Datenschutzordnung

des

Württembergischen Kegler- und Bowling-Verband e.V.

Inhaltsverzeichnis

Versionshistorie für die Datenschutzordnung

Version	Datum	Anmerkungen	Beschluss
1.0	06.04.2019	Initialfassung der Datenschutzordnung	Vorstandssitzung vom 06.04.2019

1. Einleitung

Der Vorstand des Württembergischen Kegler- und Bowling-Verband e.V. (WKBV, nachfolgend auch „Verband“ genannt) hat diese Datenschutzordnung beschlossen.

Als Verband verarbeiten wir eine Vielzahl von (auch personenbezogenen) Daten, um unsere Aufgaben und Pflichten gegenüber unseren Mitgliedern, Trainern, Ehrenamtlichen, Mitarbeitern, Vertragspartnern, Dienstleistern, öffentlichen Stellen und sonstigen Dritten zu erfüllen.
Die Sicherheit der Informationsverarbeitung und der Schutz von personenbezogenen Daten spielt eine wesentliche Rolle in unserem Verband. Diese Datenschutzordnung soll die Strategie, die Organisation und Ziele von Datenschutz und Informationssicherheit in unserem Verband in übersichtlicher Form darstellen. Sie ist von allen Mitgliedern, Beschäftigten, Trainern und Ehrenamtlichen des WKBV einzuhalten.

2. Ziele

Ziel dieser Datenschutzordnung ist es, Datenschutz und Informationssicherheit im Verband gemäß den gesetzlichen Vorgaben, insbesondere der **EU-Datenschutz-Grundverordnung (DSGVO)**, zu gewährleisten. Für diesen Zweck wird der Verband bei der Planung, Einführung und während des Ablaufs von Prozessen nachfolgende Ziele berücksichtigen:

1. Rechtmäßigkeit
2. Transparenz
3. Zweckbindung
4. Datenminimierung
5. Richtigkeit
6. Speicherbegrenzung
7. Verfügbarkeit, Integrität und Vertraulichkeit, Belastbarkeit

8. Intervenierbarkeit und Verarbeitung nach Treu und Glauben („Fairness“)

9. Rechenschaftspflicht („Accountability-Prinzip“)

Bei der konkreten Umsetzung der Ziele müssen die getroffenen Schutzmaßnahmen in einem wirtschaftlich vertretbaren Verhältnis zum Schutzbedarf der verarbeiteten Daten und Informationen stehen.

3. Verantwortlichkeit und Organisation des Datenschutzes

a) Verantwortung im Verband

Verantwortlich für den Datenschutz und die Informationssicherheit sowie deren operative Umsetzung im Verband ist der Vorstand. Er benennt ggf. Verantwortliche, die diese Funktion in seinem Auftrag wahrnehmen. Er ist für die Mitarbeiter und Ehrenamtlichen zentrale Stelle und Ansprechpartner für den Datenschutz.

Der Datenschutzverantwortliche wird mindestens einmal jährlich diese Datenschutzordnung sowie die getroffenen Maßnahmen zum Datenschutz überprüfen und bei Bedarf Anpassungen vornehmen.

Die zentrale E-Mail-Adresse für alle Belange des Datenschutzes, wie z.B. Anfragen und Beschwerden, lautet: Datenschutzverantwortlicher@WKBV.de. Diese E-Mail-Adresse muss entsprechend veröffentlicht und bekannt gemacht werden.

b) Datenschutzbeauftragter (DSB)

Aufgrund des Umfangs und der Art der Datenverarbeitung beim WKBV und der Tatsache, dass mehr als 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind, ist die Ernennung eines Datenschutzbeauftragten nach Artikel 37 Abs. 1 lit. b) und c) i.V. mit § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG, in der seit 25.05.2018 geltenden Fassung) erforderlich.

Der Datenschutzbeauftragte und der Datenschutzverantwortliche ist Ansprechpartner für das Thema Datenschutz im Verband. Er berät, kontrolliert und unterstützt den Vorstand und Beschäftigten hinsichtlich der Verarbeitung von personenbezogenen Daten im Verband. Seine weiteren Aufgaben ergeben sich vor allem aus Art. 39 DSGVO.
Im Bereich der Verarbeitung von personenbezogenen Daten ist Sorge dafür zu tragen, dass eine frühe Einbindung des Datenschutzbeauftragten oder den Datenschutzveranwortlichen bei der Planung und Einführung von neuen Prozessen, in deren Zusammenhang auch personenbezogene Daten verarbeitet werden, erfolgt. Gleiches gilt für Änderungen an bestehenden Prozessen.

