Judo Verband Pfalz e.V.

Datenschutzrichtlinie des Judo Verbandes Pfalz e.V.

02.11.2023

§ 1 Bedeutung, Ziel, Zugänglichkeit

(1) Diese Datenschutzstrategie des Judo Verbandes Pfalz e.V. (kurz >>JVP<<) ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten im Verband. Sie hat die Funktion einer Richtlinie. Der Judo Verband Pfalz e.V. verarbeitet nur selten automatisiert personenbezogene Daten (z.B. im Rahmen der Mitgliederverwaltung, der Organisation des Sportbetriebs, der Öffentlichkeitsarbeit). Um die Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) zu erfüllen, Datenschutzverstöße zu vermeiden und einen einheitlichen Umgang mit personenbezogenen Daten innerhalb des Verbandes zu gewährleisten, entwickelt der JVP diese Datenschutzstrategie.

(2) Im Rahmen dieser Richtlinie sollen die Grundrechte und Grundfreiheiten der Betroffenen, insbesondere ihr Recht auf Schutz der personenbezogenen Daten gewahrt und geschützt werden. Den Datenschutz regelt die Satzung in §2 Abs. 4: „Der JVP ist verpflichtet, die sich aus der DSGVO ergebenden Regeln des Datenschutzes zu beachten. Die Organe des JVP, seine Mitarbeiter und Mitglieder sind zur Einhaltung dieser Regeln ebenfalls verpflichtet."

(3) Diese Richtlinie verwendet das generische Maskulinum.

§ 2 Geltungsbereich

(1) Die Richtlinie gilt für alle Beschäftigten, Funktionsträger, Ehrenamtliche und Organe und ist für diese jederzeit leicht zugänglich.

(2) Die Gebote und Verbote dieser Richtlinie gelten für jeglichen Umgang mit personenbezogenen Daten, unabhängig ob dieser elektronisch, mündlich oder in Papierform erfolgt. Ebenso sind alle Arten von Betroffenen (Mitglieder, Beschäftigte, Athleten etc.) in den Geltungsbereich einbezogen.

§ 4 Datenschutzorganisation, Zuständigkeiten

(1) Der JVP ist nach aktueller Rechtslage nicht verpflichtet, einen Datenschutzbeauftragten zu benennen. Dies wird regelmäßig überprüft und dokumentiert.

(2) Wenn benannt, gelten die folgenden Punkte (2) – (4): Der Datenschutzbeauftragte überwacht die Einhaltung der DSGVO sowie anderer gesetzlicher Vorgaben, einschließlich der Vorgaben dieser und anderer Richtlinien des Unternehmens zum Datenschutz.

(3) Der Datenschutzbeauftragte nimmt seine Aufgaben weisungsfrei und unter Anwendung seines Fachwissens wahr. Er berichtet unmittelbar dem Vorstand gemäß § 26 BGB.

(4) Der Verband bzw. seine Mitarbeiter haben den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen.

(5) Der JVP beschränkt allgemein die Verarbeitung personenbezogener Daten und führt regelmäßig eine Überprüfung sämtlicher Datenverarbeitungsvorgänge im Verband durch; d.h. eine Bedarfsanalyse hinsichtlich erforderlicher Änderungen und Ergänzungen der bestehen-

den Konzepte und Dokumentationen sowie der technischen und organisatorischen Maßnahmen. Überprüfung und Bedarfsanalyse sind mit den technisch-organisatorischen Maßnahmen, dem Verarbeitungsverzeichnis und der Nutzung von externen Informationsquellen bzw. externer Beratung Teil seiner Datenschutzstrategie.

(6) Verantwortlich für die Einhaltung der datenschutzrechtlichen Vorgaben ist der Vorstand nach § 26 BGB. Funktional ist die Aufgabe der Geschäftsstelle zugeordnet.

(7) Der Vorstand nach § 26 BGB stellt sicher, dass Verzeichnisse der Verarbeitungstätigkeiten nach Art. 30 DSGVO geführt und die Informationspflichten nach Art. 13 und 14 DSGVO erfüllt werden. Er ist für die Beantwortung von Auskunftsverlangen von betroffenen Personen zuständig.

