

## **Vereinbarung zur Auftragsverarbeitung**

Zwischen

**JUGEND GRÜNDET**

**Steinbeis - Innovationszentrum Unternehmensentwicklung**

**an der Hochschule Pforzheim**

Blücherstraße 32

75177 Pforzheim

**Zentrale :**

Steinbeis Innovation gGmbH

Willi-Bleicher-Straße 19

70174 Stuttgart

(Auftragnehmerin)

und

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

(Auftraggeber)

werden folgende Regelungen zu Datenschutz und Datensicherheit

in Auftragsverhältnissen vereinbart:

## **§ 1 Präambel**

Um die Rechte und Pflichten aus dem Auftragsdatenverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtungen zu konkretisieren, schließen die Vertragsparteien nachfolgende Vereinbarung.

## **§ 2 Gegenstand des Auftrags, Art und Zweck der Vereinbarung**

Der Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten im Zuge der Teilnahme von Schülerinnen und Schülern der Auftraggeberin am bundesweiten Online-Wettbewerb JUGEND GRÜNDET.

## **§ 3 Art der personenbezogenen Daten, Kategorien betroffener Personen**

Folgende Daten der Schülerinnen und Schüler werden im Rahmen der einfachen Teilnahme an JUGEND GRÜNDET verarbeitet:

E-Mail-Adresse, Passwort, Geschlecht, Vor- und Nachname, Land, Postleitzahl, Name der Schule, Schulort (PLZ), U16 oder Ü16. Teamname, Team-ID, Wettbewerbsbeiträge, Bepunktung.

Sollten die Schülerinnen und Schüler sich für ein Pitch Event oder das Bundesfinale qualifizieren, werden darüber hinaus weitere personenbezogene Daten verarbeitet. Dafür wird dann jeweils individuell von jedem Betroffenen eine gesonderte Einwilligung in die Datenverarbeitung von der Auftragnehmerin eingeholt.

## **§ 4 Dauer des Auftrags**

Der Vertrag

- beginnt am 01. September \_\_\_\_\_ und endet am 31. Juli des Folgejahres.

oder

- beginnt am 01. September 20\_\_ und wird auf unbestimmte Zeit geschlossen.

Die Kündigung ist mit einer Frist von vier Wochen zum 31. Juli eines jeden Jahres möglich.

Unabhängig davon kann der Auftraggeber den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß der Auftragnehmerin gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, die Auftragnehmerin eine Weisung des Auftraggebers nicht ausführen kann oder will oder die Auftragnehmerin 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.

## **§ 5 Verantwortlichkeiten und Weisungen**

- (1) Der Auftraggeber ist grundsätzlich für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an die Auftragnehmerin sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Eine Einwilligung in die Datenverarbeitung wird zusätzlich von den Betroffenen individuell bei der Registrierung eingefordert. Sofern die Betroffenen Unter-16-Jahre alt sind, wird darüber hinaus die Einwilligung der Erziehungsberechtigten abgefragt. Die Auftragnehmerin verwendet die Daten für keine anderen Zwecke als in dieser Auftragsverarbeitungsvereinbarung festgelegt.
- (2) Primär weisungsbefugt im Rahmen dieses Auftragsvertrags sind die Betroffenen selbst. Im Falle einer Weisung durch einen U-16-Betroffenen wird die Einwilligung der Erziehungsberechtigten abgefragt. Im Falle einer Weisung durch den Auftraggeber wird vor der Durchführung die Einwilligung der Betroffenen und ggf. der Erziehungsberechtigten abgefragt. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist die Auftragnehmerin berechtigt, die Durchführung der Weisung auszusetzen.

