Datenschutzhandbuch des KGV

1 INHALT

2 ÜBERBLICK

Die wesentlichen rechtlichen Grundlagen zum Datenschutz enthalten die Datenschutzgrundverordnung (DSGVO) und das Bundesdatenschutzgesetz (BDSG). Seit Geltung der DSGVO müssen wir jederzeit die Einhaltung der Datenschutzgrundsätze und gesetzlichen Vorschriften der DSGVO sicherstellen und nachweisen. Verstöße gegen diese Pflichten sind bußgeldbewehrt. Bußgelder können bis zu einer Höhe von 20 Mio. EUR und bei Unternehmen bis 4% des Gesamtunternehmensumsatzes verhängt werden.

Der Schutz von personenbezogenen Daten und Informationen ist für unseren Verein daher von großer Bedeutung. Datenschutzverstöße würden nicht nur die Funktion unseres Vereins schwer beeinträchtigen, sondern außerdem zu schwerem Ansehensverlust führen und viele weitere materielle und immaterielle Schäden verursachen.

Das Anliegen dieses Datenschutzhandbuches ist es deshalb, im Interesse unseres Vereins und der betroffenen Personen, also der Personen, deren personenbezogene Daten wir erheben und verarbeiten wie z. B. Kunden, Gäste, Besucher, Mitglieder oder Mitarbeiter, den Schutz der personenbezogenen Daten vereinsintern zu regeln und so die gesetzlichen Anforderungen zu gewährleisten.

In diesem Datenschutzhandbuch werden die gesetzlichen Datenschutzgrundsätze beschrieben und darauf aufbauend sämtliche Aspekte unseres Vereinsdatenschutzes erläutert. Zum Handbuch gehören auch die in den Anlagen 1-… einbezogenen Richtlinien, Formulare und Arbeitshilfen.

Das Datenschutzhandbuch legt ferner die Struktur und die Prozesse des Datenschutzmanagements dar, die wir umgesetzt haben und die in unserer Vereinspraxis gelebt werden. Ganz entscheidend erfüllt dieses Datenschutzhandbuch mit den beigefügten Anlagen die in der DSGVO geforderten Dokumentations- und Nachweispflichten. Sie stellt eine entscheidende Säule unserer gesetzlichen Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO dar („Accountability“).

Nicht zuletzt steht und fällt der Datenschutz aber mit unseren Mitarbeiterinnen und Mitarbeitern. Gesetzliche und vereinsinterne Regelungen müssen beachtet werden. Dies verlangt von unseren Mitarbeiterinnen und Mitarbeitern ein Bewusstsein für unsere Tätigkeit, für die sich stetig verändernde technischen und rechtlichen Rahmenbedingungen und für die Risiken, die mit dem Umgang mit personenbezogenen Daten und der Benutzung technischer Systeme und Kommunikationstechnologien verbunden sind. Um diesen Herausforderungen begegnen zu können, richtet sich das Datenschutzhandbuch ausdrücklich an unsere Mitarbeiter. Wir wollen sie mit diesem Dokument für das Anliegen des Datenschutzes sensibilisieren und ihnen Informationen und Hilfestellungen an die Hand geben, die es ermöglichen, Datenschutzrisiken zu erkennen und abzuwehren.

Das Datenschutzhandbuch dient weiterhin als Einstieg und Grundlage für Prüfungen, Audits und Qualitätskontrollen.

3 PERSONENBEZOGENE DATEN

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. In der Sprache des Datenschutzes spricht man von der "betroffenen Person". Als identifizierbar wird eine betroffene Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 4 Ziff. 1 DSGVO).

Personenbezogene Daten sind daher zum Beispiel:

- allgemeine Personendaten (Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer usw.)
- Kennnummern (Sozialversicherungsnummer, Personalausweisnummer, Steuer ID, Matrikelnummer usw.)
- Bankdaten (Kontonummern, Kontostände, alle Arten von Kreditinformationen etc.)
- Online-Daten (IP-Adressen, Standortdaten usw.)
- physische Merkmale (Geschlecht, Haut- und Haarfarbe, Augenfarbe, Kleidergröße usw.)
- Besitzmerkmale (Fahrzeuge, Immobilien, Grundbucheintragungen, KfZ-Kennzeichen, Zulassungsdaten etc.)
- Kundendaten (Bestellungen, Adressdaten, Kontodaten ..)
- Werturteile (Schul- und Arbeitszeugnisse etc.)

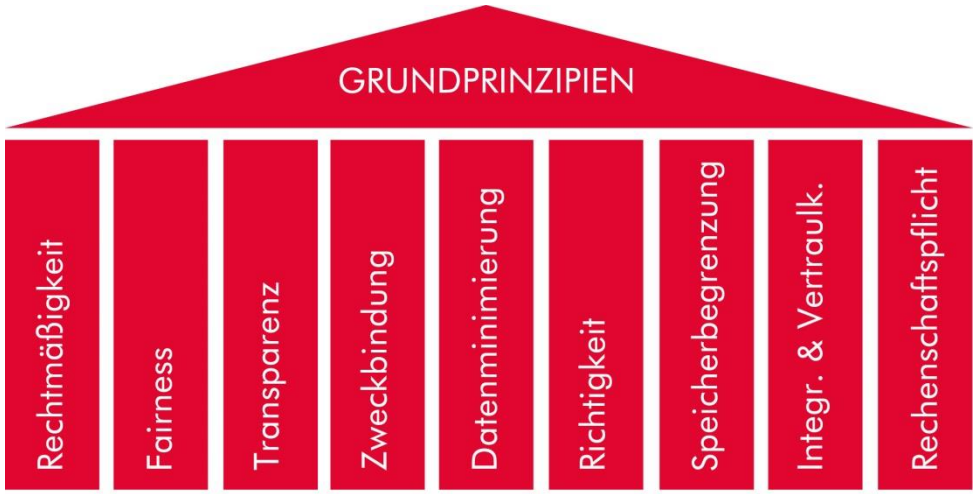
Und besonders sensible personenbezogene Daten sind solche über die ethnische Herkunft, politische Ansichten, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheitsdaten, Daten zur Sexualität eines Menschen.

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß der Charta der Grundrechte der Europäischen Union hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben.

4 DATENSCHUTZGRUNDSÄTZE

Art. 5 Abs. 1 DSGVO legt die Grundsätze der Verarbeitung personenbezogener Daten fest und definiert sie. Sie werden nachfolgend beschrieben. Ihr Verständnis ist von zentraler Bedeutung. Sie sind für die Verarbeitung von personenbezogenen Daten verbindlich. Nach Art. 5 Abs. 2 müssen wir als Verein die Einhaltung dieser Grundsätze nachweisen. Die Verletzung dieser Grundsätze der Datenverarbeitung ist gem. Art. 83 DSGVO mit Bußgeld bedroht.

Für den Umgang mit personenbezogenen Daten werden nachfolgende Grundsätze besonders beachtet:



4.1 Rechtmäßigkeit ("lawfulness")

Der Grundsatz der Rechtmäßigkeit der Verarbeitung besagt, dass personenbezogene Daten nur unter dem Vorbehalt einer gesetzlichen Erlaubnis oder einer Einwilligung erhoben und verarbeitet werden dürfen. Bei jeder Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist deshalb darauf zu achten, dass eine Rechtsgrundlage nach den Datenschutzvorschriften vorhanden ist. In Art. 6 und 9 DSGVO sind die Bedingungen aufgezählt, nach denen eine rechtmäßige Datenverarbeitung erfolgen kann. Eine Rechtsgrundlage kann insbesondere ein Vertrag mit der betroffenen Person, ein berechtigtes Interesse des Vereins unter Abwägung des Interesses und der Grundrechte und Grundfreiheiten der betroffenen Personen oder eine Einwilligung sein. Für die einzelnen Datenverarbeitungsverfahren sind die Rechtsgrundlagen in der Beschreibung zum Verzeichnis über die Verarbeitungstätigkeiten beschrieben und geprüft.

4.2 Verarbeitung nach Treu und Glauben ("fairness")

Unter diesem Gesichtspunkt sind insbesondere die Rechte der Betroffenen und die Informationspflichten in verständlicher und nachvollziehbarer Form zu erfüllen. Die Datenverarbeitung muss unter Berücksichtigung der Interessen der betroffenen Personen angemessen im Hinblick auf ihre Grundrechte

sein. Auf die verbindlich eingerichteten Datenschutzprozesse zu den Rechten der Betroffenen und zu den Informationspflichten wird verwiesen.

4.3 Transparenz ("transparancy")

Der Grundsatz der Transparenz verlangt, dass jeder Betroffene wissen soll, wer welche Daten für welche Zwecke über ihn erhebt, speichert und verarbeitet und übermittelt und wie lange die Daten gespeichert werden, und dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind (Art. 12 bis 14 DSGVO). Natürliche Personen sind über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu informieren und darüber aufzuklären, wie sie ihre diesbezüglichen Rechte geltend machen können. Die Informationen müssen einfach und verständlich sein.

4.4 Zweckbindung ("purpose limitation")

Personenbezogene Daten dürfen nur für eindeutig festgelegte und legitime Zwecke erhoben werden. Eine Weiterverarbeitung in einer Weise, die mit diesen vorab festgelegten Zwecken nicht vereinbar ist, ist verboten. Eine Verarbeitung oder Nutzung von personenbezogenen Daten für andere als den Betroffenen im Zusammenhang mit der Datenerhebung kommunizierten Zwecke ist nur unter den gesetzlich festgelegten Bedingungen (Art. 6 Abs. 4 DSGVO) und ansonsten nur mit Einwilligung der Betroffenen zulässig. Sollen erhobene Daten auch für einen anderen als den der Erhebung zugrunde liegenden Zweck verwendet werden, z. B. zu Zwecken der Werbung oder des Profilings oder für Datenübermittlungen, ist vorher der Datenschutzbeauftragte zu konsultieren. Sollte es keinen Datenschutzbeauftragten geben, muss im Falle eines Vereins, der Vorstand bzw. die Geschäftsführung hinzu gezogen werden, wenn der Geschäftsführung diese Aufgabe übertragen wurde Der Datenschutzbeauftragte prüft, ob die Verarbeitung zu dem anderen Zweck mit dem ursprünglichen Zweck der Verarbeitung vereinbar ist.

4.5 Datenminimierung ("data minimisation")

Art und Umfang der Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Art. 5 Abs. 1 lit. c) DSGVO). Ob eine Datenverarbeitung gegen den Grundsatz der Datenminimierung verstößt, hängt vielmehr von einer Angemessenheitsprüfung ab. Es dürfen nur solche Daten erhoben werden, die wirklich erforderlich sind und diese Daten dürfen nur solange gespeichert werden, wie sie tatsächlich benötigt werden. Darüber hinausgehende Erhebungen und Verarbeitungen sind unzulässig. Wer sich über die Erforderlichkeit der Daten und die Zulässigkeit der Datenverarbeitung nicht sicher ist, wendet sich an den Datenschutzbeauftragten.

4.6 Richtigkeit ("accuracy")

Die personenbezogenen Daten müssen im Hinblick auf die Zwecke ihrer Verarbeitung sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Die Verarbeitung unrichtiger Daten ist zu vermeiden. Zur Berichtigung oder Löschung unrichtiger Daten sind alle angemessenen Maßnahmen zu treffen. Eine langfristige Speicherung von Daten erfordert daher ein erhöhtes Maß eines Berichtigungsmanagements.

4.7 Speicherbegrenzung ("storage limitation")

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie erhoben worden sind, erforderlich ist. Um sicherzustellen, dass personenbezogene Daten nicht länger als nötig gespeichert werden, sind Fristen für ihre Löschung oder regelmäßige Überprüfung vorzusehen und die Daten regelmäßig zu löschen bzw. zu vernichten.

4.8 Integrität und Vertraulichkeit ("integrity and confidentiality")

Der Grundsatz der Integrität und Vertraulichkeit besagt, dass personenbezogene Daten in einer Art und Weise verarbeitet werden müssen, die eine angemessene Sicherheit gewährleistet. Davon umfasst ist der Schutz vor unbeabsichtigtem Verlust, Zerstörung und Beschädigung durch geeignete technische Maßnahmen. Bei der Verarbeitung der personenbezogenen Daten ist durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit der personenbezogenen Daten zu gewährleisten. Unbefugte dürfen keinen Zugang zu den Daten haben.

4.9 Rechenschaftspflicht ("accountability")

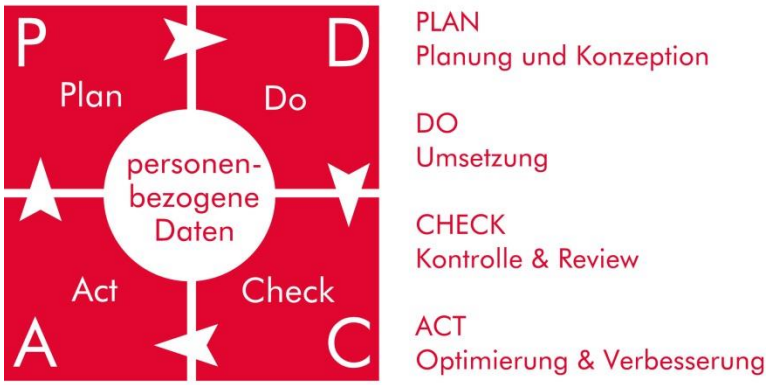
Der Grundsatz der Rechenschaftspflicht ist eine wesentliche Neuerung zum alten Datenschutzrecht. Die Dokumentations- und Nachweispflichten haben sich deutlich erhöht. Insbesondere müssen wir als Verantwortlicher für personenbezogene Daten nachweisen, dass wir die Datenschutzgrundsätze jederzeit einhalten. Zur Erfüllung dieser Rechenschaftspflicht haben wir ein stimmiges, systematisches und nachvollziehbares Datenschutzmanagement eingerichtet, dessen Dreh- und Angelpunkt die Regelungen sind, wie sie in diesem Datenschutzhandbuch festgelegt und durch die beigefügten bzw. in Bezug genommenen Anlagen konkretisiert sind. Auf der Grundlage dieser Datenschutzdokumentation ist eine Überprüfung der Einhaltung dieser Grundsätze durch Datenschutzprüfungen und Audits möglich. Die in diesem Datenschutzhandbuch zu diesem Zweck festgelegten Dokumentationen und Nachweise müssen wir daher immer aktuell und vollständig führen.

5 DATENSCHUTZMANAGEMENT

In Erfüllung der Rechenschaftspflicht („accountability“) haben wir unser Datenschutzmanagementsystem eingeführt. Als Datenschutzmanagementsystem werden die in diesem Handbuch, sowie in dessen

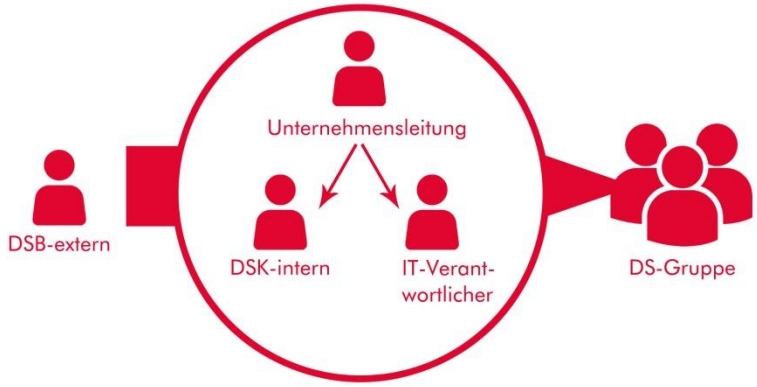
Anlagen aufgeführten Maßnahmen organisatorischer Art verstanden, die den datenschutzkorrekten Umgang mit personenbezogenen Daten gewährleisten sollen und dabei einerseits Datenschutzverletzungen vorbeugen, andererseits aber auch helfen sollen, diese nachträglich zu beheben. Unser Ziel war, den Datenschutz so zu organisieren, dass er im Verein auch in der Fläche gelebt wird und seine Umsetzung jederzeit nachgewiesen werden kann.

