Vereinbarung hinsichtlich des Datenschutzes bei einer Verarbeitung von personenbezogener Daten durch gemeinsam für die Verarbeitung Verantwortlicher gemäß Art. 26 DS-GVO

zwischen

Verband Deutscher Sporttaucher e.V.
Berliner Str. 312

63067 Offenbach

- im Folgenden "VDST" -

und

Tauchclub Octopus Weinheim e.V.
Postfach 10 11 34

69451 Weinheim

- im Folgenden "Verein" -

Präambel

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung von personenbezogenen Daten fest, so sind sie gemeinsam Verantwortliche gemäß Art. 26 Abs.1 DSGVO. Dies trifft für den Verband Deutscher Sporttaucher e.V. (folgende VDST) und die ihm angeschlossenen Vereine zu, da beide für die Erhebung, Speicherung und Nutzung der Mitgliederdaten verantwortlich sind.

1. Gegenstand und Dauer der gemeinsamen Verarbeitung

Die zwischen VDST und dem Verein geschlossene Vereinbarung umfasst die ganz oder teilweise automatisierte Verarbeitung, sowie für die nicht automatisierte Verarbeitung personenbezogener Daten der Vereinsmitglieder, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.
Die Vereinbarung beginnt mit der Mitgliedschaft des Vereines im VDST und endet somit mit der Kündigung der Mitgliedschaft bzw. mit der Auflösung des Vereines. Davon unberücksichtigt bleiben allerdings alle vereinbarten Geheimhaltungsverpflichtungen.

2. Gegenseitiges Verhältnis der Vertragspartner

Der VDST und die Vereine führen gemeinsam die Verwaltung der Mitglieder durch. Dabei gilt folgende Konstellation:
- Vereine (Tauchsportvereine, Sparten/Unterabteilungen von Sportvereinen) können durch Aufnahmeantrag Mitglied im VDST werden
- In den Vereinen werden natürliche Personen durch Aufnahmeantrag Mitglied des Vereins
- Durch die Mitgliedschaft des Vereines im VDST, werden alle Mitglieder auch automatisch Mitglied im VDST
- Die Verwaltung der Mitglieder erfolgt zentral beim VDST und dezentral im Verein

3. Art und Zweck der Verarbeitung

Der VDST und der oben genannte Verein erheben, speichern und nutzen Daten ihrer Mitglieder zum Zwecke von deren Verwaltung und zur Erbringung der in deren Satzung bzw. Geschäftsordnung festgelegten Leistungen. Dabei gilt folgende Abgrenzung der Tätigkeiten:

Aufgaben des VDST

Der VDST führt folgende Tätigkeiten durch:
- Verwaltung und Speicherung der Mitgliederdaten in einer zentralen Datenbank die von der VDST Tauchsport Service GmbH über eine Cloud-Lösung im Rahmen einer Auftragsdatenverarbeitung gemäß Art. 28 DSGVO bereitgestellt wird.
 -- Speicherung und Pflege der Mitgliederdaten
 -- Dokumentation der Brevetierungen
- Übermittlung der Mitgliederdaten an einen Verlag zum Versand der Verbandszeitschrift im Rahmen einer Auftragsdatenverarbeitung gemäß Art. 28 DSGVO
- Übermittlung der Daten zur Erbringung von Versicherungsleistungen über die VDST Tauchsport Service GmbH.

-- Unfall-, Haftpflicht- und Rechtschutzversicherung
-- Auslandsreisekrankenversicherung in Verbindung mit einer medizinischen Taucherarzt-Hotline
-- Sowohl Versicherungen als auch Taucherarzt-Hotline unterliegen der Verschwiegenheitspflicht gemäß § 203 StGB