Werden Daten dezentral durch bestimmte Funktionäre erfasst, stellt der Vorstand die Kontrolle sicher. Das bedeutet, dass die Funktionäre den Vertretern nach § 26 BGB Zugriff auf die Daten geben. Die konkrete Organisation und Arbeitsteilung orientieren sich an Satzung (§10, 11, 12) und Geschäftsordnung.

§ 3 Begriffsbestimmungen

(1) Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Betroffener). Kundendaten gehören dabei ebenso zu den personenbezogenen Daten wie Personaldaten von Beschäftigten. Beispielsweise lässt der Name eines Ansprechpartners ebenso einen Rückschluss auf eine natürliche Person zu, wie seine E-Mail-Adresse. Es genügt, wenn die jeweilige Information mit dem Namen des Betroffenen verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann. Ebenso kann eine Person bestimmbar sein, wenn die Information mit einem Zusatzwissen erst verknüpft werden muss, so z. B. beim Autokennzeichen. Das Zustandekommen der Information ist für einen Personenbezug unerheblich. Auch Fotos, Video- oder Tonaufnahmen können personenbezogene Daten darstellen.

(2) Besondere Arten personenbezogener Daten sind Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie eine eventuelle Gewerkschaftszugehörigkeit hervorgehen kann sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung einer natürlichen Person.

(3) Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(4) Einschränkung der Verarbeitung ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

(5) Profiling bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

(6) Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

(7) Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(8) Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(9) Empfänger ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

(10) Dritter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

(11) Eine Einwilligung des Betroffenen ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der der Betroffene zu verstehen gibt, dass er mit der Verarbeitung der ihn betreffenden personenbezogenen Daten einverstanden ist.

§ 5 Umgang mit personenbezogenen Daten

(1) Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten, es sei denn, eine gesetzliche Norm erlaubt explizit den Datenumgang. Personenbezogene Daten dürfen nach DSGVO grundsätzlich verarbeitet werden, wenn einer der in Art. 6 DSGVO genannten Erlaubnistatbestände zutrifft. Vornehmlich aber keinesfalls abschließend ist dies in folgenden Fallbeispielen der Fall:

- Bei einem bestehenden Vertragsverhältnis mit dem Betroffenen (Art. 6 Abs. 1 lit. b DSGVO).

Beispiel: Die Speicherung und Verwendung erforderlicher personenbezogener Daten im Rahmen des Fördervertrages, der zwischen Verband und (Kader)-Athleten geschlossen wird.

- Im Zuge vorvertraglicher/ vertragsähnlicher Maßnahmen auf Anfrage des Betroffenen sowie der Vertragsabwicklung mit dem Betroffenen (Art. 6 Abs. 1 lit. b DSGVO).

Beispiel: Wettkampf. Die Anmeldung zum Turnier erfolgt freiwillig, jeder Teilnehmer wird auf die Datenverarbeitung zum Zwecke der Durchführung des Turniers hingewiesen.

- Wenn und soweit der Betroffene eingewilligt hat (Art. 6 Abs. 1 lit. a DSGVO).

Beispiel: Der Betroffene meldet sich zum Erhalt eines Newsletters an.

- Wenn eine rechtliche Verpflichtung besteht, der der Verband unterliegt.

Beispiel: Gesetzliche Aufbewahrungsfristen nach Handelsgesetzbuch (HGB) und Abgabenordnung (AO) (Art. 6 Abs. 1 lit. c DSGVO).

- Wenn berechtigte Interessen des Verbandes bestehen, sofern nicht die Interessen oder Grundrechte des Betroffenen überwiegen, insbesondere wenn es sich um ein Kind handelt. Datenverarbeitungen unter Berufung auf ein berechtigtes Interesse sollten jedoch nicht ohne vorherige Beratung durch den Datenschutzbeauftragten vorgenommen werden (Art. 6 Abs. 1 lit. f DSGVO).