- (3) Die Auftragnehmerin verarbeitet personenbezogene Daten ausschließlich im Sinne dieser Auftragsverarbeitung, es sei denn es besteht eine anderweitige gesetzliche Verpflichtung. Im Falle einer anderweitigen Verpflichtung teilt die Auftragnehmerin dem Auftraggeber vor der Verarbeitung unverzüglich die entsprechenden rechtlichen Anforderungen 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).
- (4) Auskünfte über personenbezogene Daten der Betroffenen, die durch den Auftraggeber angefragt werden, darf die Auftragnehmerin nur nach vorheriger schriftlicher Zustimmung durch die Betroffenen erteilen.
- (5) Im Folgenden werden die weisungsberechtigten Personen beim Auftraggeber und die Weisungsempfänger bei der Auftragnehmerin genannt. 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.

Weisungsberechtigte Person des Auftraggebers ist die Schulleitung.

Weisungsempfängerin bei der Auftragnehmerin ist die Datenschutzbeauftragte, zu erreichen über [datenschutz@szue.de](mailto:datenschutz@szue.de).

## **§ 6 Vertraulichkeit**

Der Auftragnehmerin setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß der jeweils aktuell geltenden gesetzlichen Bestimmungen des BDSG und der DS-GVO auf die Vertraulichkeit verpflichtet worden sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Auftragnehmerin und jede der Auftragnehmerin 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.

## **§ 7**

### **Datensicherheit**

- (1) Die Vertragsparteien vereinbaren die in dem Anhang 1 „Technische und organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. 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 der Datenschutzgesetze und –Verordnungen zu berücksichtigen.
- (2) Anhang 1 ist Bestandteil dieser Vereinbarung.
- (3) Die Auftragnehmerin beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Sie gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der Auftragnehmerin gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

## **§ 8**

### **Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)**

- (1) Als Subunternehmer im Sinne dieser Regelung sind weitere Auftragsverarbeiter zu verstehen, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die die Auftragnehmerin z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen und Reinigung in Anspruch nimmt. Der Einsatz von Subunternehmern ist zulässig. Die Auftragnehmerin 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.

- (3) Mit dem Subunternehmer ist eine dem Datenschutzrecht entsprechende Auftragsverarbeitungsvereinbarung abzuschließen.
- (4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller gesetzlichen Voraussetzungen für eine Unterbeauftragung gestattet. Die aktuell beauftragten Subunternehmer sind in der Anlage 2 zu diesem Vertrag aufgelistet.
- (5) Jede Verlagerung der Datenverarbeitung in ein Drittland bedarf der vorherigen dokumentierten Weisung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 – 49 DS-GVO erfüllt sind.

## **§ 9 Betroffenenrechte**

- (1) Die Auftragnehmerin ist verpflichtet, den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, den Pflichten zur Beantwortung von Anträgen auf Wahrung der in Art. 12 bis 22 DS-GVO genannten Rechte der betroffenen Personen nachzukommen.
- (2) Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit besitzt, stellt die Auftragnehmerin sicher, dass der Auftraggeber die im Verantwortungsbereich der Auftragnehmerin verarbeiteten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format erhalten kann.
- (3) Im Falle, dass die Betroffenen nicht selbst gegenüber der Auftragnehmerin in die Datenverarbeitung eingewilligt haben, darf die Auftragnehmerin personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers herausgeben, berichtigen, löschen oder deren Verarbeitung einschränken. Andernfalls gilt § 5 II dieses Vertrages zur Auftragsverarbeitung entsprechend.

## **§ 10 Pflichten der Auftragnehmerin**

Die Auftragnehmerin hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gem. Art. 28 bis 36 DS-GVO. Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Datenschutzbeauftragte:

Beim Auftragnehmer in der Zentrale ist als Beauftragter für den Datenschutz Herr Alexander Stückler, [datenschutz@steinbeis.de](mailto:datenschutz@steinbeis.de) bestellt. Darüber hinaus sind die Ansprechpartner konkret für diese Auftragsverarbeitung über [datenschutz@szue.de](mailto:datenschutz@szue.de), Tel. 07231-42446-0 zu erreichen.

