

# **Anlage 2/4: Technische und organisatorische Maßnahmen (TOM)**

## **nach Art. 32 EU DSGVO**

Version: 02/2024

### **Maßnahmen zur Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**

Es sind geeignete technische und organisatorische Maßnahmen umzusetzen, welche den Anforderungen an die DSGVO genügen sowie durch geeignete Voreinstellungen sicherzustellen, dass nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

MySports berücksichtigt die Anforderungen des Art. 25 DSGVO bereits in der Konzeptionierungs- und Entwicklungsphase der Produktentwicklung. Dies wird durch proaktive Einbindung der Rechtsabteilung und des Datenschutzbeauftragten umgesetzt. Prozesse und Funktionalitäten werden dabei so aufgesetzt, dass die Datenschutzgrundsätze wie Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, etc. sowie die Sicherheit der Verarbeitung frühzeitig berücksichtigt werden.

### **Maßnahmen zur Gewährung von Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**

#### **1. Organisationskontrolle**

*Gewährleistung, dass die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird.*

##### **a. Organisationsanweisungen**

Die Ziele im Datenschutz und in der Informationssicherheit sind in einer Datenschutz- und Informationssicherheits-Richtlinie festgelegt und für alle Mitarbeiter von MySports verbindlich. Darüber hinaus sind weitere Organisationsanweisungen implementiert, um den Mitarbeitern konkrete Richtlinien im Rahmen der Verarbeitung von personenbezogenen Daten zu vermitteln (bspw. Richtlinie zum mobilen Arbeiten oder Richtlinie zur Nutzung von IT, Internet und E-Mail).

##### **b. Bestellung eines Datenschutzbeauftragten nach Art. 37 DSGVO**

Ein Datenschutzbeauftragter wurde von der Geschäftsführung bestellt. Er wirkt auf die Einhaltung der Vorschriften zum Datenschutz hin und erfüllt die Aufgaben im Sinne von Art. 39 DSGVO. Dazu zählen unter anderem die Unterstützung beim Aufbau und der Weiterentwicklung eines Datenschutzmanagementsystems, bei der Verfassung, Weiterentwicklung und Kontrolle entsprechender Richtlinien sowie die Durchführung regelmäßiger Sensibilisierungsmaßnahmen.

##### **c. Verpflichtung auf Vertraulichkeit und Datenschutz**

Alle Beschäftigten werden bei Aushändigung ihres Arbeitsvertrages bzw. spätestens zu Beschäftigungsbeginn schriftlich auf Vertraulichkeit und Datenschutz sowie auf sonstige einschlägige Gesetze verpflichtet. Die Verpflichtung gilt über die Beschäftigungsdauer hinaus. Freiberufliche Mitarbeiter oder externe Dienstleister werden schriftlich anhand von Non-Disclosure-Agreements (NDAs) zur Verschwiegenheit verpflichtet und unterzeichnen zusätzlich einen Vertrag zur Auftragsverarbeitung, sofern durch sie personenbezogene Daten im Auftrag von MySports verarbeitet werden.

#### **d. Datenschutzschulungen**

Jeder Mitarbeiter von MySports erhält mit dem Arbeitsvertrag Informationen und Merkblätter zum Datenschutz und bestätigt deren Kenntnisnahme. Zusätzlich werden regelmäßige Schulungen (primär durch den Datenschutzbeauftragten) als Sensibilisierungsmaßnahmen durchgeführt. Mitarbeiter aus besonders sensiblen Bereichen wie bspw. Personalabteilung, Produktentwicklung oder Kundenservice erhalten bei Bedarf zudem gesondert Informationen und Schulungen zu spezifischen Fachthemen. Die Mitarbeiter erhalten regelmäßig Informationen zu Neuigkeiten im Datenschutzrecht per E-Mail oder im Intranet. Die Richtlinien sind im Intranet hinterlegt und für jeden Mitarbeiter zugänglich.

#### **e. Einschränkung der Privat- und betrieblichen Nutzung von Kommunikationsmitteln**

Es ist den Mitarbeitern von MySports nicht gestattet, das betriebliche E-Mail-System zur Privatnutzung zu verwenden. Das Internetsystem und die Telefondienste dürfen nur eingeschränkt privat genutzt werden. Es ist dabei strikt auf eine Trennung von privaten und betrieblichen Daten zu achten. Weiterhin ist es den Mitarbeitern von MySports nicht gestattet, personenbezogene Daten oder sonstige Daten des Auftraggebers, insbesondere aus dem Auftrag, auf privaten Kommunikationsmitteln zu verarbeiten. Die Mitarbeiter von MySports verpflichten sich zur Einhaltung entsprechender Richtlinien, deren Einhaltung im Rahmen des zulässigen und notwendigen Umfangs kontrolliert wird. Die Mitarbeiter werden über die Gefahren und Risiken der E-Mail-Kommunikation in Kenntnis gesetzt.