Beispiel: Die Nutzung der postalischen Anschrift von Geschäftspartner zur Versendung von Weihnachtskarten.

(2) Personenbezogene Daten sind für einen zuvor festgelegten, eindeutigen und legitimen Zweck zu verarbeiten. Eine Datenhaltung ohne Zweck, so beispielsweise die Speicherung von Daten auf Vorrat, ist unzulässig.

(3) Falls möglich, sollte auf einen personenbezogenen Datenumgang verzichtet werden. Pseudonyme oder anonyme Datenverarbeitungen sind vorzuziehen.

(4) Die Änderung einer Ziel- und Zweckbestimmung, die einem Datenumgang ursprünglich zugrunde gelegt wurde, ist – neben der erklärten Einwilligung durch den Betroffenen – nur zulässig, wenn der Zweck der Weiterverarbeitung mit dem ursprünglichen Zweck vereinbar ist. Hierbei sind insbesondere die vernünftigen Erwartungen des Betroffenen hinsichtlich einer solchen Weiterverarbeitung gegenüber dem Unternehmen, die Art der verwendeten Daten, die Folgen für den Betroffenen sowie Möglichkeiten einer Verschlüsselung oder Pseudonymisierung zu berücksichtigen.

(5) Der Betroffene ist bei der Erhebung seiner personenbezogenen Daten umfassend über den Umgang mit seinen Daten zu informieren. Die Information hat die Zweckbestimmung, die Identität der verantwortlichen Stelle, die Empfänger seiner personenbezogenen Daten sowie alle sonstigen Informationen im Sinne des Art. 13 DSGVO zu beinhalten, um eine faire und transparente Verarbeitung zu gewährleisten. Die Information ist in einer verständlichen und leicht zugänglichen Form sowie einer möglichst einfachen Sprache zu verfassen.

(6) Werden personenbezogene Daten nicht beim Betroffenen erhoben, sondern beispielsweise bei einem anderen Unternehmen beschafft, ist der Betroffene nachträglich und umfassend gemäß Art. 14 DSGVO über den Umgang mit seinen Daten zu informieren. Dies gilt auch für die Änderung einer Ziel- und Zweckbestimmung der Datenverarbeitung.

(7) Personenbezogene Daten müssen sachlich richtig und, wenn nötig, auf dem neusten Stand sein. Der Umfang der Datenverarbeitung sollte hinsichtlich der festgelegten Zweckbestimmung erforderlich und relevant sein. Die jeweilige Fachabteilung hat für die Umsetzung durch die Etablierung entsprechender Prozesse Sorge zu tragen. Ebenso sind Datenbestände regelmäßig auf ihre Richtigkeit, Erforderlichkeit und Aktualität hin zu überprüfen.

§ 6 Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogene Daten dürfen grundsätzlich nur mit Einwilligung des Betroffenen oder ausnahmsweise aufgrund einer expliziten gesetzlichen Erlaubnis erhoben, verarbeitet oder genutzt werden. Ferner sind zusätzliche technische und organisatorische Maßnahmen (z. B. Verschlüsselung beim Transport, minimale Rechtevergabe) zum Schutz besonderer personenbezogener Daten zu ergreifen.

Der JVP verarbeitet grundsätzlich – bis auf wenige Ausnahmen – keine Gesundheitsdaten.

§ 7 Sicherheit und Sicherheitseinstellungen

(1) Sicherheitseinstellungen in Programmen und an sämtlichen Endgeräten dürfen nur nach Absprache mit dem Vorstand geändert werden. Im Übrigen ist es untersagt, die Konfiguration der Benutzeroberflächen und Geräte in sicherheitsrelevanten Belangen zu ändern.

(2) E-Mails mit unbekanntem Adressaten und/ oder deren komprimierte Anhänge (Beispiel: zip-Dateien) dürfen nicht ohne vorherige Prüfung geöffnet werden. Links in E-Mails dürfen bei Auffälligkeiten nicht geöffnet werden. Auffälligkeiten liegen insbesondere vor, wenn

- der Adressat der E-Mail unbekannt ist,

- der Inhalt der E-Mail keinen Bezug zur Tätigkeit des Empfängers hat

- Passwörter oder Zugangsdaten abgefragt werden.

