Frankfurt, Deutschland/EU – AWS

AWS führt täglich komplette Backups der Daten durch. Dank dieser Sicherung kann der Betrieb im Notfall sofort wieder aufgenommen werden. Die Daten werden parallel auf ein separates Backup-System in einem separaten Brandabschnitt kopiert. Zusätzlich werden die Daten auf Magnetbänder kopiert, die separat sicher aufbewahrt werden. Auf diesen Magnetbändern sind die Daten fallabhängig verschlüsselt. Die Protokolldateien der Datensicherung werden täglich überprüft.

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 Stabilitätspläne der AWS-Services werden regelmäßig überprüft. AWS betrachtet dabei die Verfügbarkeit der Kundenlösung aus der Sicht der Netzwerk- und Hardwareverfügbarkeit sowie die Verfügbarkeit der Support-Services. Regelmäßige Kontrollen werden durchführt und Prozesse und Architekturen überprüft. AWS verwaltet Vorfällen über branchenübliche diagnostische Verfahren, um die Behebung unternehmenskritischer Vorfälle voranzutreiben.

In den Rechenzentren werden die folgenden Standards gewährleistet:

- 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.

Der 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. Der Standardzeitplan ist wöchentlich volle und tägliche differentielle Backups mit Aufbewahrungsraten von acht Wochen. Somit können die Backups für jeden Tag der letzten acht Wochen präzise wiederhergestellt werden. Im Rahmen von Notfallübungen werden regelmäßige Schulungen zur Datenrettung und Datenlesbarkeit durchgeführt. Jede Woche werden alle Backups in einem sicheren Lagerschrank aufbewahrt.

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

11.1.2 Rechenzentren in Frankfurt, Deutschland – Datagroup

Datagroup führt täglich komplette Backups der Daten durch. Dank dieser Sicherung kann der Betrieb im Notfall sofort wieder aufgenommen werden. Die Daten werden parallel auf ein separates Backup-System in einem separaten Brandabschnitt kopiert. Zusätzlich werden die Daten auf Magnetbänder kopiert, die separat sicher aufbewahrt werden. Auf diesen Magnetbändern sind die Daten 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.

In den Rechenzentren werden die folgenden Standards gewährleistet:

- 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.

11.1.3 Rechenzentren in den USA (grundsätzlich in North Virginia, USA) – AWS

Die 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.

Darüber hinaus platziert AWS 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. AWS 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 Stabilitätspläne der AWS-Services werden regelmäßig überprüft. AWS betrachtet dabei die Verfügbarkeit der Kundenlösung aus der Sicht der Netzwerk- und Hardwareverfügbarkeit sowie die Verfügbarkeit der Support-Services. Regelmäßige Kontrollen werden durchführt und Prozesse und Architekturen überprüft, 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.

Der 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. 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. Das AWS Backup ist PCI-, ISO- und HIPAA-konform. Die Protokolle zu Sicherungsaktivitäten stehen für Compliance-Überprüfungen zur Verfügung.

11.1.4 Rechenzentren in der EU (grundsätzlich in den Niederlanden und Irland) – Microsoft

- Microsoft Azure bietet zuverlässige Verfügbarkeit auf Grundlage umfassender Redundanz mithilfe von Virtualisierungstechnologien. Microsoft Azure bietet zahlreiche Redundanzebenen zur Gewährleistung maximaler Verfügbarkeit von Kundendaten.
- Das Microsoft Cloud Infrastructure and Operations-Team stellt für die Azure-Infrastruktur Hochverfügbarkeit und Zuverlässigkeit, hohe Effizienz, intelligente Skalierbarkeit sicher, sodass eine sicherere, private und vertrauenswürdige Cloud gewährleistet werden kann.
- 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 Fail-over-function. Geografisch verteilte Microsoft-Betriebszentren sind 24 Stunden am Tag, 7 Tage die Woche und 365 Tage im Jahr in Betrieb. 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 unter: https://docs.microsoft.com/azure/security/azure-infrastructure-availability

11.2 Softwareplattformen

Die folgende Sicherungsstrategie findet Anwendung:

- Es wird täglich ein vollständiges Backup der Daten auf einem unabhängigen Backup-System durchgeführt. Hierdurch wird sichergestellt, dass der Auftragnehmer im Notfall sofort wieder seinen Betrieb aufnehmen kann.
- Zur Sicherung von Backups wird der AWS Service **"**AWS Backup**"** eingesetzt.
- Backups können für jeden der letzten 7 bis 60 Tage präzise wiederhergestellt werden, je nachdem, wie kritisch das System ist.