#### **f. Personalsicherheit**

MySports setzt Maßnahmen vor, während und nach der Beschäftigung zur Sicherstellung der Personalsicherheit um. Darunter fallen in der Regel:

- Überprüfung und Bestätigung angegebener akademischer und beruflicher Qualifikationen
- Vertragliche Vereinbarungen zur Festlegung von Verantwortlichkeiten und Verhaltensregeln
- Durchführung von Schulungs-, Sensibilisierungs- sowie Kontrollmaßnahmen
- Sensibilisierungs- und Sanktionsprozess bei datenschutzrechtlichen Verstößen
- Durchführung eines dokumentierten Offboarding-Prozesses (inkl. Rücknahme von Schlüsseln, Entziehung von Zugriffsrechten, Sicherstellung der ausreichenden Dokumentation, Herausgabe und Weitergabe von Daten, Informationen und Wissen etc.) bei Beendigung des Arbeitsverhältnisses

## **2. Verschlüsselung und Pseudonymisierung personenbezogener Daten**

*Gewährleistung, dass personenbezogene Daten im System nur in einer Weise gespeichert werden, die Dritten die Zuordnung zum Betroffenen nicht ermöglicht.*

#### **a. Datenbank- und Speicher-Verschlüsselung**

Auf allen von MySports eingesetzten Datenbanken wird eine Verschlüsselung „at Rest“ nach dem Stand der Technik eingesetzt, sodass die Daten aus der Datenbank nur nach ordnungsgemäßer Authentifizierung am jeweiligen Datenbank-System gelesen werden können. Die zur Speicherung von Dokumenten eingesetzten Speichermedien („Storage“) werden ebenfalls auf Dateiselebene verschlüsselt. Backups werden ausschließlich verschlüsselt aufbewahrt.

## **b. Übermittlung von Daten über verschlüsselte Datennetze oder Tunnelverbindungen („Data in Transit“)**

Alle personenbezogenen Daten, die von der MySports-Applikation an einen Client oder an andere Plattformen über ein unsicheres oder öffentliches Netzwerk übertragen werden, werden ausschließlich verschlüsselt übertragen. Dies gilt insbesondere auch für Zugriffe auf das Kunden- und Admin-System. MySports gewährleistet die Verwendung einer Verschlüsselungsmethode nach dem Stand der Technik in Abhängigkeit des auf Auftraggeber-Seite kompatiblen Verschlüsselungsalgorithmus (derzeit HTTPS-Verbindungen bzw. Transport Layer Security (TLS), Stichwort „Abwärtskompatibilität: der Auftraggeber ist dafür verantwortlich, mit dem Stand der Technik kompatible Endgeräte/ Browser einzusetzen). Administrative Zugriffe auf Server-Systeme von MySports sowie die Übertragung von Backups erfolgen ausschließlich über verschlüsselte Verbindungen, bspw. Secure Shell (SSH)- bzw. Virtual Private Network (VPN). Für den Zugriff auf Kunden-Systeme im Rahmen der Heim- und Telearbeit wird eine VPN-Verbindung verwendet. Dabei werden ausschließlich VPN-Server verwendet, welche unter der unmittelbaren Kontrolle von MySports stehen. Der Einsatz von öffentlichen VPN-Providern ist nicht zulässig.

## **c. Verschlüsselung von mobilen Datenträgern**

Mobile Datenträger, auf denen Daten von MySports genutzt oder verarbeitet werden, werden ausschließlich verschlüsselt verwendet. Dies gilt insbesondere bei der Verwendung von USB-Sticks, externen Festplatten oder Ähnlichem. Grundsätzlich ist der Einsatz von mobilen Datenträgern zur Speicherung von Kundendaten jedoch nicht gestattet.

## **d. Verschlüsselung von Datenträgern auf Laptops**

Auf allen Laptops der Mitarbeiter wird eine entsprechende Festplattenverschlüsselung nach dem Stand der Technik eingerichtet.