Aufgaben des Vereins

Der Verein führt folgende Tätigkeiten durch:
- Direkterhebung der Mitgliedsdaten durch einen Aufnahmeantrag.
-- Der Aufnahmeantrag enthält alle Hinweise über Zweck der Datenverarbeitung und über die Weitergabe der Daten an den VDST
-- Der Aufnahmeantrag enthält alle Hinweise über die beim VDST vorgenommenen Verarbeitungen und Weiterleitungen
- Der Verein speichert die Daten in einer eigenen Datenbank, die zum Abgleich in regelmäßigen Abständen an den VDST übermittelt werden oder
- Der Verein gibt neue Mitgliederdaten direkt über ein Web-Portal in die VDST Mitgliederdatenbank ein
- Darüberhinaus vom Verein genutzte Verfahren sind unter **Anlage A** beschrieben:
(bitte in der Anlage A auswählen)

4. Kategorien von Betroffenen und Art der gespeicherten Daten

Im Rahmen der unter 3 aufgeführten Verarbeitungen können Datenkategorien gemäß **Anlage A** betroffen sein:

Zusätzlich werden in der VDST-Datenbank Brevetierungen und Ausbildungsstatus gespeichert. Da diese Daten von Mitgliedern auch nach Beendigung der Mitgliedschaft abgefragt werden können, werden diese Daten nur auf Verlangen des Betroffenen gelöscht.

5. Technische und organisatorische Maßnahmen

(1) Der VDST und der Verein hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen (Einzelheiten in **Anlage B**).
(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem VDST gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

6. Pflichten der Verantwortlichen

Aus dieser Vereinbarung ergeben für die Verantwortlichen folgende Pflichten:

Pflichten des VDST

Der VDST hat zusätzlich zu der Einhaltung der Regelungen dieses Vertrags gesetzliche Pflichten gemäß Art. 26 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:
a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem in **Anhang A** zum Zweck der direkten Kontaktaufnahme mitgeteilt. Sollte dieser wechseln, werden die Vereine über die VDST-Webseite informiert.
b) Zu Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO setzt der VDST bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der VDST und jede dem diesem unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend dieser Vereinbarung verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Verarbeitung erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten in **Anlage B**).
d) Überprüfung von Auftragnehmern und deren Verpflichtung durch einen Vertrag zur Einhaltung des Datenschutzes gemäß Art. 28 DSGVO
e) Der VDST stellt Informationen gem. Art. 13 DSGVO auf Antragsformularen und auf der Webseite bereit, wie Daten im Rahmen der gemeinsamen Verarbeitung erhoben, gespeichert, verarbeitet und an wen sie zu welchen Zwecken übermittelt werden (z.B. Auftragsdatenverarbeitung gemäß Art. 28 DSGVO).

Pflichten des Vereins

Der Verein hat zusätzlich zu der Einhaltung der Regelungen dieses Vertrags gesetzliche Pflichten gemäß Art. 26 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:
a) Schriftliche Bestellung eines Datenschutzbeauftragten, soweit er gesetzlich dazu verpflichtet ist, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem in **Anhang A** zum Zweck der direkten Kontaktaufnahme mitgeteilt. Sollte dieser wechseln, darüber unverzüglich zu informieren. Ist der Verein nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet, nennt er eine Person, welche die Umsetzung der DSGVO im Verein umsetzt oder betreut.
b) Zu Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO setzt der Verein bei der Durchführung der Arbeiten nur Personen ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Verein und jede dem diesem unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend dieser Vereinbarung verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Verarbeitung erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten in **Anlage B**).
d) Überprüfung von Auftragnehmern und deren Verpflichtung durch einen Vertrag zur Einhaltung des Datenschutzes gemäß Art. 28 DSGVO
e) Der Verein stellt Informationen gem. Art. 13 DSGVO auf den Aufnahmeantrag und soweit vorhanden, auf der Webseite des Vereins in geeigneter Weise bereit, wie Daten im Rahmen

der gemeinsamen Verarbeitung erhoben, gespeichert, verarbeitet und an wen sie zu welchen Zwecken übermittelt werden (z.B. Auftragsdatenverarbeitung gemäß Art. 28 DSGVO)

Gemeinsame Verpflichtungen aus diesem Vertrag

Beide Vertragsparteien gewährleisten gemäß Art. 26 DS-GVO die Einhaltung folgender Vorgaben:
a) Der VDST und Verein arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
b) Die unverzügliche gegenseitige Information über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diese Vereinbarung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der gemeinsamen Verarbeitung ermittelt.
c) Soweit einer der Vertragspartner einer Kontrolle der zuständigen Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit den unter 3 beschriebenen Tätigkeiten ausgesetzt ist, hat ihn der jeweilige Vertragspartner zu unterstützen.

