Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Datenschutz im Verein nach der DS-GVO

Praxisratgeber

2. Auflage

Datenschutz im Verein nach der DS-GVO

Praxisratgeber

2. Auflage

Stand: 24. Juni 2020

Herausgegeben
vom Landesbeauftragten für den
Datenschutz und die Informationsfreiheit
Dr. Stefan Brink
Mitautorin: Katharina Rau
Königstraße 10a, 70173 Stuttgart
Telefon 0711/615541-0
https://www.baden-wuerttemberg.datenschutz.de
E-Mail: poststelle@lfdi.bwl.de

PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

Zur besseren Lesbarkeit wird bei verallgemeinernden Substantiven lediglich das bestimmende Geschlecht genannt. Selbstverständlich richtet sich dieser Bericht an die Angehörigen beider Geschlechter.

Vorwort

Ab dem 25. Mai 2018 wird die Datenschutz-Grundverordnung (DS-GVO) in Deutschland und in allen anderen Mitgliedstaaten der Europäischen Union geltendes Recht. Gerade kleine Vereine sind sehr verunsichert, welche Neuerungen anstehen bzw. welche neuen Anforderungen an sie gestellt werden. Noch schwieriger die Frage, wie diese Anforderungen konkret umzusetzen sind. Informationen zur DS-GVO gibt es zwar zwischenzeitlich zu Genüge, jedoch sind diese Informationen oftmals sehr theoretisch gehalten und somit für eine Umsetzung in die Praxis nicht immer hilfreich. Wir hoffen sehr, dass unsere Orientierungshilfe (abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/06/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf) nicht nur von Experten verstanden und geschätzt wird. Eine Vielzahl von Anfragen zeigt uns jedenfalls, dass neben diesen Fachinformationen auch ein dringendes Interesse an einfachen und praktischen Hinweisen für Vereine gefragt ist. Unser Praxisratgeber soll hier Abhilfe schaffen.

1. Informationspflichten

Wie und wo muss der Verein seinen Informationspflichten nachkommen?

Jeder Verein hat aus Gründen der Transparenz umfassend darüber zu informieren, wie die personenbezogenen Daten der Mitglieder (oder Dritter) verarbeitet werden. Hierfür hat der Verein zum Zeitpunkt der Erhebung (z.B. im Mitgliedsantrag) sämtliche Informationen des Art. 13 DS-GVO mitzuteilen.

Was muss rein?

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
- Kontaktdaten des Datenschutzbeauftragten
- Zwecke und Rechtsgrundlage der Verarbeitung
- Berechtigte Interessen i.S.d. Art. 6 Abs. 1 lit. f) DS-GVO
- Empfänger oder Kategorien von Empfängern
- Absicht von Drittlandtransfer sowie Hinweis auf (Fehlen von) Garantien zur Datensicherheit
- Speicherdauer der personenbezogenen Daten
- Belehrung über Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht gegen Verarbeitung)
- Hinweis auf jederzeitiges Widerrufsrecht der Einwilligung
- Hinweis auf Beschwerderecht bei einer Datenschutz-Aufsichtsbehörde
- Pflicht zur Bereitstellung der Daten
- Automatisierte Entscheidungsfindung einschließlich Profiling

Muster Informationspflichten

Ein Muster für die einfache und pragmatische Erfüllung dieser Informationspflichten nach Art. 13 DS-GVO finden Sie im Anhang.

Wie müssen die Informationen gem. Art. 13 DS-GVO zur Verfügung gestellt werden?

Wichtig ist, dass die Informationen nach Art. 13 DS-GVO gut erreichbar sind. Dies ist immer dann der Fall, wenn die Informationen auf die gleiche Art und Weise bereitgestellt werden, wie die Datenerhebung erfolgt (z.B. Datenerhebung durch Formular: Informationen werden auf dem Formular abgedruckt bzw. mit diesem ausgegeben; Datenerhebung per E-Mail: Informationen werden per E-Mail mitgeteilt). Aber auch ein Hinweis auf der Vereinswebseite kann ausreichend sein, wenn die Möglichkeit besteht, die Informationen leicht und transparent einzusehen. Hat hierbei ein Mitglied keine Möglichkeit, die Informationen auf der Webseite einzusehen, so muss der Verein seine Informationspflicht auf andere Weise, etwa durch Zusenden der Informationen per Post, erfüllen.

Müssen die Informationspflichten des Art. 13 DS-GVO für bereits nach dem Bundesdatenschutzgesetz (BDSG) erfolgte Datenerhebungen nachgeholt werden?

Nein. Bei bereits erfolgten Datenerhebungen (von Altmitgliedern) nach dem BDSG sind die Informationspflichten des Art. 13 DS-GVO nicht zu erfüllen bzw. nachzuholen. Erst für Datenerhebungen ab dem 25. Mai 2018 bzw. wenn bei Bestandsmitgliedern weitergehende Datenerhebungen/Änderungsmitteilungen erfolgen, sind die Informationspflichten zu erfüllen.

2. Einwilligungserklärung

Wann muss der Verein eine Einwilligungserklärung einholen?

Viele Vereine sind der Ansicht, dass sie von jedem Mitglied für die Verarbeitung der personenbezogenen Daten der Mitglieder zukünftig zwingend eine Einwilligungserklärung benötigen und dass ohne eine Einwilligung eine Datenverarbeitung unzulässig wäre. Dies trifft jedoch nicht zu. Ein Verein darf – auch ohne Einwilligung – solche Daten erheben,

- die für die Begründung und Durchführung des zwischen Mitglied und Verein durch den Beitritt zustande kommenden rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich sind (Art. 6 Abs. 1 lit. b) DS-GVO)
- wenn er an der Datenverarbeitung ein überwiegendes berechtigtes Interesse hat (Art. 6 Abs. 1 lit. f) DS-GVO).

In welchen Fällen der Verein Daten zur Verfolgung der Vereinsziele bzw. die Betreuung und Verwaltung der Mitglieder auf Grund des Art. 6 Abs. 1 lit. b) DS-GVO erheben darf bzw. berechtigte Interessen hieran haben, ist in unserer Orientierungshilfe „Datenschutz im Verein nach der DS-GVO (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/06/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf)“ ausführlich dargelegt. In Bezug auf die berechtigten Interessen ist es daher wichtig, dass der Verein diese darlegt und vollumfänglich über diese Interessen informiert (s. o. unter 1.)

Nur für Datenverarbeitungen, die über die gesetzlich erlaubten Verarbeitungen hinausgehen, ist eine Einwilligung erforderlich. Dies sind Fälle, in denen die Verarbeitung der personenbezogenen Daten weder zur Durchführung des Mitgliedsvertrags noch aufgrund berechtigter Interessen des Vereins erforderlich sind.

In Betracht kommen insbesondere:

- Veröffentlichung von Fotos auf der Webseite des Vereins
- Veröffentlichung von Geburtsdaten/Jubiläen im Vereinsblatt/am schwarzen Brett
- Werbung von Dritten

Welche Form muss die Einwilligung haben?

Anders als das BDSG, das für Einwilligungen grundsätzlich die Schriftform vorsieht, ermöglicht die DS-GVO die Einwilligung schriftlich, elektronisch, mündlich oder sogar konkludent abzugeben. Jedoch muss der Verein für den Fall, dass die Verarbeitung auf einer Einwilligung beruht, nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat (Art. 7 Abs. 1 DS-GVO). Aus diesem Grund ist zu anzuraten, Einwilligungen zum Zwecke des Nachweises schriftlich (d. h. mit eigenhändiger Unterschrift der betroffenen Person) einzuholen und aufzubewahren.

Muss der Verein ab dem 25. Mai 2018 von allen Mitgliedern, die bereits eine Einwilligung abgegeben haben, eine neue Einwilligung einholen?

Nein. Liegt seitens der Bestandsmitglieder bereits eine Einwilligung vor, so gilt diese weiter und muss nicht erneut eingeholt werden. Lediglich wenn es zu einer weitergehenden einwilligungspflichtigen Verarbeitung personenbezogener Daten kommen soll, ist eine neue Einwilligung notwendig. Hier hilft unsere

Muster-Einwilligung

Für jede Datenverarbeitung ist eine gesonderte Einwilligungserklärung erforderlich. Daher sollte für jede Einwilligungserklärung ein gesondertes Formular verwendet werden. Auf keinen Fall soll die Einwilligungserklärung in die Datenschutzhinweise „gepackt“ werden. Auf jedem Formular ist genau anzugeben, welche Daten zu welchem Zweck verarbeitet werden.
Ein Muster für die Einwilligung in der Veröffentlichung von Daten auf der Webseite des Vereins finden Sie im Anhang.

3. Benennung eines Datenschutzbeauftragten

Wann muss der Verein einen Datenschutzbeauftragten benennen?

Der Verein hat einen Datenschutzbeauftragen zu benennen, wenn mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder der Verein Verarbeitungen vornimmt, die einer Datenschutzfolgenabschätzung gemäß Art. 35 DS-GVO unterliegen.

Darüber hinaus muss ein Datenschutzbeauftragter benannt werden, wenn die Kerntätigkeit des Vereins in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person erforderlich macht (z.B. Videoüberwachung im Stadion) oder die Kerntätigkeit in der Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DS-GVO (z.B. Gesundheitsdaten in Selbsthilfegruppen) oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO besteht (Art. 37 Abs. 1 lit. b) und lit. c) DS-GVO).

Für die Frage, ob der Verein einen Datenschutzbeauftragten benennen muss, empfiehlt sich folgendes **Prüfschema**.

a) Sind mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt?

„Ständig" beschäftigt ist eine Person, wenn sie für diese Aufgabe auf längere Zeit vorgesehen ist und sie entsprechend wahrnimmt. Irrelevant ist, ob die Person beim Verein beschäftigt oder ehrenamtlich tätig ist. Die Aufgabe braucht auch nicht Hauptaufgabe der Person zu sein. Das Tatbestandsmerkmal „ständig" ist daher auch erfüllt, wenn die Aufgabe selbst nur gelegentlich anfällt, die betreffende Person sie aber stets wahrzunehmen hat. Nicht ständig beschäftigt ist hingegen, wer die eigentlich anderen obliegende Aufgabe gelegentlich mit übernimmt oder nur vorübergehend in diesem Bereich tätig ist. Ständig bedeutet daher, dass die Person immer dann mit der Verarbeitung personenbezogener Daten beschäftigt ist, wenn diese Tätigkeit anfällt.

✔ Ja: Datenschutzbeauftragter erforderlich

✘ Nein: weiterprüfen:

b) Nimmt der Verein Verarbeitungen vor, die einer Datenschutzfolgenabschätzung unterliegen?

Eine Datenschutzfolgeabschätzung ist nur dann erforderlich, wenn die Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen hat. Ein solch hohes Risiko ist jedoch die Ausnahme und besteht in aller Regel nicht. Mehr Informationen hierzu unten Nr. 5.

✔ Ja: Datenschutzbeauftragter erforderlich

✘ Nein: weiterprüfen:

c) Liegt die Kerntätigkeit des Vereins in Verarbeitungsprozessen, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person erforderlich macht?

Werden personenbezogene Daten nur als Nebentätigkeit und nicht als Haupttätigkeit verarbeitet, so liegt keine „Kerntätigkeit vor. Bei „klassischen" Vereinen erfolgt eine Verarbeitung personenbezogener Daten nur als notwendig anfallende Nebentätigkeit (Mitgliederverwaltung, Verarbeitung von Daten von Beschäftigten etc.). Vereine, deren Kerntätigkeit in Verarbeitungsprozessen liegt, welche eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person erforderlich machen, sind kaum denkbar.

✔ Ja: Datenschutzbeauftragter erforderlich

✘ Nein: weiterprüfen:

d) Besteht die Kerntätigkeit in der Verarbeitung besonderer Kategorien von Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten?

Besondere Kategorien von Daten sind personenbezogene Daten, aus denen die rassische, ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben und der sexuellen Orientierung. Als Beispiele kommen die Religionszugehörigkeit, Parteizugehörigkeit sowie Angaben über Krankheiten in Betracht. Hinzukommen muss jedoch auch hier, dass die Kerntätigkeit des Vereins in der Verarbeitung vorgenannter Daten liegt. Dies ist immer dann der Fall, wenn ohne die Verarbeitung dieser Daten der Zweck des Vereins nicht erreicht werden könnte. Denkbar ist dies etwa bei Selbsthilfegruppen oder Vereinen mit politischer Zielrichtung.

✔ Ja: Datenschutzbeauftragter erforderlich

✘ Nein: Kein Datenschutzbeauftragter erforderlich.

Der Verein hat die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen. Hierbei ist es ausreichend, wenn die E-Mail-Adresse des Datenschutzbeauftragten auf der Vereinshomepage frei zugänglich genannt wird.

Der Datenschutzbeauftragte ist der zuständigen Aufsichtsbehörde zu melden. Eine Meldung ist beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg ist über folgendes Online–Formular möglich:
https://www.baden-wuerttemberg.datenschutz.de/dsb-online-melden/

Welche fachlichen Qualifikationen ein Datenschutzbeauftragter erfüllen muss und was seine Aufgaben sind, siehe ab S. 31 Punkt 7.1 der Orientierungshilfe „Datenschutz im Verein nach der DS-GVO“ (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf) sowie in Kurzpapier Nr. 12 der Datenschutzkonferenz (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/01/DSK_KPNr_12_Datenschutzbeauftragter.pdf).

4. Verzeichnis von Verarbeitungstätigkeiten

Gemäß Art. 30 DS-GVO hat jeder Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten zu führen. Zwar besteht bei Verantwortlichen, bei denen weniger als 250 Mitarbeiter beschäftigt sind, zunächst eine Ausnahme von der Verzeichnisführungspflicht. Diese Ausnahme gilt jedoch unter anderem dann nicht, wenn die Verarbeitung nicht nur gelegentlich oder eine Verarbeitung sensibler Daten erfolgt.

Der Begriff „regelmäßig" ist erfüllt,wenn mindestens eine der folgenden Eigenschaften vorliegt:

- fortlaufend oder in bestimmten Abständen während eines bestimmten Zeitraums vorkommend
- immer wieder oder wiederholt zu bestimmten Zeitpunkten auftretend
- ständig oder regelmäßig stattfindend

Ein Verein beschäftigt nur 3 Mitarbeiter. Muss er trotzdem ein Verzeichnis von Verarbeitungstätigkeiten führen?

Ja, da in jedem Verein die Verarbeitung personenbezogener Daten nicht nur gelegentlich, sondern regelmäßig stattfindet (z.B. Aktualisierung Mitgliederliste, Versand von Nachrichten an Mitglieder, Einzug von Mitgliedsbeiträgen, Anmeldung zu Wettkämpfen etc.), ist auch bei Vereinen mit 3 Mitarbeitern ein Verzeichnis von Verarbeitungstätigkeiten zu führen.

Weitere Informationen zu diesem Thema finden Sie ab S. 33 unter Punkt 7.2 der Orientierungshilfe „Datenschutz im Verein nach der DS-GVO" (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf) sowie in Kurzpapier Nr. 1 der Datenschutzkonferenz (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/07/DSK_KPNr_1_Verzeichnis_Verarbeitungst%C3%A4tigkeiten.pdf).

Muster Verzeichnis von Verarbeitungstätigkeiten

Bestimmte Anforderungen an die Form stellt die DS-GVO nicht. Ein Muster für ein Verzeichnis von Verarbeitungstätigkeiten finden Sie im Anhang.
Beim Ausfüllen ist darauf zu achten, dass pro Verarbeitungstätigkeit gesondert aufgeführt wird, welche Kategorien von Personen, welche Kategorien von personenbezogenen Daten bzw. Kategorien von Empfängern jeweils betroffen sind. Auch sind die Übermittlung in ein Drittland sowie die Löschfristen jeweils gesondert anzugeben:

Beispiel für ein ausgefülltes Verzeichnis von Verarbeitungstätigkeiten:

Verarbeitungstätigkeit	Zwecke der Verarbeitung	Kategorien der betroffenen Personen	Kategorien von personenbezogenen Daten	Kategorien von Empfängern	Übermittlung an ein Drittland	Löschfristen
Mitgliederverwaltung	Mitglieder- verwaltung	Mitglieder	Name Adresse Geburtsdatum Abteilung/ Sportbereich	Keine	Nein	Nach Beendigung der Mitgliedschaft
Lohnabrechnung	Auszahlung von Gehalt, Abfuhr von Steuern und Sozialabgaben	Beschäftigte	Name Adresse Religionszugehörigkeit Steuernummer etc.	Ggf. externer Dienstleister	Nein	Gesetzl. Aufbewahrungsfrist von 10 Jahren
Veröffentlichung von Fotos auf der Vereinswebseite	Außerdarstellung, Anwerben neuer Mitglieder	Mitglieder, Besucher der Webseite	Fotos, IP-Adressen	Keine	Nein	Fotos bei Widerruf der Einwilligung, IP-Adressen nach 30 Tagen

5. Datenschutzfolgenabschätzung

Eine Datenschutzfolgenabschätzung ist nur dann erforderlich, wenn die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten für die betroffene Person zur Folge hat. Dies ist insbesondere dann der Fall, wenn eine umfangreiche Verarbeitung besonderer Kategorie von Daten erfolgt (z.B. Verarbeitung von Gesundheitsdaten) oder wenn systematische und umfassende Bewertungen persönlicher Aspekte vorgenommen werden (z.B. Profiling). Hiervon ist bei Vereinen in aller Regel nicht auszugehen, kann jedoch bei Vereinen der Straffälligenhilfe oder bei Selbsthilfegruppen ausnahmsweise der Fall sein.

Weitere Informationen zu diesem Thema finden Sie ab S. 34 unter Punkt 7.3 der Orientierungshilfe „Datenschutz im Verein nach der DS-GVO (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf)“ sowie in Kurzpapier Nr. 5 der Datenschutzkonferenz (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/DSK-Kurzpapier-5-DSFA.pdf).

6. Auftragsverarbeitung

Wann muss der Verein einen Auftragsverarbeitungsvertrag abschließen?

Wenn Dienstleister Aufgaben für den Verantwortlichen erfüllen (z.B. Adressverwaltung, externe Lohnabrechnung, Wartung IT) und in diesem Zusammenhang mit personenbezogenen Daten umgehen bzw. Einblick in diese haben, so spricht man von einer Auftragsverarbeitung. Eine solche ist auch dann gegeben, wenn ein Verein seine Mitgliederdaten nicht auf einer eigenen EDV-Anlage speichert, sondern hierfür einen Datenbankserver nutzt, den ein Dienstleistungsunternehmen zu diesem Zweck zur Verfügung stellt.

Der Verein darf nur Auftragsverarbeiter einsetzen, die eine hinreichende Garantie für eine datenschutzkonforme Datenverarbeitung gewährleisten.

Weitere Informationen zu diesem Thema finden Sie ab S. 15 unter Punkt 3.2 der Orientierungshilfe „Datenschutz im Verein nach der DS-GVO“ (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf) sowie in Kurzpapier Nr. 13 der Datenschutzkonferenz (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/02/DSK_KpNr_13_Auftragsverarbeitung.pdf).

Muster Auftragsverarbeitungsvertrag

Ein Muster für einen Auftragsverarbeitungsvertrag finden Sie im Anhang.

7. Sonstiges

Auf unserem Internetauftritt finden Sie in der Rubrik FAQs unter anderem eine Zusammenstellung der häufigsten Fragen zur „Veröffentlichung von Fotos speziell für Vereine“.

Muster für Informationspflicht bei Erhebung von personenbezogenen Daten gemäß Art. 13 DS-GVO

1. Name und Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters

Verantwortlicher im Sinne des Art. 13 Abs. 1 lit. a) DS-GVO ist
Name Verein: Straße:
PLZ, Ort:
Tel.:
E-Mail:
Vorstand:

2. Kontaktdaten des Datenschutzbeauftragten

Die Kontaktdaten des Datenschutzbeauftragten müssen selbstverständlich nur dann angegeben werden, wenn ein solcher benannt ist. Ausreichend ist hierbei die Angabe eines Funktionspostfachs.

Formulierungsbeispiel:

Unseren Datenschutzbeauftragten erreichen Sie unter folgender E-Mail-Adresse:
Datenschutzbeauftragter@Musterverein.de

3. Zwecke und Rechtsgrundlage der Verarbeitung

Bei einem Verein können je nach Ausrichtung ganz verschiedene Zwecke, für die personenbezogene Daten verarbeitet werden, anfallen. Jeder Zweck ist hierbei gesondert aufzunehmen. Auch ist für jeden Zweck gesondert die Rechtsgrundlage der Verarbeitung anzugeben. Jeder Verein sollte sich daher zunächst einen Überblick darüber verschaffen, welche Daten zu welchem Zweck verarbeitet werden und sodann prüfen, auf welcher Grundlage die Verarbeitung erfolgt. Als Rechtsgrundlage kommen insbesondre in Betracht:
Art. 6 Abs. 1 S. 1 lit. a) DS-GVO: Einwilligung der betroffenen Person
Art. 6 Abs. 1 S. 1 lit. b) DS-GVO: bei Datenverarbeitungen zur Erfüllung des Mitgliedsvertrags/ Satzung
Art. 6 Abs. 1 S. 1 lit. f) DS-GVO: bei Datenverarbeitungen zur Wahrung berechtigter Interessen des Vereins

Formulierungsbeispiele (die im Folgenden genannten Zwecke sind nur beispielhaft und nicht abschließend):

Der Musterverein verarbeitet folgende personenbezogene Daten:

- Zum **Zwecke der Mitgliederverwaltung** werden der Name, Vorname, Sportbereich/Abteilung verarbeitet (ggf. sind weitere Daten, die im konkreten Fall verarbeitet werden, zu nennen). Die Rechtsgrundlage hierfür ist Art. 6 Abs. 1 S. 1 lit. b) DS-GVO.
- Zum **Zwecke der Beitragsverwaltung** wird die Bankverbindung verarbeitet (ggf. sind weitere Daten, die im konkreten Fall verarbeitet werden, zu nennen). Die Rechtsgrundlage hierfür ist Art. 6 Abs. 1 S. 1 lit. b) DS-GVO.

- Zum **Zwecke der Lohnabrechnung** werden von den Beschäftigten des Mustervereins der Name, der Vorname, die Adresse, ggf. die Religionszugehörigkeit, Steuernummer verarbeitet (ggf. sind weitere Daten, die im konkreten Fall verarbeitet werden, zu nennen). Die Rechtsgrundlage hierfür ist Art. 6 Abs. 1 S. 1 lit. b) DS-GVO.
- Zum **Zwecke der Außendarstellung** werden Fotos der Mitglieder/von Veranstaltungen auf der Vereinswebseite www.Musterverein.de veröffentlicht. Die Rechtsgrundlage hierfür ist Art. 6 Abs. 1 S. 1 lit. a) DS-GVO.
- Zum **Zwecke der Eigenwerbung** des Mustervereins wird Werbung an die E-Mail-Adresse der Mitglieder versendet. Die Rechtsgrundlage hierfür ist Art. 6 Abs. 1 S. 1 lit. f) DS-GVO.

4. Berechtigte Interessen des Vereins

Berechtigte Interessen eines Vereins spielen immer dann eine Rolle, wenn der Verein bestimmte Daten verarbeiten möchte, diese Daten jedoch weder für die Erfüllung des Mitgliedsvertrags/Satzung benötigt werden noch eine Einwilligung der Vereinsmitglieder in die entsprechende Datenverarbeitung vorliegt. Die berechtigten Interessen können daher von Verein zu Verein ganz verschieden sein.

Formulierungsbeispiele für berechtigte Interessen (nicht abschließend):

- Der Musterverein übermittelt ohne vertragliche oder sonstige Verpflichtung auf freiwilliger Basis Mitgliederlisten an den Dachverband … (konkret benennen), um (Grund für das Interesse der Datenübermittlung nennen).
- Der Musterverein hat ein berechtigtes Interesse daran, bei dem Verkauf von Eintrittskarten für Fußballspiele Name, Vorname, Anschrift und Geburtsdatum von unbekannten Personen zu erheben, um zu überprüfen, ob gegen diese ein Stadionverbot ausgesprochen worden ist oder ob sie als gewaltbereit anzusehen sind.

5. Empfänger der personenbezogenen Daten

Übermittelt der Verein personenbezogene Daten seiner Mitglieder an Dritte, so hat der Verein hierüber zu informieren. Je nach Verarbeitungstätigkeit sind verschiedene Empfänger denkbar. Es ist daher je nach Verarbeitungstätigkeit darüber zu informieren, welche personenbezogenen Daten jeweils an welche Empfänger übermittelt werden.Das berechtigte Interesse des Vereins muss mit den Interessen der Betroffenen abgewogen warden Nur wenn deren Interessen nicht überwiegen, kann die Datenverarbeitungauf die berechtigten Interessen des Vereins gestützt werden. Das Widerspruchsrecht nach Art. 21 DS-GVO ist dann zu beachten.

Formulierungsbeispiele (nicht abschließend):

- Als Mitglied des Muster-Kreisverbandes … (Verband konkret benennen) ist der Verein verpflichtet, seine Mitglieder an den Verband zu melden. Übermittelt werden dabei Name, Adresse, … (Daten bitte konkret nennen). Bei Mitgliedern mit besonderen Aufgaben (z.B. Vorstandsmitglieder) wird zusätzlich die Bezeichnung ihrer Funktion im Verein übermittelt.
- Der Musterverein hat einen Kooperationsvertrag mit ... (Name des kooperierenden Unternehmens) abgeschlossen. Hierfür übermittelt er einmal im Jahr eine vollständige Liste der Mitglieder an ... (Name des kooperierenden Unternehmens), die den Namen, die Adresse und das Geburtsjahr enthält.
- Im Rahmen der Cloud-Mitgliederverwaltung werden die personenbezogenen Daten unserer Mitglieder bei … (Name des Cloud-Anbieters) gespeichert.

6. Drittlandstransfer

Besteht die Absicht des Vereins, personenbezogene Daten der Mitglieder an ein Drittland zu übermitteln (z.B. im Rahmen der Cloud-Mitgliederverwaltung erfolgt die Speicherung in den USA), so ist hierauf hinzuweisen.

7. Speicherdauer

Der Verein hat anzugeben, wie lange er welche Daten aufbewahrt. Grundsätzlich müssen personenbezogene Daten gelöscht werden, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Daher ist je nach Zweck der Erhebung die Speicherdauer gesondert anzugeben.

Formulierungsbeispiele (nicht abschließend):

- Die für die Daten Mitgliederverwaltung notwendigen Daten (bitte konkret nennen) werden 2 Jahre nach Beendigung der Vereinsmitgliedschaft gelöscht.
- Die für die Lohnabrechnung der im Verein beschäftigten Personen notwendigen Daten (bitte konkret nennen) werden nach 10 Jahren gelöscht (gesetzliche Aufbewahrungsfrist).
- Die für die die Beitragsverwaltung notwendigen Daten (bitte konkret nennen) werden nach 10 Jahren gelöscht.
- Die IP-Adressen, die beim Besuch der Vereinswebseite gespeichert werden, werden nach 30 Tagen gelöscht.
- Im Falle des Widerrufs der Einwilligung werden die Daten unverzüglich gelöscht.

8. Betroffenenrechte

Dem Vereinsmitglied steht ein Recht auf Auskunft (Art. 15 DS-GVO) sowie ein Recht auf Berichtigung (Art. 16 DS-GVO) oder Löschung (Art. 17 DS-GVO) oder auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) oder ein Recht auf Widerspruch gegen die Verarbeitung (Art. 21 DS-GVO) sowie ein Recht auf Datenübertragbarkeit (Art. 20 DS-GVO) zu.

Das Vereinsmitglied hat das Recht, seine datenschutzrechtliche Einwilligungserklärung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Dem Vereinsmitglied steht ferner ein Beschwerderecht bei einer Datenschutz-Aufsichtsbehörde zu.

9. Pflicht zur Bereitstellung der Daten

Üblicherweise erfolgt im Verein die Bereitstellung der Daten für den Vertragsabschluss (Mitgliedsvertrag/Satzung). Sollte darüber hinaus die Bereitstellung gesetzlich oder vertraglich vorgeschrieben sein, so ist hierauf – sowie zusätzlich auf die Folgen einer Nichtbereitstellung – hinzuweisen).

10. Automatisierte Entscheidungsfindung einschließlich Profiling

Ein Hinweis hierauf ist nur dann erforderlich, wenn eine automatisierte Entscheidungsfindung (einschließlich Profiling) gemäß Art. 22 Abs. 1 und Abs. 4 DS-GVO durch den Verein erfolgt.

Art. 22 DS-GVO findet jedoch nur dann Anwendung, wenn die die betroffene Person beschwerende Entscheidung auf eine automatisierte Verarbeitung zurückgeht (z.B. Profiling, Ablehnung Online-Kreditantrag). Eine automatisierte Entscheidungsfindung ist bei Vereinen allerdings kaum denkbar, sodass ein Hinweis hierauf nicht erfolgen muss.

Muster einer **Einwilligungserklärung** für die Veröffentlichung von Mitgliederdaten im Internet

Der Vereinsvorstand weist hiermit darauf hin, dass ausreichende technische Maßnahmen zur Gewährleistung des Datenschutzes getroffen wurden. Dennoch kann bei einer Veröffentlichung von personenbezogenen Mitgliederdaten im Internet ein umfassender Datenschutz nicht garantiert werden. Daher nimmt das Vereinsmitglied die Risiken für eine eventuelle Persönlichkeitsrechtsverletzung zur Kenntnis und ist sich bewusst, dass:

- die personenbezogenen Daten auch in Staaten abrufbar sind, die keine der Bundesrepublik Deutschland vergleichbaren Datenschutzbestimmungen kennen,
- die Vertraulichkeit, die Integrität (Unverletzlichkeit), die Authentizität (Echtheit) und die Verfügbarkeit der personenbezogenen Daten nicht garantiert ist.

Das Vereinsmitglied trifft die Entscheidung zur Veröffentlichung seiner Daten im Internet freiwillig und kann seine Einwilligung gegenüber dem Vereinsvorstand jederzeit widerrufen.

Erklärung

„Ich bestätige das Vorstehende zur Kenntnis genommen zu haben und willige ein, dass der Verein

.....
(Name des Vereins)

folgende Daten zu meiner Person:

Allgemeine Daten	Spezielle Daten von Funktionsträgern
Vorname	Anschrift
Zuname	Telefonnummer
Fotografien	Faxnummer
Sonstige Daten (z.B.: Leistungsergebnisse, Lizenzen, Mannschaftsgruppe u.ä.)	E-Mail-Adresse

wie angegeben auf folgender Internetseite des Vereins

.....
(Online-Dienst / Internet ; Zugangsadresse)

veröffentlichen darf."

Ort und Datum: Unterschrift:

....
(Bei Minderjährigen
Unterschrift eines Erziehungsberechtigten)

Verzeichnis von Verarbeitungstätigkeiten **Verantwortlicher** **gem. Artikel 30 Abs. 1 DSGVO**	Vorblatt

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Internet-Adresse

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Angaben zum Vertreter des Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)

* sofern gem. Artikel 37 DS-GVO benannt

Anrede Titel

Name, Vorname

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Verarbeitungstätigkeit: Benennung: _____	**lfd. Nr.:** _____
Datum der Einführung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a)	
Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b)	
Optional: Name des eingesetzten Verfahrens	
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ ☐ ☐
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)	☐ ☐ ☐ Besondere Kategorien personenbezogener Daten (Art. 9): ☐

Kategorien von Empfängern, gegenüber denen die personen-bezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)	☐ intern (Zugriffsberechtigte) Abteilung/ Funktion
	☐ extern Empfängerkategorie
	☐ Drittland oder internationale Organisation (Kategorie)
ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine inter-nationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt:
Nennung der konkreten Datenempfänger	☐ Drittland oder internationale Organisation (Name)
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)	

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO (Art. 30 Abs. 1 S. 2 lit. g) *Siehe TOM-Beschreibung in den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten“, Ziff. 6.7. und 6.8*

…… …… .....
Verantwortlicher Datum Unterschrift

Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO[1]

Hinweis:
Diese Formulierungshilfe ist nicht abschließend und bezieht sich in erster Linie auf die Fallgestaltung einer Auslagerung von klassischen IT-Dienstleistungen z. B. für die Lohnabrechnung oder Finanzbuchhaltung.
Je nach konkretem Anwendungsfall müssen gegebenenfalls weitere Inhalte hinzukommen, können solche weggelassen oder müssen modifiziert werden, um dem gegebenen Sachverhalt gerecht zu werden (z. B. bei Berufsgeheimnisträgern, bei Dienstleistungen zur Wartung, Datenlöschung oder -konvertierung, bei der externen Datenarchivierung).

Auftraggeber (Verantwortlicher):

Auftragnehmer (Auftragsverarbeiter):

---

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

(Gegenstand des Auftrags, konkrete Beschreibung der Dienstleistungen)

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäi- schen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Vorausset- zungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Stan- darddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags

Der Vertrag beginnt am ..... und endet am .....

[1] Diese Formulierungshilfe stellt keine Standardvertragsklauseln im Sinne von Art. 28 Abs. 8 DS-GVO dar.

oder

wird auf unbestimmte Zeit geschlossen. Kündigungsfrist ist .....

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

(nähere Beschreibung, ggf. Verweis auf Leistungsverzeichnis als Anlage etc.)

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen

technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:

(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragnehmer sind:

(Vorname, Name, Organisationseinheit, Telefon)

Für Weisung zu nutzende Kommunikationskanäle:

(genaue postalische Adresse/ E-Mail/ Telefonnummer)

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:
……..

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Ein-

holung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres folgendes vereinbart:

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

(z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.)

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb**.**

Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz Herr/Frau

---

(Vorname, Name, Organisationseinheit, Telefon)

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

oder

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

Sofern einschlägig:
Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

(Hinweis: Hier sind verschiedene Regelungsalternativen möglich. Die Parteien können ein absolutes Unterauftragsverbot vereinbaren, es kann aber auch ein Verbot mit Genehmigungsvorbehalt im Einzelfall geregelt werden. Auf letztere Möglichkeit bezieht sich der unten stehende Formulierungsvorschlag.)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in Anlage ..... mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

(Hier haben die Vertragsparteien einen Gestaltungsspielraum: Entweder werden dem Auftragnehmer allgemein Befugnisse eingeräumt, Subunternehmer zu beauftragen oder dies wird von einer Einzelgenehmigung abhängig gemacht. Einigt man sich auf eine allgemeine Befugnis des Auftragnehmers zur Beauftragung von Subunternehmern, ist jede Subbeauftragung vorher durch den Auftragnehmer dem Auftraggeber anzuzeigen. Der Auftraggeber hat dann von Gesetzeswegen ein Recht auf Einspruch gegen diese Änderung (Art. 28 Abs. 2). Das Recht des Auftraggebers zum Einspruch ist im Vertrag ausdrücklich zu erwähnen. Da das Gesetz die Folgen dieses Einspruchs nicht regelt, wird empfohlen, hierzu vertragliche Regelungen zu finden. Wird keine Regelung getroffen, ist die Bestellung des Unterauftragnehmers, gegen den Einspruch erhoben wurde, nicht möglich.)

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck

der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt:

……..

Das im Anhang …….. beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Das im Anhang ……. beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

Folgende Möglichkeiten für den Nachweis durch Zertifizierung bestehen:

> Die Bewertung des Risikos samt der Auswahl der geeigneten technischen und organisatorischen Maßnahmen des Auftragnehmers wurden am …… durch folgende unabhängige externe Stellen auditiert/zertifiziert gemäß den Regelungen nach Art. 42:
> ……
> Diese vollständigen Prüfunterlagen und Auditberichte können vom Auftraggeber jederzeit eingesehen werden.

Oder:

> Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen,

dem Auftraggeber auszuhändigen.

oder

wie folgt datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Vergütung

---

11. Haftung

Auf Art. 82 DS-GVO wird verwiesen.
Im Übrigen wird folgendes vereinbart:

---

12. Vertragsstrafe

Bei Verstoß des Auftragnehmers gegen die Regelungen dieses Vertrages, insbesondere zur Einhaltung des Datenschutzes, wird eine Vertragsstrafe von ..... Euro vereinbart.

13. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

10

Weitere Beispiele für mögliche Regelungen:

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Datum:

Unterschriften

Auftraggeber	Auftragnehmer