Als Datenschutzbeauftragter des WKBV ist derzeit ernannt:

Jochen Dannemann, Holbeinstraße 42, 70806 Kornwestheim, Telefon 07154/8019933, E-Mail: datenschutzbeauftragter@kwh-datenservice.de

Als Datenschutzverantwortlicher des WKBV ist derzeit benannt :

Wolfgang Kunkel, Jakobstrasse 34, 73734 Esslingen Telefon ¨0711 3452274, einstein1010@arcor.de

c) Verpflichtung der Mitarbeiter, Schiedsrichter, Trainer, Mannschaftsführer und Ehrenamtlichen

Jeder Mitarbeiter, Schiedsrichter, Trainer Mannschaftsführer und Ehrenamtliche trägt durch sein Verhalten zur Gewährleistung von Datenschutz und Informationssicherheit bei.

Personenbezogene Daten werden nicht eigenmächtig verarbeitet. Es wird ausschließlich die vom Verband bereitgestellte oder genehmigte Hard- und Software genutzt.

Beschäftigte, Schiedsrichter, Trainer, Mannschaftsführer und Ehrenamtliche des WKBV sind verpflichtet, alle sie oder ihre Tätigkeit betreffenden Regelungen, wie z.B. diese Datenschutzordnung, im Umgang mit personenbezogenen Daten einzuhalten. Dies gilt insbesondere für Vorgaben, die die Sicherheit personenbezogener Daten betreffen. Sollten Beschäftigte, Schiedsrichter, Trainer, Mannschaftsführer und Ehrenamtliche unsicher sein, ob und inwieweit Rechtsvorschriften oder Verbandsregelungen einzuhalten sind, haben sie sich an den Datenschutzverantwortlichen zur Klärung zu wenden.

Alle Beschäftigten, Schiedsrichter, Trainer, Mannschaftsführer und Ehrenamtlichen sind zeitnah nach Beginn der Aufnahme ihrer Tätigkeit für unseren Verband und sodann regelmäßig (mindestens jährlich) in Datenschutzschulungen mit den Rechtsvorschriften zur Verarbeitung personenbezogener Daten vertraut zu machen.

Sämtliche Personen, die mit personenbezogenen Daten des Verbands arbeiten, sind auf den vertraulichen Umgang mit diesen Daten zu verpflichten.

d) Verpflichtung von Lieferanten und Externen

Lieferanten, externe Dienstleister und sonstige Auftragnehmer sind durch gesonderte Vereinbarungen zu verpflichten, die sie betreffenden Vorgaben zu Datenschutz und Informationssicherheit einzuhalten, wenn diese Daten im Auftrag verarbeiten oder die Möglichkeit der Kenntnisnahme von personenbezogenen Daten oder als nicht öffentlich klassifizierten Informationen des Verbands haben.

4. Grundsätze für die Einrichtung oder Änderung von Verarbeitungen personenbezogener Daten

Bei der Verarbeitung personenbezogener Daten und auch bei der Einrichtung oder Änderung von den damit zusammenhängenden Prozessen sind folgende Grundsätze der Datenverarbeitung i.S.d. Art. 5 DSGVO einzuhalten:

Personenbezogene Daten müssen

1. auf Basis einer Rechtsgrundlage oder Einwilligung, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

2. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“);
3. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
4. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
5. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“);
6. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);
7. für jeden Geschäftsprozess, der die Verarbeitung personenbezogener Daten beinhaltet, muss es einen Verantwortlichen beim WKBV geben („Owner/Eigentümer“: i.d.R. der Vorstand);

5. Verarbeitung personenbezogener Daten beim WKBV und Verzeichnis von Verarbeitungstätigkeiten

a) Verzeichnis von Verarbeitungstätigkeiten

Der WKBV führt ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO. Das Verzeichnis von Verarbeitungstätigkeiten wird vom Vorstand geführt. Der Vorstand kann in Absprache eine Person für die Pflege des Verarbeitungsverzeichnisses bestimmen. Der Vorstand trägt Sorge dafür, dass das Verarbeitungsverzeichnis regelmäßig aktualisiert wird.

b) Verarbeitung von Mitgliederdaten

Im Rahmen des Mitgliedschaftsverhältnisses verarbeitet der Verband insbesondere die folgenden Daten der Mitglieder: Verein, Vorstandsdaten wie z.B. Vorname, Nachname, Anschrift (Straße, Hausnummer, Postleitzahl, Ort), Geburtsdatum, Datum des Verbandsbeitritts, Abteilungs- und ggf. Mannschaftszugehörigkeit, Bankverbindung, ggf. die Namen und Kontaktdaten der gesetzlichen Vertreter, Telefonnummern und E-Mail-Adressen, ggf. Funktion im Verband.