(3) Der Verband wird seine Mitarbeiter nie per E-Mail auffordern, Zugangsdaten preiszugeben.

(4) Bevor E-Mails versendet werden, ist darauf zu achten, ob der richtige Empfänger im Adressfeld steht. Auch der Unterschied zwischen „To:/An:“ (Empfänger), „CC:“ (Kopie) und „BCC:“ (Blindkopie) ist zu beachten. Soll ein Empfänger für andere nicht sichtbar sein, muss er stets in Blindkopie gesetzt werden. Sofern keine Erlaubnis der Kopie Empfänger vorliegt, dass deren E-Mail-Adressen und sonstige Daten an die anderen Empfänger weitergegeben werden, muss eine E-Mail stets in Blindkopie verschickt werden. Bei einer größeren Anzahl an Empfängern konsultieren Sie bitte den Vorstand zur Einrichtung einer Mailingliste. In Mails an größere Verteiler und insbesondere mehrere Personen, die weder Funktionär noch

Mitarbeiter des Verbandes sind, müssen alle diese Empfänger in BCC (Blindkopie) gesetzt werden.

(5) Es dürfen keine E-Mails an Ihre private E-Mail-Adresse weitergeleitet werden.

(6) Seitens der Mitarbeiter dürfen keine Bilder von Mitarbeitern, Veranstaltungen oder Bildern mit oder von Athleten beispielsweise bei Facebook oder über sonstige Medien veröffentlicht werden, es sei denn der Mitarbeiter wurde von der Geschäftsleitung und deren Vertreter ausdrücklich dazu ermächtigt. Zudem muss von den abgebildeten Personen eine wirksame Einwilligung vorliegen.

(7) Alle Funktionäre und Mitarbeiter verpflichten sich, die technisch-organisatorischen Maßnahmen einzuhalten, die sie betreffen (diese sind in einem separaten Dokument erfasst, sie enthalten u.a.: Zutrittskontrolle, Zugangskontrolle, Maßnahmen der Zugriffskontrolle, Gewährleistung der Vertraulichkeit durch Weitergabekontrolle).

Funktionäre und Mitarbeiter sind verpflichtet auch verpflichtet, sichere Passwörter zu nutzen und diese zu schützen; zur Nutzung einer Anti-Viren-Software auf allen privaten Geräten, die (auch) für Verband benutzt werden; zur Anwendung aktueller Sicherheitstechnik und Verschlüsselung; zum Einsatz von Systemsperren und aktueller Software sowie eines Backup-Systems.

Die Weitergabe von vertraulichen Daten auf physischen Datenträgern muss der Vorstand gemäß §26 BGB genehmigen.

§ 8 Datenübermittlung

(1) Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis oder der Einwilligung des Betroffenen zulässig.

(2) Befindet sich der Empfänger personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen Betroffener. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist oder beispielsweise über besondere Vertragsklauseln nicht hergestellt werden kann.

(3) Die Nutzung von WhatsApp oder ähnlicher Messenger-Dienste (beispielsweise Facebook-Messenger) auf Smartphones und Tablets oder sonstigen Geräten des Verbandes oder auf privaten Geräten zur Verbandskommunikation ist untersagt. Als Alternative für die informelle Kommunikation ist Threema zur Nutzung erlaubt.

(4) Die Nutzung von Cloud-Diensten (Dropbox, iCloud, etc.) ist untersagt, sofern der JVP dies nicht ausdrücklich vorsieht oder erlaubt.

§ 9 Externe Dienstleister

(1) Sofern externe Dienstleister Zugriff auf personenbezogene Daten erhalten sollen, ist der Vorstand BGB§26 vorab zu informieren.