7. Auftragsverhältnisse gem. Art. 28 DSGVO

(1) Als Auftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der unter 3 aufgeführten Verarbeitungen beziehen. Nicht hierzu gehören Nebenleistungen, die der VDST z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Vertragspartner ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten der gemeinsamen Verarbeitung auch bei ausgelagerten Leistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
(2) Die Vertragspartner verpflichten sich, bei Weitergabe der Daten an einen Dienstleister, alle gemäß Art. 28 DSGVO geforderten Maßnahmen zu ergreifen.

8. Rechte von Betroffenen

(1) Betroffene haben gem. Art. 15 DSGVO das Recht Auskunft zu verlangen, welche Daten und zu welchen Zweck über sie gespeichert wurden. Dieses Auskunftsverlangen kann sowohl an den VDST als auch an den Verein gerichtet werden.
(2) Betroffene haben gemäß Art. 16 DSGVO das Recht, von den Verantwortlichen unverzüglich die Berichtigung unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung haben diese auch das Recht zur Vervollständigung unvollständiger personenbezogener Daten. Diese Forderung ist an den Verein zu richten, da dieser in der gemeinsamen Verarbeitung die Erhebende Stelle ist.
(3) Das Recht auf Löschung der Daten gem. Art 17 DSGVO bzw. der Einschränkung der Verarbeitung gem. Art. 18 DSGVO kann nur wahrgenommen werden, wenn es hierfür ausreichende Gründe gibt und der notwendige Zweck hierdurch nicht aufgehoben bzw. eingeschränkt wird. Der Betroffene muss jedoch immer auf die Folgen einer Löschung oder Einschränkung, soweit sie durchsetzbar ist, hingewiesen werden.

Hierzu müssen beide Verantwortlichen Verfahren einrichten, mit denen oben aufgeführte Punkte datenschutzkonform umgesetzt werden können.

9. Mitteilung bei Verstößen

(1) Die Verantwortlichen verpflichten sich zur Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, zur Meldepflichten bei Datenpannen und zur Datenschutz-Folgeabschätzungen bei sensiblen Daten. Hierzu gehören u.a.
a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Vertragspartner zu melden
c) die Verpflichtung, den Vertragspartner im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Vertragspartners für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Vertragspartners im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

10. Löschung und Rückgabe von personenbezogenen Daten

Sollte die Mitgliedschaft des Vereins beim VDST beendet werden, endet hiermit auch die gemeinsame Verantwortung für die Mitgliedsdaten der Vereinsmitglieder des Vereins.
(1) Die Daten der ausgeschiedenen Mitglieder werden für eine weitere Verarbeitung gesperrt jedoch nicht gelöscht, da auch ehemalige Mitglieder Anspruch haben, dass Tauchlizenzen bei Verlust neu ausgestellt werden.
Diese Sperrung betrifft die Weitergabe der Daten an Auftragnehmer bzw. Dritte, die an der satzungsgemäßen Leistungserbringung beteiligt sind.
Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(2) Sollte ein ehemaliges Mitglied die Löschung seiner Daten verlangen, wird diesem Begehren mit Hinweis auf die Folgen nachgekommen.

Weinheim, 16.05.2018

gez.
Armin Steininger

(gesetzlicher Vertreter des Vereins Tauchclub Octopus Weinheim e.V.)