## **e. Verschlüsselter Austausch von Informationen und Dateien**

Grundsätzlich erfolgt der Austausch von Informationen und Dateien zwischen Auftraggeber und MySports direkt verschlüsselt über die MySports-Applikation (siehe b.). Sofern personenbezogene Daten oder vertrauliche Informationen des Auftraggebers auf Server übertragen werden müssen, die nicht über TLS-verschlüsselte HTTPS-Uploads gesendet werden können, so werden diese mit Secure File Transfer Protocol (SFTP) oder einem anderen verschlüsselten Mechanismus nach dem Stand der Technik übertragen. Der Auftraggeber ist dafür verantwortlich, diesen sicheren Datentransport bei Bedarf einzufordern oder bereitzustellen.

## **f. E-Mail-Verschlüsselung**

Grundsätzlich werden alle von Mitarbeitern von MySports oder innerhalb der MySports- Applikation versendeten E-Mails mit TLS verschlüsselt. Ausnahmen können sein, wenn der empfangende Mailserver kein TLS unterstützt. Der Auftraggeber trägt dafür Sorge, dass entsprechende im Rahmen des Auftrags verwendete Mailserver TLS-Verschlüsselung unterstützen. Auf Anfrage stellt MySports eine Möglichkeit zum verschlüsselten Versand von Inhalten bereit (bspw. S/MIME).

## **3. Zutrittskontrolle**

*Verwehrung des Zugangs zu IT-Systemen und Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.*

#### **a. Elektronische Türsicherung**

Die Eingangstüren zu den Räumlichkeiten von MySports sind grundsätzlich verschlossen und elektronisch gesichert. Eine Öffnung der Türen erfolgt über einen personengebundenen elektronischen Schlüssel.

#### **b. Kontrollierte Schlüsselvergabe**

Es erfolgt eine zentrale, dokumentierte Schlüsselvergabe an die Mitarbeiter von MySports. Diese elektronischen Schlüssel könnten zentral von der Geschäftsführung bzw. Personalabteilung deaktiviert werden.

#### **c. Beaufsichtigung und Begleitung von Fremdpersonen**

Ein Zutritt externer Dienstleister und sonstiger Fremdpersonen darf nur durch vorheriger Autorisierung und Begleitung durch einen Mitarbeiter von MySports erfolgen.

#### **d. Sicherung von Räumlichkeiten mit erhöhtem Schutzbedarf**

Räumlichkeiten oder Schränke mit erhöhtem Schutzbedarf, beispielsweise Router-Raum, Büro der Personalabteilung, Schrank mit Vertragsunterlagen etc., werden grundsätzlich nach Verlassen oder Nutzung verschlossen. Ein Zutritt zu diesen Räumlichkeiten wird nur autorisiertem Personal gewährt.

#### **e. Geschlossene Türen und Fenster**

Mitarbeiter sind organisatorisch dazu angewiesen, Fenster und Türen außerhalb der Bürozeiten geschlossen bzw. verschlossen zu halten.

#### **f. Physische und umgebungsbezogene Sicherheit der Server-Systeme in den Rechenzentren**

MySports setzt ausschließlich Server-Systeme von Rechenzentrumsbetreibern ein, die eine gültige Zertifizierung nach ISO/IEC 27001 besitzen und demnach entsprechende technische und organisatorische Maßnahmen zur physischen und umgebungsbezogenen Sicherheit umsetzen, bspw.

- Das Rechenzentrum und die dort verwendeten Systeme sind in unscheinbaren Gebäuden untergebracht, die von außen nicht sofort als Rechenzentrum zu erkennen sind.
- Das Rechenzentrum selbst ist durch physische Sicherheitsmaßnahmen geschützt, um den unberechtigten Zutritt sowohl weiträumig (z. B. Zaun, Wände) als auch in den Gebäuden selbst zu verhindern.
- Der Zutritt zum Rechenzentrum wird durch elektronische Zugangskontrollen verwaltet und durch Alarmanlagen gesichert, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird.
- Die Zutrittsberechtigung wird von einer berechtigten Person genehmigt und innerhalb von 24 Stunden entzogen, nachdem ein Mitarbeiter- oder Lieferantendatensatz deaktiviert wurde.
- Alle Besucher müssen sich ausweisen und registrieren und werden stets von berechtigten Mitarbeitern begleitet.
- Zutritt zu sensiblen Bereichen wird zusätzlich durch Videoüberwachung überwacht.
- Ausgebildete Sicherheitskräfte bewachen das Rechenzentrum und die unmittelbare Umgebung davon 24 Stunden am Tag, 7 Tage die Woche.

### **4. Zugangskontrolle**

*Verhinderung der Nutzung und Verarbeitung von datenschutzrechtlich geschützten Daten durch Unbefugte.*

## a. Verwendung von Authentifizierungsverfahren

Zugänge, die den Zugriff auf personenbezogene Daten ermöglichen, erfolgen stets über verschlüsselte Protokolle: SSH, SSL/ TLS, HTTPS oder vergleichbare Protokolle.