(2) Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Die Auswahl ist zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:

- Fachliche Eignung des Auftragnehmers für den konkreten Datenumgang
- Technisch-organisatorische Sicherheitsmaßnahmen
- Erfahrung des Anbieters im Markt
- Sonstige Aspekte, die auf eine Zuverlässigkeit des Anbieters schließen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten etc.)

(3) Soll ein Dienstleister personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, bedarf es des Abschlusses eines Vertrags zur Auftragsverarbeitung. Hierin sind Datenschutz- und IT-Sicherheitsaspekte zu regeln.

(4) Der Dienstleister ist im Hinblick auf die mit ihm vertraglich vereinbarten technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

§ 10 Datenminimierung, Löschvorschriften

(1) Der Umgang mit personenbezogenen Daten ist an dem Ziel auszurichten, so wenige Daten wie möglich von einem Betroffenen zu erheben, zu verarbeiten oder zu nutzen („Datenminimierung“). Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist. Beispielsweise wird es im Rahmen einer statistischen Auswertung von Daten nicht notwendig sein, den vollen Namen eines Betroffenen zu kennen und zu verwenden. Vielmehr kann diese Information durch einen Zufallswert ersetzt werden, der eine Unterscheidbarkeit der zugrunde liegenden Information ebenfalls gewährleisten kann.

(2) Entsprechendes gilt für die Auswahl und Gestaltung von Datenverarbeitungssystemen. Der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern, so insbesondere den Grundsatz der Datenminimierung.

(3) Das Löschkonzept wird regelmäßig überprüft und entsprechende Löschroutinen sind eingeführt.

(4) Daten und Informationen, welche von Funktionsträgern, Ehrenamtlichen und Mitarbeitenden des JVP verarbeitet werden sind spätestens mit Ende der Tätigkeit für den JVP an diesen herauszugeben und auf privaten Endgeräten unwiederbringlich nach dem Stand der Technik zu löschen.

(5) Handelt es sich um ein technisches Gerät des Verbandes, muss dieses zurückgegeben werden. Verwiesen wird außerdem auf das Berechtigungskonzept des Verbandes.

§ 11 Rechte von Betroffenen

(1) Betroffene haben das Recht auf Auskunft über die im Unternehmen über ihre Person gespeicherten personenbezogenen Daten.

(2) Bei der Bearbeitung von Anträgen ist die Identität des Betroffenen zweifelsfrei festzustellen. Bei begründeten Zweifeln an der Identität können zusätzliche Angaben vom Antragsteller angefordert werden.

(3) Die Auskunftserteilung erfolgt schriftlich, es sei denn der Betroffene hat den Antrag auf Auskunft elektronisch gestellt. Der Auskunft ist eine Kopie der Daten des Betroffenen beizufügen, die, neben den zur Person vorhandenen Daten, auch die Empfänger von Daten, den Zweck der Speicherung sowie alle weiteren gesetzlich geforderten Informationen nach Art. 15 DS-GVO beinhaltet, um den Betroffenen die Verarbeitung bewusst zu machen und die Rechtmäßigkeit selbst beurteilen zu lassen. Auf besonderen Wunsch des Betroffenen werden die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt.

(4) Betroffene haben einen Anspruch auf Berichtigung ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen. Ebenso können sie die Vervollständigung unvollständiger personenbezogener Daten verlangen.

(5) Der Betroffene hat das Recht auf Löschung seiner personenbezogenen Daten unter den folgenden Voraussetzungen:

- die Kenntnis der Daten ist für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich
- der Betroffene hat eine Einwilligung widerrufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung
- ihre Verarbeitung ist unzulässig,
- der Betroffene legt Widerspruch gegen die Verarbeitung zu Werbezwecken ein oder beruft sich auf ein Widerspruchsrecht aufgrund einer besonderen – zu begründenden – persönlichen Situation,
- es handelt sich um besondere personenbezogene Daten, deren Richtigkeit nicht bewiesen werden kann, oder
- es besteht eine anderweitige rechtliche Verpflichtung zur Datenlöschung.