Offenbach am Main, 16.05.2018

gez.
Prof. Dr. Franz Brümmer
Präsident

Erich Sämann
Vizepräsident Finanzen
(gesetzliche Vertreter des Verband Deutscher Sporttaucher e.V.)

[Diese Vereinbarung ist ohne Unterschrift gültig]

Anlage A: Details zum Auftrag

1. Zusätzlich zu [3. Art und Zweck der Verarbeitung], [Aufgaben des Vereins] geführte Tätigkeiten

Zusätzlich zu den unter den [Aufgaben des Vereins] aufgeführten Verfahren, führt der Verein noch folgende Tätigkeiten durch:

2. Art der Daten

Sowohl beim VDST als auch im Verein werden folgende Mitgliederdaten gespeichert:

Daten von zum VDST-Jahresbeitrag gemeldeten Mitglieder

- ☑ Mitgliedsnummer
- ☑ Adressdaten
- ☑ Nationalität
- ☑ Kommunikationsdaten
- ☑ Geburtsdatum
- ☑ Geschlecht
- ☑ Mitgliederstatus
- ☑ Eintrittsdatum
- ☑ Bankverbindung

Daten von inaktiven Mitgliedern

- ☑ Mitgliedsnummer
- ☑ Adressdaten
- ☑ Nationalität
- ☑ Kommunikationsdaten
- ☑ Geburtsdatum
- ☑ Geschlecht
- ☑ Mitgliedsstatus
- ☑ Eintrittsdatum
- ☑ Bankverbindung

Daten von ausgetretenen Mitgliedern

- ☑ Mitgliedsnummer
- ☑ Adressdaten
- ☑ Nationalität
- ☑ Kommunikationsdaten
- ☑ Geburtsdatum
- ☑ Geschlecht
- ☑ Mitgliedsstatus
- ☑ Ein- und Austrittsdatum
- ☑ Bankverbindung

Zusätzlich werden beim VDST gespeichert

- ☑ Erlangte Brevets, Spezial- und Aufbaukurse

☑ Ausbilderstatus (wenn zutreffen)

Im Verein werden zusätzlich noch folgende Daten gespeichert:

3. Kategorien der betroffenen Personen

Daten folgende Betroffene können im Verein gespeichert sein:

☑ Mitgliederdaten

4. Zuständige Datenschutzverantwortliche

Für den VDST stehen folgende Kontaktdaten zum Datenschutzbeauftragten zur Verfügung:
Lothar Becker, Tel. +49 (0)8061 495743, Email: datenschutz@vdst.de

Für den Verein ist folgende Person für den Datenschutz verantwortlich:

5. Auftagsdatenverarbeiter und Dritte, die für VDST oder Verein tätig werden

Für den VDST sind folgende Auftragsdatenverarbeiter gem. Art. 28 DSGVO zur Erbringung der oben aufgeführten Leistungen tätig:

Hosting der VDST-Server in einem externen Rechenzentrum

Marini Systems GmbH
Kaiserstraße 57
60329 Frankfurt am M

Mittwald CM Service GmbH & Co. KG
Königsberger Straße 6
32339 Espelkamp

Druck und Versand der Verbandszeitschrift "Sporttaucher"

Dierichs Druck + Media GmbH & Co. KG
Frankfurter Straße 168
34121 Kassel

BWH GmbH
Beckstraße 10
30457 Hannover

Versicherungen des VDST

Europa-Versicherung AG
Piusstr. 137
50931 Köln

HDI-Gerling Firmen und Privat Versicherung AG
HDI-Platz 1
30659 Hannover

Dritte oder Empfänger personenbezogener Daten gem. Art. 4 Abs. 9 und 10 DSGVO zur Abwicklung von Tätigkeiten gem. Art. 6 Abs. 1 lit a) - c) DSGVO
(Stellen, die als Verantwortliche im Sinne des Art. 24 DSGVO agieren)

Abwicklung der Hotline und der Tauchsportversicherungen
(Dritte, die auch zur Verschwiegenheit gem. § 203 StGB verpflichtet sind)