(2) Datensicherheit:

Die Auftragnehmerin unterstützt den Auftraggeber bei der Einhaltung der in Art. 32 – 36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorheriger Konsultationen. Hierzu gehören insbesondere:

- 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.
- Die Verpflichtung, den Auftraggeber unverzüglich zu informieren, wenn ihr eine Verletzung des Schutzes personenbezogener Daten bekannt wird.
- Die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflichten gegenüber den Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
- Die Unterstützung des Auftraggebers für dessen Datenschutz-Folgeabschätzung.
- Die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

## **§ 11 Kontrollrechte des Auftraggebers**

Die Auftragnehmerin verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle im schriftlichen Verfahren erforderlich sind.

## **§ 12 Haftung**

Soweit der Auftraggeber zum Schadenersatz wegen einer unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen des Auftragsverhältnisses gegenüber der betroffenen Person verpflichtet ist, bleibt ihm der Rückgriff bei der Auftragnehmerin vorbehalten, wenn die Auftragnehmerin gegen die Pflichten aus diesem Vertrag oder aus BDSG, DS-GVO und sonstigen Vorschriften über Datenschutz schuldhaft verstoßen hat oder gegen die ausdrückliche Weisung des Auftraggebers gehandelt hat.

## **§ 13 Datenlöschungen**

- (1) Die Löschung der Wettbewerbsdatenbank erfolgt regelmäßig nach Ende des jeweiligen Wettbewerbsjahres.
- (2) Die Auftragnehmerin löscht spätestens nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten der Betroffenen, sofern nicht nach einer gesetzlichen Norm eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.
- (3) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch die Auftragnehmerin entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

## § 14 Schlussbestimmungen

- (1) Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrere Regelungen werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine solche Regelung ersetzen, die der unwirksamen Regelung wirtschaftlich und datenschutzrechtlich am ehesten entspricht.
- (2) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
- (3) Die folgenden Anhänge sind integraler Bestandteil dieser Vereinbarung:  
Anlage 1: Technische und organisatorische Maßnahmen  
Anlage 2: Subunternehmer

\_\_\_\_\_, den ..... Pforzheim, den 1. September \_\_\_\_\_

*F. Metzba*

.....  
Im Namen des Auftraggebers

.....  
Franziska Metzbaur  
Projektleitung  
JUGEND GRÜNDET

## **Anlage 1**

### **Technische und organisatorische Maßnahmen**

#### **(1) Allgemeine Angaben**

- **Angaben zum Unternehmen des Auftragnehmers**

#### **JUGEND GRÜNDET**

Steinbeis - Innovationszentrum Unternehmensentwicklung

an der Hochschule Pforzheim

Blücherstraße 32

75177 Pforzheim

Zentrale :

Steinbeis Innovation gGmbH

Willi-Bleicher-Straße 19

70174 Stuttgart

- Ansprechpartner bei der Auftragnehmerin zu erreichen über [datenschutz@szue.de](mailto:datenschutz@szue.de)
- Datenschutzbeauftragter beim Auftragnehmer

Bei der Auftragnehmerin in der Zentrale ist als Beauftragter für den Datenschutz Herr Alexander Stückler, [datenschutz@steinbeis.de](mailto:datenschutz@steinbeis.de) bestellt. Darüber hinaus sind die Ansprechpartner konkret für diese Auftragsverarbeitung über [datenschutz@szue.de](mailto:datenschutz@szue.de), Tel. 07231-42446-0 zu erreichen.

- Ort der Datenverarbeitung

Die Daten werden im Inland, in einem Mitgliedsstaat der EU oder in einem anderen Vertragsstaat des Abkommens über den EWR verarbeitet oder genutzt. Kundendaten werden nur dann durch einen Unterauftragnehmer außerhalb der EU/EWR verarbeitet, wenn durch den Abschluss eines EU-Standardvertrages das angemessene Datenschutzniveau hergestellt worden ist.