Unser Datenschutzmanagement folgt dabei dem sogenannten PDCA-Zyklus („Plan-Do_Check-Act“) nach W. Edwards Deming. Sämtliche von uns ergriffene Maßnahmen sind nicht lediglich eingeführt worden. Sondern Sie unterliegen einem kontinuierlichen Verbesserungsprozess, wie er auch allen Qualitätsmanagement-Systeme zugrunde liegt.



6 DATENSCHUTZORGANISATION UND VERANTWORTLICHKEITEN

Im Folgenden werden die Verantwortlichkeiten und Aufgaben im Hinblick auf den Datenschutz und die IT-Sicherheit im Verein dargestellt. Sämtliche Ansprechpartner inklusive ihrer Kontaktdaten werden als **Anlage 1** beigefügt.



Anlage 1: Ansprechpartner und ihre Kontaktdaten
Dieses Schaubild zeigt die Grundausrichtung im Falle eines externen DSB

Name	Funktion	Telefon	E-Mail

	Datenschutzbeauftragter		
	Datenschutzkoordinator		
	Vorstandsmitglied		
	IT-Verantwortlicher		
	Geschäftsführer		

6.1 Vereinsleitung

Der Vereinsvorstand trägt die Gesamtverantwortung für den Datenschutz und die IT-Sicherheit im Verein. Dies betrifft insbesondere die Beachtung der Datenschutzgrundsätze, sowie die Gestaltung und Einhaltung der gesetzlichen Regelungen.

6.2 Datenschutzkoordinator – intern

Zur Erreichung der Ziele des Datenschutzhandbuches haben wir zusätzlich einen internen Datenschutzkoordinator (DSK-intern) benannt. Der DSK-intern unterstützt den Vereinsvorstand und den DSB bei der Umsetzung des Datenschutzes im Verein. Er ist die Schnittstelle zwischen Vereinsleitung, DSB und Datenschutzgruppe. Er fungiert zudem als der vereinsinterne Ansprechpartner für die Mitarbeiter und Fachabteilungen, insbesondere bei der Einführung neuer Verarbeitungen, sowie Software- und IT-Systemen. Damit wollen wir sicherstellen, dass datenschutzrelevante Aspekte vereinsintern von Beginn an beachtet und dokumentiert werden. Dem DSK-intern obliegen die folgenden Aufgaben:

- Dokumentation: Erstellung und Führung des Verzeichnisses von Verarbeitungstätigkeiten (Art 30 DSGVO)
- Prüfung gemeldeter neuer Verarbeitungstätigkeiten und Koordinierung der Einführung neuer Prozesse und Systeme
- Unterstützung der Vereinsleitung bei der Auswahl und späteren Auditierung externer Dienstleister (Auftragsverarbeiter), sowie Einholung und Verwaltung von Auftragsverarbeitungsverträge, bei denen das Verein entweder Auftraggeber oder Auftragnehmer ist
- Pflege und Aktualisierung der Datenschutzbestimmungen
- Bearbeitung, Beantwortung und Dokumentation von Betroffenenanfragen, insbesondere von Auskunfts- oder Löschungsersuchen
- Untersuchung und Dokumentation aller datenschutzrelevanten Vorfälle, insbesondere von Datenschutzverstößen
- Einholung und Dokumentation der Verpflichtungserklärungen der Mitarbeiter
- Einleitung, Steuerung und Dokumentation von Sensibilisierungs- und Schulungsmaßnahmen, wobei die Durchführung von Schulungen durch den DSB stattfinden

- Koordinierung, Steuerung und Dokumentation des Datenschutzmanagements: dies betrifft insbesondere die Planung und Protokollierung der Arbeit der Datenschutzgruppe und die Erarbeitung konkreter Verbesserungsvorschläge für den Datenschutz im Verein
- Erstellung eines jährlichen Berichts über den Stand des Datenschutzes im Verein und über die Arbeit bzw. Arbeitsergebnisse der Datenschutzgruppe.
- Planung, Koordinierung und Dokumentation der Durchführung von Datenschutz-Folgenabschätzungen

Der DSK-intern informiert den DSB und die Vereinsleitung unverzüglich in Textform (Brief, E-Mail oder Fax) über alle datenschutzrelevanten Prozesse, Vorhaben und Vorfälle im Verein. Der DSB steht dem DSK-intern bei der Wahrnehmung seiner Aufgaben im Übrigen beratend zur Seite. Er wird auf Anfrage eine rechtliche Einschätzung abgeben und dem DSK-intern Formulare und Arbeitshilfen zur Verfügung stellen.

7.2. IT-Verantwortlicher

Zur Erreichung der Ziele des Datenschutzhandbuches haben wir weiterhin einen internen IT-Verantwortlichen benannt. Dem IT-Verantwortlichen obliegen die folgenden Aufgaben:

- Beratung des Vereinsvorstands bei der Planung, Umsetzung und Verbesserung der Informationssicherheit und des technischen Datenschutzes im Verein. Der IT-Verantwortliche hat insbesondere über technische Neuerungen und mögliche Schwachstellen in der Sicherheitsarchitektur des Vereins zu informieren
- Dokumentation: Erstellung und Führung des Dokuments mit der Zusammenstellung der technischen und organisatorischen Maßnahmen des Vereins (TOMs)
- Dokumentation: Erstellung und Führung des IT-Sicherheitskonzeptes
- Dokumentation: Erstellung und Führung des Löschkonzeptes
- Dokumentation: Erstellung und Führung des Backup- und Recovery-Konzeptes
- Dokumentation: Erstellung und Führung des Berechtigungskonzeptes
- Unterstützung bei der Planung, Umsetzung und Verbesserung technischer und organisatorischer Maßnahmen bei neuen und bei bestehenden Verarbeitungstätigkeiten.
- Erarbeitung konkreter Verbesserungsvorschläge für den Datenschutz im Verein
- Empfehlung und Einschätzung im Hinblick auf die Beschaffung neuer Hard- und Software im Verein
- Erarbeitung von Lösungen zu „Privacy by design“, „Privacy by default“ und dem Recht auf Datenportabilität.

6.3 Datenschutzgruppe

Um sämtliche datenschutzrechtliche Belange laufend zu erfassen, zu bewerten und zu verbessern (PDCA) sowie zur Erfüllung unserer Rechenschaftspflicht zur Einhaltung der Grundsätze gem. Art 5 Abs. 1 DSGVO hat unser Verein eine Datenschutzgruppe gebildet.

Die Datenschutzgruppe besteht aus dem zuständigen Mitglied des Vereinsvorstandes, dem DSB, dem DSK-intern, dem IT-Verantwortlichen sowie je nach Bedarf weiteren Teilnehmern, soweit ihre Fachbereiche betroffen sind. Die Datenschutzgruppe soll mindestens halbjährlich zusammentreten. Beschlüsse kann die Datenschutzgruppe jederzeit auch im Umlaufverfahren treffen. Der DSK-intern wird zu den Terminen der Datenschutzgruppe einladen, die Tagesordnungspunkte sammeln und vorbereiten, sowie über die Arbeitsergebnisse und -berichte Protokoll führen.

Die Datenschutzgruppe wird mit dem Ziel einer regelmäßigen Überprüfung und Verbesserung insbesondere evaluieren,

- Ob das „Verzeichnis der Verarbeitungstätigkeiten“ auf dem aktuellen Stand ist oder überarbeitet werden muss
- Ob die ergriffenen technischen und organisatorischen Maßnahmen unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitungen sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen korrekt umgesetzt werden. Darüber hinaus ist zu prüfen, ob sie nach wie vor geeignet und angemessen sind. In diesem Zuge ist auch zu klären, ob sich der Stand der Technik verändert hat
- Ob die Datenschutzprozesse funktionieren (z.B. zur Wahrung der Betroffenenrechte, zum Verhalten bei Datenpannen)
- Ob der Beschäftigtendatenschutz funktioniert (z.B. Schulungsmaßnahmen wirken, Richtlinien eingehalten werden). Dies betrifft auch die regelmäßige Überarbeitung und Vervollständigung von Mitarbeiterrichtlinien.
- Ob die Datenschutzbestimmungen in Erfüllung der Informationspflichten aus Art. 12 ff. DSGVO aktuell sind.
- Ob und mit welchem Ergebnis Audits bei Auftragsverarbeitern durchgeführt worden sind oder noch anstehen
- Ob neue Verarbeitungstätigkeiten eingeführt werden sollen, welche Risiken diese mit sich bringen und ob es diesbezüglich einer Folgenabschätzung bedarf.

Darüber hinaus dient die Datenschutzgruppe der Klärung offener Fragen, der Erarbeitung von Lösungen für aufgetretene Probleme im Vereinsschutz und der Verabschiedung von Optimierungsmaßnahmen.

Die Protokolle werden vom DSK-intern ausgefertigt und zur Erfüllung unserer Dokumentations- und Nachweispflicht gem. § 5 Abs. 2 DSGVO aufbewahrt.

6. DATENVERARBEITUNG

Jede Verarbeitung personenbezogener Daten muss rechtlich zulässig sein. Dies beinhaltet die Wahrung der Datenschutzgrundsätze.

7.1. Einführung neuer oder Änderung bestehender Verarbeitungstätigkeiten

Vor der Aufnahme eines neuen oder der Änderung eines bestehenden Datenverarbeitungsprozesses bedarf es einer Meldung durch den zuständigen Mitarbeiter oder die zuständige Fachabteilung an den DSK-intern unter Verwendung des Formblatts „Meldung neue Verarbeitungstätigkeit“. Diese enthält eine Festlegung der Zwecke der Verarbeitung und eine erste Risikoeinschätzung des zuständigen Mitarbeiters/ der zuständigen Fachabteilung.

Anlage 4: Meldung neue Verarbeitungstätigkeit

Verzeichnis von Verarbeitungstätigkeiten
Gem. Art. 30 Abs. 1 DSGVO

Hauptblatt

1. Verantwortlicher (Art. 30 Abs. 1 lit. a DS-GVO)
Name: …
Anschrift: …
Telefon: …
Fax: …
E-Mail: …
Internetadresse: …

: …

2. Gesetzlicher Vertreter
Name: … (Vereinsvorstand)
Telefon: …
E-Mail: …

3. Leiter der Datenverarbeitung
Name: …
Telefon: …
E-Mail: …

4. Zuständige Aufsichtsbehörde
Name: Der Hessische Beauftragte für Datenschutz und Informationsfreiheit
Anschrift: Gustav-Stresemann-Ring 1,Wiesbaden
Telefon: 0611

5.Regelungen zur Datensicherheit
[Verweis auf übergreifende IT-Sicherheitskonzepte, die grds. für alle Verarbeitungstätigkeiten gelten]

7. Regelungen zur Datenlöschung
[Verweis auf übergreifende Löschkonzepte, die grds. für alle Verarbeitungstätigkeiten gelten]

Ort/Datum: _____ Ort/Datum: _____

_____ _____
Verantwortlicher (Geschäftsführer) Datenschutzbeauftragter

Datum der Anlegung: *…*
Datum der letzten Änderung: *…*

Der DSK-intern wird die neue bzw. geänderte Verarbeitungstätigkeit in Abstimmung mit dem DSB und dem IT-Verantwortlichen prüfen. Dabei ist klären, ob die beabsichtigte Verarbeitungstätigkeit von einer Rechtsgrundlage gedeckt ist, ob die bestehenden technischen und organisatorischen Maßnahmen geeignet und angemessen sind und ob es für die Verarbeitungstätigkeit der Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO bedarf.

Der IT-Verantwortliche hat bei jeder Einführung neuer oder der Änderung bestehender Verarbeitungstätigkeiten Lösungen zu „Privacy By Design“ und „Privacy By Default“ vorzuschlagen.

Die Prüfung und ihr Ergebnis sind schriftlich durch den DSK-intern zu dokumentieren und der Datenschutzgruppe vorzustellen. Diese entscheidet über die Durchführung einer Folgenabschätzung.

6.4. Folgenabschätzung

Das Institut der Datenschutz-Folgenabschätzung (DSFA) ist im deutschen Datenschutzrecht bereits seit langem in ähnlicher Form unter der Bezeichnung „Vorabkontrolle“ bekannt.

Eine DSFA ist immer dann durchzuführen, wenn besonders sensible Daten verarbeitet werden oder die Datenverarbeitung dazu bestimmt war, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, Leistungen oder seines Verhaltens zu bewerten. In diesen Fällen müssen wir die dem Verfahren innewohnenden besonderen Risiken für die Rechte und Freiheiten des Betroffenen prüfen und eine Stellungnahme abgeben. Die Datenschutz-Folgenabschätzung dient also der Bewertung von Risiken und deren mögliche Folgen für die persönlichen Rechte und Freiheiten der betroffenen Personen.

Die Datenschutzgruppe wird jeden neuen oder geänderten Verarbeitungsprozess auf Grundlage der Vorprüfung des DSK-intern danach untersuchen, ob mit der Verarbeitung voraussichtlich ein hohes Risiko für personenbezogene Daten einhergeht und eine DSFA notwendig ist. Ist dies der Fall, beschließt die Datenschutzgruppe die Durchführung einer DSFA und bestimmt eine Arbeitsgruppe für deren Durchführung. Die Folgenabschätzung kann auch durch externe, fachkundige Personen übernommen – mit Ausnahme des DSB - übernommen werden.

Die jeweilige Verarbeitung darf grundsätzlich erst nach Durchführung der DSFA und entsprechender Freigabe durch die Vereinsleitung in Betrieb genommen werden. Der DSB steht bei der Durchführung der Folgenabschätzung auf Anfrage für die Beratung zur Verfügung.

Das Ergebnis der DSFA wird der Vereinsleitung mitgeteilt. Diese entscheidet über die Freigabe des Verarbeitungsprozesses.

Sollte die DSFA ergeben, dass das mit dem Verarbeitungsprozess verbundene Risiko nicht durch technische und organisatorische Maßnahmen eingedämmt werden kann, wird die Vereinsleitung darüber entscheiden, ob von der beabsichtigten Verarbeitungstätigkeit Abstand genommen oder die Aufsichtsbehörde i.S.d. Art. 36 DSGVO konsultiert werden soll.

6.5. Verzeichnis der Verarbeitungstätigkeiten

Wir sind gesetzlich gem. Art. 30 DSGVO verpflichtet, alle Prozesse, die personenbezogene Daten betreffen, in einem sogenannten Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren. Der DSK-intern führt ein solches Verzeichnis für unseren Verein. Soweit wir als Auftragsverarbeiter tätig sind, besteht daneben ein Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter i.S.d. Art. 30 Abs. 2 DSGVO.

Der DSK-intern trägt Sorge dafür, dass die Verarbeitungsverzeichnisse regelmäßig durch die Datenschutzgruppe auf ihre Aktualität überprüft und angepasst werden.

Alle Beschäftigten, die für die Einrichtung oder Durchführung von Verarbeitungen personenbezogener Daten in unserem Verein verantwortlich sind, sind bei einer Einführung oder Änderung von Verarbeitungen und/oder Geschäftsprozessen verpflichtet, dieses dem DSK-intern in Textform (Brief, E-Mail, Fax) mitzuteilen.