- **Authentifizierungsverfahren IT-System/ Laptop**
  - Authentifizierung mit Benutzername und Passwort
- **Authentifizierungsverfahren Kunden-System** (Kunden-System = Zugang für Administratoren und Nutzer des Auftraggebers)
  - Authentifizierung mit E-Mail-Adresse
  - Selbstgewähltes Passwort (8 Zeichen, Zahlen, Buchstaben und Sonderzeichen; Speicherung via Bcrypt-Hash, Einhaltung technisch erzwungen)
  - Rate-Limiter und Captcha-System, um Anmeldeöglichkeiten einzuschränken
- **Authentifizierungsverfahren Admin-System** (Admin-System = Zugang zu Kunden-Systemen via Benutzeroberfläche für Mitarbeiter im Bereich Kundenservice sowie Produktentwicklung von MySports, wenn dies vom Kunden für Support-Zwecke freigeschaltet wurde)
  - Authentifizierung mit E-Mail-Adresse
  - Selbstgewähltes Passwort (8 Zeichen, Zahlen, Buchstaben und Sonderzeichen)
  - Rate-Limiter und Captcha-System, um Anmeldeöglichkeiten einzuschränken
- **Authentifizierungsverfahren Server-/ Datenbank-System** (Server-/ Datenbank-System = Zugang auf die gespeicherten Daten durch Produktentwicklung des Auftragnehmers)
  - Administrative Zugriffe erfolgen über VPN und/oder SSH

## b. Benennung von Support- und Weisungsberechtigten und entsprechende Authentifizierung

Der Auftraggeber kann über die Systemeinstellungen Support- und Weisungsberechtigte bestimmen, welche MySports Weisungen entsprechend des Auftragsverarbeitungsvertrages erteilen können. Die Zuordnung zu einem Support- und Weisungsberechtigten erfolgt dabei über die von der MySports angegebenen Kontaktdaten (bspw. Name, E-Mail-Adresse, Telefonnummer, Benutzerkennung). Das Kundenservice-Team von MySports ist dazu angehalten, ausschließlich Weisungen von den benannten Personen anzunehmen bzw. Auskünfte zu erteilen und deren Identität im Vorfeld entsprechend zu überprüfen. Bei telefonischen Anfragen ist im Vorfeld der in MySports gespeicherte persönliche Telefon PIN zu verifizieren.

## c. Verwendung sicherer Passwörter

Bei der Vergabe und regelmäßigen Aktualisierung von sicheren Passwörtern sind die Maßgaben des BSI IT Grundschutz oder anderer äquivalenter, anerkannter Sicherheitsstandards für den MySports Account sowie für die Laptops, Computer oder sonstige mobile Endgeräte zu berücksichtigen (d.h. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennwortes). Nutzer von MySports sind dazu angehalten, vergleichbare Maßnahmen zur Sperrung bei Inaktivität treffen. Der Auftraggeber hat dafür Sorge zu tragen.

## d. Verbot der Weitergabe von Passwörtern und Nutzung von „Shared Accounts“

Sowohl für Nutzer von MySports als auch Mitarbeiter gilt das Verbot der Weitergabe von Passwörtern für die Nutzung von MySports sowie die Nutzung von sogenannten „Shared Accounts“ für den Zugang zu Kunden-, Admin- und administrativen Systemen (d.h. ausschließliche Nutzung persönlicher und individueller User Login bei Anmeldung am System).

## e. Automatische Sperrung bei Inaktivität

Laptops der Mitarbeiter von MySports werden bei Nichtbenutzung vom Benutzer mit Passwortschutz gesperrt. Zusätzlich wird eine automatische Bildschirmsperre mit Passwortschutz nach 10 Minuten

Inaktivität eingerichtet. Nutzer von MySports sind dazu angehalten, vergleichbare Maßnahmen zur Sperrung bei Inaktivität zu treffen. Der Auftraggeber hat dafür Sorge zu tragen.

#### **f. Einsatz von Anti-Viren-Software**

Laptops der Mitarbeiter von MySports sind mit einer dem Stand der Technik entsprechende und aktuell gehaltene Anti-Viren-Software auf allen betrieblichen oder betrieblich genutzten IT-Systemen ausgestattet. Es dürfen grundsätzlich keine Rechner ohne residenten Virenschutz betrieben werden, es sei denn, es sind andere äquivalente Sicherheitsmaßnahmen nach dem Stand der Technik getroffen oder ein Risiko besteht nicht. Vorgegebene Sicherheitseinstellungen dürfen nicht deaktiviert oder umgangen werden.