Besteht eine Verpflichtung zur Löschung und wurden die personenbezogenen Daten zuvor öffentlich gemacht, sind weitere Verantwortliche für die Datenverarbeitung über ein Löschbegehren des Betroffenen hinsichtlich aller Kopien seiner Daten sowie aller Links zu diesen Daten zu informieren.

(6) Der Betroffene kann die Einschränkung der Verarbeitung seiner Daten verlangen, wenn

- die Richtigkeit der personenbezogenen Daten strittig ist, jedoch nur so lange, wie die Richtigkeit durch die zuständige Fachabteilung überprüft wird oder

- die Verarbeitung unzulässig ist, der Betroffene die Datenlöschung aber ablehnt, oder

- das Unternehmen die personenbezogenen Daten für Zwecke der Verarbeitung nicht mehr benötigt, der Betroffene die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder

- der Betroffene Widerspruch gegen die Verarbeitung aufgrund einer besonderen Situation eingelegt hat und die zuständige Fachabteilung noch mit der Prüfung des Widerspruchs befasst ist.

(7) Der Betroffene ist spätestens innerhalb eines Monats über alle ergriffenen Maßnahmen, die auf seinen Antrag hin erfolgt sind, zu informieren.

(8) Der Datenschutzbeauftragte steht bei der Wahrung der Betroffenenrechte beratend zur Verfügung.

§ 12 Auskunftsersuchen Dritter über Betroffene

Sollte eine Stelle Informationen über Betroffene fordern, so beispielsweise Athleten oder Trainer, ist eine Weitergabe von Informationen nur zulässig, wenn

- die Auskunft gebende Stelle ein berechtigtes Interesse hierfür darlegen kann, und

- eine gesetzliche Norm zur Auskunft verpflichtet, sowie

- die Identität des Anfragenden oder der anfragenden Stelle zweifelsfrei feststeht.

§ 13 Verarbeitung personenbezogener Daten im Rahmen der Öffentlichkeitsarbeit

(1) Die werbliche Ansprache von Betroffenen per Brief, Telefon, Fax, oder E-Mail ist grundsätzlich nur zulässig, wenn der Betroffene zuvor in die Verwendung seiner Daten zu Werbezwecken eingewilligt hat.

(2) Ausnahmen sind nur beim Vorliegen einer Erlaubnisnorm zulässig.

(3) Die Veröffentlichung personenbezogener Daten, insbesondere von Fotos und Videos, die außerhalb öffentlicher Veranstaltungen erhoben und erstellt wurden, erfolgt ausschließlich auf Grundlage einer Einwilligung der betroffenen Personen.

(4) Auf der Internetseite des Verbandes werden auch Daten der Mitglieder des Gesamtvorstandes mit Vornamen, Nachname, Funktion, E-Mail-Adresse und Telefonnummer veröffentlicht. Dies kann auch weitere Funktionäre (Ehrenrat, Kassenprüfer) betreffen.

(5) Die Einrichtung und Unterhaltung von Auftritten im Internet obliegt dem Pressereferenten. Änderungen dürfen ausschließlich durch berechtigte Funktionäre vorgenommen werden, die zu diesem Zweck einen Login mit entsprechender Berechtigungsstufe erhalten. Die Pressereferenten sind stets zur Einhaltung datenschutzrechtlicher Vorschriften verpflichtet.

(6) Verantwortlich für die Einhaltung der Datenschutzbestimmungen im Zusammenhang mit Online-Auftritten ist der Vorstand gemäß §26 BGB und die von ihm beauftragten Funktionäre. Dieselben Personen sind auch für den Inhalt, einschließlich Rechtschreibung und Grammatik, und die Einhaltung einschlägiger gesetzlicher Vorgaben außerhalb des Datenschutzes verantwortlich. Die Pressereferenten sind verpflichtet, sich Beiträge ggf. vom Vorstand gemäß §26 BGB vor Veröffentlichung freigeben zu lassen.