Anlage 5: Verzeichnis der Verarbeitungstätigkeiten

Verarbeitungstätigkeit Nr. …

Angaben zur Verarbeitungstätigkeit

1. Name der Verarbeitungstätigkeit: …

Beschreibung der Verarbeitungstätigkeit:
…

Angaben zur Verarbeitungstätigkeit

2. Zwecke der Verarbeitung
…

3. Kreis der betroffenen Personengruppen

Kategorien betroffener Personen	**Kategorien personenbezogener Daten**
3.1 …	…

Kategorien von Empfängern und Datenübermittlung

4. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden

4.1 Unternehmensinterne Empfänger
4.1.1 Abteilung: …
…

4.2 Externe Empfänger und Dritte (jeder andere Empfänger, auch Konzernunternehmen)
4.2.1 Externe Stelle: …
…

5. Datenübermittlungen in Drittländer
Übermittlung: ☐ Nein ☐ Ja ☐ Ist geplant

Name des Drittlandes: …
Empfänger im Drittland: …
Angabe der geeigneten Garantien: …

Löschfristen

6. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

Kategorien personenbezogener Daten	Löschfrist
Zu 3.1 …	…

Technische und organisatorische Maßnahmen

7. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen
Die ergriffenen Schutzmaßnahmen ergeben sich aus
- ☐ IT-Sicherheitskonzept
- ☐ Berechtigungskonzept
- ☐ Löschkonzept
- ☐ Notfall- und Recovery-Konzept
- ☐ Technische und organisatorische Maßnahmen des Auftragsverarbeiters
- ☐ Datenschutz-Zertifizierung
- ☐ …

Ergänzend und/oder abweichend sind vom Verantwortlichen für diese Verarbeitung folgende Schutzmaßnahmen ergriffen worden:
- ☐ Pseudonymisierung personenbezogener Daten: …
- ☐ Verschlüsselung personenbezogener Daten: …
- ☐ Gewährleistung der Vertraulichkeit der Systeme und Dienste: …
- ☐ Gewährleistung der Integrität der Systeme und Dienste: …
- ☐ Gewährleistung der Verfügbarkeit der Systeme und Dienste: …
- ☐ Gewährleistung der Belastbarkeit der Systeme und Dienste: …
- ☐ Wiederherstellung der Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall: …
- ☐ Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen: …
- ☐ Maßnahmen zur datenschutzfreundlichen Technikgestaltung und Voreinstellung („Privacy by design“ und „Privacy by default“)
- ☐ …

Rechtsgrundlage der Verarbeitungstätigkeit

8. Rechtsgrundlage der Verarbeitungstätigkeit

- ☐ Einwilligung
- ☐ Vertragserfüllung oder -anbahnung
- ☐ Erfüllung einer rechtlichen Verpflichtung
- ☐ Schutz lebenswichtiger Interessen einer natürlichen Person
- ☐ Wahrung der überwiegenden berechtigten Interessen des Verantwortlichen
- ☐ Spezialgesetzliche Regelung (Erlaubnis) außerhalb der DS-GVO
- ☐ Kollektivvereinbarung (z.B. Betriebsvereinbarung, Tarifvertrag)
- ☐ Wahrnehmung von arbeits- und sozialrechtlichen Rechten und Pflichten des Verantwortlichen
- ☐ Patientenbehandlung
- ☐ …

Mittel der Verarbeitung

9. Hardware, die für diese Verarbeitung eingesetzt wird
…

10. Software, die für diese Verarbeitung eingesetzt wird
…

11. Speicherort der Daten
- ☐ Lokal auf dem Rechner des einzelnen Beschäftigten
- ☐ Lokaler Server des Verantwortlichen. Server: …
- ☐ Auf Servern eines Dienstleisters
- ☐ Cloud. Cloud-Service: …
- ☐ …

Eingebundene Auftragsverarbeiter

12. Eingebundene Auftragsverarbeiter (z.B. externe Dienstleister): ☐ Nein ☐ Ja

Unternehmen:	…
Dienstleistung:	…
Verträge:	…

Zugriffsberechtigte Personen oder Personengruppen

13. Zugriffsberechtigte Personen oder Personengruppen

Kategorien personenbezogener Daten	Zugriffsberechtigte Personen(gruppe)	Zugriffsrecht (*V = Vollzugriff (beinhaltet Recht zur Berechtigungsvergabe), L = nur lesend, LS = lesend und schreibend*)
…	…	…

Anmerkungen

…

Ort/Datum: _____

_____
Verantwortlicher

7. SICHERHEITSMAßNAHMEN

Zur Einhaltung der datenschutzrechtlichen Vorschriften müssen wir Vorkehrungen zum Schutz der von uns verarbeiteten personenbezogenen Daten treffen. Nach Art. 32 und Art. 24 DSGVO ist es erforderlich, geeignete technische und organisatorische Maßnahmen auszuwählen und umzusetzen, die ein, dem Risiko angemessenes Schutzniveau gewährleisten. Es gilt dabei ein risikobasierter Ansatz. Die Auswahl der Sicherheitsmaßnahmen ist an den konkreten Verarbeitungstätigkeiten und den damit verbundenen Gefahren auszurichten. Umso höher die Risiken für die betroffenen Personen sind, umso stärker und umfassender müssen unsere Sicherheitsmaßnahmen sein. Diese schließen insbesondere Maßnahmen zur

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste unseres Vereins im Zusammenhang mit der Verarbeitung
- Maßnahmen zur Gewährleistung der Verfügbarkeit und schnelle
- Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Die ergriffenen Sicherheitsmaßnahmen unseres Vereins sind vom IT-Verantwortlichen zu dokumentieren. Die Dokumentation erfolgt zum einen in der Zusammenstellung unserer technischen und organisatorischen Maßnahmen und ausführlich in unserem IT-Sicherheitskonzept.

Anlage 6: Zusammenstellung technische und organisatorische Maßnahmen

8. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUM DATENSCHUTZ

Technische und Organisatorische Maßnahmen

1. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

- **Die übliche, alltägliche Nutzung von personenbezogenen Daten findet ausschließlich über Nutzernamen und E-Mail-Adressen statt. Alle Details dieser Daten werden gesondert und zentral verwaltet und sind nur durch Hinzuziehen weiterer Informationen zugänglich. Eine Pseudonymisierung im eigentlichen Sinne findet nicht statt.**

2. Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)

- **Die Übertragung von personenbezogenen Daten, insbesondere wenn diese über das (offene) Internet erfolgt, findet in verschlüsselter Form statt. Als Verschlüsselung wird HTTPS/SSL verwendet. Ausgewählte Daten, insbesondere Passwörter werden zusätzlich gehasht (MD5) und nur in dieser Form übertragen und abgelegt.**

8.4.

8.5. **3. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

- *Zutrittskontrolle*
  Eingangstür: Der Zugang zu den Büroräumen ist stets verschlossen und kann nicht ohne Schlüssel von außen geöffnet werden.
- Schließsystem: Die Eingangstür ist mit einem Sicherheits-Schließsystem ausgestattet.
- **Interne Türen: Alle Räume innerhalb der Büroräume der MUSTERFIRMA, die sensible Daten in digitaler oder in Papierform enthalten, z.B. Serverraum und Sekretariat, sind mit eigenen Türen zusätzlich gesichert. Diese Türen verfügen über Sicherheitsschlösser.**
- **Die Serverracks innerhalb der Serverräume sind zusätzlich verschlossen und haben eigene Sicherheitsschlösser.**
- **Schlüsselregelung: Die fest angestellten Mitarbeiter der MUSTERFIRMA haben einen Schlüssel für das Schließsystem der Eingangstür. Die Ausgabe des Schlüssels wird unter Festhaltung des Namens und durch Quittierung des Erhalts durch den Empfänger dokumentiert. Die Rückgabe des Schlüssels erfolgt mit Beendigung des Vertragsverhältnisses. Schlüssel für die oben genannten internen Räume haben nur sehr kleine Gruppen von ausgewählten Mitarbeitern. Die Ausgabe und Rückgabe ist ebenso geregelt wie bei der Eingangstür.**
- **Schlüsselverlust: Bei Verlust des eines Schlüssels werden alle relevanten Schlüssel ausgetauscht**
- **Video: Die Eingangstür zu den Büroräumen wird durch eine Videokamera mit Bewegungssensor überwacht.**
- **Alarmanlage: Die Büroräume sind an Notausgängen mit einem Alarmsystem mit direkter Verbindung zum Sicherheitsdienst gesichert.**
- **Besucher: Besucher der Büroräume werden am Empfang begrüßt und kontrolliert. Während des gesamten Aufenthalts in den Büroräumen der MUSTERFIRMA werden die Besucher durch fest angestelltes Personal begleitet.**
- **Reinigungspersonal: Die Büroräume der MUSTERFIRMA werden durch ausgewähltes Reinigungspersonal gereinigt. Ausnahme ist der Serverraum, der durch IT-Personal gereinigt wird.**

- *Zugangskontrolle*

  - **Alle IT-Systeme der MUSTERFIRMA sind nur die ausgewählte Nutzer nutzbar. Die Auswahl der jeweiligen Nutzer erfolgt nach dem Prinzip den Nutzerkreis so klein wie möglich zu halten.**
  - **Jedem Benutzer ist ein spezielles Benutzerprofil zugeordnet, dass dem Benutzer ausschließlich den Umfang an Rechten zugesteht, der für die jeweilige Arbeit notwendig ist. Insbesondere wird der Zugang zu personenbezogenen Daten restriktiv behandelt und nur kleinen Benutzerkreisen zugestanden.**
  - **Die Systeme der MUSTERFIRMA sind mittels Single-Sign-On mit LDAP erreichbar. Die Anmeldung eines Benutzers erfolgt mit einer Kombination aus Nutzernamen und Passwort. Im LDAP ist ein System von Benutzergruppen realisiert, dass jedem LDAP-Nutzer nur die Rechte zugesteht, die er unbedingt benötigt.**
  - **Ausgewählte Systeme, die personenbezogene Daten halten, verfügen zusätzlich über eine 2-Faktor-Authetifizierung.**
  - **Die Passwörter der lokalen Benutzer auf den Mitarbeiter-Rechnern müssen mindestens 10 Zeichen lang sein, ein Sonderzeichen und eine Zahl enthalten. Dies wird über eine MDM-Software gesteuert. Die Passwörter für den LDAP-Zugang folgen grundsätzlich keiner allgemeinen Beschränkung. Die Vergabe von LDAP-Passwörtern für Admins geschieht, ebenso wie die Vergabe anderer Administratoren-Passwörter ausschließlich über die Software PW-Gen.**

- **Die internen Systeme, die personenbezogene Daten verarbeiten, sind über das Internet nur via VPN erreichbar. Ausnahmen bilden JIRA (Ticketverwaltung) und Confluence (Wissensmanagement)**
- **Die Windows-Systeme sind mit der Anti-Virus-Software von Kapersky ausgestattet.**
- **Auf allen Rechnern der Mitarbeiter der MUSTERFIRMA findet eine Festplattenverschlüsselung statt.**
- **Die Kundensysteme und die interne Systeme, die von der MUSTERFIRMA betrieben werden, sind untereinander und nach außen durch virtuelle Firewall Appliances abgesichert.**

- *Zugriffskontrolle*
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.
  - **Alle Nutzer der Systeme der MUSTERFIRMA haben einen, im Rahmen ihrer Aufgaben, maximal beschränkten Zugriff aus diese Systeme. Diese Beschränkung wird sowohl durch ein abgestuftes Rechte-Konzept im LDAP, als auch durch eine entsprechende Konfiguration einzelner Systeme abgebildet.**
  - **Der Vollzugriff zu den Servern ist ausschließlich für eine kleine Gruppe von Administratoren freigegeben.**
  - **Die Zugriffsrechte sind pro Nutzer dokumentiert, jeder Zugriff wird durch die IT-Systeme protokolliert.**
  - **Der Zugriff auf die Systeme der Kunden der MUSTERFIRMA ist auf eine kleine Gruppe von Mitarbeitern beschränkt und erfolgt ausschließlich über IPsec-Verbindungen.**
  - **Physische Datensätze auf Papier werden nach Ablauf der Aufbewahrungsfrist mit einem Aktenvernichter nach Vernichtungsstufe P4 (DIN66399) vernichtet.**
  - **Datensätze auf physischen Datenträgern (CD etc.) werden ggf. nach Ablauf der Aufbewahrungsfrist mit einer Low-Level-Formartierung gelöscht und mit einem Hammer vernichtet.**

- *Trennungskontrolle*
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing.
  - **Daten die zu unterschiedlichen Zwecken erhoben werden, werden grundsätzlich in physisch voneinander getrennten Systemen gespeichert.**
  - **In einigen der IT-Systeme findet eine Software-seitige Trennung der Daten durch eine logische Mandantentrennung statt.**
  - **Bei der Entwicklung von Kundensystemen findet eine Trennung nach Test- und Produktivsystem statt. Test- und Produktivsysteme sind gemäß ihrer Sicherheitsanforderungen mit unterschiedlichen Zugängen und Nutzungsrechten versehen.**

8.6. **4. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**

- *Weitergabekontrolle*
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.
  - **Die Weitergabe von Daten erfolgt ausschließlich in anonymisierter und/oder pseudonymisierter Form statt.**
  - **Die elektronische Weitergabe von Daten erfolgt stets via VPN-Standleitung und/oder in verschlüsselter Form.**

- *Eingabekontrolle*
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.
  - **Alle IT-Systeme, die personenbezogene Daten verarbeiten, protokollieren den persönlichen Login eines Bearbeiters. Alle bearbeitenden Aktionen, wie anlegen, ändern und löschen können so dem betreffenden Bearbeiter zugeordnet werden.**

8.7. **5. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

- *Verfügbarkeitskontrolle*
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne.

- **Durch eine Einhaltung der vorgeschriebenen Aufbewahrungsfristen ist die Verfügbarkeit aller Daten grundsätzlich gewährleistet**
- **Die Serverräume sind so ausgestattet, dass ein störungsfreier Betrieb und damit die ständige Verfügbarkeit der Daten gewährleistet ist. Dazu gehört insbesondere die Ausstattung mit Feuerlöschgeräten und Klimaanlage.**
- **Alle Systeme, die bei unseren Hostern MUSTERHOSTER betrieben werden, sind über deren Infrastruktur mit einer unterbrechungsfreien Stromversorgung ausgestatttet. Dies sind alle Kundensysteme, JIRA, Confluence und die Versionskontrolle sowie die Build- und Archivserver. Die internen Systeme, insbesondere DATEV werden bei einem Stromausfall 10 Minuten weiterbetrieben.**

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
  - **Durch die Sicherung der Daten in Form von Backups ist eine schnelle Wiederherstellbarkeit bei Systemausfällen gewährleistet.**

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

- Datenschutz-Management
  - **Der Datenschutz-Manager überprüft turnusmäßig alle relevante Prozesse, Maßnahmen und die Dokumentation.**
  - **Im Zuge neuer Kundenprojekte finden Audits durch externe Prüfer statt, während derer sowohl die Maßnahmen als auch die entsprechende Dokumentation überprüft, bewertet und evaluiert werden.**

- Incident-Response-Management
  - **Das Incident-Response-Management folgt, je nach Schwere des jeweiligen Zwischenfalls, einem Vorgehen, das in der Verantwortung der zuständigen Mitarbeiter liegt. Die technische Leitung wird in jedem Fall informiert und entscheidet dann angemessene Maßnahmen.**

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) – „Privacy by default“ und „Privacy by design“
  - **Die Maßnahmen zur Erfassung von personenbezogenen Daten sind aktuell in der Prüfung und werden nach und nach gemäß den Richtlinien auf „Privacy by default“ und „Privacy by design“ umgestellt.**

- *Auftragskontrolle*
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.
  - **Eine Verarbeitung von Daten im Zuge von Aufträgen erfolgt nur nach entsprechender Weisung des Auftraggebers. Dies ist in den jeweiligen Vertragsdokumenten entsprechend festgehalten.**

Technische und Organisatorische Maßnahmen

7. Bewertung und Dokumentation der Risiken und Maßnahmen

Risiko der Verarbeitungstätigkeiten des Unternehmens für die Rechte und Freiheiten betroffener Personen

☒ Gering ☐ Normal ☐ Hoch ☐ Sehr hoch

Begründung: Die MUSTERFIRMA sichert personenbezogene Daten angemessen in Bezug zu ihrer Sensibilität.

Eintrittswahrscheinlichkeit des Risikos (z.B. Datenpanne/ Schaden):

☒ Gering ☐ Normal ☐ Hoch ☐ Sehr hoch

Erwartete Schwere eines Schadens:

☐ Gering ☒ Normal ☐ Hoch ☐ Sehr hoch

Entsprechen die ergriffenen technischen und organisatorischen Maßnahmen dem aktuellen Stand der Technik?

☒ Ja ☐ Nein

Begründung: Als IT-Unternehmen ist die MUSTERFIRMA stets auf dem neuesten Stand der Technik. Das gilt sowohl für die von uns entwickelte Software, als auch für alle intern genutzte Hard- und Software.

