Auftrag zur Datenverarbeitung

zwischen

der durch die unterzeichnende/n Person/en vertretene gemeinnützige Organisation

- Verantwortlicher - nachstehend **Auftraggeber** genannt

und

Kreissportbund Stade e.V.

Am Schwingedeich 1

21680 Stade

vertreten durch den Vorstand

- Auftragsverarbeiter - nachstehend **Auftragnehmer** genannt

Inhalt

Auftragsverarbeitung (AV)

§ 1 Präambel

1) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers im Rahmen der Durchführung des zwischen den Parteien bestehenden Vertrages. Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer findet derzeit ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt..
2) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag. Diese Auftragsvereinbarung (Im Folgenden: „AV“ oder „Vereinbarung“) konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien bei der Umsetzung der Zusammenarbeit und findet auf sämtlichen Tätigkeiten Anwendung, die mit dem Vertragsverhältnis in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers mit personenbezogenen Daten des Auftraggebers in Berührung kommen.
3) Sofern in dieser Vereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird damit allgemein die Verwendung von personenbezogenen Daten verstanden. Eine Verwendung personenbezogener Daten umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung sowie das Anonymisieren, Pseudonymisieren, Verschlüsseln oder die sonstige Nutzung von Daten.
4) Diese Vereinbarung regelt die wechselseitigen datenschutzrechtlichen Verpflichtungen nach den Artt. 28 ff. DS-GVO zwischen dem Auftragnehmer und dem Auftraggeber.
5) Gegenstand dieser AV ergibt sich aus dem zwischen den Parteien vereinbarten **Nutzungsbedingungen über die Nutzung der „Digitalen Talentkarte“.** (im Folgenden: „Vertrag“ oder „Vertragsverhältnis“). Die Parteien sind sich einig, dass durch schriftliche Vereinbarung diese AV auch weiteren zwischen den Parteien geschlossenen Verträgen zugrunde gelegt werden kann, die von dem vorstehend benannten Lizenzauftrag noch nicht umfasst waren.

§ 2 Gegenstand und Dauer der AV

1) Inhaltlicher Geltungsbereich

   Gegenstand des Vertragsverhältnisses ist die Erbringung von Leistungen, wie sie in dem Vertrag zwischen den Parteien spezifiziert ist. Diese AV gilt für sämtliche Tätigkeiten im Zusammenhang mit diesem Vertragsverhältnis bei denen Beschäftigte und/oder gem. nachstehendem § 7 Subunternehmer des Auftragnehmers personenbezogene Daten des Auftraggebers verarbeiten.

2) Dauer der AV

   Die Dauer der AV richtet sich nach dem zwischen dem Auftragnehmer und dem Auftraggeber bestehenden Vertrag.

3) Anlagen zu dieser AV

   Die technischen und organisatorischen Maßnahmen gem. Art. 28 Abs. 3 lit. c, Art. 32 DS-GVO sind in der Anlage 1 geregelt.

§ 3 Art, Umfang und Zweck der vorgesehenen Verarbeitung der personenbezogenen Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art, Umfang und Zweck der vorgesehenen Verarbeitung von Daten:

1) Art der Daten

   Im Rahmen des Vertragsverhältnisses verarbeitet der Auftragnehmer folgende Kategorien von Daten des Auftraggebers:

☒ Vorname und Name der Nutzer der Digitalen Talentkarte
☒ Kommunikationsdaten (z.B. E-Mail und Telefonnummer)
☒ IP-Adresse
☒ Dateneingaben aus den Eingabefeldern des Formulars, insbesondere Informationen über Engagementpräferenzen und Talente.

2) Umfang der Datenverarbeitung

Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen und Nutzen der Daten für die jeweiligen Zwecke

3) Zweck der Datenverarbeitung

Zweck der Datenverarbeitung ist die Erfüllung des zwischen den Parteien geschlossenen Vertrages.

4) Kategorien der betroffenen Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☒ Auftraggeber
☒ Interessenten/Nutzer der Digitalen Talentkarte

5) Ort der Datenverarbeitung

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.

§ 4 Technisch-organisatorische Maßnahmen

1) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Die technisch-organisatorischen Maßnahmen des Auftragnehmers sind dem Vertrag als Anlage 1 beigefügt.
2) Zur Gewährleistung der Sicherheit und Vertraulichkeit der Daten hat der Auftragnehmer die technisch-organisatorischen Maßnahmen gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO, getroffen.
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.

§ 5 Berichtigung, Löschung und Sperrung von Daten

1) Die im Auftrag des Auftraggebers verarbeiteten personenbezogenen Daten darf der Auftragnehmer nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Wenn sich eine betroffene Person zu diesem Zweck direkt an den Auftragnehmer wendet, hat dieser ein solches Ersuchen unverzüglich an den Auftraggeber weiterzuleiten.

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

§ 6 Pflichten des Auftragnehmers

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

a) 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 den personenbezogenen Daten des Auftraggebers hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in dieser Vereinbarung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

b) Die Umsetzung und Einhaltung aller für diese Vereinbarung erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO.

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

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

e) 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.

f) 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.

g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieser Vereinbarung.

h) Der Auftragnehmer wird dem Auftraggeber über die technischen und organisatorischen Maßnahmen sowie Ereignisse, die für die Sicherheit oder Vertraulichkeit der Daten von Bedeutung sind, regelmäßig unterrichten. Störungen oder sonstige Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers wird er diesem unverzüglich mitteilen und das weitere Vorgehen mit ihm abstimmen.

§ 7 Einschaltung von Subunternehmern / Unterauftragsverhältnisse

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-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der 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.

2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) unter den Voraussetzungen des Absatzes 2 lit. b) dieses Abschnitts einsetzen.

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

Firma Unterauftragnehmer	**Anschrift/Land**	**Leistung**
Fly.io	2261 Market Street #4990 San Francisco, CA 94114	Hosting Website und digitale Talentkarte
Amazon Web Services, Inc.	410 Terry Avenue North Seattle WA 98109 United States	Versand von E-Mails
MongoDB Inc.	Building 2, Number 1 Ballsbridge Shellbourne Road Ballsbridge, D04 Y3X9 Dublin, Ireland	Speicherung von Daten in einer Datenbank

Die Sicherheitskonzepte der Unterauftragnehmer liegen dieser Vereinbarung als Anlage 2 bei.

b) Der Wechsel eines bestehenden Unterauftragnehmers und/oder die Auslagerung auf Unterauftragsnehmer ist zulässig, soweit:
   - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit (mindestens 14 Tage) vorab schriftlich oder in Textform anzeigt und
   - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich gegen die geplante Auslagerung Einspruch erhebt und
   - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

Erhebt der Auftraggeber Einspruch, obwohl dem Wechsel und/ oder der Auslagerung eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde liegt und ohne dass dem Einspruch des Auftraggebers ein berechtigtes Interesse an der Ablehnung des Unterauftragnehmers zugrunde liegt, kann der Auftragnehmer diese Vereinbarung und den zugehörigen Vertrag fristlos kündigen.

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.

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 Abs. 1 Satz 2 eingesetzt werden sollen.

5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 8 Kontrollrechte des Auftraggebers, Mitwirkungspflichten des Auftragnehmers

1) Der Auftraggeber hat das Recht, im Benehmen 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.

   Der Auftragnehmer hat das Recht, einen vom Auftraggeber zur Kontrolle benannten Dritten abzulehnen, wenn dieser Dritte nach Einschätzung des Auftragnehmers nicht hinreichend qualifiziert ist oder es sich um einen Wettbewerber des Auftragnehmers handelt. Sofern der Auftragnehmer einen Dritten aus den vorstehenden Gründen ablehnt, ist der Auftraggeber verpflichtet, einen anderen Dritten für die Prüfung zu benennen oder kann alternativ die Kontrolle selbst durchführen.
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.
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).

§ 9 Mitzuteilende Verstöße

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

   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

Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete besondere Arten personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) oder personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den

Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder personenbezogene Daten zu Bank- oder Kreditkartenkonten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers.

§ 10 Weisungsbefugnisse

1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
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.
3) Der Auftraggeber benennt dem Auftragnehmer im Erstellungsprozess der digitalen Talentkarte diejenigen Personen, die zur Erteilung von Weisungen an den Auftragnehmer berechtigt sind.

§ 11 Löschung und Rückgabe von personenbezogenen Daten

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.
2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Vertrages – 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.
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.

§ 12 Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

§ 13 Teilunwirksamkeit

Für den Fall, dass einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sind oder werden, oder für den Fall, dass diese Vereinbarung unbeabsichtigte Lücken enthält, wird dadurch die Wirksamkeit der übrigen Bestimmungen dieser Vereinbarung nicht berührt. Anstelle der unwirksamen, undurchführbaren oder fehlenden Bestimmung gilt eine solche wirksame und durchführbare Bestimmung als zwischen den Parteien vereinbart, wie sie die Parteien unter Berücksichtigung des wirtschaftlichen Zwecks dieser Vereinbarung vereinbart hätten, wenn ihnen

beim Abschluss dieser Vereinbarung die Unwirksamkeit, Undurchführbarkeit oder das Fehlen der betreffenden Bestimmung bewusst gewesen wäre. Die Parteien sind verpflichtet, eine solche Bestimmung in gebotener Form, jedoch zumindest schriftlich, zu bestätigen.

§ 14 Schlussbestimmungen

1) Für diesen Vertrag gilt deutsches Recht mit Ausnahme der Bestimmungen des internationalen Privatrechts.
2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform und eines ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Stade, den 26.09.2024

(Auftragnehmer)

Anlagen

Anlage 1: technisch-organisatorische Maßnahmen

Anlage 2: Sicherheitskonzepte Unterauftragnehmer

Anlage 1: Technisch-Organisatorische Maßnahmen (TOM)

1. Vertraulichkeit (Art. 32 I lit. b DSGVO)

a. Zutrittskontrolle

Es ist zu unterscheiden zwischen dem Gebäude, in dem der Auftragnehmer seine Räumlichkeiten hat und zwischen den Gebäuden der Rechenzentren der Subunternehmer, wo sich jegliche Server befinden.

In den Räumlichkeiten des Auftragnehmers befinden sich lediglich Unterlagen in Bezug auf die Organisation der Projekte sowie Backups von Dokumenten und E-Mailpostfächern.

Gebäude allgemein:
Personenbezogene Daten und Datenverarbeitungsgeräte (z.B. Speichermedien) werden in abschließbaren Räumen und/oder abschließbaren Schränken verwahrt. Bei Abwesenheit werden die verschließbaren Bereiche abgeschlossen. Hierbei werden alle relevanten Türen, Fenster, Schränke berücksichtigt.

Der schlüsselbasierte Zutritt ist nur den Mitarbeitenden und Vorstandsmitgliedern des Auftragnehmers möglich. Für Dritte sind die Räumlichkeiten, in denen Backups und Unterlagen aufbewahrt werden, nicht frei zugänglich.

Rechenzentrumsräume:
Kundendaten werden in Rechenzentren der Subunternehmen verarbeitet und gespeichert. Informationen zu deren Sicherheitsmaßnahmen sind in Anlage 2 beigefügt.

b. Zugangskontrolle

Daten werden auf verschlüsselten und/oder passwortgeschützten Systemen abgespeichert.

Es existieren interne Richtlinien zur Passwortkomplexität.

Handys sind mit einem sicheren Zugangscode geschützt. PCs und Laptops sind mit individuellen Benutzerkonten eingerichtet.

Zur Anmeldung wird ein Benutzername und ein Passwort abgefragt.

Auf genutzten Datenverarbeitungsgeräten ist eine aktuelle Virenschutz-Software installiert.

c. Zugriffskontrolle

Der Zugriff auf Backups ist nur Systemadministratoren möglich. Die Anzahl der Systemadministratoren ist auf das „Notwendigste“ reduziert.

Für Systemadministratoren besteht die Erfordernis einer Multi-Faktor-Authentifizierung.

Technischen Supportdienstleistern und sonstigen für Betrieb und Wartung notwendigen externen Dienstleistern ist der Zugriff auf Kundendaten nur erlaubt, wenn dies erforderlich ist. Der Zugriff auf Kundendaten ist auf Personen beschränkt, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen.

d. Pseudonymisierung (Art. 32 I lt. a DSGVO, Art. 25 I DSGVO)
Sofern personenbezogene Daten zum Zweck der Analyse von User-Verhalten gesammelt und verarbeitet werden, findet für diese Daten eine Pseudonymisierung statt.

2. Integrität (Art. 32 I lit. b DSGVO)

a. Weitergabekontrolle

Es findet grundsätzlich kein physischer Transport statt. Soweit dies erforderlich ist, werden Transportpersonal sowie -fahrzeuge sorgfältig ausgewählt.

Eine ggf. erforderliche Weitergabe von Daten erfolgt soweit möglich in anonymisierter Form. In diesem Fall wird dokumentiert, wer der Empfänger der Daten ist sowie wie mit diesen umzugehen ist und ggf. wann diese zu löschen ist.

b. Eingabekontrolle
Es bestehen Mechanismen zur Protokollierung der Eingabe, Änderung und Löschung von Daten. Entsprechende Berechtigungen werden anhand eines Berechtigungskonzepts vergeben.

3. Verfügbarkeitskontrolle (Art. 32 I lit. b DSGVO)
Bezüglich der Verfügbarkeit der Server der digitalen Talentkarte wird auf die TOM der Subunternehmer in Anlage 2 verwiesen.

Es gibt ein Konzept zur regelmäßigen Sicherung aller Daten des Auftragnehmers. Dieses wird regelmäßig überprüft. Die Datensicherung des Vereins erfolgt an einem geschützten Ort und ist vor unberechtigten Zugriffen geschützt.

Die in einzelne digitale Talentkarten eingegebenen Daten, welche durch den Auftragnehmer unmittelbar an den Auftraggeber weitergeleitet werden, sind von diesem Konzept nicht umfasst. Für die Sicherung ist der Auftraggeber selbst verantwortlich.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 I lit. d DSGVO; Art. 25 Abs. 1 DSGVO)
Es findet keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne die entsprechende Weisung des Auftraggebers statt.

Sämtliche Mitarbeiter, die für die Verarbeitung von personenbezogenen Daten verantwortlich sind, werden im Hinblick auf Datenschutz entsprechend sensibilisiert – auch im Hinblick auf das Weisungsrecht des Auftraggebers.

Eine Auseinandersetzung mit dem System sowie der Funktionsfähigkeit und eine Risikoabwägung findet regelmäßig statt.

Anlage 2: Sicherheitskonzepte Unterauftragnehmer

Die TOM der beauftragten Unterauftragnehmer stehen online beziehungsweise auf der Folgeseite in der aktuellen Fassung zur Verfügung:

MongoDB: https://www.mongodb.com/legal/data-processing-agreement

Amazon Web Services: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

Fly.io: siehe Folgeseite

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

1. Technical and organizational measures baseline Physical Access Controls

Data Processor shall take reasonable measures to prevent physical access, such as secured buildings, to prevent unauthorized persons from gaining access to personal data.

2. System Access Controls

Data Processor shall take reasonable measures to prevent personal data from being used without authorization. These controls shall vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or logging of access on several levels.

3. Data Access Controls

Data Processor shall take reasonable measures to provide that personal data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the personal data to which they have privilege of access; and, that personal data cannot be read, copied, modified or removed without authorization in the course of processing. The Data Processor shall take reasonable measures to implement an access policy under which access to its system environment, to personal data and other data by authorized personnel only.

4. Transmission Controls

Data Processor shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of personal data by means of data transmission facilities is envisaged so personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

5. Input Controls

Data Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom personal data has been entered into data processing systems, modified or removed. Data Processor shall take reasonable measures to ensure that (i) the personal data source is under the control of data exporter; and (ii) personal data integrated into

Data Processor's systems is managed by secured file transfer from the Data Processor and data subject.