Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen tuesday.sport IT-Service GmbH gemäß Art. 32 Abs. 1 DSGVO

Vorbemerkung

Dieses Dokument ist Teil der Datenschutzdokumentation des Datenschutzmanagements der tuesday.sport IT-Service GmbH (tuesday.sport).

Diese Dokument gilt für die informationsverarbeitenden Systeme, Netzwerke und Produkte sowie Dokumente und Informationen von tuesday.sport, mit denen personenbezogene Daten verarbeitet (erhoben, genutzt und gespeichert) werden.

Allgemeiner Zweck der vorliegenden technischen und organisatorischen Maßnahmen der tuesday.sport IT-Service GmbH ist es, das Risiko physischer, materieller oder immaterieller Beeinträchtigungen an datenverarbeitenden Systemen, Netzwerken und Produkten sowie der Rechte und Freiheiten von betroffenen Personen bzw. deren Daten zu verhindern bzw. zu reduzieren. Hierzu werden Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits- und Trennungskontrollen vorgehalten.

Die persönliche Verantwortung jedes Mitarbeiters für die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen wird durch regelmäßige Schulungsmaßnahmen, Infomärkte und zentral bereitgestellte Informationen gestärkt.

Die nachfolgende Auflistung dient nur der erläuternden Darstellung gesetzlicher Anforderungen in Bezug auf den Datenschutz für die Informationsverarbeitung von tuesday.sport. Die Rechte und Pflichten in Bezug auf den Datenschutz von tuesday.sport als Auftragsverarbeiter bzw. Verantwortlicher im Sinne der Datenschutzbestimmungen ergeben sich aus den vertraglichen Vereinbarungen und den gesetzlichen Bestimmungen.

Technische Änderungen und/oder Änderungen in der Organisation, die keinen Einfluss auf die Erfüllung der gesetzlichen Anforderungen der DSGVO, BDSG, etc. in der jeweils aktuellen Fassung haben, bedürfen keiner gesonderten Information gegenüber Vertragspartnern von tuesday.sport.

Dieses Dokument besitzt ausschließlich Gültigkeit in Bezug auf Vertragspartner von tuesday.sport.

Angaben zum Datenschutzbeauftragten, Rechenzentrum, zu Unterauftragnehmern sowie (geplanten) Zertifizierungen, DataGovernance-Dokumenten und Prüfungen sind über die Anlage zu diesem Dokument zugänglich.

Eine Änderung der getroffenen Maßnahmen behält tuesday.sport sich vor, sofern das Schutzniveau nach DSGVO nicht unterschritten wird.

Diese Version des Dokuments ersetzt alle früheren Versionen und Ausgaben. Sofern vertragliche oder gesetzliche Festlegungen dieses Dokument oder Teile hiervon berühren, haben diese Vorrang. Die Aktualisierung und Weiterentwicklung dieses Dokuments obliegt dem Datenschutzmanagement von tuesday.sport.

1. Vertraulichkeit (Art 32 Abs. 1 Buchst. b) DSGVO)

1.1 Zutrittskontrolle

Regelungsgegenstand:

Das Ziel einer Zutrittskontrolle ist es, Unbefugten den Zutritt (z.B. zu Datenverarbeitungsanlagen) zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Der Begriff des Zutritts ist dabei räumlich zu verstehen. Der Grad der Schutzmaßnahmen richtet sich dabei nach dem Grad der Schutzbedürftigkeit der Daten.

Maßnahmen am Standort Georg-Brauchle-Ring 93, 80992 München:

- Einsatz eines analogen und elektronischen Schließsystems inklusive Protokollierung zum und im Gebäude.
- Verschluss der Zutrittsmöglichkeiten zum Gebäude außerhalb der Geschäftszeiten. Mitarbeiter sind angewiesen, Fenster außerhalb der Geschäftszeiten geschlossen zu halten und diese beim Verlassen des Gebäudes zu kontrollieren.
- Zutritt zum Gebäude ist Gästen während der Geschäftszeiten nur nach Anmeldung am Empfang und Eintragung in eine Besucherliste gestattet.
- Ausschließlicher Betrieb von externen Servern bei zertifizierten Dienstleistern.

Maßnahmen am Standort der netlogix GmbH & Co. KG:

Die Maßnahmen zur Zutrittskontrolle sowie weiterer, infrastruktureller Themen des Rechenzentrums, in dem ein Housing von Servern stattfindet, sind den technischen und organisatorischen Maßnahmen der netlogix GmbH & Co. KG sowie der noris network AG zu entnehmen (siehe Anhang).