Wenn nein, welche zusätzlichen technischen und organisatorischen Maßnahmen würden dem aktuellen Stand der Technik entsprechen? Und warum wurden sie nicht ergriffen?
-

Sind die ergriffenen technischen und organisatorischen Maßnahmen den festgestellten Risiken angemessen?

☒ Ja ☐ Nein

Anmerkungen

-

Ort/Datum: _____

_____
Verantwortlicher

Anlage 7: IT-Sicherheitskonzept

Ist von jedem Verein selbst zu erstellen

Die regelmäßige Evaluation unserer Sicherheitsmaßnahmen erfolgt durch die Datenschutzgruppe. Änderungen bestehender Sicherheitsmaßnahmen oder die Einführung neuer Sicherheitsmaßnahmen sind in der Datenschutzgruppe zu besprechen und von dem Vereinsvorstand zu verabschieden.

9. DATENSCHUTZ DURCH TECHNIKGESTALTUNG UND DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

Art. 25 DSGVO regelt den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen. Wir sind verpflichtet, auch in Abwägung von Kosten und Nutzen dazu, geeignete technische und organisatorische Maßnahmen zu treffen, sowohl um der Verordnung als auch den betroffenen Personen zu genügen. Dies wird auch als „Privacy By Design“ bezeichnet. Der Datenschutz soll schon in der Konzeptionsphase berücksichtigt werden.

Darüber hinaus sind wir verpflichtet durch Voreinstellungen das Prinzip der Erforderlichkeit und Datensparsamkeit umzusetzen. Dies wird „Privacy By Default“ genannt. Die Maßnahmen, Vorkehrungen und Funktionen zur datenschutzfreundlichen Technikgestaltung und zum datenschutzfreundlichen Design sind zu dokumentieren.

10.1. Beschaffung von Hard- und Software

Die gewünschte Beschaffung von Hard- und Software ist zunächst dem IT-Verantwortlichen zur Prüfung und Einschätzung vorzulegen. Die Prüfung und ihr Ergebnis sind durch den IT-Verantwortlichen zu dokumentieren und der Datenschutzgruppe vorzustellen. Diese entscheidet über die Beschaffung von Hard- und Software.

Bereits bei der Auswahl von Hard-und Software ist das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium zu berücksichtigen. Der IT-Verantwortliche führt eine Liste sämtlicher verwendeter Hardware und Softwareprogramme, die der DSK-intern und der DSB jederzeit einsehen bzw. abrufen kann.

10.2. Softwareentwicklung

Bei der Softwareentwicklung – z.B. auch im Rahmen unserer Webseiten – sind ebenfalls die unter a. bezeichneten Anforderungen zu beachten und zu erfüllen.

10.3. Implementation von Datenverarbeitungsverfahren

Bei der Implementierung von Verfahren zur Verarbeitung von personenbezogenen Daten ist auf Beschränkung des Funktionsumfangs, eine Minimierung von personenbezogenen Daten, auf eine Rechtebeschränkung auf den nötigen Umfang und die Nutzung von Sicherheitsfunktionen zu achten.

11. MITARBEITER

11.1. Verpflichtung auf Vertraulichkeit der Mitarbeiter

Die personenbezogenen Daten unterliegen der Vertraulichkeit gem. Art. 5 Abs. 1 DSGVO. Jeder Mitarbeiter und jede Mitarbeiterin, der/die Umgang mit personenbezogenen Daten sonstigen Geheimnissen oder vertraulichen Daten hat, ist auf einen vertraulichen Umgang und die Einhaltung der geltenden Datenschutzbestimmungen zu verpflichten. Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars und in Abstimmung zwischen DSK-intern und Personalabteilung. Mitarbeiter, die besonderen Geheimhaltungsverpflichtungen (z.B. Fernmeldegeheimnis nach § 88 TKG) unterliegen, werden von den Vorgesetzen ergänzend schriftlich verpflichtet. Die jeweilige Verpflichtungserklärung ist zu den Personalakten zu nehmen.

Anlage 8: Muster Verpflichtungserklärungen

Ort, Datum

Verpflichtung zur Wahrung der Vertraulichkeit, des Datenschutzes, sowie des Fernmeldegeheimnisses

Sehr geehrte(r) Frau/Herr …

da Sie im Rahmen Ihrer Tätigkeit in unserem Verein möglicherweise mit personenbezogenen Daten in Kontakt kommen, verpflichten wir Sie hiermit zur Beachtung des Datenschutzes, insbesondere zur Wahrung der Vertraulichkeit.

Ihre Verpflichtung besteht umfassend. Personenbezogene Daten – also alle Informationen, die sich auf einen benannten oder identifizierbaren Menschen beziehen – dürfen nicht unbefugt erhoben, genutzt, weitergegeben oder sonst verarbeitet werden. Sie sind verpflichtet, personenbezogene Daten vertraulich zu behandeln und ausschließlich auf unsere Weisung zu verarbeiten.

Sie sind im Zusammenhang mit der Verarbeitung personenbezogener Daten weiterhin zur Einhaltung der Datenschutzgrundsätze aus Art. 5 Abs. 1 Datenschutzgrundverordnung (DSGVO) verpflichtet, die Sie dem beigefügten Merkblatt im Wortlaut entnehmen können.

Verstöße gegen Datenschutzbestimmungen können nach § 42 BDSG sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden. Datenschutzverstöße stellen zugleich eine Verletzung arbeits- oder dienstrechtlicher Pflichten dar und können entsprechende Konsequenzen nach sich ziehen. Ihre sich ggf. aus dem Arbeits- bzw. Dienstvertrag ergebende allgemeine Geheimhaltungsverpflichtung wird durch diese Erklärung nicht berührt.

Datenschutzverstöße sind ebenfalls mit möglicherweise sehr hohen Bußgeldern für das Unternehmen bedroht, die gegebenenfalls zu Ersatzansprüchen Ihnen gegenüber führen können.

Darüber hinaus möchten wir Sie darüber belehren, dass Sie auch nach § 88 Telekommunikationsgesetz (TKG) zur Wahrung des Fernmeldegeheimnisses verpflichtet sind. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche. Verstöße gegen das Fernmeldegeheimnis können nach § 206 Strafgesetzbuch (StGB), ggf. auch nach anderen Gesetzen, mit Bußgeld, Geld- oder Freiheitsstrafe geahndet werden.

Ihre Verpflichtung zur Wahrung des Datenschutzes und der Beachtung des Fernmeldegeheimnisses besteht ohne zeitliche Begrenzung und auch nach Beendigung Ihrer Tätigkeit für unser Unternehmen fort.

Ein unterschriebenes Exemplar dieses Schreibens reichen Sie bitte an die Geschäftsstelle zurück.

Ort/Datum: _____

_____
Verein

Ich bestätige, dass ich heute auf die Wahrung des Datenschutzes und die Beachtung des Fernmeldegeheimnisses verpflichtet und über deren Bedeutung belehrt worden bin. Die sich daraus ergebenden Verhaltensweisen wurden mir mitgeteilt. Meine Verpflichtung auf die Wahrung des Datenschutzes und die Beachtung des Fernmeldegeheimnisses habe ich hiermit zur Kenntnis genommen.

Das Merkblatt zur Verpflichtungserklärung mit dem Abdruck der hier genannten Vorschriften habe ich erhalten.

Ort/Datum: _____

_____

Mitarbeiter

11.1Richtlinien

Um einen gesetzeskonformen Umgang mit personenbezogenen Daten in unserem Verein sicherzustellen, haben wir einzelne Aspekte in internen Richtlinien geregelt.

Anlage 9: Richtlinie private E-Mail und Internetnutzung

Richtlinie zur Nutzung von Internet und E-Mail **am Arbeitsplatz**

… [Name des Vereins] erlässt folgende Dienstanweisung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz:

1. Geltungsbereich und Zweckbestimmung

1.1 Diese Dienstanweisung regelt die Grundsätze für den Zugang und des betrieblichen Kommunikationssysteme E-Mail und Internet bei ... (VEREIN) und gilt für alle Beschäftigten, inklusive Praktikanten, Hilfskräften, ehrenamtlichen und freien Mitarbeitern, denen ein Internetanschluss und/oder ein betrieblicher E-Mail-Account von ... (VEREIN) zur Verfügung gestellt wird. Diese werden nachfolgend zusammen als Beschäftigte bezeichnet.

1.2 Ziel dieser Dienstanweisung ist die Herstellung der Transparenz der vereinsinternen Regelungen zur E-Mail und Internetnutzung, die Sicherstellung der Vereinskommunikation auch im Falle der Erkrankung, des Ausscheidens eines Beschäftigten, die Sicherung der Persönlichkeitsrechte der Beschäftigten und die Gewährleistung des Schutzes ihrer personenbezogenen Daten.

2. Grundsatz

E-Mail- und Internetzugang werden von ... (VEREIN) ausschließlich zu dienstlichen Zwecken bereitgestellt und dürfen nur zu betrieblichen Zwecken genutzt werden, soweit nicht diese Dienstanweisung ausdrücklich Ausnahmen vorsieht.

3. E-Mail-Nutzung

3.1 Der betriebliche E-Mail-Account (... (VEREIN)-E-Mail-Adresse) darf ausschließlich betrieblich genutzt werden. Zur betrieblichen Nutzung im Sinne dieses Absatzes gehört auch die sogenannte betrieblich veranlasste Privatnutzung, etwa wenn der Beschäftigte wegen kurzfristiger Überstunden einen privaten Termin absagt.

3.2 ... (VEREIN) gestattet dem Beschäftigten in geringfügigem Umfang (15 Minuten pro Tag) die private Nutzung eines privaten Webmail-Accounts. Diese Gestattung gilt nur, soweit die ordnungsgemäße Erbringung der Arbeitsleistung und sonstiger dem Beschäftigte obliegender Pflichten nicht beeinträchtigt wird.

3.3 Für betriebliche Kommunikation darf ausschließlich der betriebliche E-Mail-Account (... (VEREIN)-E-Mail-Adresse) und keine privaten E-Mail-Account genutzt werden.

3.4 Die Umleitung, Weiterleitung oder Speicherung dienstlicher Informationen, Nachrichten oder Dateien (insbesondere E-Mails) an private E-Mail-Accounts ist verboten.

3.5 Gehen auf dem betrieblichen E-Mail-Account Nachrichten mit privatem Inhalt ein, ist der Absender darauf hinzuweisen, dass der betriebliche E-Mail-Zugang nur für betriebliche Zwecke verwendet werden darf und daher keine weiteren privaten Nachrichten an die betriebliche Anschrift gesandt werden sollen. Enthält die Nachricht ausschließlich private Inhalte, ist sie unverzüglich durch den Beschäftigten zu löschen; sie darf zuvor an einen privaten E-Mail-Account des Beschäftigten weitergeleitet werden. Ebenfalls zulässig ist die Weiterleitung der ausschließlich privaten Teile einer gemischt betrieblich-privaten Nachricht. Die Löschung einer gemischt betrieblich-privaten Nachricht außerhalb des normalen Geschäftsgangs ist nur mit schriftlicher oder elektronischer Zustimmung des Vorgesetzten gestattet. Nicht gelöschte Nachrichten privaten Charakters gelten hinsichtlich der Zugriffsrechte von ... (VEREIN) als betriebliche Nachrichten, so dass der Beschäftigte auch in seinem eigenen Interesse seiner Löschpflicht nachkommen sollte.

4. Abwesenheit, Ausscheiden

4.1 Um sicherzustellen, dass eingehende betriebliche Nachrichten stets rechtzeitig bearbeitet werden können, soll jeder Beschäftigte im Einvernehmen mit der Geschäftsführung bzw. dem Vorstand mindestens einen Vertreter benennen, der bei Abwesenheit des Beschäftigten auf den betrieblichen E-Mail-Account des Beschäftigten zugreifen kann. Benennt ein Beschäftigter keinen Vertreter oder ist bei Abwesenheit des Beschäftigten kein benannter Vertreter anwesend, bestimmt die Geschäftsführung bzw. der zuständige Vertreter des Vorstandes - siehe Anlage 1 Kontaktliste - einen oder mehrere Vertreter und informiert den Beschäftigten hierüber. Hat der Beschäftigte einen Vertreter benannt, ist die Bestimmung eines weiteren Vertreters durch den Vorgesetzten nur bei Abwesenheit des Beschäftigten und aller Vertreter von mindestens einem Tag oder bei schriftlich gegenüber dem betrieblichen Datenschutzbeauftragten zu begründender Gefahr im Verzug zulässig.

4.2 Vertreter gemäß Ziffer 4.1 dürfen nur während der Abwesenheit oder nach Beendigung des Beschäftigungsverhältnisses auf dessen E-Mail-Zugang zugreifen. Erkennbar private Nachrichten dürfen durch Vertreter nicht geöffnet werden. Ergibt sich der private Charakter erst nach dem Öffnen, ist die Nachricht umgehend zu schließen; über den Inhalt ist Stillschweigen zu bewahren.

4.3 Mit Beendigung des Beschäftigungsverhältnisses steht der betriebliche E-Mail-Account dem jeweiligen Beschäftigten nicht mehr zur weiteren Nutzung zur Verfügung. Zur Aufrechterhaltung des Geschäftsbetriebs wird einem Vertreter Zugriff gewährt bzw. eingehende Nachrichten an diesen weiterleiten. Alle Absender sind durch den Vertreter oder automatisch darauf hinzuweisen, dass der Beschäftigte nicht mehr unter dieser Anschrift erreichbar ist und wer neuer betrieblicher Kontakt ist.

4.5 Nach der Beendigung des Beschäftigungsverhältnisses oder wenn ein Beschäftigter bis zur rechtlichen Beendigung freigestellt ist, sind eingehende oder gespeicherte private Nachrichten des Beschäftigten zu löschen. Erkennbar private Nachrichten dürfen durch Vertreter nicht geöffnet werden. Ergibt sich der private Charakter erst nach dem Öffnen, ist die Nachricht umgehend zu schließen und zu löschen; über den Inhalt ist Stillschweigen zu bewahren.

5. Private Nutzung des Internet

5.1 Die private Nutzung des Internet in geringfügigem Umfang (15 Minuten pro Tag) ist zulässig, soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit des Internet für dienstliche Zwecke nicht beeinträchtigt werden und die private Nutzung keine negativen Auswirkungen auf die Bewältigung der Arbeitsaufgaben hat.

5.2 Das Abrufen von Informationen oder Inhalten, die für ... (VEREIN) Kosten verursachen, ist für den Privatgebrauch unzulässig. Im Rahmen der privaten Nutzung dürfen keine kommerziellen oder sonstigen geschäftliche Zwecke verfolgt werden.

5.3 Private E-Mails dürfen grundsätzlich nur über die Nutzung Webmail-Dienste versandt und empfangen werden. Über die dienstlichen E-Mail-Adressen eingehende private E-Mails sind wie private schriftliche Post zu behandeln. Eingehende private, aber fälschlich als Dienstpost behandelte E-Mails sind den betreffenden Beschäftigten unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben. Private E-Mails sind von Beschäftigten als solche zu kennzeichnen.

5.4 Die Beschäftigten haben jede Nutzung des Internets zu unterlassen, die geeignet ist, den Interessen von ... (VEREIN) oder dessen Ansehen in der Öffentlichkeit zu schaden, die Sicherheit der Vereins-IT von ... (VEREIN) zu beeinträchtigen oder die gegen geltende Rechtsvorschriften verstößt. Dies gilt vor allem für

- das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
- das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen, oder
- die Nutzung von Online-Spieleplattformen.

Abrufen und Aufrufen heißt auf im Netz vorhandene Informationen mit IT-Systemen von ... (VEREIN) zugreifen. Verbreiten heißt einer Vielzahl von Personen oder einem unbestimmten Personenkreis über Internet-Dienste unter Verwendung von IT-Systemen von ... (VEREIN) anbieten.

5.5 Aus Wirtschaftlichkeits- oder IT-Sicherheitsgründen kann die Internetnutzung beschränkt werden. Dies kann die Sperrung bestimmter Dienste der Internetnutzung (Sperrung bestimmter Angebote, Domains oder Ports) und eine Beschränkung des Datentransfers beinhalten

6. Inkrafttreten

6.1 Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist von zwei Wochen gekündigt werden. Im Falle einer Kündigung ist jede private Nutzung des Internetzuganges, auch der Empfang und das Versenden privater E-Mails über die dienstliche E-Mail-Adresse bis zum Abschluss einer neuen Vereinbarung untersagt.

