Dokumentation:
Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

von

Deutscher Olympischer Sportbund e.V.
Otto-Fleck-Schneise 12
60528 Frankfurt am Main

Der Deutsche Olympische Sportbund (DOSB) hat folgende technische und organisatorische Maßnahmen zur Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 DSGVO getroffen:

§ 1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Folgende Maßnahmen verhindern, dass unbefugte Personen Zutritt zu Datenverarbeitungsanlagen haben:

☒ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)

☒ Türsicherungen (elektrische Türöffner, Generalschlüssel)

☒ Sicherheitstüren / -fenster

☐ Gitter vor Fenstern/Türen

☐ Zaunanlagen

☒ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe

☒ Werkschutz, Empfang

☐ Alarmanlage

☒ Videoüberwachung

☒ Spezielle Schutzvorkehrungen des Serverraums (Zugang über Schlüssel, Schließsystem Serverschränke)

☒ Spezielle Schutzvorkehrungen für die Aufbewahrung von Backups und anderen Datenträgern (Systemseitige Sicherung, keine mobilen Backups/Datenträger)

☒ Nicht-reversible Vernichtung von Datenträgern

☒ Mitarbeiter- und Berechtigungsausweise

☐ Sperrbereiche

☒ Besucherregelung (z.B. Abholung am Empfang, Dokumentation von Besuchszeiten, Begleitung nach dem Besuch bis zum Ausgang)

1.2. Zugangskontrolle

Folgende Maßnahmen verhindern, dass Dritte unbefugten Zugang zu Datenverarbeitungsanlagen haben:

☒ Persönlicher und individueller Login bei Anmeldung am System/Netzwerk

☒ Autorisierungsprozess für Zugangsberechtigungen

☒ Begrenzung der befugten Benutzer

☒ Single Sign-On

☐ BIOS-Passwörter

☒ Kennwortverfahren

☒ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff

☒ Token, Zwei-Faktor-Authentifizierung

☒ Protokollierung des Zugangs (Protokollierung des Zugangs möglich, aber aus Mitbestimmungsgründen nicht aktiv)

☒ Zusätzlicher Login für bestimmte Anwendungen

☐ Automatische Sperrung der Clients nach Zeitablauf ohne Useraktivität

☒ Firewall

1.3. Zugriffskontrolle

Folgende Maßnahmen stellen sicher, dass Dritte keinen unbefugten Zugriff auf Daten haben:

☒ Verwaltung und Dokumentation von differenzierten Berechtigungen

☒ Abschluss von Verträgen zur Auftragsverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von Daten Gegenstand der Leistung des Auftragnehmers ist.

☐ Auswertungen/Protokollierungen von Datenverarbeitungen

☐ Autorisierungsprozess für Berechtigungen

☐ Genehmigungsroutinen

☒ Profile/Rollen

☐ Verschlüsselung von Datenträgern

☐ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf mobile Datenträger (z.B. Kopierschutz, Sperrung von USB-Ports, Data Loss Prevention System/DLP)

☐ Mobile Device Management (MDM)

☐ Vier-Augen-Prinzip

☐ Funktionstrennung (Segregation of Duties)

☒ Fachkundige Aktenvernichtung gemäß DIN 66399

☐ Nicht-reversible Löschung von Datenträgern

☐ Sichtschutzfolien für mobile Datenverarbeitungsanlagen

1.4. Trennungskontrolle

Folgende stellen sicher, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

☒ Speicherung der Datensätze in physikalisch getrennten Datenbanken

☐ Verarbeitung auf mindestens logisch getrennten Systemen

☒ Zugriffsberechtigungen nach funktioneller Zuständigkeit

☒ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen

☒ Mandantenfähigkeit von IT-Systemen (Anwendungsspezifisch)

☒ Verwendung von Testdaten (Anwendungsspezifisch)

☒ Trennung von Entwicklungs- und Produktionsumgebung (Anwendungsspezifisch)