MD-Medicus Gesellschaft für medizinische Serviceleistungen mbH
Industriestrasse 2a
D-67063 Ludwigshafen

Verschiedene Versicherungen die für die VDST Tauchsportversicherungen Leistungen erbringen

Sonstige Empfänger von Daten

Finanzdienstleister zur Abwicklung von Zahlungstätigkeiten

Versanddienstleister wie DHL, UPS

Für den Verein sind folgende Auftragsdatenverarbeiter gem. Art. 28 DSGVO zur Erbringung der oben aufgeführten Leistungen tätig:

(bitte nachstehend aufführen)

Anlage B: Technische und organisatorische Maßnahmen

B.1 Technische und oranisatorische Maßnahmen VDST

1. Vertraulichkeit

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu den vom Auftragnehmer zwecks Erbringung der Verarbeitung genutzten technischen Einrichtungen zu verwehren.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Räume, in denen Daten der Mitglieder verarbeitet oder gespeichert werden, können nicht betreten werden. Hier sind entsprechende Zutrittskontrollsysteme (Schlüssel, Chipkarte) eingesetzt.

• Datenverarbeitungsgeräte (Monitore, Drucker, etc.) auf denen Daten der Mitglieder verarbeitet oder ausgegeben werden sind so aufgestellt, dass keinen Einblick oder Zugriff durch Unbefugte möglich ist.

1.2 Zugangskontrolle

Es ist zu verhindern, dass die zur Erbringung der beschriebenen IT-Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) von Unbefugten genutzt werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Passwortregeln sind in einer allgemein gültigen Policy geregelt

• Pro Benutzer ein entsprechendes Benutzerkonto

• Passwortlänge von mindestens 8 Stellen

• Verhinderung von Trivialpasswörtern durch die Pflicht zur Eingabe von Ziffern, Groß- und Kleinbuchstaben

• Regelmäßige Passwortwechsel, spätestens nach 90 Tagen

• Gleiches Passwort kann erst nach 8 Wechsel wieder verwendet werden

• Maximal 1 Passwortwechsel innerhalb von 10 Tagen

• Werden Daten von Mitgliedern auf mobilen Datenträgern gespeichert, werden diese verschlüsselt.

1.3 Zugriffskontrolle

Es ist sicherzustellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert oder verändert werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Verwaltung von Berechtigungen mit differenzierten Berechtigungen

• Gruppenkonzept

• Dokumentation von Berechtigungen

1.4 Weitergabekontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Die Übertragung von personenbezogenen Daten per Email darf nur verschlüsselt erfolgen

• Die Verbindung zu und von den Netzen des VDST darf nur verschlüsselt erfolgen

• Der Versand oder Transport von personenbezogenen Daten auf mobilen Datenträger (Sicherungsbänder, USB-Sticks, Speicherkarten etc.) darf nur verschlüsselt erfolgen

• Der Zugriff bei Fernwartungs- bzw. Serviceleistungen auf Datenverarbeitungsanlagen des VDST darf nur über sicherer verschlüsselte Verbindungen erfolgen

• Drahtlose Übertragung (WLAN) von personenbezogenen Daten der Mitglieder darf nur verschlüsselt erfolgen

1.5 Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Vereinsbezogene logische Datentrennung

• Physikalische Trennung durch Speicherung in einem externen Rechenzentrum

• Zugriffsberechtigungen

1.6 Verschlüsselung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Verschlüsselte Datenübertragung (VPN, verschlüsselte Internetverbindungen via TLS/SSL)

2. Integrität

2.1 Eingabekontrolle

Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Zugriffsrechte

• Systemseitige Protokollierungen von Logins

• Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten

2.2 Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle gem 1.4 dienen auch der Sicherstellung der Integrität.

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Einrichtung von entsprechenden Datensicherungsverfahren wie z.B. Bandsicherung, Datenspiegelung, Snapshot

• Räumliche Trennung der Sicherungsdaten. Diese muss so gestaltet sein, dass auch Katastrophen-Ereignisse nicht zum Verlust von Daten führen.