6.2 Alle Beschäftigten bestätigen schriftlich die Kenntnisnahme. Ein Abdruck der Vereinbarung wird ihnen zusammen mit einer Kopie der Bestätigung ausgehändigt.

Ort/Datum: _____

_____
Geschäftsführer

Anlage: Erklärung zur Nutzung der dienstlichen E-Mail-Adresse und des dienstlichen Internetzugangs

Anlage
Erklärung zur Nutzung
der dienstlichen E-Mail-Adresse und des dienstlichen Internetzugangs

Ich habe die „Richtlinie zur Nutzung von Internet und E-Mail am Arbeitsplatz“ zur Kenntnis genommen.

Ich möchte den Internetzugang in dem von der Dienstanweisung erlaubten Umfang auch privat nutzen. Ich verpflichte mich, dabei diese Dienstanweisung, sonstige Bestimmungen sowie die allgemeinen Gesetze einzuhalten und für private E-Mails ausschließlich über Webmail-Dienste zu nutzen.

Im Hinblick auf meinen betrieblichen E-Mail-Account willige ich ein, dass im Fall meiner Verhinderung (z.B. infolge von Urlaub oder Krankheit) bzw. bei Beendigung des Arbeitsverhältnisses zur Aufrechterhaltung des Dienstbetriebes eine Einsichtnahme in meine betrieblichen E-Mails (inkl. der nicht erkennbar als privat gekennzeichneten E-Mails) durch meinen dienstlichen Vertreter erfolgen kann.

Mir ist bekannt, dass ich im Fall des Eingangs privater E-Mails auf meinem dienstlichen E-Mail-Account meine Kommunikationspartner darauf hinzuweisen habe, dass es sich um ein dienstliches E-Mail-Postfach handelt und im Übrigen die private Nutzung untersagt ist.

Ort/Datum: _____

_____
Beschäftigter

12. WAHRUNG DER BETROFFENENRECHTE

Die Datenschutz-Grundverordnung (DSGVO) sieht in den Art. 12 ff. DSGVO Rechte der von einer Verarbeitung personenbezogener Daten betroffenen Personen vor, die von uns einzuhalten und umzusetzen sind. Betroffene Personen sind insbesondere Kunden, Mitarbeiter oder Besucher unserer Webseiten.

12.1. Information der betroffenen Personen

Die Stärkung der Betroffenenrechte durch klare Prozesse und konkrete Vorgaben, ist eines der wichtigsten Ziele des Datenschutzes. Auf diesem Weg wird dem Grundsatz der Transparenz zur Geltung verholfen. Daher informieren wir bei jeder Datenerhebung die betroffenen Personen (z. B. durch einen schriftlichen Hinweis) über die in Art. 13 DSGVO genannten Hintergründe, also u.a. wer ihre Daten zu welchem Zweck erhebt, aus welchem Grund und wie lange die Daten etwa gespeichert werden. Die Modalitäten des Art. 12 DSGVO sind dabei zu beachten. Die Information der Betroffenen über die Datenverarbeitung und die Betroffenenrechte erfolgt im Regelfall mittels Datenschutzbestimmungen.

Im Verzeichnis der Verarbeitungstätigkeiten hat der DSK-Intern in Abstimmung mit dem DSB die Verarbeitungen zu identifizieren, für die betroffenen Personen Datenschutzinformationen zur Verfügung gestellt werden müssen. Inhalt, Art und Umfang der Informationserteilung sind ebenfalls mit dem DSB abzusprechen.

Nicht für jede Verarbeitungstätigkeit sind separate Datenschutzbestimmungen zu erstellen. Es können mehrere Verarbeitungen in bereichsspezifischen Datenschutzbestimmungen zusammengefasst werden, die sich an einen bestimmten Betroffenenkreis richten.

Der DSK-intern hat in Abstimmung mit dem DSB und den fachverantwortlichen Stellen sicherzustellen, dass die Datenschutzbestimmungen den betroffenen Personen auch in geeigneter Weise zur Verfügung gestellt werden (z.B. durch Veröffentlichung auf der Webseite, Zusendung, Abdruck auf Vertragsformular).

Bei jeder Änderung oder Überprüfung von Verarbeitungstätigkeit sind ggf. auch die entsprechenden Datenschutzbestimmungen von der Datenschutzgruppe auf ihre Aktualität zu untersuchen und ggf. durch den DSK-intern anzupassen.

12.2. Vorgehen bei Geltendmachung von Betroffenenrechten

Vorgänge über die Wahrnehmung von Rechten der Betroffenen (Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und ggf. des Rechts auf Datenübertragbarkeit.) werden vom DSK-intern (ALTERNATIV: …) bearbeitet und dokumentiert und sind diesem unverzüglich zuzuleiten. Dies gilt jedoch nicht für Anfragen der Datenschutzaufsichtsbehörden. Diese sind unverzüglich dem DSB vorzulegen und von diesem zu beantworten.

Der DSK-intern schaltet bei schwierigen, umfangreichen oder problematischen Anfragen von Betroffenen den DSB und die Vereinsleitung ein und stimmt mit diesem die weitere Bearbeitung ab. Betroffene Mitarbeiter können sich zur Wahrnehmung Ihrer Rechte auch direkt an den DSB wenden.

Anlage 10: Prozess Wahrung Betroffenenrechte

I. Einleitung

Die Datenschutz-Grundverordnung (DSGVO) sieht in den Art. 12 ff. DSGVO Rechte der von einer Verarbeitung personenbezogener Daten betroffenen Personen vor, die von … [Verein] einzuhalten und umzusetzen sind. Betroffene Personen sind insbesondere Kunden, Mitarbeiter oder Besucher unserer Webseiten. Mit dem vorliegenden Dokument werden die Betroffenenrechte dargestellt und die Umsetzungsmaßnahmen im Verein festgelegt.

II. Rechte der betroffenen Person

Die folgende Auflistung umfasst die zentralen Rechte von Betroffenen nach der DSGVO.

1. Auskunft (Art. 15 DSGVO)

Eine betroffene Person kann von uns zunächst eine Bestätigung darüber verlangen, ob wir überhaupt personenbezogene Daten von ihr verarbeiten. Liegt eine solche Verarbeitung vor, haben wir über die folgenden Informationen Auskunft zu erteilen:

- zu welchen Zwecken die Daten verarbeitet werden
- die Kategorien der verarbeiteten personenbezogenen Daten
- die Empfänger bzw. die Kategorien von Empfängern, denen die personenbezogenen Daten des Betroffenen offengelegt wurden oder noch offengelegt werden. Sofern Daten in Drittländern verarbeitet werden, unterrichten wir auch darüber, ob und falls ja aufgrund welcher Garantien ein angemessenen Schutzniveaus gem. Art. 45, 46 DS-GVO beim Datenempfänger in dem Drittland sichergestellt ist
- die geplante Dauer der Speicherung. Falls konkrete Angaben hierzu nicht möglich sind, müssen Kriterien für die Festlegung der Speicherdauer (z.B. gesetzliche Aufbewahrungsfristen) mitgeteilt werden
- das Bestehen eines Rechts auf Berichtigung oder Löschung der personenbezogenen Daten, eines Rechts auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung (siehe unten);
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- alle verfügbaren Informationen über die Herkunft der Daten, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Bei einer Datenverarbeitung zu wissenschaftlichen, historischen oder statistischen Forschungszwecken kann das Auskunftsrecht insoweit beschränkt werden, als es voraussichtlich die Verwirklichung der

Forschungs- oder Statistikzwecke unmöglich macht oder ernsthaft beeinträchtigt und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist.

Der Betroffene hat schließlich das Recht, eine Kopie ihrer personenbezogenen Daten zu verlangen. Datenkopien stellen wir grundsätzlich in elektronischer Form zur Verfügung stellen, sofern sie nichts anderes angegeben haben. Die erste Kopie ist kostenfrei, für weitere Kopien kann ein angemessenes Entgelt verlangt werden. Die Bereitstellung erfolgt vorbehaltlich der Rechte und Freiheiten anderer Personen, die durch die Übermittlung der Datenkopie beeinträchtigt sein können.

2. Berichtigung (Art. 16 DSGVO)

Der Betroffene hat weiterhin das Recht, von uns die Berichtigung seiner Daten zu verlangen, sofern diese unrichtig, unzutreffend und/oder unvollständig sein sollten. Das Recht auf Berichtigung umfasst das Recht auf Vervollständigung durch ergänzende Erklärungen oder Mitteilungen. Eine Berichtigung und/oder Ergänzung hat unverzüglich – d. h. ohne schuldhaftes Zögern – zu erfolgen.

Bei Datenverarbeitung zu wissenschaftlichen, historischen oder statistischen Forschungszwecken kann das Recht auf Berichtigung kann insoweit beschränkt werden, als es voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich macht oder ernsthaft beeinträchtigt und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist.

3. Löschung (Art. 17 DSGVO)

3.1 LÖSCHUNGSPFLICHT

Der Betroffene von uns verlangen, dass die ihn betreffenden personenbezogenen Daten unverzüglich gelöscht werden. Wir sind dann verpflichtet, diese Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Der Betroffene hat seine Einwilligung widerrufen, auf die sich die Verarbeitung stützte und es fehlt an einer anderen Rechtsgrundlage für die Verarbeitung.
- Der Betroffene hat gem. Art. 21 Abs. 1 DSGVO Widerspruch gegen die Verarbeitung eingelegt und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder der Betroffene legt gem. Art. 21 Abs. 2 DSGVO Widerspruch gegen die Verarbeitung zum Zwecke der Direktwerbung ein.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich.
- Die personenbezogenen Daten von Minderjährigen wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DSGVO erhoben.

3.2 INFORMATION AN DRITTE

Wenn wir die personenbezogenen Daten des Betroffenen öffentlich gemacht und zu deren Löschung verpflichtet sein sollten, so haben wir unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, zu treffen, um Dritte, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass der Betroffene die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

3.3 AUSNAHMEN

Das Recht auf Löschung besteht nicht, soweit die Verarbeitung erforderlich ist

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
- zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der EU oder Deutschlands erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die uns übertragen wurde;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Art. 9 Abs. 2 lit. h und i sowie Art. 9 Abs. 3 DSGVO;
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DSGVO, soweit das unter Abschnitt a) genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

4. Einschränkung der Datenverarbeitung (Art. 18 DSGVO)

Der Betroffene hat auch das Recht, die Verarbeitung seiner personenbezogenen Daten in folgenden Fällen einschränken zu lassen:

- Wenn der Betroffene die Richtigkeit seiner personenbezogenen Daten bestritten hat, kann er von uns verlangen, dass seine Daten für die Dauer der Richtigkeitsprüfung für andere Zwecke nicht genutzt und insoweit eingeschränkt werden.
- Bei unrechtmäßiger Datenverarbeitung kann der Betroffene anstelle der Datenlöschung nach Art. 17 Abs. 1 lit. d DSGVO die Einschränkung der Datennutzung nach Art. 18 DSGVO verlangen;
- Benötigen der Betroffene seine personenbezogenen Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, werden seine personenbezogenen Daten im Übrigen aber nicht mehr benötigt, dann kann er von uns die Einschränkung der Verarbeitung auf die vorgenannten Rechtsverfolgungszwecke verlangen;
- Hat der Betroffene gegen eine Datenverarbeitung Widerspruch nach Art. 21 Abs. 1 DSGVO eingelegt und steht noch nicht fest, ob unsere Interessen an einer Verarbeitung seinen Interessen überwiegen, kann der Betroffene verlangen, dass seine Daten für die Dauer der Prüfung für andere Zwecke nicht genutzt und insoweit eingeschränkt werden.

Wurde die Verarbeitung personenbezogenen Daten des Betroffenen eingeschränkt, dürfen diese Daten – von ihrer Speicherung abgesehen – nur mit Ihrer Einwilligung oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der EU oder eines Mitgliedstaats verarbeitet werden. Wurde die Einschränkung der Verarbeitung nach den o.g. Voraussetzungen eingeschränkt, ist der Betroffene zu unterrichtet, bevor die Einschränkung wieder aufgehoben wird.

Bei Datenverarbeitung zu wissenschaftlichen, historischen oder statistischen Forschungszwecken kann das Recht auf Einschränkung der Verarbeitung insoweit beschränkt werden, als es voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich macht oder ernsthaft beeinträchtigt und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist.

5. Recht auf Unterrichtung

Wenn der Betroffene das Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung geltend gemacht hat, sind wir verpflichtet, allen Empfängern, denen die betreffenden personenbezogenen Daten offengelegt wurden, diese Berichtigung, Löschung der Einschränkung mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Dem Betroffenen steht das Recht zu, über diese Empfänger unterrichtet zu werden.

6. Datenübertragbarkeit (Art. 20 DSGVO)
Der Betroffene das Recht, die personenbezogenen Daten, die er uns bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Außerdem kann er diese Daten einem anderen Verantwortlichen ohne Behinderung durch uns übermitteln, sofern

- die Verarbeitung auf einer Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO oder Art. 9 Abs. 2 lit. a DSGVO oder auf einem Vertrag gem. Art. 6 Abs. 1 lit. b DSGVO beruht und
- die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

In Ausübung dieses Rechts hat der Betroffene ferner das Recht, zu erwirken, dass seine personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist. Freiheiten und Rechte anderer Personen dürfen hierdurch nicht beeinträchtigt werden. Das Recht auf Datenübertragbarkeit gilt nicht für eine Verarbeitung personenbezogener Daten, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die uns übertragen worden ist.

7. Widerspruchsrecht (Art. 21 DSGVO)
Der Betroffene hat das Recht, aus Gründen, die sich aus seiner besonderen Situation ergeben, jederzeit gegen die Verarbeitung seiner personenbezogenen Daten, die aufgrund von Art. 6 Abs. 1 lit. e oder f DSGVO erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling.

Nach einem Widerspruch verarbeiten wir Ihre personenbezogenen Daten nicht mehr, es sei denn wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen. Wir müssen die Verarbeitung ebenfalls nicht einstellen, wenn sie der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

Werden die personenbezogenen Daten des Betroffenen verarbeitet, um Direktwerbung zu betreiben, hat er das Recht, jederzeit Widerspruch gegen die Verarbeitung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. Wenn der Betroffene der Verarbeitung für Zwecke der Direktwerbung widerspricht, so werden die Sie betreffenden personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

Bei Datenverarbeitung zu wissenschaftlichen, historischen oder statistischen Forschungszwecken hat der Betroffene das Recht, aus Gründen, die sich aus seiner besonderen Situation ergeben, der Verarbeitung zu widersprechen. Sein Widerspruchsrecht kann insoweit beschränkt werden, als es voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich macht oder ernsthaft beeinträchtigt und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist.

8. Widerruf von Einwilligungen (Art. 7 Abs. 3 DSGVO)
Der Betroffene hat das Recht, bei einer Verarbeitung, die auf einer Einwilligung beruht, seine Einwilligung jederzeit zu widerrufen. Der Widerruf gilt ab dem Zeitpunkt seiner Geltendmachung. Er wirkt mit anderen Worten für die Zukunft. Die Verarbeitung wird durch den Widerruf der Einwilligung also nicht rückwirkend rechtswidrig.

III. Umsetzung der Betroffenenrechte
1. Information des Betroffenen

Bei jeder Datenerhebung sind die Betroffenen in geeigneter Weise gem. Art. 13, 14 DSGVO zu informieren. Die Modalitäten des Art. 12 DSGVO sind dabei zu beachten. Die Information der Betroffenen über die Datenverarbeitung und die Betroffenenrechte erfolgt im Regelfall mittels Datenschutzbestimmungen.

Um Betroffenen die Geltendmachung Ihrer Rechte zu erleichtern, sind nicht nur in den Datenschutzbestimmungen, sondern auch im Impressum auf der Webseite die Kontaktdaten für alle Fragen des Datenschutzes anzugeben.