c) Weitergabe von Mitgliederdaten an den Württembergischen Landessportbund (WLSB)

Als Mitglied des Württembergischen Landessportbundes e.V. (WLSB) ist der Verband verpflichtet, seine Mitglieder an den WLSB zu melden. Übermittelt werden dabei Vor- und Nachname, das Geburtsdatum, das Geschlecht, ausgeübte Sportarten und die Verbandsmitgliedsnummer. Bei Mitgliedern/Ehrenamtlichen mit besonderen Aufgaben werden zusätzlich die vollständige Adresse, die Telefonnummer, die E-Mail-Adresse, Beginn und Ende der Funktion sowie die Bezeichnung der Funktion im Verband übermittelt.

d) Weitergabe von Mitgliederdaten an den Bundesverband

Im Rahmen der Zugehörigkeit zu über geordneten Verbänden werden personenbezogene Daten der Mitglieder an diese weitergeleitet, soweit die Mitglieder eine Berechtigung zur Teilnahme am Wettkampfbetrieb der Verbände beantragen (z.B. Startpass, Spielerpass, Schiedsrichter Lizenz, Trainer Lizenz) und an solchen Veranstaltungen teilnehmen.

Dies ist derzeit:

Deutscher Kegler- und Bowlingbund e.V. und Deutscher Kegler Bund Classic e.V.

e) Datenverarbeitung im Rahmen der Öffentlichkeitsarbeit

Im Rahmen der Öffentlichkeitsarbeit über Verbandsaktivitäten werden personenbezogene Daten in Aushängen, in der Verbandszeitung und in Internetauftritten veröffentlicht und an die Presse weitergegeben. Hierzu zählen insbesondere die Daten, die aus allgemein zugänglichen Quellen stammen: Teilnehmer an sportlichen Veranstaltungen, Mannschaftsaufstellung, Ergebnisse, und Klassen Zugehörigkeit. (U14, U18, Aktiv,…)

Die Veröffentlichung von Fotos und Videos, die außerhalb öffentlicher Veranstaltungen gemacht wurden, erfolgt ausschließlich auf Grundlage einer Einwilligung der abgebildeten Personen.

Auf der Internetseite des Verbands werden die Daten der Mitglieder des Vorstands, der Sektionsvorstände, Bezirksvorstände, Schiedsrichter, Rechtsausschuss, Öffentlichkeitsarbeit und der Übungsleiterinnen und Übungsleiter mit Vorname, Nachname, Funktion, E-Mail-Adresse und Telefonnummer veröffentlicht.

f) Verwendung und Herausgabe von Mitgliederdaten und -listen

Listen von Mitgliedern oder Teilnehmern werden den jeweiligen Mitarbeiterinnen und Mitarbeitern im Verband (z.B. Vorstandsmitgliedern Sektions- und Bezirksvorständen, Schiedsrichter, Übungsleitern) insofern zur Verfügung gestellt, wie es die jeweilige Aufgabenstellung erfordert. Beim Umfang der dabei verwendeten personenbezogenen Daten ist das Gebot der Datensparsamkeit zu beachten (zur Pflicht zur Verschlüsselung solcher Listen s. Kapitel 10 Buchst. e).

Macht ein Mitglied glaubhaft, dass es eine Mitgliederliste zur Wahrnehmung satzungsgemäßer oder gesetzlicher Rechte benötigt (z.B. um die Einberufung einer Mitgliederversammlung im Rahmen des Minderheitenbegehrens zu beantragen), stellt der Vorstand eine Kopie der Mitgliederliste mit Vornamen, Nachnamen und Anschrift als Ausdruck oder als Datei zur Verfügung. Das Mitglied, welches das Minderheitenbegehren initiiert, hat vorher eine Versicherung abzugeben, dass diese Daten ausschließlich für diesen Zweck verwendet und nach der Verwendung vernichtet werden.

g) Kommunikation per E-Mail

Beim Versand von E-Mails an eine Vielzahl von Personen, die nicht in einem ständigen Kontakt per E-Mail untereinanderstehen und/oder deren private E-Mail-Accounts verwendet werden, sind die E-Mail-Adressen als „bcc“ zu versenden.

h) WKBV-aktiv Internet Zugriff

Den betroffenen Personen (Spielführer, Schiedsrichter, Funktionären aus Sektion und Bezirk, werden darauf hingewiesen, dass die zum Spielbetrieb zur Verfügung gestellten Daten, ebenfalls der Vertraulichkeit und Geheimhaltung unterliegen. Die vergebenen Zugangsdaten zu WKBV-aktiv, dürfen nicht an andere Personen weiter gegeben werden oder anderen Personen zu Verfügung gestellt werden.