§ 14 Datengeheimnis

(1) Allen Mitarbeitenden, Funktionsträgern und Ehrenamtlichen des JVP ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Sie sind vor Aufnahme ihrer Tätigkeit auf einen vertraulichen Umgang mit personenbezogenen Daten zu verpflichten. Die Verpflichtung erfolgt durch den Vorstand gemäß § 26 BGB unter Verwendung des hierzu vorgesehenen Formulars.

(2) Das gilt entsprechend für beispielsweise Berater und projektbezogene Dienstleister im Verband, die Umgang mit personenbezogenen Daten haben.

(3) Personenbezogene Daten werden auf der Grundlage der datenschutzrechtlichen Anforderungen verarbeitet, d.h. wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlaubt oder eine Verarbeitung dieser Daten vorgeschrieben ist.

§ 15 Beschwerden

(1) Jeder Betroffene hat das Recht, sich über eine Verarbeitung seiner Daten zu beschweren, sollte er sich hierdurch in seinen Rechten verletzt fühlen. Ebenso können Beschäftigte Verstöße gegen diese Datenschutzrichtlinie jederzeit anzeigen.

(2) Die zuständige Stelle für die oben genannten Beschwerden wird im § 4 benannt: ist ein Datenschutzbeauftragter benannt, ist dieser für Beschwerden zuständig – wenn nicht, ist es der Vorstand gemäß §26 BGB.

§ 16 Verfügbarkeit, Vertraulichkeit und Integrität von Daten

(1) In Abhängigkeit der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit hat für jedes Verfahren eine dokumentierte Schutzbedarfsfeststellung und Analyse hinsichtlich der Risiken für Betroffene zu erfolgen.

(2) Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten wird ein allgemeines Sicherheitskonzept in Abhängigkeit der Schutzbedarfsfeststellung und Risikoanalyse erstellt, das für alle Verfahren verbindlich ist. Hierin ist insbesondere der Stand der Technik ebenso zu berücksichtigen, wie Mittel und Maßnahmen zur Verschlüsselung und Datensiche-

rung. Das Sicherheitskonzept ist hinsichtlich der Wirksamkeit der dort vorgesehenen technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen, zu bewerten und zu evaluieren.

(3) Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Türen unbesetzter Räume sind zu verschließen. Wirksame Maßnahmen zur Zugangskontrolle an Geräten müssen vorhanden und aktiviert sein. Systemzugänge sind in Abwesenheit stets zu sperren. Bildschirmsperren sind bei sämtlichen Endgeräten bei Verlassen des Arbeitsplatzes zu aktivieren.

(4) Passwörter ermöglichen einen Zugang zu Systemen und den darin gespeicherten personenbezogenen Daten. Sie stellen eine persönliche Kennung des Nutzers dar und sind nicht übertragbar. Es ist sicherzustellen, dass Passwörter stets unter Verschluss gehalten werden. Passwörter müssen eine minimale Länge von acht Zeichen aufweisen und aus einem Zeichenmix (Groß- und Kleinbuchstaben sowie Sonderzeichen) bestehen. Passwörter dürfen nicht in einem Wörterbuch vorkommen oder aus leicht zu erratenden Begriffen gebildet werden, insbesondere nicht Begriffe, die im Zusammenhang mit dem Verband stehen. Passwörter dürfen nicht weitergegeben werden oder auf einem Zettel notiert werden.

(5) Smartphones und Tablets sind mit zusätzlichen PINs zusätzlich zu den SIM-PINs zu versehen oder mit Fingerabdruckschutz zu versehen.

(6) Zugriffe auf personenbezogene Daten sollen nur diejenigen Personen erhalten, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen („Need-to-know-Prinzip“). Zugriffsberechtigungen müssen genau und vollständig festgelegt und dokumentiert sein.

(7) Datenübertragungen durch öffentliche Netze sind nach Möglichkeit zu verschlüsseln. Eine Verschlüsselung hat zwingend zu erfolgen, falls der Schutzbedarf der personenbezogenen Daten dies erfordert.

(8) Zu unterschiedlichen Zwecken erhobene personenbezogene Daten sind getrennt voneinander zu verarbeiten. Die Trennung von Daten ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen.