Der Datenschutzkoordinator (DSK) führt das Verzeichnis der Verarbeitungstätigkeiten (VVT). In Abstimmung mit dem Datenschutzbeauftragten (DSB) werden die Verarbeitungen im VVT identifiziert, für die betroffenen Personen Datenschutzinformationen zur Verfügung gestellt werden müssen. Art und Umfang der Informationserteilung sind ebenfalls mit dem DSB abzusprechen.

Nicht für jede Verarbeitungstätigkeit sind separate Datenschutzbestimmungen zu erstellen. Es können mehrere Verarbeitungen in bereichsspezifischen Datenschutzbestimmungen zusammengefasst werden, die sich an einen bestimmten Betroffenenkreis richten. Im Verein existieren die folgenden Datenschutzbestimmungen:

Datenschutzbestimmungen Webseite
Datenschutzbestimmungen Mitarbeiter
Datenschutzbestimmungen Mitglieder…

Der Datenschutzkoordinator hat in Abstimmung mit dem DSB und den fachverantwortlichen Stellen sicherzustellen, dass die Datenschutzbestimmungen den betroffenen Personen auch in geeigneter Weise zur Verfügung gestellt werden (z.B. durch Veröffentlichung auf der Webseite, Zusendung, Abdruck auf Vertragsformular).

Bei jeder Änderung oder Überprüfung von Verarbeitungstätigkeit sind ggf. auch die entsprechenden Datenschutzbestimmungen auf ihre Aktualität zu untersuchen und ggf. anzupassen. Anpassungen der Datenschutzbestimmungen erfolgen nach Beauftragung durch das Verein durch den DSB.

2. Vorgehen bei Geltendmachung von Betroffenenrechten

2.1 Verantwortliche Stelle im Verein

Für die Bearbeitung und Beantwortung sämtlicher Anfragen zu Betroffenenrechten ist die

Vereinsinterne Stelle: …
Mitarbeiter: …
Telefon: …
Fax: …
E-Mail: …

Vereinsintern zuständig. Dies gilt jedoch nicht für Anfragen der Datenschutzaufsichtsbehörden – diese sind unverzüglich dem DSB vorzulegen und von diesem zu beantworten.

2.2 Erfüllung

Alle Mitarbeiter der … [Verein], sowie der DSB sind verpflichtet, jede Anfrage bzgl. der oben beschriebenen Betroffenenrechte unverzüglich nach Zugang der Mitteilung an … [Vereinsinterne Stelle] weiterzuleiten. Die Weiterleitung kann z.B. per E-Mail an die vorgenannte E-Mail-Adresse erfolgen.

Die … [Vereinsinterne Stelle] wird jede Anfrage dokumentieren. Bei schwierigen, umfangreichen oder problematischen Anfragen von Betroffenen ist die … [Vereinsinterne Stelle] verpflichtet, unverzüglich den DSK, den DSB und die Vereinsleitung zu informieren und das weitere Vorgehen abzustimmen.

Betroffenenanfragen sind unverzüglich, spätestens aber binnen innerhalb eines Monats nach Eingang der Betroffenenanfrage bei der … [Verein] gegenüber dem Betroffenen zu beantworten. Eine Fristverlängerung auf drei Monate ist gem. Art. 12 Abs. 3 DSGVO ausnahmsweise möglich.

Die … [Vereinsinterne Stelle] hat bei der Beantwortung von Betroffenenanfragen sicherzustellen, dass vor der Erteilung von Information an den Betroffenen vorab überprüft wurde, dass die Person diejenige ist, für die 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 dürfen. Bei Fehlen einer Zustimmung ist die Auskunft schriftlich zu erteilen. Zur Erfüllung von Auskunftsersuchen hat die … [Vereinsinterne Stelle] das als Anlage 1 beigefügte Auskunfts-Formular zu verwenden.

Die … [Vereinsinterne Stelle] hat dafür Sorge zu tragen, dass die geltend gemachten Betroffenenrechte auch im Übrigen umgesetzt werden. Sie veranlasst ggf. bei den entsprechenden Fachabteilungen die erforderlichen Maßnahmen (z.B. die Löschung der Daten) und dokumentiert den Inhalt, die Durchführung, sowie Erledigung dieser Maßnahmen.

Beschwerden der Betroffenen in Datenschutzangelegenheiten werden ebenfalls von … [Verein] nach den Vorgaben des Beschwerdemanagements bearbeitet und sind dem DSB zu melden.

Ort/Datum: _____ Ort/Datum: _____

_____ _____

Geschäftsführer Datenschutzbeauftragter

13. DATENSCHUTZVERLETZUNGEN

Bei einer möglichen Verletzung des Schutzes von personenbezogenen Daten, insbesondere bei einem Verlust der Vertraulichkeit durch eine unbefugte Offenbarung oder Datenübermittlung, unbefugte Zugriffe oder Verarbeitungen oder durch Verlust, Zerstörung oder Verfälschung der Daten, ist es notwendig, unverzüglich zu reagieren.

Für die Bearbeitung von Datenschutzverletzungen haben wir mit „Data Breach-Prozess“ die Sofortmaßnahmen und einen verbindlichen Ablaufplan festgelegt, mit dem wir Datenpannen reagieren. Dies schließt neben der Dokumentation die Prüfung der Melde- und Benachrichtigungspflicht gem. Art. 33, 34 DSGVO ein.

Anlage 11: Prozessablauf und zu verwendende Dokumente bei Datenschutzverstößen

Data Breach Prozess
Ablaufplan bei Datenschutzverletzungen in Unternehmen

1. Feststellung der betroffenen Daten und Personen
Zunächst haben die beteiligten Mitarbeiter so weit wie möglich unverzüglich festzustellen, welche Daten voraussichtlich von der Datenschutzverletzung betroffen sind. Diese Feststellung umfasst zumindest die Datenkategorie und die ungefähre Anzahl der betroffenen Datensätze.

Anschließend stellen die beteiligten Mitarbeiter fest, welche natürlichen Personen von der Datenpanne betroffen sind. Das umfasst zumindest die Kategorien betroffener Personen und die (ungefähre) Anzahl der betroffenen Personen.

2. Beweissicherung
Das Unternehmen sollte frühzeitig eine Sicherungskopie zur Dokumentation der Datenschutzverletzung und der als Reaktion unternommenen Maßnahmen erstellen. Dabei achtet das Unternehmen darauf, trotz der gebotenen Eile keine weiteren Datenschutzverletzungen zu verursachen.

Eine frühzeitige und gründliche Dokumentation der Umstände der Datenschutzverletzungen und der vom Unternehmen eingeleiteten Maßnahmen ist in rechtlicher Hinsicht ausgesprochen wichtig. In Folge (möglicher) Datenschutzverstöße sind Beschwerden von betroffenen Personen, Nachforschungen der Aufsichtsbehörden und Schadensersatzansprüche nicht unwahrscheinlich. Aufgrund der in Art. 24 Abs. 1 DSGVO geregelten Beweislastumkehr muss das Unternehmen dann beweisen können, dass es sich rechtskonform verhalten hat. Hierfür ist eine umfassende Dokumentation erforderlich.

3. Sofortige Benachrichtigung der Geschäftsführung und des Datenschutzbeauftragten
Die beteiligten Mitarbeiter unterrichten die Geschäftsführung, den Datenschutzbeauftragten und die IT-Abteilung des Unternehmens so frühzeitig wie möglich über die Datenschutzverletzung.

Die Geschäftsführung, der Datenschutzbeauftragte, der Datenschutzmanager und ggf. das Datenschutzteam und die IT-Abteilung werden dann unverzüglich das weitere Vorgehen gem. Ziffer 4-10 abstimmen und koordinieren.

4. Protokollierung und Dokumentation der Datenschutzverletzung
Das Unternehmen protokolliert die festgestellten Informationen über die Datenschutzverletzung umfassend. Auch Benachrichtigungen innerhalb des Unternehmens und gegebenenfalls die Hinzuziehung externer Datenschutzexperten protokolliert das Unternehmen.

An dieser Stelle sollte das Unternehmen feststellen, ob die erstellte Dokumentation ausreicht, um in einem späteren möglichen Gerichtsverfahren beweisen zu können, dass es entsprechend der gesetzlichen Anforderungen gehandelt hat.

5. Prüfung der Datenschutzverletzung auf Risiko für Rechte und Freiheiten natürlicher Personen
Das Unternehmen prüft in einem weiteren Arbeitsschritt, ob die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Dem Verantwortlichen soll nach der DSGVO nur dann der Aufwand der Meldung aufgebürdet werden, wenn ein Schadenseintritt beim Betroffenen möglich erscheint. Unter Risiko ist in diesem Sinne die erhöhte Eintrittswahrscheinlichkeit eines drohenden Schadensereignisses zu verstehen. Ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht insbesondere, wenn ihnen Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile drohen. Ist dies nachweislich nicht der Fall, kann eine Unterrichtung der Aufsichtsbehörde ausnahmsweise unterbleiben.

Das Unternehmen dokumentiert den gesamten Vorgang und trifft die erforderlichen Maßnahmen zur Beseitigung der Datenschutzverletzung.

Sofern jedoch ein mögliches Risiko für die Rechte und Freiheiten natürlicher Personen besteht, fährt das Unternehmen mit Punkt 6 fort.

6. Meldung an die Aufsichtsbehörde, Art. 33 DSGVO
Das Unternehmen meldet die Datenschutzverletzung an die jeweils zuständige Aufsichtsbehörde. Diese Meldung muss unverzüglich erfolgen, möglichst nach 72 Stunden. Sollte eine Meldung innerhalb dieser Frist nicht möglich sein, muss das Unternehmen bei einer späteren Meldung dann auch begründen, warum die Frist von 72 Stunden nicht eingehalten wurde. Wenn nicht alle Informationen für die Meldung gleich vorliegen, ist ggf. auch eine schrittweise Meldung möglich.

Die Meldung ist zwar grundsätzlich formlos möglich. Für einen rechtssicheren Nachweis sollte das Unternehmen allerdings die Textform verwenden. Dabei ist das Unternehmen gut beraten, auch den direkten (etwa telefonischen) Kontakt zur zuständigen Aufsichtsbehörde zu suchen. Hat man dies getan, so kann man in einer schriftlichen beziehungsweise in Textform verfassten Meldung gleich auch auf die zuvor erfolgte telefonische oder sonstige Kommunikation Bezug nehmen.

Die Meldung selbst sollte zumindest die folgenden Informationen beinhalten (Art. 33 Abs. 3 DSGVO):

- eine inhaltlich an Art. 4 Nr. 12 DSGVO orientierte **Beschreibung der Art der Datenschutzverletzung** (Einordnung in Kategorie: Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugter Zugang; zusätzlich zur Angabe der Kategorien enthält die Meldung auch die ungefähre Anzahl der betroffenen Datensätze und Personen;
- Name und Kontaktdaten des **Datenschutzbeauftragten**
- eine Beschreibung ergriffener oder vorgeschlagener **Maßnahmen** zur Beseitigung der Verletzung oder Milderung der Auswirkungen.

Ein Formular für die Meldung von Datenschutzverletzungen ist als Anlage 1 beigefügt.

7. Prüfung der Folgen der Datenschutzverletzung auf hohes Risiko für die persönlichen Rechte und Freiheiten betroffener Personen
Ferner muss das Unternehmen prüfen, ob die Datenschutzverletzung ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

Ist dies der Fall, muss das Unternehmen die von der Datenschutzverletzung betroffenen Personen unterrichten, sofern nicht einer der in Art. 34 Abs. 3 DSGVO Ausnahmetatbestände vorliegt.

Ein solches hohes Risiko liegt in der Regel beispielsweise dann nahe, wenn die Datenschutzverletzung besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO oder Daten über Straftaten oder strafrechtliche Verurteilungen gem. Art. 10 DSGVO betrifft. Außerdem kann ein hohes Risiko bei automatisierten Entscheidungen im Einzelfall und Profiling (vgl. Art. 22 DSGVO) sowie bei systematischer Überwachung öffentlich zugänglicher Bereiche (vgl. Art. 35 DSGVO) gegeben sein.

Falls dies nachweislich nicht der Fall ist, kann das Unternehmen den Vorgang an dieser Stelle abschließen, indem es erforderliche Maßnahmen zur Beseitigung der Datenschutzverletzung sowie zur Vermeidung von Wiederholungen trifft. Zudem sollte der Verantwortliche auch hier für eine genaue Dokumentation der Datenschutzverletzung und der getroffenen Vorkehrungen sorgen.

Wenn hingegen ein hohes Risiko für die persönlichen Freiheiten und Rechte natürlicher Personen vorliegt, fährt das Unternehmen im vorliegenden Ablaufplan mit Punkt 8 fort und prüft bestehende Ausnahmen von der Benachrichtigungspflicht der Betroffenen.

8. Prüfung bestehender Ausnahmen von der Benachrichtigungspflicht der Betroffenen
Das Unternehmen prüft an dieser Stelle, ob eine der in Art. 34 Abs. 3 lit. a), lit. b) oder lit c) DSGVO geregelten Ausnahmen von der Pflicht zur Unterrichtung der betroffenen Personen vorliegt.

a. Prüfung der Sicherheitsvorkehrungen
So ist eine Unterrichtungspflicht gem. Art. 34 Abs. 3 lit. a) DSGVO etwa dann ausgeschlossen, wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat (insbesondere solche Vorkehrungen, durch die die personenbezogenen Daten für alle unbefugten Personen unzugänglich gemacht werden, wie z. B. Verschlüsselung) und wenn er es diese Vorkehrungen auf die von der Datenschutzverletzung betroffenen personenbezogenen Daten angewandt hat.

Eine Unterrichtung kann gem. Art. 34 Abs. 3 lit. b) DSGVO auch dann unterbleiben, wenn das Unternehmen durch auf den Datenschutzverstoß nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person aller Wahrscheinlichkeit nicht mehr besteht.

Falls das Unternehmen eine oder beide Fragen (nachweislich) bejaht, sollte es den gesamten Vorgang dokumentieren und erforderliche Maßnahmen zur Beseitigung der Datenschutzverletzung treffen. Falls dies bei beiden Fragen nicht der Fall ist, sollte das Unternehmen mit Punkt 8b des Ablaufplans fortfahren.

b. Prüfung des unverhältnismäßigen Aufwands der Benachrichtigung der betroffenen Person
Eine Unterrichtungsplicht liegt auch dann nicht vor, wenn die Benachrichtigung der betreffenden Personen mit einem unverhältnismäßigen Aufwand verbunden wäre. Anders als bei den im Punkt 8a genannten Ausnahmen, entfällt die Unterrichtungspflicht nicht vollständig. In diesem Fall muss der Verantwortliche den Datenschutzverstoß öffentlich bekanntmachen oder ähnliche Maßnahmen ergreifen, durch die er die betroffenen Personen vergleichbar wirksam informiert (Art. 34 Abs. 3 lit. c) DSGVO).

Wenn keine der in Punkt 8a und b genannten Ausnahmen greift, ist die betroffene Person gemäß Punkt 9 dieses Ablaufplans zu benachrichtigen.

9. Benachrichtigung der betroffenen Person

Das Unternehmen benachrichtigt die betroffene Person von der Datenschutzverletzung. Die Unterrichtung erfolgt unverzüglich (vgl. Erwägungsgrund 86). Das Unternehmen muss die betroffene Person individuell und in klarer und einfacher Sprache informieren. Die Form der Benachrichtigung muss zudem präzise, transparent, verständlich und leicht zugänglich sein.

Als Mindestinhalt muss die Benachrichtigung der betroffenen Person die folgenden Punkte enthalten:

- Name und Kontaktdaten des **Datenschutzbeauftragten** (falls kein Datenschutzbeauftragter vorhanden ist, der sonstigen zuständigen Stelle für den Datenschutz);
- eine Beschreibung der **wahrscheinlichen Folgen** der Datenschutzverletzung für die betroffenen Personen, also vor allem die zu erwartenden Folgen für die Rechte und Freiheiten der Betroffenen;
- eine Beschreibung ergriffener oder vorgeschlagener **Maßnahmen** zur Beseitigung der Verletzung oder Milderung der Auswirkungen.

Ein Formular zur Benachrichtigung betroffener Person ist als Anlage 2 beigefügt.