12. BELASTBARKEIT VON VERARBEITUNGSSYSTEMEN UND -DIENSTEN

Art. 32 DSGVO 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.

12.1 Rechenzentren

Die Rechenzentren, die von Tivian eingesetzt werden, gewährleisten die Ausfallsicherheit durch eine Vielzahl von Maßnahmen (siehe ober unter Kapitel 11). Dazu gehören:

- Der Einsatz skalierbarer Netzwerkkomponenten, ohne Betriebsunterbrechung erweiterbare Ressourcen (“On the Fly”)
- Fehlertolerante Hardwarekomponenten
- Modernste Netzwerkinfrastruktur
- Bereitstellung von ausreichend qualifiziertem Personal sowie
- Permanente Überwachung des Betriebszustandes.

12.2 Geschäftsstellen – Alle Büros

Die Betriebssicherheit der Geschäftsstellen von Tivian wird durch eine Vielzahl von Maßnahmen gewährleistet. Hierzu gehören:

- Der Einsatz skalierbarer technischer Komponenten
- Eine vorausschauende Bedarfsplanung
- Die Bereitstellung von ausreichend qualifiziertem Personal sowie
- Die permanente Überwachung des Betriebszustandes

12.3 Softwareplattformen

Die Softwareplattformen von Tivian stellt die Ausfallsicherheit durch eine Vielzahl von Maßnahmen sicher. Dazu gehören:

- Der Einsatz skalierbarer Datenbanken
- Moderne Programmiertechnologie
- Agile Entwicklung sowie
- Der Einsatz leistungsfähiger Softwarekomponenten

13. TRENNUNGSKONTROLLE

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

13.1 Softwareplattformen

Die folgenden Maßnahmen werden u.a. getroffen:

- Trennung der personenbezogenen Daten an verschiedenen Speicherorten durch organisatorische und räumliche Trennung (Mandantenfähigkeit)
- Die Datenverarbeitungssysteme für besonders sensible Daten sind physisch und organisatorisch getrennt
- Entwicklungs-, Test- und Produktivsysteme sind physisch voneinander getrennt und unterliegen separaten Sicherheitseinschränkungen
- Vor einer Überführung von personenbezogenen Daten aus Produktiv- in Testumgebungen werden diese anonymisiert.
- Trennung der Daten nach Mandanten / Kunden
- Erstellen eines Berechtigungskonzepts

14. PSEUDONYMISIERUNG UND VERSCHLÜSSELUNG PERSONENBEZOGENER DATEN

Art. 25 Abs.1 sowie Art.32 Abs.1 lit. a) DSGVO verlangen, dass personenbezogene Daten möglichst pseudonymisiert und verschlüsselt verarbeitet werden. Art. 32 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.

14.1 Rechenzentren

Die Kommunikation zwischen den Tivian-Rechenzentren und Dritten erfolgt ausschließlich in verschlüsselter Form. Unter "Dritte" sind neben den Kunden auch Lieferanten, Auftragsverarbeiter und alle anderen Personen, die beim Zugriff auf sämtliche Plattformen personenbezogene Daten verarbeiten, miteinbezogen. Hierbei werden Technologien verwendet, die die jeweils gültigen gesetzlichen Anforderungen erfüllen und dem Stand der Technik entsprechen. Sämtliche erfolgten Backups werden verschlüsselt gespeichert.

14.2 Softwareplattformen

Tivians Softwareplattformen speichern 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, mittels Überschreibens durch ein Skript in der Datenbank ersetzt.

[TIVIAN]

15. AUFBEWAHRUNG UND LÖSCHUNG

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

15.1 Rechenzentren

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

15.2 Software

15.2.1 Standardeinstellung: vom Kunden festgelegte Aufbewahrungszeit für persönliche Daten

Die Tivian Software wird den Kunden von Tivian zur Verfügung gestellt, damit sie Umfragen und Fragebögen erstellen können. 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 Backups werden spätestens 60 Tage nach der Löschung der Originaldaten gelöscht (überschrieben). Das Löschen erfolgt in Übereinstimmung mit den aktuellen Löschroutinen von Tivian.

15.2.1 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 Backups werden spätestens 60 Tage nach der Löschung der Originaldaten gelöscht (überschrieben). Das Löschen erfolgt in Übereinstimmung mit den aktuellen Löschroutinen von Tivian.