#### **g. „Clean Desk Policy“**

Mitarbeiter von MySports sind dazu angehalten, personenbezogene Daten von Kunden nicht auszudrucken oder lokal zu speichern, Arbeitsmaterialien grundsätzlich nicht offen herumliegen zu lassen und ordentlich zu verstauen. Unterlagen mit personenbezogenen Daten sind nach Gebrauch entweder in abschließbaren Schränken oder Schubfächern zu verstauen oder datenschutzgerecht zu entsorgen.

#### **h. Öffentliche drahtlose Netzwerke und Verbindung mit dem Firmennetz**

Öffentliche drahtlose Netzwerke werden ausschließlich über eine VPN-Verbindung, welche von MySports bereitgestellt wird, verwendet.

### **5. Zugriffskontrolle**

*Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.*

#### **a. Rollen- und Berechtigungskonzept**

- **Rollen- und Berechtigungskonzept Kunden-System**  
Administratoren des Auftraggebers können ein mehrstufiges Rollenkonzept zur Rechtevergabe individuell konfigurieren und dabei zwischen Ansichts-, Vorschlags- und Bearbeitungsrechten je Funktion bzw. Bereich innerhalb von MySports für individuelle Nutzer unterscheiden.
- **Rollen- und Berechtigungskonzept Admin-System**  
Der Zugriff auf das Admin-System ist grundsätzlich auf geschulte Mitarbeiter im Bereich Kundenservice und Produktentwicklung beschränkt. Mitarbeiter aus dem Vertriebs- und Finance-Team haben über das Admin-System lediglich Zugriff auf Kunden-Systeme während der kostenfreien Testphase bzw. auf entsprechende Abrechnungsdaten und können somit keine Kundendaten einsehen.
- **Rollen- und Berechtigungskonzept Server-/ Datenbank-System**  
Der Zugriff auf das Server-/ Datenbank-System ist grundsätzlich auf eine begrenzte Anzahl geschulter Mitarbeiter im Bereich Produktentwicklung und Infrastruktur beschränkt.

#### **b. Kontrolle der Zugriffsberechtigung für MySports auf Kunden-Systeme durch Auftraggeber**

Der Auftraggeber hat die über die Systemeinstellungen im Kunden-System die Möglichkeit zu entscheiden, ob MySports Zugriff auf das Kunden-System nehmen kann. Die Berechtigung des Zugriffs ist dabei als Voreinstellung deaktiviert und kann von dazu berechtigten Mitarbeitern des Auftraggebers jederzeit aktiviert oder deaktiviert werden.

### **c. Vergabe von Zugriffsrechten**

Die Vergabe von Zugriffsrechten erfolgt bei MySports grundsätzlich nach dem „Need-to-Know“-Prinzip. Zugänge erhalten demnach ausschließlich Personen, die ihn nachvollziehbar benötigen und solange sie ihn benötigen. Den Bedarf muss die beantragende Person bei der Beantragung schlüssig begründen. Das Berechtigungskonzept ist rollenbasiert. Jedem Mitarbeiter wird grundsätzlich eine bestimmte Rolle zugewiesen. Von dieser Rolle abweichende Berechtigungen müssen begründet sein. Die Zugriffsberechtigungen werden zentral dokumentiert sowie unmittelbar nach Erlöschen der Notwendigkeit des Zugriffs vom Administrator entzogen. Die Zugänge werden auf die minimal notwendigen Privilegien beschränkt. Zugriffe auf Admin-System oder Server-/ Datenbank-System werden durch das Management, die Leitung der Infrastruktur-Abteilung oder den Information Security Manager freigegeben und erfolgen in der Regel nach dem 4-Augen-Prinzip. Die Administratoren bzw. der Information Security Manager prüfen regelmäßig, ob erteilte Berechtigungen noch erforderlich sind. Vorgesetzte sind darüber hinaus verpflichtet, im Falle von Aufgabenwechsel von Mitarbeitern eine entsprechende Korrektur von Berechtigungen bei der IT-Administration zu beantragen. Im Falle des Ausscheidens von Mitarbeiter informieren die Personalverantwortlichen die Administratoren bzw. die Personalabteilung unverzüglich über anstehende Veränderungen, damit die entsprechenden Berechtigungen entzogen werden können. Der Entzug von Berechtigungen hat nach Möglichkeit binnen 24 Stunden nach Ausscheiden eines Mitarbeiters zu erfolgen.