## **(2) Technische und organisatorische Maßnahmen:**

Die Auftragnehmerin gewährleistet laufend die Umsetzung und Befolgung folgender IT-Sicherheitsmaßnahmen und –anforderungen:

### **(2.1) Zutrittskontrolle:**

Technische und organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten, gewährleistet der Auftragnehmer wie folgt:

- (x) Festlegung befugter Personen inklusive Umfang der jeweiligen Befugnisse
- (x) Ausgabe von Zutrittsberechtigungsausweisen
- (x) Existenz von Regelungen für Unternehmensexterne
- (x) Umsetzung einer Schlüsselregelung
- (x) Protokollierung der ein- und ausgehenden Personen
- (x) Physische Maßnahmen vorhanden und regelmäßig überprüft:
- (x) Gesicherter Eingang (z. B. abschließbare Türen, Ausweisleser)
- (x) Einbruchhemmende Fenster
- (x) Gerätesicherung gegen Diebstahl, Manipulation oder Beschädigung
- (x) Unterteilung in verschiedene Sicherheitszonen

### **(2.2) Zugangskontrolle:**

Die Auftragnehmerin trifft folgende Maßnahmen zur Zugangskontrolle:

- (x) Konzeption und Implementierung eines Berechtigungskonzepts
- (x) Berechtigungskonzept für Endgeräte (Rechner)
- (x) Berechtigungskonzept für Software/Systeme
- (x) Identifikation und Berechtigungsprüfung eines Benutzers
- (x) Implementierung eines Systems zur Verwaltung von Benutzeridentitäten

- (x) Monitoring der Zugangsversuche mit Reaktion auf Sicherheitsvorfälle
- (x) Festlegung und Kontrolle der Zugangsbefugnisse
- (x) Authentisierungsverfahren dem Schutzbedarf der Informationen entsprechend (Klassifizierung)
- (x) Verschlüsselung
- (x) Angemessener Passwortschutz (Verhaltensregeln, verschlüsselte Archive)
- (x) Spezielle Sicherheitssoftware (z. B. Anti-Malware, VPN oder Firewall)
- (x) Existenz von Regelungen für Unternehmensexterne
- (x) Zugangsfunktion über Token

### **(2.3) Zugriffskontrolle:**

Der Zugriff auf Datenverarbeitungssysteme bei der Auftragnehmerin erfolgt anhand:

- (x) Berechtigungs- und Rollenkonzept für Applikationen
- (x) Umsetzung von Regelungen zur Zugriffs- und Benutzerberechtigung
- (x) Überprüfung der Berechtigungen
- (x) Funktionsbegrenzung (funktional/zeitlich)
- (x) Zugriffsbeschränkungen (gemäß „Need-to-Know“ und „Least Privilege“)
- (x) Verschlüsselte Speicherung der Daten
- (x) Protokollierung
- (x) Protokollierung des lesenden Zugriffs
- (x) Protokollierung des schreibenden Zugriffs
- (x) Protokollierung von unberechtigten Zugriffsversuchen
- (x) Regelmäßige Auswertung
- (x) Anlassbezogene Auswertung

- (x) Umsetzung von Regelungen zur Löschung von Daten
- (x) Umsetzung von Regelungen zum Umgang mit elektronischen Speichermedien
- (x) Umsetzung von Regelungen zur Entsorgung von Speichermedien
- (x) Integritätskontrolle

#### **(2.4) Weitergabekontrolle:**

Beschreibung der Weitergabe bei der Auftragnehmerin: Grundsätzlich verbleiben personenbezogene Daten innerhalb der Datenverarbeitungssysteme. Zur Datenübertragung zwischen den Applikationen und Servern werden State-of-the-Art Verschlüsselungsverfahren verwendet (SSL-basiert: FreeBSD, SSH, HTTPS).

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- (x) Vollständige Dokumentation der Formen der Weitergabe von Daten (z. B. Ausdruck, Datenträger, automatisierte Übermittlung)
- (x) Auflistung der Empfänger der Daten
- (x) Dokumentationen der Schnittstellen und der Abruf- und Übermittlungsprogramme
- (x) Für Ausdrücke und Datenträger: Durchführung von regelmäßigen Bestandskontrollen
- (x) Sicherungen des Transports (z. B. Behälter, Verschlüsselung von Speichermedien, Übergabeprotokolle)
- (x) Für elektronische Weitergaben: Verschlüsselung der Datenübermittlung, Durchführung von Protokollierungen der Datenweitergabe oder Übermittlung, Durchführung von Plausibilitäts-, Vollständigkeits- und Richtigkeitsprüfungen, Maßnahmen zur Verhinderung von unkontrollierten Informationsabflüssen (z. B. Deaktivierung der USB-Schnittstellen, regelmäßige Kontrolle der zulässigen Empfänger, technische Beschränkung auf zulässige Empfänger)

### **(2.5) Eingabekontrolle:**

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

- (x) Protokollierung der Eingaben und Überprüfung der Protokolle
- (x) Organisatorisch festgelegte Zuständigkeiten für die Eingabe

### **(2.6) Auftragskontrolle:**

Es muss dafür Sorge getragen werden, dass die Daten nur gemäß dem ursprünglichen Zweck und damit entsprechend seinem Auftrag verwendet werden.

- (x) Strikte Einhaltung der im vorliegenden Auftragsdatenverarbeitungs-Vertrag festgeschriebenen Vereinbarungen
- (x) Konzept dahingehend, wie die regelmäßige Kontrolle des Auftragsprozesses erfolgt (z. B. Vorlage von Self-Assessments, Vorlage der Verträge mit Unterauftragnehmern, Durchführung von Kontrollen bei Subunternehmern durch den Auftragnehmer)

### **(2.7) Verfügbarkeitskontrolle:**

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

- (x) Regelmäßige Kontrolle des Systemzustands (Monitoring)
- (x) Backup- und Wiederanlaufkonzept (regelmäßige Datensicherungen)
- (x) Datenarchivierungskonzept
- (x) Vorhandensein eines Notfallkonzepts (Business Continuity, Disaster Recovery)
- (x) Regelmäßige Tests des Notfallkonzepts
- (x) Vorhandensein von redundanten IT-Systemen (z. B. Server, Speicher)
- (x) Funktionsfähige physische Schutzeinrichtungen (Brandschutz, Energie, Klima)

### **(2.8) Trennungskontrolle:**

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind getrennt zu verarbeiten.

- (x) Dokumentation der Funktionstrennung
- (x) Vorhandensein von Richtlinien und Arbeitsanweisungen
- (x) Vorhandensein von Verfahrensdokumentationen
- (x) Physische Trennung
- (x) Trennung auf Systemebene
- (x) Trennung auf Datenebene
- (x) Trennung von Produktiv- und Testsystemen
- (x) Regelmäßige Prüfung der bestimmungsgemäßen Nutzung der Informationen und IT-Systeme

### **(2.9) Darüber hinausgehende Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit:**

- (x) Schriftlich fixierte Regelungen der Verantwortlichkeiten für Datenschutz
- (x) Schriftlich fixierte Regelungen der Verantwortlichkeiten für Informationssicherheit
- (x) Existenz eines angemessenen Informationssicherheitsmanagements
- (x) Existenz eines angemessenen Incident Managements
- (x) Durchführung einer Informationsklassifizierung
- (x) Regelmäßige Aufklärung und Sensibilisierung der Mitarbeitenden und Führungskräfte



## Anlage 2 Genehmigte Subunternehmer

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

- **Serverhoster:**

bringe Informationstechnik GmbH  
Zur Seeplatte 12  
76228 Karlsruhe  
<https://bringe.com/home#about>