- Alle im Auftrag verarbeiteten Daten werden grundsätzlich in Sicherheitsbereichen gespeichert. Der Zutritt ist nur Berechtigten über Schleusen mit Buchungsstellen möglich und wird visuell vom Sicherheitsdienst überwacht.
- Die Zutrittskontrollen zu den Rechenzentren-Standorten sind lückenlos.
- Im Auftrag verarbeitete Daten werden grundsätzlich in Sicherheitsbereichen verarbeitet, die innerhalb der kontrollierten Bereiche durch zusätzliche Maßnahmen wie eingeschränkten Zutrittsberechtigungen und ergänzenden Personenkontrollen beim Betreten und Verlassen der Sicherheitsbereiche geschützt werden.

1.2 Zugangskontrolle

Regelungsgegenstand:

Das Ziel einer Zugangskontrolle ist es, mithilfe geeigneter Maßnahmen zu verhindern, dass Unbefugte in Datenverarbeitungsanlagen und -systeme, mit denen personenbezogene Daten verarbeitet oder genutzt werden, eindringen oder diese nutzen können.

Maßnahmen:

- Es erfolgt eine personenbezogene Vergabe von Benutzerkennungen auf Weisung der Geschäftsführung. Nach Ausscheiden von Mitarbeitern werden Benutzerkennungen umgehend gesperrt.
- Die Authentifizierung von Benutzern erfolgt weitestgehend über zentrale Authentifizierungssysteme. Systeme, die eine zentrale Authentifizierung im Einzelfall nicht erlauben, sind erfasst, um eine Sperrung von Benutzerkennungen auch in diesen Systemen sicherzustellen.

- Passwortregeln stellen sicher, dass sichere Benutzerpasswörter verwendet werden. Die Benutzer werden regelmäßig dafür sensibilisiert, für externe Systeme getrennte und jeweils nur einmalig verwendete Passwörter zu nutzen.
- Für besonders kritische Systeme kommen Zwei-Faktor-Authentifizierungsmechanismen zum Einsatz.
- Auf (mobilen) Arbeitsplatzrechnern und Serverkonsolen wird eine automatische Bildschirmsperre nach Inaktivität für einen bestimmten Zeitraum administrativ erzwungen.
- Das Unternehmensnetzwerk ist segmentiert. Insbesondere sind Netzwerkbereiche mit öffentlich erreichbaren Diensten von privaten Netzen getrennt. Dienstnetzwerke sind von Anwendernetzen getrennt.
- Der Übergang zwischen Netzwerksegmenten wird durch den Einsatz von Firewalls auf dem Stand der Technik eingeschränkt und wo nötig protokolliert.
- Für den elektronischen Transport werden Verschlüsselungsverfahren eingesetzt, die dem Stand der Technik entsprechen (https-, VPN- oder TLS-Verbindung mit Zwei-Faktor-Authentisierung bzw. Übertragungsvorgaben gemäß den Standards von Institutionen wie den Finanzbehörden, Sozialversicherungsträgern, etc.).
- Auf (mobilen) Arbeitsplatzrechnern wird Virenschutzsoftware eingesetzt.
- Es wird auf ein Incident-Response-Management bzw. ein Informationssicherheits-Managementsystem zugegriffen.

1.3 Zugriffskontrolle

Regelungsgegenstand:

Das Ziel einer Zugriffskontrolle ist es, zu gewährleisten, dass ausschließlich die zur Benutzung der Datenverarbeitungssysteme Berechtigten auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung und Nutzung und nach der Speicherung nicht unbefugt gelesen, vervielfältigt, verändert oder entfernt werden können.

Maßnahmen:

- Sämtliche verwendete Arbeitsplatzrechner verfügen mindestens über ein Zugangskontrollsystem bestehend aus UserID und Passwort.
- Die eingesetzten IT-Systeme haben ein dediziertes Rechtesystem. Datenzugriffe und Datenveränderungen erfolgen nur auf Basis von zuvor festgelegten Rollen und individuellen Berechtigungen..
- Der Zugriff auf Benutzerkennungen und Passwörter innerhalb des unternehmensweiten Passwortsafes wird restriktiv vergeben und ist auf die Datensätze beschränkt, die von einer Personengruppe oder Einzelperson zur Erfüllung ihrer Aufgaben benötigt werden.
- Es bestehen vorgeschriebene Regeln zur Passwortvergabe. Diese betreffen die notwendige Komplexität, die Lebensdauer des Passwortes sowie die Wiederverwendung alter Passwörter.
- Die Vergabe von Benutzerrechten für Dienste, Anwendungen und Datenbanken erfolgt restriktiv. Die Rechtevergabe erfolgt auf Weisung der Geschäftsführung. Administrative Rechte werden nur jenen Benutzern vergeben, die diese zur Erfüllung ihrer Aufgaben benötigen.
- Der Zugriff auf Anwendungen wird durch die von den Anwendungen oder Diensten bereitgestellten Logmechanismen protokolliert.
- Zugriffe auf im Auftrag verarbeitete Daten, die zur Serviceerbringung und Auskunftserteilung an Verantwortliche erfolgen, werden grundsätzlich protokolliert. Die Verarbeitung der im Auftrag verarbeiteten Daten erfolgen ausschließlich nach dem mit dem Auftraggeber festgelegten Verfahren.

- Die IT-Systeme werden auf die Wirksamkeit eingesetzter Maßnahmen gegen das Eindringen seitens unbefugter Dritter getestet.
- Zur Prüfung der Wirksamkeit der Absicherungsmaßnahmen werden bei sensiblen Systemen Penetrationen durchgeführt.
- Defekte oder alte Datenträger werden nach Stand der Technik vernichtet.
- Die Vernichtung von Akten wird wahlweise vor Ort mittels eines Aktenvernichters mit Partikelschnitt oder durch einen zertifizierten Dienstleister durchgeführt. Die Vernichtung wird durch den Dienstleister protokolliert.

1.4 Trennungskontrolle

Regelungsgegenstand:

Das Ziel des Trennungsgebots ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten ebenfalls getrennt voneinander verarbeitet werden.

Maßnahmen:

- Es existiert das Prinzip der Mandaten- und Funktionstrennung zwischen Produktion und Entwicklung. Die eingebundenen Abteilungen sind funktionell, organisatorisch oder räumlich getrennt.
- Schutzwürdige Daten werden den Mitarbeitern nur in dem Umfang zur Verfügung gestellt, wie es für die zugewiesene Aufgabenerfüllung unbedingt erforderlich ist.
- Der Übergang vom Entwicklungssystem zum Produktionssystem ist durch entsprechende Werkzeuge gesichert und nachvollziehbar dokumentiert. Dazu gehört auch ein Workflow-gestütztes Genehmigungsverfahren.

2. Integrität (Art. 32 Abs. 1 Buchst. b) DSGVO)

2.1 Weitergabekontrolle

Regelungsgegenstand:

Das Ziel einer Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, vervielfältigt, verändert oder entfernt werden können und dass überprüft sowie festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahmen:

- Die Datenübertragung erfolgt verschlüsselt.
- Fernzugriffe und Verbindungen zu entfernten Netzwerken werden grundsätzlich durch VPN-Technologie mit starker Verschlüsselung abgesichert, sofern dies durch den Kunden möglich ist.
- Daten werden auf Backupmedien verschlüsselt gespeichert.
- Die Speicherung von personenbezogenen Daten oder Datenbeständen, die solche Daten enthalten könnten, durch Endanwender auf mobilen Datenträgern (mobile Festplatten, USB, Stick o.Ä.) ist durch die Geschäftsführung untersagt.

- Der physikalische Transport von Datenträgern mit personenbezogenen Daten wird nicht durch Dritte durchgeführt.
- Die Aufbewahrung von Datenträgern oder mobilen Geräten in Fahrzeugen darf nur im nicht sichtbaren Bereich (z.B. Kofferraum) erfolgen. Eine sichtbare Aufbewahrung ist durch die Geschäftsführung untersagt.

2.2 Eingabekontrolle

Regelungsgegenstand:

Das Ziel einer Eingabekontrolle ist es, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten in die Systeme und Anlagen zur Datenverarbeitung eingegeben, verändert oder entfernt worden sind.

Maßnahmen:

- Die Nachvollziehbarkeit von Eingaben, Änderungen oder Löschungen von Daten wird, sofern technisch und soweit rechtlich möglich, insbesondere im Ticketsystem der Tuesday.sport IT-Service GmbH, durch personenbezogene Benutzerkennungen sichergestellt.
- Die Dateneingabe und die Verarbeitung der im Auftrag verarbeiteten Daten erfolgen ausschließlich nach dem mit dem Auftraggeber festgelegten Verfahren.