### **d. Einsatz einer Paketfilter-Firewall**

Die Server von MySports nutzen Paketfilter-Firewalls, die sicherstellen, dass keine Dienste direkt aus dem Internet erreichbar sind. Öffentlich erreichbare Dienste werden über Loadbalancer oder Bastion-Hosts geleitet, die ausschließlich die Protokolle, die für den jeweiligen Dienst benötigt werden, zulassen.

### **e. Protokollierung von An- und Abmeldevorgängen**

Anmeldeversuche zum und sowie Abmeldevorgänge von Admin-, Kunden-System und Server-Systemen/-Software werden protokolliert (min. E-Mail-Adresse, Benutzer ID, IP-Adresse, Ergebnis des Anmeldeversuchs sowie Zeitstempel) und derzeit für bis zu 30 Tage aufbewahrt. Diese Protokolle können auf Anfrage und/ oder bei konkretem Verdacht ausgewertet werden.

### **f. Löschung und Vernichtung von Datenträgern**

Nicht mehr verwendete oder aussortierte Datenträger werden gemäß ihrer Schutzklasse (1-3 i.S.d. DIN 66399) ordnungsgemäß gelöscht und/oder vernichtet. Die Vernichtung wird entsprechend dokumentiert.

## **6. Trennbarkeit**

*Gewährleistung, dass zu unterschiedlichen Zwecken erhobene, personenbezogene Daten getrennt verarbeitet werden können und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.*

### **a. Trennung von Entwicklungs-, Test- und Betriebsumgebungen**

Daten aus der Betriebsumgebung dürfen nur in Test- oder Entwicklungsumgebungen überführt werden, wenn sie vor der Überführung vollständig anonymisiert wurden. Die Übertragung der anonymisierten Daten muss verschlüsselt oder über ein vertrauenswürdiges Netz erfolgen. Software, die in die Betriebsumgebung überführt werden soll, muss zuerst in einer identischen Test-Umgebung („Staging“) getestet werden. Programme für Fehleranalysen oder das Erstellen/ Kompilieren von Software dürfen in der Betriebsumgebung nur verwendet werden, wenn sich dies nicht vermeiden lässt. Dies ist vor allem dann der

Fall, wenn Fehlersituationen von Daten abhängig sind, die aufgrund der Anforderungen für die Anonymisierung bei der Überführung in Testumgebungen verfälscht würden.

### **c. Softwareseitige Mandantentrennung**

MySports stellt die getrennte Verarbeitung und Speicherung von Daten unterschiedlicher Auftraggeber über eine logische Mandantentrennung auf Basis einer Multi-Tenancy- Architektur sicher. Die Zuordnung und Identifizierung der Daten erfolgt dabei über die Zuweisung einer eindeutigen Kennung je Auftraggeber (bspw. Kundennummer/ „Company ID“). Die Absicherung der Architektur erfolgt durch die Implementierung von Integrationstests, welche sicherstellen, dass keine Datenbank-Abfragen ohne Abfrage und Zuordnung zu dieser Kennung durchgeführt werden und das Risiko der Umgehung der Mandantentrennung durch Programmierfehler minimiert wird. Regelmäßige Security- Audits sowie verbindliche Code-Reviews (4-bis 6-Augen-Prinzip) sichern die Architektur zusätzlich ab.

## **Maßnahmen zur Gewährleistung von Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**

### **7. Transport- und Weitergabekontrolle**

*Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird.*

#### **a. Transportverschlüsselung („Data in Transit“)**

Siehe „Verschlüsselung und Pseudonymisierung personenbezogener Daten“, Sicherstellung der Integrität der Daten beim Transport durch das Berechnen von Prüfsummen.

#### **b. Verbot der Weitergabe an unberechtigte Dritte**

Eine Weitergabe von personenbezogenen Daten, die im Auftrag des Auftraggebers erfolgt, darf jeweils nur in dem Umfang der Weisungen und soweit dies zur Erbringung der vertraglichen Leistungen für den Auftraggeber erforderlich ist, stattfinden. Insbesondere ist eine Weitergabe von personenbezogenen Daten aus dem Auftrag an unberechtigte Dritte, bspw. durch Speicherung in einem anderen Cloud-Speicher, nicht zulässig.

#### **c. Protokollierung der Weitergabe von Daten**

Siehe “Protokollierung von Systemaktivitäten innerhalb des Admin- und Kunden-Systems sowie Auswertung” unter “8. Eingabekontrolle”.

### **8. Eingabekontrolle**

*Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.*

#### **a. Protokollierung von Systemaktivitäten innerhalb des Admin- und Kunden-Systems sowie Auswertung**

Wesentliche Systemaktivitäten werden protokolliert (min. Benutzer ID, Rechte gemäß Rollenkonzept, IP Adresse, Systemkomponenten oder Ressourcen, Art der durchgeführten Aktivitäten sowie Zeitstempel) und

derzeit für bis zu 30 Tage aufbewahrt. Dazu zählen insbesondere die Eingabe, Änderung und Löschung von Daten, Nutzern und Berechtigungen sowie die Änderung von Systemeinstellungen. Auf Anfrage und/ oder bei konkretem Verdacht kann eine entsprechende Auswertung der Protokolle durchgeführt werden.

## **9. Verfügbarkeitskontrolle**

*Gewährleistung, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.*

### **a. Datensicherungsverfahren/ Backups**

MySports setzt zur Gewährleistung einer angemessenen Verfügbarkeit ein Backup-Konzept für die Datenbank mit den darauf gespeicherten Daten des Auftraggebers sowie das Speichermedium mit entsprechenden gespeicherten Dokumenten nach dem Stand der Technik um.

### **b. Geo-Redundanz in Bezug auf Server-Infrastruktur der Produktiv-Daten und Backups**

Zur Sicherstellung der Geo-Redundanz im Falle eines unvorhergesehenen Ereignisses, beispielsweise einer Naturkatastrophe, stellt MySports sicher, dass entsprechende Vorgaben der räumlichen Trennung in Bezug auf die Server-Infrastruktur der Produktiv- Daten und Backups gewährleistet ist. Dies kann durch die Verwendung unterschiedlicher Rechenzentren in ausreichender Entfernung oder von Rechenzentren unterschiedlicher Verfügbarkeitszonen sichergestellt werden.

### **c. Kapazitätsmanagement**

Es existiert ein Kapazitätsmanagement inkl. Überwachung und automatischer Benachrichtigung der zuständigen Mitarbeiter von MySports bei Kapazitätsengpässen.

### **d. Warnsysteme zur Überwachung der Erreichbarkeit und des Zustandes der Server- Systeme**

Es existiert ein Warnsystem zur Überwachung der Erreichbarkeit und des Zustandes der Server-Systeme. Bei Ausfällen wird die Infrastruktur-Abteilung automatisch benachrichtigt, um unmittelbar Maßnahmen zur Problembeseitigung zu ergreifen.

### **e. IT-Störungsmanagement („Incident Response Management“) (nach 16 ISO/IEC 27002:2017)**

Es existiert ein Konzept und dokumentiertes Verfahren zum Umgang mit Störungen und sicherheitsrelevanten Ereignissen („Incidents“). Dies umfasst insbesondere die Planung und Vorbereitung der Reaktion auf Vorfälle, Verfahren zur Überwachung, Erkennung und Analyse von sicherheitsrelevanten Ereignissen sowie die Festlegung entsprechender Verantwortlichkeiten und Meldewege im Falle einer Verletzung des Schutzes personenbezogener Daten im Rahmen der gesetzlichen Vorgaben.

### **f. Weitere Maßnahmen zur Gewährleistung der Verfügbarkeit in den Rechenzentren**

Im Rechenzentrum ist eine automatische Branderkennung und -bekämpfung installiert. Das System zur Branderkennung setzt Rauchsensoren in der gesamten Umgebung der Rechenzentren, in mechanischen und elektrischen Bereichen der Infrastruktur, Kühlräumen und sowie in den Räumen, in denen die Generatoren untergebracht sind, ein.

Alle Stromversorgungssysteme sind redundant. Eine unterbrechungsfreie Stromversorgung (USV) sorgt im Fall eines Stromausfalls dafür, dass kritische Bereiche der Anlage weiterhin mit Strom versorgt werden. Das Rechenzentrum verfügt darüber hinaus über Generatoren, die die gesamte Anlage mit Notstrom versorgen können. Das Rechenzentrum verfügt über eine Klimatisierung und Temperaturkontrolle. Es werden vorbeugende Wartungsmaßnahmen durchgeführt, um den fortlaufenden Betrieb der Anlagen zu gewährleisten.

## **10. Wiederherstellbarkeit**

*Gewährleistung, dass eingesetzte Systeme im physischen oder technischen Störfall wiederhergestellt werden können.*

### **a. Regelmäßige Tests der Datenwiederherstellung („Restore-Tests“)**

Es werden regelmäßige vollständige Restore-Tests zur Sicherstellung der Wiederherstellbarkeit im Falle eines Notfalls/ einer Katastrophe durchgeführt.