16. INCIDENT-RESPONSE-MANAGEMENT

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 verantwortlichen Stellen, "ohne unangemessene Verzögerung" benachrichtigen, nachdem Tivian von einem Datenverstoß erfahren hat.

16.1 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 leitet in einem solchen Fall sofortige Gegenmaßnahmen ein, um den jeweiligen Angriff zu stoppen, bevor dieser Schäden anrichten kann, die eine Datenschutzverletzung nach sich ziehen.

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.

16.2 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.

16.3 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 Datenverarbeitungsverzeichnis 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 sowie den Prozess zur Benachrichtigung des Kunden im Falle eines Verstoßes zu unterstützen. In der anschließenden Kommunikation mit dem Kunden wird die Art des Verstoßes und Empfehlungen zur Minderung möglicher negativer Auswirkungen beschrieben.

[TIVIAN]

17. INTERNE KONTROLLE

Dieser Abschnitt beschreibt die implementierten Maßnahmen, um sicherzustellen, dass interne Richtlinien, einschließlich der in diesem Dokument beschriebenen Richtlinien, durch die Organisation eingehalten werden. Zudem wird im Folgenden der Prozess zur regelmäßigen Überprüfung, Begutachtung und Bewertung der Wirksamkeit dieser technischen und organisatorischen Maßnahmen festgelegt.

17.1 Überwachung der Softwareplattformen

Die folgenden Maßnahmen sind Beispiele der eingesetzten Überwachungsmaßnahmen unserer Softwareplattformen:

- Alarme werden rund um die Uhr ausgegeben
- Alarme werden sofort von qualifiziertem technischen Personal der Tivian aufgenommen
- Das Überwachungssystem ist redundant ausgelegt und wird von einem externen Überwachungstool überwacht
- Ein weiteres Monitoring-System gibt Einblicke in die Performance der Plattformen von weltweiten Orten.

17.2 Sicherheitsaudits

Regelmäßige Audits der Hosting-Umgebung sind Teil der ISO 27001-Zertifizierungsanforderungen, denen die von Tivian eingesetzten Rechenzentren unterworfen sind.

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.

17.3 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

Um die Vertraulichkeit, Integrität und Verfügbarkeit unserer Softwareplattform gem. Art. 32 Abs. 1 lit. c) und d) sicherzustellen, werden ein- bis zweimal jährlich entsprechende technische Maßnahmen durchgeführt.

Ein Infrastrukturtest unserer Hosting-Umgebung findet jedes Jahr statt.

17.4 Penetrationstests

Die Ergebnisse der regelmäßigen und automatisierten Schwachstellenscans werden durch den IT-Sicherheitsbeauftragten überprüft und verarbeitet.

In regelmäßigen Abständen werden die Systeme von Tivian durch einen externen Dienstleister auf Schwachstellen untersucht.

17.5 Informationssicherheitsbeauftragter

Tivian hat einen internen Informationssicherheitsbeauftragten bestellt, zu dessen Hauptaufgaben die Entwicklung, Einrichtung und Überwachung eines Informationssicherheits-Managementsystems (ISMS) gehört.

17.6 Datenschutzbeauftragter

Tivian hat sowohl einen externen Datenschutzbeauftragten benannt als auch einen internen Privacy Counsel eingestellt, zu deren Hauptaufgaben die regelmäßige Kontrolle der Verarbeitungstätigkeiten und Datenschutzmaßnahmen sowie die Gewährleistung von Compliance zu den anwendbaren Datenschutzgesetzen gehört.

17.7 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.

17.8 Risikoanalyse

Regelmäßig findet eine Risikoanalyse durch den IT- Informationssicherheitsbeauftragten gemeinsam mit den IT-Verantwortlichen statt, um die aktuelle Bedrohungslage einzuschätzen und Maßnahmen zur Umsetzung abzuleiten.

18. DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN (ART. 25 DSGVO)

18.1 "Privacy by Default"

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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten betroffener Personen werden geeignete technische und organisatorische Maßnahmen implementiert, die dafür ausgelegt sind, die Rechte der betroffenen Personen zu schützen. Die folgenden Maßnahmen werden u.a. getroffen:

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.
- Es wird die einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen eingehalten

18.2 "Privacy by Design"

Die folgenden Maßnahmen werden u.a. getroffen:

- Bei der Entwicklung unserer Software wird es darauf geachtet, dass lediglich die personenbezogenen Daten erhoben werden, die zur Erfüllung des jeweiligen Zwecks auch tatsächlich erforderlich sind.