• Einsatz von unterbrechungsfreien Stromversorgungen, die gewährleistet, dass Daten nicht während der Speicherung oder Übertragung verloren gehen.

• Einrichtung von Schutzmaßnahmen, die Angriffe durch unbefugte Dritte verhindern (Virenschutz, Firewall, Spyware Detection, Paketfilter, DMZ etc.)

3.2 Rasche Wiederherstellbarkeit

Es müssen Maßnahmen getroffen werden, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beim Auftragnehmer umgesetzte Maßnahmen:

• IT-Notfallpläne und Wiederanlaufpläne

• Regelmäßige Datenwiederherstellungen

4. Weitere Maßnahmenbereiche

4.1 Auftragskontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur ensprechend den Weisungen des Auftraggebers verarbeitet werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Sorgfältige Auswahl von Dienstleistern

• Überprüfung vor der Beauftragung, ob die Vorgaben des Datenschutzes eingehalten werden

• Vertrag zur Auftragsdatenverarbeitung gem. Art. 28 DS-GVO mit Regelungen zu den Rechten und Pflichten des Auftragnehmers

• Regelmäßige Überprüfung der Dienstleister

• Benennung eines Datenschutzbeauftragten (sofern gesetzlich gefordert)

4.2 Datenschutz-Managementsystem

Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen

Maßnahmen implementiert sein.

Beim Auftragnehmer umgesetzte Maßnahmen:

• IT-Sicherheitskonzept

• Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen

• Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO)

• Durchführung regelmäßiger interner Audits durch den DSB

• Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (audatis MANAGER)

B.2 Technische und oranisatorische Maßnahmen Verein

1. Vertraulichkeit

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu den vom Auftragnehmer zwecks Erbringung der Verarbeitung genutzten technischen Einrichtungen zu verwehren.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Der Verein trägt dafür dafür Sorge, dass Unbefugte keinen Einblick oder Zugriff auf Datenverarbeitungsgeräte (PC's, Laptops, Monitore, Drucker, etc.) erlangen können, auf denen Daten der Mitglieder verarbeitet oder ausgegeben werden

1.2 Zugangskontrolle

Es ist zu verhindern, dass die zur Erbringung der beschriebenen IT-Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) von Unbefugten genutzt werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Der zur Verarbeitung benutzte Rechner ist durch Benutzerkonto und Passwort geschützt

• Das Benutzerkonto hat keine lokalen Administrationsrechte. Werden diese benötigt, muss ein zusätzliches Administrationskonto erstellt werden.

• Passwortlänge hat mindestens 8 Stellen

• Trivialpasswörter sind durch die Pflicht zur Eingabe von Ziffern, Groß- und Kleinbuchstaben und Sonderzeichen ausgeschlossen

• In den Passwörtern sind weder Wörter noch Ziffern- oder Zeichenfolgen enthalten

• Regelmäßige Passwortwechsel erfolgen spätestens nach 90 Tagen

• Mindestens 4 Wechsel bis zur erneuten Benutzung eines Passwortes

1.3 Zugriffskontrolle

Es ist sicherzustellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert oder verändert werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Es werden Maßnahmen ergriffen, die verhindern, dass Unbefugte Zugriff auf die Mitgliederdaten erlangen können, z.B.

• - Eigene Passwort geschützte Rechner für die Mitgliederverwaltung, Kassenführung, Jugendarbeit etc.