3. Verfügbarkeit (Art. 32 Abs. 1 Buchst. b) DSGVO

Regelungsgegenstand:

Das Ziel der Verfügbarkeitskontrolle ist es, zu gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust physisch sowie auch logisch geschützt sind.

Maßnahmen:

- Es werden regelmäßig Backups erstellt und auf diese auf Funktionalität überprüft. Die Backups werden in verschiedenen Brandabschnitten gesichert und auf verschiedenen Servern gelagert.
- Von allen produktiven Serversystemen werden regelmäßig Backups erstellt. Backups werden in einem getrennten Brandabschnitt und auf verschiedenen Servern verschlüsselt gelagert.
- Sämtliche Systeme können über redundante Systeme und höchst verfügbar sowie georedundant aufgebaut werden. Durch umfassendes Monitoring (z.B. Incident-Response-Management) kann im Vorfeld bereits auf potentielle Störfälle reagiert werden.
- Durch regelmäßige Wartung der Produktionsanlagen besitzen die technischen Anlagen beim Housing-Partner der tuesday.sport eine hohe Verfügbarkeit. Dies wird durch tuesday.sport durch entsprechende Serviceverträge für Wartung und Entstörung mit den Housing-Partnern sichergestellt. Die Abwicklung von Wartungsaufträgen wird überwacht und begleitet, die korrekte Umsetzung der vertraglich vereinbarten Leistungen wird kontrolliert. Abweichungen werden zeitnah geklärt.
- Maßnahmen für den Fall physischer oder technischer Zwischenfälle werden über einen Notfallplan aktiviert (siehe Alarmierung von Polizei und Feuerwehr) und sind in einem Plan zur Wiederherstellbarkeit (siehe Redundanz, Monitoring, Incident-Response-Management, Backups) dokumentiert. Die Maßnahmen werden regelmäßig geprüft und aktualisiert.
- Der Serverraum wird durch ein System zur Raucherkennung überwacht.
- Der Serverraum verfügt über ein geeignetes Feuerlöschgerät, das regelmäßig kontrolliert wird.
- Der Serverraum wird von einer ausreichend dimensionierten, unterbrechungsfreien Stromversorgung vor plötzlichen Stromausfällen geschützt.

- Die Stromversorgung (24/7 Stromversorgungsprinzip) für die IT-Systeme ist redundant aufgebaut (Klimazellen) und erlaubt mit USV (Unterbrechungsfreie Stromversorgung) und Dieselaggregaten die Leistungsversorgung, so dass selbst im Fall auftretender Fehlfunktionen keine Systemausfälle zu erwarten sind.
- Es erfolgen regelmäßige Brandschutzbegehung.
- Die Klimatisierung des Rechenzentrums erfolgt über redundante Klimaanlagen und räumlich getrennte, redundante Kältezentralen, die im Verbund arbeiten. In den einzelnen EDV-Bereichen werden beispielsweise die Raumtemperatur und die Feuchte geregelt und überwacht. Durch die Erhöhung der Kühlleistung kann auch bei Störfällen in einzelnen Anlagen die geforderte Klimaleistung erbracht werden. Gebäudeleit- und -überwachungssysteme stellen den laufenden Betrieb sicher.

4. Belastbarkeit (Art. 32 Abs. 1 Buchst. b) DSGVO

Regelungsgegenstand:

Das Ziel der Belastbarkeitskontrolle ist es, Systemstabilität zu gewährleisten, indem Systemüberlastungen oder Systemabstürze vermieden bzw. reduziert werden.

Maßnahmen:

- Die Dienstleister der tuesday.sport führen eine laufende Überwachung der Nutzung der Dienste und der Auslastung der Systeme durch. Die Dienstleister liefern regelmäßig einen entsprechenden Bericht an tuesday.sport.
- Der Housing-Dienstleister hat ein Notfallkonzept umgesetzt. Dieses Notfallkonzept wird laufend fortgeschrieben und regelmäßig auf Wirksamkeit geprüft.
-
- tuesday.sport legt die Speicher-, Zugriffs- und Leitungskapazitäten der Systeme und Dienste so aus, dass sie auch an Tagen mit prognostizierter Spitzenbelastung ohne merkliche Verzögerung von Zugriffs- oder Übertragungszeiten genutzt werden können.
- Nach einem physischen oder technischen Ausfall eines Teil-Rechenzentrums übernimmt die verbliebene Infrastruktur die Verarbeitung. Für alle IT- und TK-Systeme besteht ein Wiederanlaufkonzept, nach dem die Redundanz innerhalb festgelegter Fristen wiederhergestellt wird. Das Wiederanlaufkonzept wird laufend fortgeschrieben und regelmäßig auf Wirksamkeit geprüft.