10. Dokumentation des gesamten Vorgangs und erforderliche Maßnahmen zur Beseitigung der Datenschutzverletzung

Abschließend sollte das Unternehmen den gesamten Vorgang angemessen dokumentieren. Zudem trifft es die erforderlichen Maßnahmen, um die Datenschutzverletzung zu beseitigen. Auch hier ist eine enge Abstimmung mit der für die IT-Sicherheit zuständigen Unternehmensfunktion ratsam.

Ferner ist zu prüfen, ob man das Datenschutz-Management-System entsprechend der hinzugewonnenen Erkenntnisse aus der möglichen Datenschutzpanne anpassen sollte.

Ort/Datum: _____ Ort/Datum: _____

_____ _____

Geschäftsführer Datenschutzbeauftragter

Anlage 1
Meldung Datenschutzverletzung an Aufsichtsbehörde

Der Thüringische Landesbeauftragte für den Datenschutz

Meldung von Verletzungen des Schutzes personenbezogener Daten gem. Art. 33 DSGVO

Ort/Datum

Sehr geehrte Damen und Herren,

in obiger Angelegenheit haben wir Grund zu der Annahme, dass sich in unserem Unternehmen eine Datenschutzverletzung ereignet hat.

1. Verantwortlicher:
Für die Datenverarbeitung verantwortlich ist die

… [Verein, Anschrift, Kontaktdaten, Vertretungsberechtigte Person]

2. Datenschutzbeauftragter:
Externer betrieblicher Datenschutzbeauftragter des Verantwortlichen ist

3. Kategorie der Datenschutzverletzung
☐ Vernichtung ☐ Verlust ☐ Veränderung ☐ unbefugte Offenlegung ☐ unbefugter Zugang

4. Beschreibung der Art der Datenschutzverletzung:
… *[z.B. Einbruchsdiebstahl in den Geschäftsräumen, ein Laptop der Marke MacBook-Pro wurde entwendet.]*

a. Kategorien und ungefähre Zahl der betroffenen Personen:
… *[z.B. Kundendaten, ca. 50 betroffene Personen]*

b. betroffene Kategorien und ungefähre Zahl der personenbezogenen Datensätze:
… *[z.B. Name, Anschrift, E-Mail-Adresse, ca. 50 Datensätze]*

5. Beschreibung der wahrscheinlichen der Datenschutzverletzung:
… *[z.B.* Weitergabe der Kundendaten, Weitergabe der Passwörter, Kontaktaufnahme durch Unbefugte, Inanspruchnahme durch Unbefugte]

6. Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der der Datenschutzverletzung:
… [z.B. Anzeige bei der zuständigen Polizeidienststelle; Zurücksetzung der Passwörter, Sperren der Kundenzugänge und Reaktivierung durch Kunden]

Maßnahmen zur Abmilderung der Auswirkungen der Verletzung:
…

7. Datum und Uhrzeit des Vorfalls:
…

Begründung, falls die Meldung länger als 72h nach dem Vorfall erfolgte:
…
Für Rückfragen und die Abstimmung des weiteren Vorgehens stehe ich jederzeit zur Verfügung.

Mit freundlichen Grüßen

Geschäftsführer

Anlage 2
Benachrichtigung betroffener Personen

… [Anschrift Betroffener]

Benachrichtigung betroffener Personen über Datenschutzverletzung gem. Art. 34 DSGVO

Ort/Datum

Sehr geehrte(r) Frau/Herr …

mit diesem Schreiben möchten wir Sie in Kenntnis setzen, dass es in unserem Unternehmen eine leider eine Datenpanne gegeben hat. Von dieser Datenschutzverletzung sind nach unserem bisherigen Kenntnisstand auch personenbezogene Daten von Ihnen betroffen sind.

1. Verantwortlicher:
Für die Datenverarbeitung verantwortlich ist die

… [Unternehmen, Anschrift, Kontaktdaten, Vertretungsberechtigte Person]

2. Datenschutzbeauftragter:
Externer betrieblicher Datenschutzbeauftragter des Verantwortlichen ist

3. Kategorie der Datenschutzverletzung
☐ Vernichtung ☐ Verlust ☐ Veränderung ☐ unbefugte Offenlegung ☐ unbefugter Zugang

4. Beschreibung der Art der der Datenschutzverletzung:
… *[z.B. Einbruchsdiebstahl in den Geschäftsräumen, ein Laptop der Marke MacBook-Pro wurde entwendet.]*

5. Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung:
… *[z.B.* Weitergabe der Kundendaten, Weitergabe der Passwörter, Kontaktaufnahme durch Unbefugte, Inanspruchnahme durch Unbefugte]

6. Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der der Datenschutzverletzung:
… [z.B. Anzeige bei der zuständigen Polizeidienststelle; Zurücksetzung der Passwörter, Sperren der Kundenzugänge und Reaktivierung durch Kunden]

Maßnahmen zur Abmilderung der Auswirkungen der Verletzung:
…
Wir bedauern diesen Vorfall außerordentlich. Für Rückfragen stehen wir jederzeit zur Verfügung.

Mit freundlichen Grüßen

… (Funktion im Verein))

Anlage 3
Mitarbeiteranweisung bei Datenschutzverletzungen

Der Verein] ist bestrebt, die internen Abläufe im Rahmen von möglicherweise auftretenden Datenschutzverletzungen im Verein zu optimieren und damit ihren gesetzlichen Pflichten nach Art. 33, 34 DSGVO nachzukommen.

Dazu muss der Verein Verletzungen des Schutzes personenbezogener Daten (**„Datenschutzverletzungen“**) ggf. den zuständigen Behörden melden und die von der Datenschutzverletzung betroffenen Personen benachrichtigen. Eine Datenschutzverletzung liegt bei jeder Verletzung der Datensicherheit vor, die zur Vernichtung, zum Verlust, oder zur Veränderung, zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führt. *(Zum besseren Verständnis sollte das Unternehmen hier beispielhaft darstellen, welche Datenschutzverletzungen im Unternehmen auftreten könnten, z. B. die Offenlegung von Kundendaten infolge eines Hackerangriffs usw.)*

Sollten Sie den Verdacht haben, dass Sie eine mögliche Datenschutzverletzung entdeckt haben, ist unverzügliches Handeln notwendig. In einem solchen Fall handeln Sie bitte nach folgendem Ablaufplan:

1. **Feststellung der betroffenen Daten**
   Stellen Sie zunächst nach Möglichkeit fest, welche Daten von der Datenschutzverletzung voraussichtlich betroffen sind. Dabei sollten Sie zumindest die Datenkategorie *(z. B. Kreditkartendaten, Bankverbindungsdaten, Gesundheitsdaten von Mitarbeitern)* und eine ungefähre Anzahl der betroffenen Datensätze feststellen.

2. **Feststellung der betroffenen Personen**
   Prüfen Sie anschließend, welche natürlichen Personen voraussichtlich von der möglichen Datenschutzpanne betroffen sind. Dabei sollten Sie zumindest feststellen, welche Personenkategorien *(z.B. Kunden, Mitarbeiter)* betroffen sind und wie hoch die Anzahl der betroffenen Personen in etwa ist.

3. **Beweissicherung**
   Bitte achten Sie dringend darauf, dass Sie keine weiteren Daten löschen und unverzüglich Sicherungsmaßnahmen durchführen, wo dies geboten ist.

4. **Sofortige Benachrichtigung des Vorstandes und des Datenschutzkoordinators**
   Benachrichtigen Sie unverzüglich die Geschäftsführung und den Datenschutzbeauftragten des Unternehmens über die mögliche Datenschutzverletzung, sowie die IT-Abteilung.

   Für die Datenschutzpannen zuständig im Vorstand ist …, erreichbar unter ….
   ….
   Für die Datenschutzpannen zuständig in der IT-Abteilung ist …, erreichbar unter ….

5. **Protokollierung und Dokumentation der Datenschutzverletzung**

Ort/Datum: _____

14. DATENVERARBEITUNG IM AUFTRAG

14.1. Abgrenzung

Wie jeder andere Verein auch, übernehmen wir nicht alle Aufgaben und Tätigkeiten selbst, sondern greifen auf die Hilfe externer Dienstleister zurück. Wenn Dienstleister Aufgaben für andere erfüllen und bei der Erfüllung mit personenbezogenen Arten umgehen, spricht man von einer Auftragsverarbeitung. Eine Auftragsverarbeitung liegt dann vor, wenn wir allein über Zwecke und Mittel der Verarbeitung entscheiden, d.h. der Dienstleister (Auftragsverarbeiter) weisungsabhängig den Auftrag erfüllt – quasi als unser verlängerter Arm. Keine Auftragsverarbeitung liegt vor bei der Inanspruchnahme von externen Fachleistungen, wie z.B. Steuer- oder Vereinsberatung vor.

14.2. Auswahl und Kontrolle der Auftragnehmer

Bei der Auswahl der Auftragnehmer für eine Datenverarbeitung im Auftrag ist darauf zu achten, ob der Auftragnehmer durch technische und organisatorische Maßnahmen hinreichende Garantien für den Schutz der Rechte der betroffenen Personen bietet. Der Auftragnehmer hat dabei insbesondere Auskunft über seine Sicherheitsmaßnahmen zu erteilen. Die vom Auftragnehmer eingerichteten technischen und organisatorischen Maßnahmen sind vom DSK-intern in Abstimmung mit dem DSB in geeigneter Weise zu überprüfen. Je nach Wichtigkeit der Dienstleistung kann diese Überprüfung auch ein Audit beim Auftragnehmer beinhalten. Die Überprüfung ist zu dokumentieren.

14.3. Verträge über eine Datenverarbeitung im Auftrag

Über die Beauftragungen sind Verträge nach den Vorgaben des Art. 28 DSGVO abzuschließen. Diese Verträge müssen insbesondere unser Weisungsrecht bestimmen, den Auftragnehmer zur Vertraulichkeit und Einhaltung der Sicherheit der Verarbeitung verpflichtet, Kontrollrechte des Auftraggebers vorsehen und schließlich festlegen, was mit den Daten nach der Beendigung des Vertragsverhältnisses geschehen soll. Zur Vertragsverhandlung, -ergänzung und zum -abschluss ist bei Bedarf vom DSK-intern der DSB hinzuzuziehen. Sollte ausnahmsweise die Vergabe von Unteraufträgen gestattet werden, so ist darauf zu achten, dass die vertraglichen Verpflichtungen, denen der Auftragsverarbeiter gegenüber dem Auftraggeber unterliegt, in gleicher Weise an den Unterauftragnehmer weitergegeben werden. Bestehende Unterauftragnehmer sind im Vertrag zu benennen, die Hinzuziehung weiterer Auftragnehmer soll nur nach unserer vorherigen Genehmigung erlaubt sein. Nach Möglichkeit sollte für sämtliche Auftragsverarbeitungsverträge das vom DSB geprüfte Muster verwendet werden.

Anlage 12: Muster Auftragsverarbeitungsverträge

Vertrag zur Auftragsverarbeitung

zwischen dem/der

.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

.....

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

14.4. **Präambel**

Der Auftragnehmer ist als weisungsgebundener Dienstleister des Auftraggebers tätig. Der vorliegende Vertrag zur Auftragsverarbeitung konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien aus der zugrundeliegenden Leistungsvereinbarung/Hauptvertrag vom ….. Sie findet Anwendung auf alle Tätigkeiten, die mit der Dienstleistungsbeziehung in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

14.5.

Die Parteien sind sich darüber einig, die gesetzlichen Regelungen der Datenschutzgrundverordnung (DS-GVO) bereits im Zeitraum ab Vertragsschluss bis zum In-Kraft-Treten der Verordnung am 25.05.2018 als individualvertragliche Vereinbarung zu behandeln und anzuwenden. Dies gilt jedoch nur, soweit die Regelung nicht im Widerspruch zu zwingen Vorschriften des bis dahin geltenden Bundesdatenschutzgesetzes (BDSG) stehen. Sollte eine Bestimmung dieses Vertrages ab Vertragsschluss bis zum 25.05.2018 gegen das BDSG verstoßen, wird sie durch die entsprechende gesetzliche Bestimmung des BDSG ersetzt.

14.6. **1. Gegenstand und Dauer des Auftrags**

1.1 Gegenstand

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/SLA/..... vom ....., auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: …… (Definition der Aufgaben)

1.2 Dauer

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum .....

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von ..... zum ..... gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

14.7. **2. Konkretisierung des Auftragsinhalts**

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

- ☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom .....

oder

- ☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: .....

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in …….

- ☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);
- ☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);
- ☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);
- ☐ wird hergestellt durch genehmigte Verhaltensregeln (Artt 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).
- ☐ wird hergestellt durch sonstige Maßnahmen: ……. (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO)

2.2 Art der Daten

- ☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

- ☐ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)
  - ☐ Personenstammdaten
  - ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
  - ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
  - ☐ Kundenhistorie
  - ☐ Vertragsabrechnungs- und Zahlungsdaten
  - ☐ Planungs- und Steuerungsdaten
  - ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
  - ☐ ...

2.3 Kategorien betroffener Personen

- ☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

- ☐ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
  - ☐ Kunden
  - ☐ Interessenten

- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ ...

14.8. **3. Technisch-organisatorische Maßnahmen**

3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.2 Der Auftragnehmer hat die Sicherheit gem. Artt. 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.

3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

3.4 Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisato-rischen Maßnahmen ist als **ANLAGE 1** zu diesem Vertrag beigefügt.

14.9. **4. Berichtigung, Einschränkung und Löschung von Daten**

4.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

14.10. **5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☐ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.
   - ☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
   - ☐ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
   - ☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

c) ☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

d) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt 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 Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

14.11. **6. Unterauftragsverhältnisse**

6.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-oder Transportdienstleistungen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung

c) ☐ Die Auslagerung auf Unterauftragnehmer oder

☐ der Wechsel des bestehenden Unterauftragnehmers

sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

6.3 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.4 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Ziffer 6.1 Satz 2 eingesetzt werden sollen.

6.5 Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

14.12. **7. Kontrollrechte des Auftraggebers**

7.1 Der Auftraggeber hat das Recht, in Abstimmung mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- ☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- ☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- ☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

14.13. **8. Mitteilung bei Verstößen des Auftragnehmers**

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. 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 Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber 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 Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

14.14. **9. Weisungsbefugnis des Auftraggebers**

9.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

9.2 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

14.15. **10. Löschung und Rückgabe von personenbezogenen Daten**

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. 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.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

10.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Ort/Datum: _____ Ort/Datum: _____

_____ _____

Auftraggeber Auftragnehmer

ANLAGE 1 – TECHNISCH-ORGANISATORISCHE MAßNAHMEN

1. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können,

sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

- **…**

2. Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)
Kryptografische Maßnahmen, durch die personenbezogene Daten derart verändert werden, dass sie – insbes. während ihres Übertragungsvorgangs – ohne einen Schlüssel nicht mehr les- oder verstehbar sind.

- **…**

14.16.

14.17. **3. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

- *Zutrittskontrolle*
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
  - **…**

- *Zugangskontrolle*
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
  - **…**

- *Zugriffskontrolle*
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
  - **…**

- *Trennungskontrolle*
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
  - **…**

14.18. **4. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**

- *Weitergabekontrolle*
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
  - **…**

- *Eingabekontrolle*
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;
  - **…**

14.19. **5. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

- *Verfügbarkeitskontrolle*
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

- …

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);
  - …

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

- Datenschutz-Management;
  - …

- Incident-Response-Management;
  - …

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) – „Privacy by default“ und „Privacy by design“
  - …

- *Auftragskontrolle*
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.
  - …

14.21.

14.22. Übersicht über Beauftragungen (Auftragsverarbeitungsverzeichnis)

Über die bestehenden Beauftragungen führt der DSK-intern eine Auftragsverarbeitungsübersicht.