• - Zugriff darf nur für Personen ermöglicht werden, die Zugriff auf Mitgliederdaten aufgrund ihrer Funktion im Verein benötigen

1.4 Weitergabekontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Die Übertragung von personenbezogenen Daten per Email erfolgt nur verschlüsselt (z.B. Verteilung der Mitgliederliste an Vorstände und Funktionäre)

• Die Verbindung zu und von den Netzen des VDST erfolgt verschlüsselt über eine SSL verschlüsselte Eingabemaske

• Der Versand oder Transport von personenbezogenen Daten auf mobilen Datenträger (USB-Sticks, Speicherkarten etc.) erfolgt nur verschlüsselt

• Der Zugriff bei Fernwartungs- bzw. Serviceleistungen auf Datenverarbeitungsanlagen des Vereins erfolgt nur über sicherer verschlüsselte Verbindungen

• Drahtlose Übertragung (WLAN) von personenbezogenen Daten der Mitglieder erfolgt nur verschlüsselt (die Verschlüsselung wird immer an den Stand der Technik angepasst)

1.5 Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Bei der Verarbeitung wird sichergestellt, dass eine "Vermischung" mit anderen Daten des Vereins und auch unbefugte Zugriffe Dritter (auch versehentlich) unmöglich sind.

1.6 Verschlüsselung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Werden Mitgliederdaten auf mobilen Geräten (Notebook, externe Datenträger, IPad etc.) gespeichert, müssen die Datenbestände verschlüsselt werden

• Die Weitergabe von Mitgliederdaten per Email darf nur verschlüsselt erfolgen

• Funkverbindungen (Bluetooth, WLAN) müssen verschlüsselt eingerichtet werden und müssen dem Stand der Technik entsprechen

2. Integrität

2.1 Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle gem 1.4 dienen auch der Sicherstellung der Integrität.

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Es sind entsprechenden Datensicherungsverfahren wie Plattensicherung, Datenspiegelung etc. eingerichtet

• Die Sicherungsdaten werden räumlich getrennt aufbewahrt. Diese ist so gestaltet, dass auch Katastrophen-Ereignisse nicht zum Verlust von Daten führen (z.B. Auslagerung der Sicherungsmedien, Spiegelung in eine Cloud)

• Es wurden Schutzmaßnahmen getroffen, die Angriffe durch unbefugte Dritte verhindern (Virenschutz, Firewall am DSL-Router etc.)

• Es werden eine externen Geräte (Smartphones oder Tabletts) mit SIM-Karte im gleichen Netz betreiben, in dem die Mitgliederverwaltung und die Übertragung zum VDST durchgeführt wird

3.2 Rasche Wiederherstellbarkeit

Es müssen Maßnahmen getroffen werden, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Es wurden Notfallpläne erstellt, mit denen fachkundige Dritte die Daten des Vereins wieder herstellen können

• Die Sicherungsdaten werden in regelmäßigen Abständen überprüft und ggf. Wiederherstellungstests durchgeführt

4. Weitere Maßnahmenbereiche

4.1 Auftragskontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur ensprechend den Weisungen des Auftraggebers verarbeitet werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

• Sorgfältige Auswahl von Dienstleistern

• Überprüfung vor der Beauftragung, ob die Vorgaben des Datenschutzes eingehalten werden

• Vertrag zur Auftragsdatenverarbeitung gem. Art. 28 DS-GVO mit Regelungen zu den Rechten und Pflichten des Auftragnehmers

• Regelmäßige Überprüfung der Dienstleister

• Benennung eines Datenschutzbeauftragten (sofern gesetzlich gefordert)

4.2 Datenschutz-Managementsystem

Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert sein.

Beim Auftragnehmer umgesetzte Maßnahmen:

• IT-Sicherheitskonzept ist tabellarisch erstellt (z.B. mit Excel)

• Es wurden Verfahren eingeführt, die die Nachvollziehbarkeit von Sicherheitsverstößen und Problemen ermöglicht (z.B. Meldesystem für auffällige Emails)

• Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO)

• Datenschutz und IT-Sicherheit werden regelmäßiger durch den Datenschutzbeauftragten oder, falls dieser nicht bestellt werden muss, durch Sachkundigen durchgeführt

• Alle Dokumentationen, Verfahrensbeschreibung, Auftragsdatenverarbeitungsvorgänge etc. werden in einem übersichtlichen System verwaltet