6. Datenschutz-Folgenabschätzung

Der Datenschutzverantwortliche wird jeden neuen, gemeldeten Verarbeitungsprozess dahingehend prüfen, ob damit voraussichtlich ein hohes Risiko für personenbezogene Daten einhergeht. Gleiches gilt für die Veränderung von Verarbeitungsprozessen. Wenn ein voraussichtlich hohes Risiko besteht, wird der Vorstand darüber entscheiden, ob und wie eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen ist.

Ist eine DSFA erforderlich, darf die jeweilige Verarbeitung grundsätzlich erst nach Durchführung der DSFA und entsprechender Freigabe durch den Vorstand begonnen werden.

Die DSFA kann vom Verantwortlichen oder auch durch externe, fachkundige Personen durchgeführt werden. Der Datenschutzbeauftragten (DSB) steht bei der Durchführung der DSFA auf Anfrage für die Beratung zur Verfügung.

Sollte die DSFA ergeben, dass das mit dem Verarbeitungsprozess verbundene Risiko nicht durch technische und organisatorische Maßnahmen eingedämmt werden kann, wird der Vorstand darüber entscheiden, ob eine vorherige Konsultation mit der Aufsichtsbehörde i.S.d. Art. 36 DSGVO durchzuführen ist.

Derzeit ist für die bestehenden Prozesse keine DSFA erforderlich.

7. Löschung von Daten

Die Löschfristen für die jeweiligen Verarbeitungsprozesse sind im Verzeichnis von Verarbeitungstätigkeiten aufgeführt. Die Überprüfung, ob Daten zu löschen sind, hat mindestens einmal jährlich stattzufinden. Daten müssen gelöscht werden, wenn der Zweck der Verarbeitung weggefallen ist oder Daten nicht für anderweitige Zwecke z.B. gesetzlich vorgeschriebene Aufbewahrungsfristen im Bereich des Handels- und Steuerrechts oder Gesundheitsrechts benötigt werden. Des Weiteren ist eine Löschung nicht erforderlich, wenn die zu löschenden Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden. Die Löschung von Daten oder die Einschränkung der Verarbeitung aufgrund von Betroffenenrechten sind in Kapitel 9 geregelt. Über die Löschung von Daten ist ein Löschprotokoll anzufertigen.

8. Meldepflichten bei Datenschutzverletzungen

Um Datenschutz und Informationssicherheit im Verband zu gewährleisten, ist jeder Beteiligte verpflichtet, **Vorfälle im Bereich des Datenschutzes unverzüglich** und direkt **an den Vorstand oder die Geschäftsstelle und dem Datenschutzverantwortlichen zu melden.** Ein Datenschutzvorfall liegt insbesondere vor, wenn die Annahme besteht, dass die Datensicherheit, insbesondere die Vertraulichkeit von Daten, gefährdet sein kann. Ein Datenschutzvorfall liegt auch bei jedem Sachverhalt vor, bei dem die Annahme besteht, dass Dritte unbefugt Zugriff oder Zugang zu personenbezogenen Daten haben oder hatten

Der Vorstand, unterstützt durch die Geschäftsstelle und des Datenschutzverantwortlichen, untersucht unverzüglich jeden Vorfall oder jede Meldung („Vorfälle“) einer **Verletzung des Schutzes personenbezogener Daten**.

Jeder Vorfall wird vom Vorstand, unterstützt durch die Geschäftsstelle und des Datenschutzverantwortlichen, in Textform dokumentiert. Dabei werden Zeitpunkt der Kenntnisnahme, Sachverhaltsdarstellung und getroffene Maßnahmen dokumentiert. Bei jedem Vorfall ist zunächst zu prüfen, ob eine Verletzung des Schutzes personenbezogener Daten vorliegt und die Verletzung voraussichtlich zu einem Risiko für die Betroffenen führt. Im Falle eines Risikos muss dafür Sorge getragen werden, dass binnen 72 Stunden nach Kenntnis von dem Vorfall eine Meldung an die für den WKBV zuständige **Aufsichtsbehörde für den Datenschutz** erfolgt. Dies ist derzeit der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Baden-Württemberg, Homepage: https://www.baden-wuerttemberg.datenschutz.de

Sollte die Frist von 72 Stunden bereits verstrichen sein, wird gleichwohl so schnell wie möglich eine Meldung an die Aufsichtsbehörde erfolgen. Dieser Meldung ist dann eine Begründung für die Verzögerung beizufügen

Die Meldung muss insbesondere beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Sollten die genannten Informationen nicht binnen der 72-Stunden-Frist ermittelt oder zusammengestellt werden können, hat gleichwohl eine Meldung an die Aufsichtsbehörde zu erfolgen. Die o.g. Inhalte sind dann unverzüglich an die Aufsichtsbehörde nachzureichen.

Wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein **hohes Risiko** für von dem Vorfall Betroffenen hat, so benachrichtigt der Vorstand oder der Datenschutzverantwortliche die **betroffenen Personen** unverzüglich von der Verletzung.

Dabei sind insbesondere etwaige Ausnahmeregelungen nach Art. 34 Abs. 3 DSGVO in Erwägung ziehen.

9. Rechte auf Auskunft, Löschung, Widerspruch und weitere Betroffenenrechte aus den Art. 15-22 DSGVO

Jede Person kann seine Betroffenenrechte nach den Art. 15-22 DSGVO gegenüber dem WKBV geltend machen.

Dies beinhaltet insbesondere das Recht auf **Auskunft, Berichtigung** und **Löschung** von personenbezogenen Daten sowie das Recht auf **Einschränkung der Verarbeitung** sowie das Recht auf **Widerspruch** gegen eine Verarbeitung von Daten (z.B. auch gegen die Verwendung von Daten für Werbezwecke).

Alle Beschäftigten, Trainer Schiedsrichter und Ehrenamtlichen des WKBV sind verpflichtet, einen von einem Betroffenen geltend gemachten **Anspruch auf Auskunft**, Berichtigung, Löschung oder einen Widerspruch unverzüglich nach Zugang der Mitteilung an den Vorstand oder die Geschäftsstelle oder Datenschutzverantwortlichen weiterzuleiten. Die Weiterleitung kann z.B. auch per E-Mail an die E-Mail-Adresse: Datenschutzverantwortlicher@WKBV.de erfolgen.

Der Vorstand, unterstützt durch die Geschäftsstelle, wird die Anfrage dokumentieren und unverzüglich, spätestens aber **innerhalb eines Monats** nach Eingang der Mitteilung des Betroffenen bei der VMX Union gegenüber dem Betroffenen beantworten.

Bei der Beantwortung von Anfragen von Betroffenen ist vor der Erteilung von Information an den Betroffenen sicherzustellen, dass die Person diejenige ist, für die sie sich ausgibt, um zu verhindern, dass personenbezogene Daten an Unbefugte gelangen. Im Fall einer Auskunftserteilung per E-Mail ist von dem Betroffenen vorab die Zustimmung einzuholen, dass die Informationen per E-Mail zur Verfügung gestellt werden. Bei Fehlen einer Zustimmung ist die Auskunft schriftlich zu erteilen.

10. Vorgaben zur IT-Sicherheit

Um die Integrität, Verfügbarkeit und Vertraulichkeit der IT-Systeme auf Dauer zu gewährleisten, sind die nachfolgenden Vorgaben von allen Beschäftigten, Trainern und Ehrenamtlichen einzuhalten.

Sofern nachfolgend von IT-Systemen die Rede ist, sind darunter ausnahmslos alle Geräte oder Anwendungen (Hard- und Software) zu verstehen, mit denen Informationen elektronisch verarbeitet oder übertragen werden können. Dazu gehören insbesondere PCs, Notebooks/Laptops, Tablet PCs (z.B. iPad), Telefone, Mobiltelefone, Server, Speichermedien, Netzwerktechnologie, Softwareprodukte und Drucker.

a) Allgemeine Verhaltensrichtlinien

Die Nutzung der IT-Systeme und Applikationen im Verband ist ausschließlich für Verbandszwecke und in jeweils erlaubten Umfang zur Aufgabenerledigung zulässig. Abweichungen hiervon bedürfen der Erlaubnis des Vorstands. Es darf nur die Software auf IT-Systemen des Verbands installiert werden, die vom Verband freigegeben worden ist.

Der Arbeitsplatz bzw. die Geschäftsstelle des Verbands ist von den Nutzern so zu gestalten, dass Besucher oder sonstige Dritte keinen Zugang zu personenbezogenen Daten bekommen können, ohne hierfür berechtigt zu sein. So sind Büros nach dem Verlassen des Arbeitsplatzes grundsätzlich zu verschließen.