Anlage 13: Auftragsverarbeitungsverzeichnis

Verzeichnis von Verarbeitungstätigkeiten des Auftragsverarbeiters gem. Art. 30 Abs. 2 DSGVO

Angaben zum Auftragsverarbeiter

1. Auftragsverarbeiter (Auftragnehmer/Dienstleister)

Name:	…
Gesetzlicher Vertreter:	… (Geschäftsführer)
Anschrift:	…
Telefon:	…
Fax:	…
E-Mail:	…
Internetadresse:	…

2. Externer Datenschutzbeauftragter des Auftragsverarbeiters

Name:	Arne Platzbecker
Anschrift:	HABEWI GmbH & Co. KG, Palmaille 96, 22767 Hamburg
Telefon:	040/ 1818980 - 0
Fax:	040/ 1818980 - 99
E-Mail:	platzbecker@bkp-kanzlei.de

Angaben zum Auftraggeber

3. Auftraggeber (Verantwortlicher für die Datenverarbeitung)

Name:	…
Gesetzlicher Vertreter:	… (Geschäftsführer)
Anschrift:	…
Telefon:	…
Fax:	…
E-Mail:	…
Internetadresse:	…

4. Datenschutzbeauftragter des Auftraggebers

Name:	…
Anschrift:	…
Telefon:	…
Fax:	…
E-Mail:	…
Internetadresse:	…

Angaben zu den Dienstleistungen

5. Kategorien von Verarbeitungen

Der Auftragnehmer ist als weisungsgebundener Dienstleister des Auftraggebers tätig. Der Auftragnehmer erbringt die nachfolgend wiedergegebenen Dienstleistungen auf Grundlage der Leistungsvereinbarung/Hauptvertrag vom … und des Auftragsverarbeitungsvertrages vom …:

a. … [Abstrakte Beschreibung des Leistungsgegenstands oder der Leistungsgegenstände]
b. … [Abstrakte Beschreibung des Leistungsgegenstands oder der Leistungsgegenstände]

Unterauftragnehmer/ Subdienstleister

4. Subdienstleister (Unterauftragnehmer) eingebunden: ☐ Nein ☐ Ja

Name:	…
Anschrift:	…
Telefon:	…

Fax: …
E-Mail: …
Internetadresse:

Technische und organisatorische Maßnahmen zum Datenschutz (Art. 32 Abs. 1 DSGVO)

7. Technische und organisatorische Maßnahmen zum Datenschutz
Die vom Auftragnehmer ergriffenen technischen und organisatorischen Maßnahmen sind in der beigefügten Anlage 1 zu diesem Verzeichnis von Verarbeitungstätigkeiten beigefügt.

Ort/Datum: _____

_____
Auftragsverarbeiter (Auftragnehmer)

Datum der Anlegung: …
Datum der letzten Änderung: …

14.23. Kontrollen, Audits

In den Auftragsverarbeitungsverträgen sind uns umfassende Kontrollrechte einzuräumen. Es muss uns auch möglich sein, die Umsetzung der mitgeteilten technischen und organisatorischen Maßnahmen des Auftragnehmers vor Ort zu überprüfen. Diese Kontrollen sind vom DSK-intern durchzuführen. Bei Bedarf können externe Sachverständige mit eingebunden werden.

15. GEMEINSAM VERANTWORTLICHE

Sollen Datenverarbeitungsverfahren in gemeinsamer Verantwortung mit anderen Stellen eingerichtet und betrieben werden, sind die Einzelheiten der Zusammenarbeit, insbesondere die Verpflichtungen zur Wahrnehmung der Rechte der Betroffenen, in einem Vertrag gem. Art. 26 DSGVO zu regeln. Der DSB ist bei der Gestaltung der vertraglichen Regelungen hinzuzuziehen. Die Tatsache der gemeinsamen

Verantwortung ist in der jeweiligen Beschreibung des Verfahrens im Verzeichnis über die Verarbeitungstätigkeiten zu dokumentieren.

16. DATENSPEICHERUNG UND LÖSCHUNG VON DATEN

16.1. Speicherung

Die Speicherung von Daten erfolgt grundsätzlich auf der technischen Infrastruktur des Vereins – insbesondere auf den Vereinsservern. Eine Speicherung auf mobilen Datenträgern (USB-Sticks) oder Cloudanbietern (z.B. Dropbox, Evernote) ist grundsätzlich untersagt.

16.2. Aufbewahrungsfristen

In Einhaltung des Grundsatzes der Datenminimierung sind personenbezogene Daten nur so lange zu speichern, wie es für die Erfüllung der Verarbeitungstätigkeit erforderlich ist. Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten sind von allen Mitarbeitern zu beachten. Die definierten Löschfristen sind im Verzeichnis der Verarbeitungstätigkeiten und im Löschkonzept unseres Vereins dokumentiert.

Anlage 14: Löschkonzept

Löschkonzept

Nach Art. 5 Abs. 1 lit. e DSGVO gilt der Grundsatz der Speicherbegrenzung ("storage limitation").
Personenbezogene Daten dürfen nur solange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Danach sind die Daten zu löschen. Wir sind dazu gesetzlich verpflichtet, Fristen für die Löschung und Überprüfung von gespeicherten personenbezogenen Daten der verschiedenen Kategorien in Zusammenarbeit mit dem DSB zu erstellen. Sowohl die Fristen, als auch die Art und Weise der erforderlichen Löschung sind nachfolgend bestimmt:

1. Keine Aufbewahrungspflichten

1.1 Soweit gesetzliche Aufbewahrungspflichten nicht einschlägig sind, gilt, dass zu löschen ist, sobald der Verarbeitungszweck weggefallen ist. Dies ist beispielsweise dann der Fall, wenn ein Vertrag von beiden Seiten erfüllt ist oder eine Einwilligungserklärung widerrufen wird.

1. 2. Soweit wir personenbezogene Daten aufgrund einer Einwilligung verarbeiten, daraufhin Dienstleistungen anbieten und der Betroffene über einen Zeitraum von mehr als 2 Jahren keinen Gebrauch von dieser Dienstleistung macht, löschen wir den Kunden aus unseren Bestandsdaten, sofern nicht aus anderen Gründen eine Pflicht zur weiteren Speicherung vorliegt.

2. DIN-66398 Erforderlichkeit eines Löschkonzepts

In der DIN-Norm 66398 („Leitlinie Löschkonzept“) sind die wichtigsten Informationen niedergelegt von Löschregeln bis hin zur Dokumentation der Löschung. Eine hilfreiche Zusammenfassung der einschlägigen DIN-Norm ist abrufbar unter https://www.secorvo.de/publikationen/din-66398-hammer-2016.pdf.

Anlage 1 enthält eine Übersicht über die Schutzklassen und Sicherheitsstufen der DIN-Norm 66399.

Anlage 1- Schutzklassen

Schutzklasse 1	**Normaler Schutzbedarf** für interne Daten (z. B. Telefonlisten, Lieferantendateien, Adressdatenbanken, Notizen) – werden diese Daten nicht entsprechend geschützt, besteht die Gefahr, dass ein Betroffener in seiner Stellung und seinen wirtschaftlichen Verhältnissen beeinträchtigt wird, zudem hätte die unbefugte Kenntnisnahme der Daten negative Auswirkungen für die speichernde Stelle
Schutzklasse 2	**Hoher Schutz** für vertrauliche Daten (z. B. Personal- und Finanzdaten), bei diesen Daten besteht die Gefahr, dass ein Betroffener in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird, außerdem hätte die unbefugte Kenntnisnahme der Daten erhebliche negative Auswirkungen für die speichernde Stelle
Schutzklasse 3	**Sehr hoher Schutzbedarf** für besonders vertrauliche und geheime Daten (Daten, die – wenn sie nicht entsprechend geschützt werden – zu einer Gefahr für Leib oder Leben von Personen oder für die Freiheit eines Betroffenen führen können), außerdem hätte die unbefugte Kenntnisnahme der Daten ernsthafte (existenzbedrohende) Auswirkungen für die speichernde Stelle und würde gegen Berufsgeheimnisse, Verträge oder Gesetze verstoßen (z. B. Forschungs- und Entwicklungsdokumente, Verschlusssachen, **Gesundheitsdaten**)

Sicherheitsstufen

Sicherheitsstufe 1	**Allgemeine Daten** Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen ohne besondere Hilfsmittel und ohne Fachkenntnisse, jedoch nicht ohne besonderen Zeitaufwand, möglich ist. Papiere und Filme in Originalgröße: Materialteilchenfläche max. 2.000 mm², Streifenbreite max. 12 mm, Streifenlänge unbegrenzt, Toleranz für 10 % der Fläche des Materials: maximal 3800 mm² Kunststoff wie Identifikationskarte oder Mikrofilm: Materialteilchenfläche max. 160 mm², Toleranz für 10 % der Fläche des Materials: maximal 480 mm² Optische Datenträger: Materialteilchenfläche max. 2000 mm², Toleranz für 10 % der Fläche des Materials: maximal 3800 mm² Magnetische Datenträger: Medium muss funktionsunfähig sein

	Festplatten: Festplatte muss funktionsunfähig sein Halbleiterspeicher (z.B. Speichersticks, Chipkarten, mobile Kommunikationsmittel): Datenträger muss funktionsunfähig sein
Sicherheitsstufe 2	**Interne Daten** (z.B. Aushänge und Formulare) Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen mit Hilfsmitteln und nur mit besonderem Zeitaufwand möglich ist. Papiere und Filme in Originalgröße: Materialteilchenfläche max. 800 mm², Streifenbreite bis max. 6 mm, Streifenlänge unbegrenzt, Toleranz für 10 % der Fläche des Materials: maximal 2000 mm² Kunststoff wie Identifikationskarte oder Mikrofilm: Materialteilchenfläche max. 30 mm², Toleranz für 10 % der Fläche des Materials: maximal 90 mm² Optische Datenträger: Materialteilchenfläche max. 800 mm², Toleranz für 10 % der Fläche des Materials: maximal 2000 mm² Magnetische Datenträger: Medium mehrfach zerteilt und Materialteilchenfläche max. 2000 mm², Toleranz für 10 % der Fläche des Materials: maximal 3800 mm² Festplatten: Datenträger beschädigt Halbleiterspeicher: Datenträger muss zerteilt sein
Sicherheitsstufe 3	**Sensible Daten** (Unterlagen mit vertraulichen Daten) Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen nur unter erheblichem Aufwand (Personen, Hilfsmittel, Zeit) möglich ist. Papiere und Filme in Originalgröße: Materialteilchenfläche max. 320 mm², Streifenbreite max. 2 mm, Streifenlänge unbegrenzt, Toleranz für 10 % der Fläche des Materials: maximal 480 mm² Kunststoff wie Identifikationskarte oder Mikrofilm: Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm² Optische Datenträger: Materialteilchenfläche max. 160 mm², Toleranz für 10 % der Fläche des Materials: maximal 480 mm² Magnetische Datenträger: Materialteilchenfläche max. 320 mm², Toleranz für 10 % der Fläche des Materials: maximal 800 mm² Festplatten: Datenträger verformt Halbleiterspeicher: Datenträger muss zerteilt sein und Materialteilchenfläche max. 160 mm², Toleranz für 10 % der Fläche des Materials: maximal 480 mm²

Sicherheitsstufe 4	**Besonders sensible Daten** (z. B. Gehaltsabrechnungen, Personaldaten/-akten, Arbeitsverträge, medizinische Daten, Steuerunterlagen von Personen) Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen, die im Falle kleiner Auflagen sehr aufwändig sind, möglich ist. Papiere und Filme in Originalgröße: Materialteilchenfläche max. 160 mm² und für gleichförmige Partikel: Streifenbreite max. 6 mm, Toleranz für 10 % der Fläche des Materials: maximal 800 mm² Kunststoff wie Identifikationskarte oder Mikrofilm: Materialteilchenfläche max. 2,5 mm², Toleranz für 10 % der Fläche des Materials: maximal 7,5 mm² Optische Datenträger: Materialteilchenfläche max. 30 mm², Toleranz für 10 % der Fläche des Materials: maximal 90 mm² Magnetische Datenträger: Materialteilchenfläche max. 160 mm², Toleranz für 10 % der Fläche des Materials: maximal 480 mm² Festplatten: Datenträger mehrfach zerteilt und verformt und Materialteilchenfläche max. 2000 mm², Toleranz für 10 % der Fläche des Materials: maximal 3800 mm² Halbleiterspeicher: Datenträger muss zerteilt sein und Materialteilchenfläche max. 30 mm², Toleranz für 10 % der Fläche des Materials: maximal 90 mm²
Sicherheitsstufe 5	**Geheim zu haltende Daten** (Datenträger mit geheim zu haltenden Informationen mit existenzieller Wichtigkeit für eine Person, eine Behörde, ein Unternehmen oder eine Einrichtung) Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass es nach dem Stand der Technik unmöglich ist, auf ihnen wiedergegebene Informationen zu reproduzieren Papiere und Filme in Originalgröße: Materialteilchenfläche max. 30 mm² und für gleichförmige Partikel: Streifenbreite max. 2 mm, Toleranz für 10 % der Fläche des Materials: maximal 90 mm² Kunststoff wie Identifikationskarte oder Mikrofilm: Materialteilchenfläche max. 1 mm², Toleranz für 10 % der Fläche des Materials: maximal 3 mm² Optische Datenträger: Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm² Magnetische Datenträger: Materialteilchenfläche max. 30 mm², Toleranz für 10 % der Fläche des Materials: maximal 90 mm²

	Festplatten: Datenträger mehrfach zerteilt und verformt und Materialteilchenfläche max. 320 mm², Toleranz für 10 % der Fläche des Materials: maximal 800 mm² Halbleiterspeicher: Datenträger muss zerteilt sein und Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm²
Sicherheitsstufe 6	**Geheime Hochsicherheitsdaten** (z.B. geheimdienstliche oder militärische Bereiche) Datenträger mit geheim zu haltende Unterlagen, wenn außergewöhnliche Sicherheitsvorkehrungen einzuhalten sind Papiere und Filme in Originalgröße: Materialteilchenfläche max. 10 mm² und für gleichförmige Partikel: Streifenbreite max. 1 mm, Toleranz für 10 % der Fläche des Materials: maximal 30 mm² Kunststoff wie Identifikationskarte oder Mikrofilm: Materialteilchenfläche max. 0,5 mm², Toleranz für 10 % der Fläche des Materials: maximal 1,5 mm² Optische Datenträger: Materialteilchenfläche max. 5 mm², Toleranz für 10 % der Fläche des Materials: maximal 15 mm² Magnetische Datenträger: Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm² Festplatten: Datenträger mehrfach zerteilt und verformt und Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm² Halbleiterspeicher: Datenträger muss mehrfach zerteilt sein und Materialteilchenfläche max. 1 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm²
Sicherheitsstufe 7	**Top Secret Hochsicherheitsdaten** (Datenträger mit strengst geheim zu haltende Daten, bei denen höchste Sicherheitsvorkehrungen einzuhalten sind) Papiere und Filme in Originalgröße: Materialteilchenfläche max. 5 mm² und für gleichförmige Partikel: Streifenbreite max. 1 mm, Toleranz für 10 % der Fläche des Materials: keine Toleranz zugelassen Kunststoff wie Identifikationskarte oder Mikrofilm: Materialteilchenfläche max. 0,2 mm², Toleranz für 10 % der Fläche des Materials: keine Toleranz zugelassen Optische Datenträger: Materialteilchenfläche max. 0,2 mm², Toleranz für 10 % der Fläche des Materials: maximal 0,6 mm² Magnetische Datenträger: Materialteilchenfläche max. 2,5 mm², Toleranz für 10 % der Fläche des Materials: maximal 7,5 mm² Festplatten: Datenträger mehrfach zerteilt und verformt und Materialteilchenfläche max. 5 mm², Toleranz für 10 % der Fläche des Materials: maximal 15 mm²

	Halbleiterspeicher: Datenträger muss mehrfach zerteilt sein und Materialteilchenfläche max. 0,5 mm², Toleranz für 10 % der Fläche des Materials: maximal 1,5 mm²

Zuordnung der Sicherheitsstufen zu den Schutzklassen

Schutzklasse:	**Sicherheitsstufen:**						
	1	2	3	4	5	6	7
1	x	x	x				
2				x	x		
3				x	x	x	x

16.3. Löschung von Daten

Die Durchführung der Löschung von Daten betrifft sowohl die Vernichtung von Papierdokumenten, als auch die Löschung elektronischer Datensätze erfolgt gemäß unserem Löschkonzept.