§ 2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1. Weitergabekontrolle

Es ist sichergestellt, dass Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert, entfernt oder sonst verarbeitet werden können und überprüft werden kann, welche Personen oder Stellen Zugriff auf Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

☐ Verschlüsselung von E-Mail oder E-Mail-Anhängen

☐ Verschlüsselung von Datenträgern

☒ Gesicherter File Transfer (Anwendungsspezifisch)

☐ Physikalische Transportsicherung

☐ Verpackungs- und Versandvorschriften

☒ Qualifizierte elektronische Signatur (Anwendungsspezifisch)

☒ Verschlüsseltes WLAN

☒ Fernwartungskonzept (Verschlüsselung, Challenge-Response, Einmal-Passwort)

☐ Mobile Device Management (MDM)

☐ Data Loss Prevention System (DLP)

☐ Regelung zum Umgang mit mobilen Datenträgern (z.B. Laptop, USB-Stick, Mobiltelefon)

☐ Protokollierung von Datenübertragung oder Datentransport

☐ Protokollierung von lesenden Zugriffen

☐ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten

2.2 Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

☐ Zugriffsrechte

☒ Systemseitige Protokollierungen (Protokollierung des Zugangs möglich, aber aus Mitbestimmungsgründen nicht aktiv)

☒ Dokumenten Management System (DMS) / Enterprise Content Management System (ECMS) mit Änderungshistorie (Anwendungsspezifisch)

☐ Sicherheits-/Protokollierungssoftware

☒ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten

☒ Vieraugenprinzip (Prozessbezogen)

☐ Data Loss Prevention System (DLP)

§ 3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Durch folgende Maßnahmen ist sichergestellt, dass Daten gegen zufällige Zerstörung oder Verlust geschützt und für den DOSB stets verfügbar sind:

☒ Sicherheitskonzept für Software- und IT-Anwendungen (Anwendungsspezifisch)

☒ Backup Verfahren

☒ Gewährleistung der Datenspeicherung im gesicherten Netzwerk

☒ Bedarfsgerechtes Einspielen von Sicherheits-Updates

☒ Spiegeln von Festplatten

☒ Unterbrechungsfreie Stromversorgung (USV)

☒ Geeignete Archivierungsräumlichkeiten für Papierdokumente

☒ Brand- und/oder Löschwasserschutz des Serverraums

☐ Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten

☒ Klimatisierter Serverraum

☒ Virenschutz

☒ Firewall

☐ Notfallplan

☐ Erfolgreiche Notfallübungen

☒ Redundante, örtlich getrennte Datenaufbewahrung (Anwendungsspezifisch)

§ 4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1. Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

☒ Datenschutz-Richtlinie des DOSB

☒ Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit

☒ Benennung eines Datenschutzbeauftragten

☒ Verpflichtung der Mitarbeiter auf die Vertraulichkeit

☒ Hinreichende Schulungen der Mitarbeiter im Datenschutz

☒ Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO)

☒ Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)

☒ Externe Prüfung oder Auditierung

4.2. Management bei Datenschutzverletzungen

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

☒ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)

☐ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber betroffenen Personen (Art. 34 DSGVO)

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Datenschutzfreundliche Voreinstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Verarbeitungen zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben oder Eingabemöglichkeiten festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden. Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden) oder die Verfügbarkeit bestimmter Verarbeitungen, Funktionen oder Protokollierungen.

4.4. Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass Daten nur nach Weisungen des DOSB bei Auftragnehmern einer Auftragsverarbeitung verarbeitet werden:

☒ Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten der Parteien

☒ Prozess zur Erteilung und/oder Befolgung von Weisungen

☒ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern

☐ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung

☐ Unabhängige Auditierung der Weisungsgebundenheit

☒ Verpflichtung der Beschäftigten auf die Vertraulichkeit

☐ Vereinbarung von Vertragsstrafen für Verstöße gegen Weisungen

☐ formalisiertes Auftragsmanagement

☐ dokumentiertes Verfahren zur Auswahl von Unterauftragnehmern