Informationen in Papierform sind so abzulegen, dass Besucher oder sonstige Dritte keine Kenntnisnahme von den Daten erhalten können. Vertrauliche Informationen sind stets unter Verschluss zu halten.

b) Passwörter

Soweit technisch möglich sind alle IT-Systeme und Applikationen erst nach hinreichender Authentifizierung nutzbar. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Benutzername/Passwort. Soweit möglich oder angeordnet, werden Zwei-Faktor-Authentifizierungs-Systeme verwendet.

Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist komplex zu gestalten und muss mindestens 3 der nachfolgenden 4 Kategorien enthalten:

1. Großbuchstaben
2. Kleinbuchstaben
3. Sonderzeichen
4. Ziffern

Die Passwörter sind so zu wählen, dass sie nicht durch Dritte leicht zu erraten sind. Vor- und Familiennamen oder Geburtstage sowie Namen von Angehörigen sind nicht zur Passwortwahl geeignet. Gleiches gilt für trivial angeordnete Zahlenkombinationen (z.B. 12345678).

Passwörter sollten regelmäßig, mindestens nach 90 Tagen, gewechselt werden. Bereits genutzte Passwörter dürfen nicht noch einmal wiederverwendet werden. Von diesem Passwortwechsel kann in begründeten Fällen abgewichen werden. Voraussetzung dafür ist, dass die Passwortsicherheit dann in einer dem Stand der Technik entsprechenden anderen Weise gewährleistet werden. Dazu können Methoden der 2-Faktor-Authentifizierung oder erheblich höhere Passwortlängen gehören.

c) Nutzung von verbandseigenen E-Mail-Konten:

Die vom Verband vergebenen E-Mail-Konten dürfen nur für Verbandszwecke genutzt werden.

d) Verhalten bei Sicherheitsvorfällen

Sollte ein Mitarbeiter, Schiedsrichter, Trainer oder Ehrenamtliche merken, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnte, hat dieser sich unverzüglich an den Vorstand oder an den Datenschutzverantwortlichen zu wenden. Dies gilt insbesondere dann, wenn die Gefährdung sich auf personenbezogene Daten bezieht.

e) Speicherorte, mobile Datenträger und mobile IT-Systeme, Verschlüsselung

Beim WKBV können Daten auf verschiedenen IT-Systemen gespeichert werden. Die Speicherung von Daten hat grundsätzlich auf den Rechnern zu erfolgen, die vom Verband genehmigt werden.

Werden ausnahmsweise mobile IT-Systeme oder Datenträger außerhalb der Geschäftsstelle des Verbands verwendet, hat der Nutzer in besonderem Maße Sorge dafür zu tragen, dass Dritte keine Kenntnis von Informationen erhalten können, die mit dem mobilen IT-System verarbeitet werden. Dies beinhaltet insbesondere die sorgfältige und sichere Verwahrung des mobilen IT-Geräts oder Datenträgers, um diese vor Diebstahl und Verlust zu schützen. Zusätzlich dürfen Daten nur **verschlüsselt** gespeichert werden. Außerdem muss der verwendete Computer, Laptop, o.ä. gemäß dieser Richtlinie geschützt sein, in jedem Fall jedoch durch ein entsprechendes **Passwort**.

Dateien, die außerhalb der Geschäftsstelle gespeichert werden, müssen gelöscht werden, sobald der Zweck für die Verarbeitung wegfällt, spätestens jedoch nach einem Jahr.

Der Nutzer darf das ihm zur Verfügung genehmigte mobile IT-System oder den mobilen Datenträger nicht anderen Personen zur Nutzung überlassen.

Der Datenaustausch mobiler Endgeräte über das Internet hat i.d.R. nur über gesicherte WLAN oder Bluetooth Verbindung oder LAN zu erfolgen. Dies gilt insbesondere, wenn sensible Daten auf den mobilen Endgeräten verarbeitet werden.

f) Datensicherungen:

Datensicherungen sind mindestens monatlich anzufertigen und außerhalb der Geschäftsstelle aufzubewahren. Datensicherungen bzw. externe Datenträger müssen verschlüsselt werden.

g) Diebstahl und Verlust

Sollte ein Datenträger oder ein mobiles IT-System gestohlen werden oder verloren gehen, hat der Nutzer dies unverzüglich nach Kenntnisnahme an den Vorstand oder die Geschäftsstelle zu melden. Die Meldung muss so schnell wie möglich erfolgen, da in diesen Fällen gesetzliche Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen bestehen können, die im Falle einer zu späten Meldung Bußgelder in erheblicher Höhe nach sich ziehen können.

h) IT-Angriffe von außen

Auf den Rechnern und Routern des Verbands werden aktuelle Virenscanner eingesetzt. Die Virenscanner werden regelmäßig gewartet und aktualisiert, um eine Anpassung an neue Gefahrenlagen zu gewährleisten. Daneben werden alle Server-IT-Systeme und alle kritischen IT-Systeme durch **Firewall-Technologie** gesichert und überwacht. Ein Zugriff unbefugter Dritter von außen wird auf diese Weise wesentlich erschwert. Die Firewall-Technologie wird regelmäßig gewartet und aktualisiert, um eine Anpassung an neue Gefahrenlagen zu gewährleisten.

Zudem kommen Systeme zum Einsatz, mit denen E-Mails mit unverlangter Werbung gefiltert werden. Diese E-Mails werden im Posteingang entsprechend gekennzeichnet (SPAM).

i) Einbruch und Diebstahl

Alle Büro- und Geschäftsräume sind vor dem Zutritt unbefugter Dritter gesichert. Dies gilt insbesondere für den Zutritt zu Gebäuden außerhalb der Büro- und Geschäftszeiten.

j) Protokollierung

In der IT-Infrastruktur werden verschiedene Informationen protokolliert, um Störungen, Ausfälle und Sicherheitsvorfälle schnell identifizieren und beheben zu können. Dabei werden die einschlägigen datenschutzrechtlichen Bestimmungen eingehalten und die Persönlichkeitsrechte der Mitarbeiter gewahrt.

Während des Regelbetriebs der IT-Infrastruktur werden von verschiedenen Systemen (insbesondere von Servern und Firewalls) Verbindungsdaten (Datum, Uhrzeit, Adressen von Absender und Empfänger, die Art der übertragenen Daten, das übertragene Datenvolumen usw.) protokolliert.

Im Zuge der Nutzung der IT-Infrastruktur werden Daten protokolliert, aus denen auch das Nutzerverhalten ganz oder in Teilen nachvollzogen werden kann (Zeitpunkt der An- und Abmeldung an IT-Systemen, Datum und Uhrzeit von Änderungen in Dateien, usw.).

Um gesetzliche Anforderungen zu erfüllen, archiviert der Verband alle ein- und ausgehenden E-Mails mindestens für die Dauer gesetzlicher Aufbewahrungspflichten. Diese können bis zu zehn Jahre betragen.

Das Erheben dieser Protokolldaten ist für den sicheren und rechtskonformen Betrieb der IT-Infrastruktur notwendig.

Die Protokolldaten werden ausschließlich zu folgenden Zwecken verwendet:

- Analyse und Korrektur von Störungen, Ausfällen und Sicherheitsvorfällen
- Gewährleistung der Sicherheit der IT-Infrastruktur
- Optimierung der IT-Infrastruktur
- für Statistiken über die Nutzung der IT-Infrastruktur sowie für
- nicht personenbezogene Stichprobenkontrollen sowie Auswertungen gemäß diesem Datenschutzhandbuch (siehe Abschnitt „Missbrauchskontrolle“)
- Die Protokolldaten werden nicht zur Leistungs- und Verhaltenskontrolle der Mitarbeiter eingesetzt.

k) Missbrauchskontrolle

Für das Erkennen von Störungen, Ausfälle und Sicherheitsvorfällen findet eine nicht-personenbezogene Auswertung der Protokolldaten durch gesondert beauftragte Personen statt. Eine personenbezogene Auswertung der Protokolldaten findet nur statt, wenn aufgrund einer Stichprobenkontrolle, einer Meldung oder anderer Verdachtsmomente ein konkreter Verdacht auf eine missbräuchliche, unerlaubte oder

strafbare Nutzung der IT-Infrastruktur besteht. In diesem Falle ist folgende Vorgehensweise verbindlich:

- Eine personenbezogene Überprüfung der Protokolldaten erfolgt nur bei einem gewichtigen Missbrauchsverdacht, Bagatellfälle rechtfertigen die Überprüfung nicht.
- Sie wird nach dem Prinzip der Datensparsamkeit durchgeführt.
- Sie erfolgt unter zwingender Beteiligung des Datenschutzbeauftragten.
- Wird der Verdacht durch die Überprüfung nicht bestätigt, so werden die für die Überprüfung erhobenen Daten und Aufzeichnungen unverzüglich gelöscht. Der nicht bestätigte Verdacht darf keinerlei weitere Folgemaßnahmen – insbesondere keine gezielten Stichproben gegen den Mitarbeiter – nach sich ziehen.
- Bei Gefahr im Verzug werden durch den WKBV weitere gefährdende oder strafbare Handlungen – eventuell unter Einschaltung der Strafverfolgungsbehörden – unmittelbar unterbunden, insbesondere werden die erforderlichen technischen Abwehrmaßnahmen ohne Verzögerung ergriffen, auch wenn hierbei personenbezogene Daten erhoben oder eingesehen werden müssen.