(9) Wartungsarbeiten an Systemen oder Telekommunikationseinrichtungen durch externe Dienstleister sind zu beaufsichtigen. Ferner ist zu gewährleisten, dass Dienstleister nicht unbefugt auf personenbezogene Daten zugreifen können. Fernwartungszugänge sind nur im Einzelfall zu gewähren und müssen dem Prinzip der minimalen Rechtevergabe folgen. Fernwartungsaktivitäten sind nach Möglichkeit aufzuzeichnen oder zu protokollieren.

(10) Ausdrucke mit personenbezogenen Daten oder Datenträger wie CDs, USB-Sticks oder Festplatten dürfen keinesfalls einfach weggeworfen oder weggegeben werden, sondern müssen ordnungsgemäß geschreddert oder durch die EDV-Abteilung sicher gelöscht werden.

§ 17 Verletzungen des Schutzes von Daten („Datenpanne“)

(1) Sollten personenbezogene Daten in der Verantwortlichkeit des JVP unrechtmäßig Dritten offenbart worden sein, ist darüber unverzüglich der Vorstand nach § 26 BGB zu informieren. Dieser zieht den Datenschutzbeauftragten oder einen externen Berater im Rahmen der Sachverhaltsaufklärung hinzu.

(2) Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen, insbesondere die empfangende Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.

(3) Die Erfüllung einer etwaigen Informationspflicht wird gegenüber der Aufsichtsbehörde ausschließlich durch den Vorstand nach § 26 BGB oder einer durch ihn beauftragten Person erfolgen. Der Datenschutzbeauftragte oder ein externer Berater ist jedoch stets zu involvieren und vorab zu Rate zu ziehen. Betroffene werden, sofern erforderlich durch den Vorstand informiert, wobei der Datenschutzbeauftragte oder der externe Berater hinzugezogen wird.

§ 18 Folgen von Verstößen

(1) Ein fahrlässiger oder gar mutwilliger Verstoß gegen diese Richtlinie kann arbeitsrechtliche Maßnahmen nach sich ziehen, einschließlich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

(2) Fast alle Verstöße gegen das Datenschutzrecht können mit Geldbuße bestraft werden (Art. 83 DS-GVO). Diese Geldbuße kann bis zu 20.000.000 EUR pro Verstoß betragen oder bis zu vier Prozent des weltweiten Jahresumsatzes, je nachdem, was höher ist. Geldbußen können sogar gegen einzelne Mitarbeiter verhängt werden: Geben Sie beispielsweise ohne eine entsprechende Anweisung des Vorstandes personenbezogene Daten weiter oder nutzen Sie sie für Ihre eigenen Zwecke, können Sie persönlich mit einer Geldbuße bis zu 20.000.000 EUR bestraft werden. Zudem sind bestimmte Verstöße gegen das Datenschutzrecht Straftaten, die mit Gefängnis bestraft werden können (§ 42 BDSG): Beispiel: Jemand verkauft weisungswidrig eine Festplatte mit personenbezogenen Daten, anstatt sie zu zerstören.

Verstöße gegen das Datenschutzrecht können zudem nach anderen Gesetzen strafbar sein, z. B. nach § 17 UWG (Verrat von Geschäfts- und Betriebsgeheimnissen), § 202 a StGB (Ausspähen von Daten) oder § 263 a StGB (Computerbetrug).

§ 19 Rechenschaftspflicht

Die Einhaltung der Vorgaben dieser Richtlinie muss jederzeit nachgewiesen werden können. Hierbei ist insbesondere auf die Nachvollziehbarkeit und Transparenz getroffener Maßnahmen zu achten, so beispielsweise über zugehörige Dokumentationen.

§ 20 Aktualisierung der Richtlinie; Nachweisbarkeit

(1) Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.

(2) Änderungen an dieser Richtlinie sind formlos wirksam. Die Funktionsträger, Mitarbeitenden und Ehrenamtlichen des JVP sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.