5. Verfahren zur regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 Buchst. d) DSGVO

5.1 Allgemeine Verfahren

Regelungsgegenstand:

Auflistung der allgemeinen Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung.

Maßnahmen:

- Bestehen eines zertifizierten Informationssicherheits-Managementsystem gemäß ISO / IEC 27001 des Housing-Dienstleister der tuesday.sport IT-Service GmbH für den Bereich des Rechenzentrums (Stand Zertifizierungsdatum 20.02.2020).
- BSI-basierte Risikoanalyse und Maßnahmenkatalog der tuesday.sport IT-Service GmbH.

- Regelmäßige interne Überprüfungen der IT-Systeme durch die tuesday.sport IT-Service GmbH und Risikobewertung aller Verarbeitungen hinsichtlich der Rechte und Freiheiten natürlicher Personen.
- Initiierung eines ISO-27001-Zertifizierungsverfahrens zur Einführung eines Datenschutz-Management-Systems für die tuesday.sport im Auftrag des Bayerischen Landes-Sportverband e.V.
- Erstellung von Datenschutzfolgenabschätzungen, sofern notwendig.
- Prüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen durch den Informationssicherheitsbeauftragten der tuesday.sport IT-Service GmbH.
- Bestellung, Konsultation und Prüfungen des Datenschutzbeauftragten.

5.2 Auftragskontrolle

Regelungsgegenstand:

Das Ziel einer Kontrolle von Aufträgen zur Datenverarbeitung Sinne von Art. 28 DSGVO ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend des Auftrags und der Weisungen des Auftragsgebers verarbeitet werden können.

Maßnahmen:

- Dienstleistungsverhältnisse werden schriftlich vereinbart.
- Regelungen zum Einsatz von Unterauftragnehmern.
- Definition des Gegenstands der Verarbeitung.
- Vertragliche Abgrenzung der Verantwortlichkeiten (bei gemeinsamer Verantwortung).

Anhang

I) Datenschutzbeauftragter

Angaben zum Datenschutzbeauftragten der tuesday.sport IT-Service GmbH mit Stand von Mai 2021:

Professor Dr. Rolf Lauser
Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau
Tel.: 08131/511750
Fax: 08131/511619
E-Mail: rolf@lauser-nhk.de

II) Rechenzentrum

Angaben zum Rechenzentrum der tuesday.sport IT-Service GmbH mit Stand von Mai 2021:

noris network AG
Rechenzentrum Nürnberg
Thomas-Mann-Straße 16-20
90471 Nürnberg
Deutschland

III) Dokumentation, Zertifizierung und Prüfungsergebnisse zur Datensicherheit

Die tuesday.sport IT-Service GmbH veröffentlicht einschlägige Dokumente, Zertifikate und Prüfergebisse zur DataGovernance (Datenschutz, Informationssicherheit, Auditierung) unter:
www.tuesday.sport.de/datenschutz

Mit Beginn Q2 2021 wird ein ISO-27001-Zertifizierungsverfahrens mit Einführung eines Datenschutz-Management-Systems für die tuesday.sport IT-Service GmbH im Auftrag des Bayerischen Landes-Sportverband e.V. avisiert.

IV) Unterauftragnehmer

Liste der Subdienstleister der tuesday.sport IT-Service GmbH mit Stand von Mai 2021:

Name	Adresse	Dienstleistung
Netlogix GmbH	www.netlogix.de	DevOps Dienstleistungen
CIB Software GmbH	www.cib.de	Software-Entwicklungsleistungen
Zweitag GmbH	www.zweitag.de	Software-Entwicklungsleistungen
S2 Design	www.s2-design.de	Software-Entwicklungsleistungen
OTS GmbH	http://www.ots-ag.de	Software-Entwicklungsleistungen
CIT GmbH	http://www.cit.de	Software-Entwicklungsleistungen
WWWAN GmbH	www.wwwan.de	IT-Dienstleistungen
m-net	www.m-net.de	Hosting-Dienstleistungen
Sportvita GmbH & Co. KG	www.sportvita.de	Software-Entwicklungsleistungen
Kultsoftware UG	www.kultsoftware.com	Software-Entwicklungsleistungen