### **b. Notfallplan („Disaster Recovery Concept“)**

Es existiert ein Konzept zur Behandlung von Notfällen/ Katastrophen sowie ein entsprechender Notfallplan. MySports stellt die Wiederherstellung aller Systeme auf Basis der Datensicherungen/ Backups, in der Regel innerhalb von 24 Stunden, sicher.

## **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)**

## **11. Maßnahmen**

*Darstellung der Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.*

### **a. Risikomanagement**

Es existiert ein Prozess zur Analyse, Bewertung und Zuordnung von Risiken, zur Ableitung von Maßnahmen auf Basis dieser Risiken sowie einer regelmäßigen Bewertung der Wirksamkeit dieser Maßnahmen.

### **b. Auftragskontrolle**

*Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen Auftraggebers verarbeitet werden können.*

#### **i. Verarbeitung auf Weisung**

Die Mitarbeiter von MySports sind dazu angewiesen, personenbezogene Daten des Auftraggebers aus dem Auftrag ausschließlich auf dokumentierte Weisung im Rahmen des Auftragsvertrags und der Nutzungsvereinbarung zu verarbeiten. Gemäß Auftragsvertragsvertrag nimmt MySports Weisungen des Auftraggebers in schriftlicher Form sowie über die hierfür von Auftragnehmer angebotenen elektronischen Formate entgegen. Mündliche Weisungen sind nur in Eilfällen gestattet und durch den Auftraggeber unverzüglich schriftlich oder in einem hierfür von MySports angebotenen elektronischen Format zu bestätigen.

#### **ii. Sorgfältige Lieferantenauswahl**

Die Beauftragung von Lieferanten/Drittanbietern erfolgt bei Auslagerungen auf Basis eines sorgfältigen Auswahlprozesses in Zusammenarbeit mit dem Datenschutzbeauftragten und Rechtsabteilung nach festgelegten Kriterien, insbesondere hinsichtlich Datenschutz und IT-Sicherheit, dabei insbesondere ...

- Prüfung der Dokumentation und Einhaltung der technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO

- Je nach Schutzniveau und Umfang der personenbezogenen Daten, soweit möglich, Beauftragung von nur ISO/IEC 27001 zertifizierten Unternehmen (gilt in jedem Fall für Rechenzentren)

Zur Risikoprävention wird im Rahmen des Prozesses ebenfalls eine Risikobewertung für die jeweiligen Lieferanten durchgeführt, sofern der Drittanbieter regelmäßig mit personenbezogenen Daten arbeitet.

### **iii. Auftragsverarbeitung gemäß Art. 28 DS-GVO**

Eine Beauftragung und Nutzung eines Unterauftragnehmers erfolgt ausschließlich im Einklang des Auftragsverarbeitungsvertrags zwischen MySports und dem Auftraggeber, gesetzlichen Bestimmungen, sowie nach Abschluss einer entsprechenden Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO zwischen MySports und dem Unterauftragnehmer. Diese Vereinbarung hat nach Möglichkeit regelmäßig mindestens folgende Aspekte zu berücksichtigen:

- Vereinbarung wirksamer Kontrollrechte (im Einklang mit Rechten des Auftraggebers, nach Möglichkeit auch Vor-Ort-Kontrollen)
- Vereinbarung entsprechender Kontroll- und Auskunftsrechte bei der Beauftragung weiterer Unterauftragnehmer
- Vereinbarung von Vertragsstrafen bei Verstößen, sofern notwendig und möglich
- Ausschließliche Verarbeitung auf dokumentierte Weisung
- Ausschluss unzulässiger Verarbeitungsschritte
- Verbot der Anfertigung von Kopien von personenbezogenen Daten (ausgenommen Sicherungskopien/ Backups)
- Verpflichtung der Mitarbeiter des Unterauftragnehmers auf Vertraulichkeit
- Mitwirkung bei der Wahrung der Betroffenenrechte etc.
- Bestellung eines Datenschutzbeauftragten, sofern gesetzlich vorgeschrieben
- Informationspflichten bei meldepflichtigen Verletzungen des Schutzes personenbezogener Daten nach den Art. 33 und 34 DS-GVO, Betriebsstörungen sowie sonstigen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten
- Sicherstellung der Löschung/ Vernichtung von Daten nach Beendigung des Auftrags

### **iv. Durchführung regelmäßiger Kontrollen/ EINFORDERUNG VON NACHWEISEN**

MySports wird sich vor Beginn der Beauftragung und danach regelmäßig von der Einhaltung der technischen und organisatorischen Maßnahmen der von ihr eingesetzten Unterauftragnehmer überzeugen bzw. diese nachweisen lassen.