11. Notfallmanagement

a) Definition Notfall

Ein Notfall ist ein unerwünschtes, zeitlich nicht vorhersehbares Ereignis, das den Geschäftsbetrieb nachhaltig gefährden kann. Zur Bewältigung des Notfalls Im Falle eines Notfalls gelten die nachfolgenden Regeln mit dem Zweck, den Geschäftsbetrieb aufrechtzuerhalten bzw. unverzüglich wieder einen Zustand einer funktionsfähigen IT-Infrastruktur herzustellen.

b) Generelles Verhalten

Beim **Auftreten eines Notfalles** ist ein besonnenes Vorgehen besonders geboten. Vorrangig ist in einem Notfall Ruhe zu bewahren. Die Situation ist unverzüglich zu analysieren, und der Vorstand zu informieren.

Dasselbe gilt bei einem reinen **Verdacht auf Unregelmäßigkeiten**, die auf einen Notfall oder sich ankündigenden Notfall hindeuten.

c) Feuer

In allen Räumen, in denen sich IT-Systeme befinden, die für den laufenden Geschäftsbetrieb zwingend erforderlich oder kritisch sind, sind Rauchmelder und/oder Brandmeldeanlagen in Betrieb.

Darüber hinaus befinden sich in allen Gebäuden an mehreren Stellen die erforderlichen Feuerlöscher. Diese sind gut sichtbar angebracht und im Bedarfsfall zu nutzen. Im Falle eines Brandes ist zudem unverzüglich die Feuerwehr zu informieren.

Ferner ist der Vorstand sofort zu informieren.

Im Falle eines größeren Brandereignisses werden die Beschäftigten an den jeweiligen Standorten umgehend evakuiert. Fluchtwegepläne hängen in jedem Gebäude an gut sichtbarer Stelle aus.

d) Wasser

Größere Wasserschäden, die die für den Geschäftsbetrieb erforderlichen, kritischen IT-Systeme negativ beeinträchtigen könnten, stellen aufgrund der Lage nur ein sehr geringes Risiko dar. Es ist regelmäßig nicht damit zu rechnen, dass ein Wasserschaden zu einer Beeinträchtigung der kritischen IT-Systeme führt. Die IT-Systeme befinden sich an Orten, an denen kein Hochwasser zu befürchten ist. Auch Schäden durch Wasserleitungen sind aufgrund der räumlichen Gegebenheiten äußerst unwahrscheinlich.

Sollte dennoch ein Wasserschaden auftreten, der eine Gefahr für die kritischen IT-Systeme oder andere IT-Systeme darstellen könnte, ist sofort der Vorstand zu informieren. Diese wird dann nach Sichtung der Lage die weiteren erforderlichen Maßnahmen vornehmen.

e) Stromausfall

Alle kritischen IT-Systeme, die für den Geschäftsbetrieb unerlässlich sind, verfügen über eine unterbrechungsfreie Stromversorgung (USV). Diese trägt Sorge dafür, dass Stromausfälle von mehreren Minuten überbrückt und im Falle eines längeren Stromausfalls die IT-Systeme geordnet heruntergefahren werden können, um die Integrität der Daten zu gewährleisten.

f) Notfall-Verantwortlicher

Im Verband gibt es einen Notfall-Verantwortlichen, der bei Vorliegen eines Notfalles für die Veranlassung der jeweils vorgesehenen und gebotenen Maßnahmen verantwortlich ist. Hierbei handelt es sich um eines oder mehrere Mitglieder des Vorstands.

g) Wiederanlaufplan

Im Falle eines Funktionsausfalles eines IT-Systems wird die Ursache des Vorfalls unverzüglich untersucht. Parallel dazu werden sofort Maßnahmen in die Wege geleitet, um einen Wiederanlauf des IT-Systems oder eines Alternativsystems kurzfristig zu ermöglichen.

12. Sanktionen

Ein Verstoß gegen diese Datenschutzordnung kann ein Verstoß gegen die Mitgliedschaftspflichten eines Verbandsmitglieds oder eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

Präsident
Siegfried Schweikhardt

Vize Präsident
Ernst Lange

Vize Präsident
Werner Knöbl

Datenschutzverantwortlicher Wolfgang Kunkel