AUFTRAGSVERARBEITUNGSVERTRAG NACH ART. 28 DSGVO

PRÄAMBEL

Der Auftragnehmer wird hinsichtlich der Bereitstellung der *KURABU*-Online-Plattform („**Plattform**“) auf der Basis des auf den „Allgemeine Geschäftsbedingungen für SaaS Leistungen von *KURABU*“ beruhenden Vertrags („**Hauptvertrag**“) für den Auftraggeber als Auftragsverarbeiter tätig und verarbeitet personenbezogene Daten in diesem Zusammenhang ausschließlich im Auftrag und nach Weisung des Auftraggebers. Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten, schließen die Parteien die vorliegende Auftragsverarbeitungsvereinbarung.

1. GEGENSTAND, DAUER UND SPEZIFIZIERUNG DER AUFTRAGSVERARBEITUNG

1.1 Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben: Der Auftragnehmer stellt dem Auftraggeber ein Web-Interface, eine Web-Applikation sowie eine Mobile-App (iOS & Android) zur Nutzung der Plattform durch den Auftraggeber und dessen Mitglieder bereit. Dazu zählt insbesondere die Bereitstellung folgender Funktionen und Teildienste:

- Rollen- & Rechteverwaltung, Anlage und Verwaltung von Administratoren und sonstigen Nutzern
- Mitgliederverwaltung, Rechnungstellung,
- Protokoll- und Anwesenheitslisten,
- Erstellung, Versendung und Empfang von E-Mail- und Push-Nachrichten (standardisiert und personalisiert).

1.2 Die Dauer der Datenverarbeitung ergibt sich aus dem Hauptvertrag.

1.3 Verarbeitete Datenkategorien:

- Titel, Name, Vorname, Position (optional), ggf. Teamleiterstatus,
- Geburtsdatum, Geschlecht, Profil-Bild
- Anschrift, Telefonnummer, E-Mail-Adresse, Rechnungsanschrift,
- Vereinszugehörigkeit (Mitglied seit/bis),

- Bankdaten/bevorzugte Zahlungsmethode (Banküberweisung oder SEPA – Mandats-ID, Datum der Mandatsunterschrift, Kontoinhaber, IBAN, BIC, Bankname)

1.4 Kategorien betroffener Personen:

- Vereinsleitung,
- Betreuer/Teamleiter,
- Vereinsmitglieder.

2. ORT DER DATENVERARBEITUNG

Die vertraglich vereinbarte Verarbeitung durch den Auftragnehmer selbst findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Der Auftragnehmer setzt für die vereinbarte Verarbeitung allerdings auch Unterauftragnehmer ein, die - in dem in der Anlage 1 beschriebenen Umfang und unter Wahrung der besonderen Voraussetzungen für die Übermittlung in ein Drittland nach Art. 44 ff. DSGVO - Verarbeitungen in einem Drittland (den USA) durchführen. Der Auftraggeber stimmt dieser Verarbeitung durch die Unterauftragnehmer des Auftragnehmers hiermit zu. Jede weitere Verlagerung von Verarbeitungstätigkeiten in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen für die Übermittlung in ein Drittland nach Art. 44 ff. DSGVO erfüllt sind.

3. LAUFZEIT, KÜNDIGUNG UND GÜLTIGKEIT

3.1 Dieser Vertrag (Auftragsverarbeitungsvereinbarung) gilt für die gesamte Dauer der Nutzung der Plattform durch den Auftraggeber.

3.2 Der Auftraggeber kann diesen Vertrag ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellen einen schweren Verstoß dar.

4. PFLICHTEN DES AUFTRAGNEHMERS

4.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und auf dokumentierte Weisungen des Auftraggebers verarbeiten, es sei denn, es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn es der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

4.2 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.

4.3 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

4.4 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

4.5 Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

4.6 Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Die vertragsgegenständlichen Daten sind nach Auftragsende nach Wahl des Auftraggebers entweder zurückzugeben oder zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht.

4.7 Der Auftraggeber legt den oder die Weisungsberechtigten fest. Der Auftragnehmer legt Weisungsempfänger fest. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und in schriftlicher oder elektronischer Form die Nachfolger oder Vertreter mitzuteilen. Sofern der Auftraggeber dem Auftragnehmer gegenüber keinen Weisungsberechtigten benennt, gelten diejenigen, die die *KURABU* Plattform anlegen als weisungsberechtigt.

5. UNTERSTÜTZUNGSPFLICHTEN DES AUFTRAGNEHMERS

5.1 Der Auftragnehmer ergreift die in Anlage 2 beschriebenen technische und organisatorische Maßnahmen (Art. 32 DSGVO).

5.2 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und den technischen Entwicklungen. So kann der Auftragnehmer alternative Maßnahmen ergreifen, die eine angemessene Sicherheit der Daten gewährleisten. Das Sicherheitsniveau muss jederzeit mindestens dem Sicherheitsniveau der in Anlage 2 aufgeführten Maßnahmen entsprechen. Alle wesentlichen Änderungen der technischen und organisatorischen Maßnahmen sind zu dokumentieren.

5.3 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Auftraggeber bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO. Im Einzelnen bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen an die Aufsichtsbehörde, der Benachrichtigung betroffener Personen bei einer Verletzung, der Datenschutz-Folgenabschätzung und bei der Konsultation der zuständigen Aufsichtsbehörde.

5.4 Sofern sich eine betroffene Person oder eine Datenschutzaufsichtsbehörde im Zusammenhang mit den unter dieser Vereinbarung verarbeiteten personenbezogenen Daten direkt an den Auftragnehmer wendet, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich.

6. PRÜFUNGSRECHTE DES AUFTRAGGEBERS

6.1 Der Auftragnehmer stellt dem Auftraggeber auf dessen Anfrage alle erforderlichen Informationen zum Nachweis der in diesem Vertrag und Art. 28 DSGVO geregelten Pflichten zur Verfügung. Insbesondere erteilt der Auftragnehmer dem Auftraggeber Auskünfte über die gespeicherten Daten und die Datenverarbeitungsprogramme.

6.2 Der Auftraggeber hat das Recht, in jährlichen Abständen oder anlassbezogen – grundsätzlich nach Terminvereinbarung – die Einhaltung der Pflichten aus diesem Vertrag und aus Art. 28 DSGVO zu überprüfen, und beim Auftragnehmer Inspektionen vor Ort durchzuführen oder durch von ihm beauftragte und im Einzelfall zu benennender Dritter durchführen zu lassen. Der Auftragnehmer ermöglicht dies und trägt dazu bei.

6.3 Der Auftragnehmer hat dem Auftraggeber auf Anforderung geeigneten Nachweis über die Einhaltungen der Verpflichtungen gemäß Art. 28 Abs. 1 und Abs. 4 DSGVO zu erbringen. Dieser Nachweis kann durch die Bereitstellung von Dokumenten und Zertifikaten, die genehmigte Verhaltensregeln i. S. v. Art. 40 DSGVO oder genehmigte Zertifizierungsverfahren i. S. v. Art. 42 DSGVO abbilden, erbracht werden.

7. DATENSCHUTZBEAUFTRAGTER DES AUFTRAGNEHMERS

Der Datenschutzbeauftragte des Auftragnehmers ist zu erreichen unter: datenschutz@kurabu.com.

8. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Der Auftragnehmer führt geeignete technische und organisatorische Maßnahmen so durch, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist. 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 DSGVO, 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.

9. UNTERAUFTRAGNEHMER

9.1 Der Auftragnehmer wird bei der Erbringung der Leistungen Unterauftragsverarbeiter einsetzen und mit diesen im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Der Auftragnehmer wird insbesondere eine Vereinbarung nach Maßgabe des Art. 28 DSGVO abschließen und sämtliche Pflichten dieser Vereinbarung an den Unterauftragnehmer weitergeben. Soweit erforderlich, wird der Auftragnehmer auch die Anforderungen der Art. 44 ff. DSGVO einhalten.

9.2 Für den Einsatz von Unterauftragsverarbeitern ist die Zustimmung des Auftraggebers erforderlich. Der Auftraggeber erklärt sich hiermit mit den in Anlage 1 genannten Subunternehmen einverstanden.

9.3 Der Auftragnehmer wird während der Vertragslaufzeit möglicherweise weitere Unterauftragsverarbeiter einsetzen oder bereits genannte Unterauftragsverarbeiter ersetzen. Der Auftragnehmer wird den Auftraggebern in diesem Fall rechtzeitig über jeden neuen Unterauftragsverarbeiter informieren. Der Auftragnehmer erhält die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben.

Wenn der Auftraggeber einem neuen Unterauftragsverarbeiter nicht zustimmt, kann der Auftraggeber den Hauptvertrag vor Ablauf der geltenden Kündigungsfrist mit schriftlicher Mitteilung kündigen.

10. HAFTUNG

Es gelten die gesetzlichen Haftungsbestimmungen nach Art. 82 DS-GVO.

11. SCHLUSSBESTIMMUNGEN

11.1 Soweit in dieser Auftragsverarbeitungsvereinbarung keine abweichende Regelung getroffen wurde, finden die Regelungen des Hauptvertrags Anwendung.

11.2 Änderungen dieser Auftragsverarbeitungsvereinbarung bedürfen der Schriftform.

ANLAGE 1 – Genehmigte Unterauftragnehmer

Die im Folgenden aufgelisteten Unterauftragnehmer von *KURABU* werden bei Erteilung des Auftrags genehmigt.

Name Unterauftragnehmer	**Anschrift/ Land**	**Beschreibung der Datenverarbeitung**
Heroku eine Salesforce.com, Inc. Company	The Landmark @ One Market, Suite 300, San Francisco, California 94105, USA	Hosting von Backenddaten (Mitgliederddaten, Beschreibungen, Daten des Vereins) ➔ Aktueller Unterauftragnehmer ist Heroku Neuer Unterauftragnehmer bis Ende Quartal 2 2023 ist Amazon Web Services in Frankfurt/Deutschland. • https://devcenter.heroku.com/articles/gdpr • https://aws.amazon.com/de/security/
Froala Editor an Idera, Inc. Company	10801 N Mopac Expressway, Suite 100 Austin, TX. 78759 United States	Hosting von Backenddaten (Beschreibungen zu einem Newsartikel, Kategorie, Team, