Vereinbarung zur Auftragsverarbeitung

zwischen

Schulträger/Schule mit vollständiger Adresse und vertretungsberechtigte Personen

- *Verantwortlicher – nachfolgend Auftraggeber genannt*

und

Michael Butzke
handelnd unter mb-mediasports©
Sommerhalde 38
75015 Bretten

- *Auftragsverarbeiter - nachstehend* ***Auftragnehmer*** *genannt -*

Vereinbarung zur Auftragsverarbeitung

Da wir personenbezogene Daten in Ihrem Auftrag verarbeiten, liegt eine sogenannte Auftragsverarbeitung vor. Nach Artikel 28 der EU-Datenschutz-Grundverordnung (DSGVO) ist zwischen dem Verantwortlichen und dem Auftragsverarbeiter ein Auftragsverarbeitungsvertrag abzuschließen.

1. Gegenstand und Dauer der Vereinbarung

Gegenstand der mit diesem Auftragsverarbeitungsvertrages ist die Datenverarbeitung im Rahmen der „Motorischen Test NRW (MT1)“. Die Dauer des Vertrages richtet sich nach der Dauer der Datenverarbeitung. Sie beginnt mit Abschluss des Vertrages und Registrierung im jeweiligen Portal des Auftragnehmers durch den Auftraggeber. Die Laufzeit richtet sich nach dem zwischen den Parteien geschlossenen Leistungsvertrag.

2. Konkretisierung des Inhalts der Vereinbarung

2.1. Art und Zweck der vorgesehenen Verarbeitung von Daten

Zweck der Datenverarbeitung ist die Erfassung der Messdaten der Kinder, die an dem „Motorischen Test NRW (MT1)“ teilnehmen in pseudonymisierter Form, sowie die weitere Nutzung dieser Messdaten für wissenschaftliche Zwecke in anonymisierter Form.

2.2. Kategorien der von der Verarbeitung betroffenen Personen

Bei den von der Verarbeitung betroffenen Personen handelt es sich um Kinder, die die Schule des Verantwortlichen besuchen und auf freiwilliger Basis am „Motorischen Test 1 (MT1)“ teilnehmen.

2.3. Arten der von der Verarbeitung betroffenen personenbezogenen Daten

Es werden folgende Daten in pseudonymisierter Form durch den Auftragnehmer verarbeitet: Pseudonymisierungskennzeichen, Geschlecht, Schule, Klasse, Anschrift, Geburtsdatum, Größe, Gewicht, sportliche Ergebnisse mit jeweiligem Datum.

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. 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. Für Einzelheiten wird auf Anlage 1 zu diesem Vertrag verwiesen.

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 in der Anlage 1 zu diesem Vertrag festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten, Rechte Betroffener

4.1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern 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. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

Soweit vom Leistungsumfang umfasst, sind ein Löschkonzept, das Recht des Betroffenen auf Löschung, Berichtigung, Einschränkung der Verarbeitung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

4.2. Ist im Rahmen der vorgesehenen Bearbeitung (s. 2.1.) eine wissenschaftliche Nutzung vorgesehen, findet die Verarbeitung personenbezogener Daten entsprechend der gesetzlichen Grundlagen für die Verarbeitung von wissenschaftlichen Daten gem. Art.9 DS-GVO, Abs.2, lit. h und i, Art. 89, Abs. 1-4 und § 27 BDSG, Abs. 1, 2, 3, 4 statt.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

- Bestellung/Benennung eines Datenschutzbeauftragten (z.B. bDSB)
- Die Wahrung der Vertraulichkeit gemäß Art. 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.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 lit. c, 32 DS-GVO. Für Einzelheiten wird auf Anlage 1 zu diesem Vertrag verwiesen.
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- 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.
- 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.
- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen (i. S. d. der Anlage 1 zu diesem Vertrag), 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.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

6.1. Die vertraglich vereinbarten Leistungen werden durch Beschäftigte des Auftragnehmers und teilweise unter Einschaltung der in der **Anlage 2** genannten Subunternehmer durchgeführt. Der Auftraggeber stimmt der Unterbeauftragung dieser Subdienstleister zu. Der Auftragnehmer ist damit im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann.

6.2. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgt, stellt der Auftragnehmer sicher, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Dieser Vereinbarung (z. B. EU-Standarddatenschutzklausel) tritt der Auftraggeber hiermit bei. Der Auftragnehmer bleibt dem Auftraggeber gegenüber primär verantwortlich, dass die Subdienstleister in Drittstaaten ihre Pflichten gemäß diesem Vertrag erfüllen. Der Auftragnehmer hat zu diesem Zweck entsprechende abgeleitete Kontrollpflichten gegenüber den Subdienstleistern in Drittstaaten und kann hierfür die in diesem Vertrag beschriebenen Kontrollbefugnisse des Auftraggebers wahrnehmen. Der Auftraggeber bleibt verpflichtet, die Ausübung der Kontrollbefugnisse zu überwachen und kann jederzeit auch selbst diese Kontrolle gegenüber den Subdienstleistern unmittelbar in den Drittstaaten ausüben.

Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

6.3. Ein Subunternehmerverhältnis im Sinne dieser Bestimmung liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Aufraggeber genutzt werden. Nicht hierzu gehören ferner Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Entsorgung von Datenträgern und sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen.

7. Nachweis und Überprüfung

7.1. Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören. Der Auftraggeber wird dem Auftragnehmer die Kontrolle mindestens zwei Monate im Voraus ankündigen. Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit. Der Aufwand für den Auftragnehmer durch eine Inspektion ist grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

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 aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren soweit solche verfügbar sind.

7.4. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Im Übrigen erfolgt die Durchführung der Überprüfung auf Kosten des Auftraggebers.

8. Mitteilung bei Verstößen des Auftragnehmers/Anfragen und Rechte des Betroffenen

8.1. Der Auftragnehmer unterstützt den Auftraggeber im Falle von Verstößen des Auftragnehmers bei der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.
Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

8.2. Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisung ab.

9. Weisungsbefugnis des Auftraggebers

9.1. Die beschriebene Datenverarbeitung erfolgt ausschließlich auf Grundlage dieses Vertrags zum Datenschutz, den zwischen den Parteien geschlossenen und zu schließenden eingangs genannten Verträgen und nach dokumentierter Weisung des Verantwortlichen. Ausgenommen hiervon ist eine Datenverarbeitung auf Grundlage einer zwingenden rechtlichen Verpflichtung des Auftragnehmers, sowie die Datenverarbeitung zu wissenschaftlichen Zwecken. Im Falle einer zwingenden rechtlichen Verpflichtung des Auftragnehmers teilt der Auftragnehmer dem Auftraggeber diese zwingende rechtliche Verpflichtung mit, sofern das einschlägige Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die Weisungen werden anfänglich durch diese Vereinbarung festgelegt und können jederzeit vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelanweisung). Dies umfasst auch Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

9.2. Alle erteilten Weisungen werden sowohl vom Auftragnehmer als auch vom Auftraggeber unverzüglich dokumentiert und -sofern mündlich erfolgt- dem Verantwortlichen unverzüglich nach erfolgter Dokumentation mindestens in Textform zur Verfügung gestellt (Bestätigung). Der Auftragnehmer wird Datum, Uhrzeit und den Namen der Person, welche die mündliche Weisung erteilt hat, sowie den Grund, warum keine Weisung mindestens in Textform erfolgen konnte, dokumentieren.

9.3. 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.

10. Haftung

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.
Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

11. Löschung und Rückgabe von personenbezogenen Daten

11.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen hiervon sind Kopien, Duplikate und Sicherheitskopien, die zur Erfüllung der in der Leistungsvereinbarung und der Auftragsvereinbarung genannten Leistungen erforderlich sind sowie von Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Ist im Rahmen der vorgesehenen Bearbeitung (s. 2.1.) eine wissenschaftliche Nutzung vorgesehen, gilt Abs.4.2 dieser Vereinbarung.

11.2. 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, sofern nicht nach dem Unionsrecht oder dem Recht der BRD eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Gleiches gilt für Test- und Ausschussmaterial. Eine schriftliche Bestätigung der Löschung ist auf Anforderung vorzulegen. Ist im Rahmen der vorgesehenen Bearbeitung (s. 2.1.) eine wissenschaftliche Nutzung vorgesehen, gilt Abs.4.2 dieser Vereinbarung. Wählt der Auftraggeber die Rückgabe, kann der Auftragnehmer eine angemessene Vergütung verlangen.

11.3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Erbringung der Leistung 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.

11.4. Bei Rückgabe eines Gerätes, gleich aus welchem Grund, ist der Auftraggeber für die Löschung seiner auf dem Gerät befindlichen Daten selbst verantwortlich. Entsprechendes gilt für den Abbau von kundeneigenen, nicht dem Service unterliegenden Teilen vor dem Austausch von Geräten oder Geräteteilen.

12. Sonstiges

12.1. Die Vereinbarung beginnt mit dem Abschluss durch den Kunden. Sie endet mit Ende des letzten Vertrages unter der jeweiligen Kundennummer. Sollte eine Auftragsverarbeitung noch nach Beendigung dieses Vertrages stattfinden, gelten die Regelungen dieser Vereinbarungen bis zum tatsächlichen Ende der Verarbeitung.

12.2. mb-mediasports© kann die Vereinbarung nach billigem Ermessen mit angemessener Ankündigungsfrist ändern. Es gilt Ziffer 8. AGB.

12.3. Ergänzend gelten die AGB des Auftragnehmers. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zur Auftragsverarbeitung den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarungen im Übrigen nicht.

12.4. Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand für sämtliche sich aus der Vereinbarung ergebenen Streitigkeiten ist das für Bretten zuständige Amtsgericht/ Landgericht.

Kommune (Stempel)	mb-mediasports©
	
für den Auftraggeber	für den Auftragnehmer
Name:	Name: Michael Butzke
Funktion:	Funktion: Geschäftsführer

Anlagen:
Anlage 1: Technisch-organisatorische Maßnahmen
Anlage 2: Unterauftragnehmer

Anlage 1 zur Vereinbarung zur Auftragsverarbeitung - Technische und Organisatorische Sicherheitsmaßnahmen gemäß Art 32 DSGVO

Version 1.0 (Strato AG)

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

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen Datenverarbeitungsanlagen untergebracht sind.
Festlegung von Sicherheitsbereichen

- Realisierung eines wirksamen Zutrittsschutzes
- Protokollierung des Zutritts
- Festlegung Zutrittsberechtigter Personen
- Verwaltung von personengebundenen Zutrittsberechtigungen
- Begleitung von Fremdpersonal
- Überwachung der Räume

1.2 Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

- Festlegung des Schutzbedarfs
- Zugangsschutz
- Umsetzung sicherer Zugangsverfahren, starke Authentisierung
- Umsetzung einfacher Authentisierung per Username Passwort
- Protokollierung des Zugangs
- Monitoring bei kritischen IT-Systemen
- Gesicherte (verschlüsselte) Übertragung von Authentisierungsgeheimnissen
- Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
- Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)
- Festlegung befugter Personen
- Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen
- Automatische Zugangssperre und Manuelle Zugangssperre

1.3 Zugriffskontrolle

Es kann nur auf die Daten zugegriffen, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

- Erstellen eines Berechtigungskonzepts
- Umsetzung von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
- Vermeidung der Konzentration von Funktionen

1.4 Verwendungszweckkontrolle

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

- Datensparsamkeit im Umgang mit personenbezogenen Daten
- Getrennte Verarbeitung verschiedener Datensätze
- Regelmäßige Verwendungszweckkontrolle und Löschung
- Trennung von Test- und Entwicklungsumgebung

1.5 datenschutzfreundliche Voreinstellungen

- Sofern Daten zur Erreichung des Verwendungszwecks nicht erforderlich sind, werden die technischen Voreinstellungen so festgelegt, dass Daten nur durch eine Aktion der Betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen
- Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland
- Protokollierung von Übermittlungen gemäß Protokollierungskonzept
- Sichere Datenübertragung zwischen Server und Client
- Sicherung der Übertragung im Backend
- Sichere Übertragung zu externen Systemen
- Risikominimierung durch Netzseparierung
- Implementation von Sicherheitsgateways an den Netzübergabepunkten
- Härtung der Backendsysteme
- Beschreibung der Schnittstellen
- Umsetzung einer Maschine-Maschine-Authentisierung
- Sichere Ablage von Daten, inkl. Backups
- Gesicherte Speicherung auf mobilen Datenträgern
- Einführung eines Prozesses zur Datenträgerverwaltungen
- Prozess zur Sammlung und Entsorgung
- Datenschutzgerechter Lösch- und Zerstörungsverfahren
- Führung von Löschprotokollen

2.2 Eingabekontrolle

Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingaben
- Dokumentation der Eingabeberechtigungen

3. Verfügbarkeit, Belastbarkeit, Desaster Recovery

3.1 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Brandschutz
- Redundanz der Primärtechnik
- Redundanz der Stromversorgung
- Redundanz der Kommunikationsverbindungen
- Monitoring
- Resourcenplanung und Bereitstellung
- Abwehr von systembelastendem Missbrauch
- Datensicherungskonzepte und Umsetzung
- Regelmäßige Prüfung der Notfalleinrichtungen

3.2 Desaster Recovery – Rasche Wiederherstellung nach Zwischenfall Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

- Notfallplan
- Datensicherungskonzepte und Umsetzung

4. Datenschutzorganisation

- Festlegung von Verantwortlichkeiten
- Umsetzung und Kontrolle geeigneter Prozesse
- Melde- und Freigabeprozess
- Umsetzung von Schulungsmaßnahmen
- Verpflichtung auf Vertraulichkeit
- Regelungen zur internen Aufgabenverteilung

• Beachtung von Funktionstrennung und –zuordnung
• Einführung einer geeigneten Vertreterregelung

5. Auftragskontrolle
Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
• Auswahl weiterer Auftragnehmer nach geeigneten Garantien
• Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern
• Abschluss einer Vereinbarung zur Auftragsverarbeitung mit STRATO

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)
• Informationssicherheitsmanagement nach ISO 27001
• Prozess zur Evaluation der Technischen und Organisatorischen Maßnahmen
• Prozess Sicherheitsvorfall-Management
• Durchführung von technischen Überprüfungen

Anlage 2: Unterauftragnehmer

Strato AG	Pascalstraße 10 10587 Berlin	Internet- und IT-Infrastruktur-Dienstleister, Deutschland Wir setzen Server und Serverservices der Strato AG ein. Die Rechenzentren der Strato AG sind der physikalische Speicherort der im Rahmen der Auftragsverarbeitung verarbeiteten Daten und befinden sich ausschließlich in Deutschland.
Godaddy Inc.	14455 North Hayden Road, Suite 219, Scottsdale, AZ 85260	Internet-Service-Provider, USA Wir nutzen ergänzende Leistungen von GoDaddy Inc. – und zwar ausschließlich Domainname- und Mailserverservices. Die Webadresse/URL „motoriktest.eu“ wird aus wirtschaftlichen Gründen bei diesem Domainregistrar verwaltet. Sollten Sie emailbezogene Dienste im Rahmen der Auftragsverarbeitung durch die eingesetzte Software nutzen, bedienen wir uns u.a. Mailservern dieses Internetdiensteanbieters.
Microsoft Corporation	One Microsoft Way Redmond, WA 98052-6399	Internet- und IT-Infrastruktur-Dienstleister, USA Sollten Sie im Rahmen der Nutzung der Software statistische Auswertungen direkt in der Webanwendung nutzen bzw. als Leistung beauftragt haben, setzen wir u.a. Cloudservices ein. Es handelt sich dabei um die Software „PowerBi©“.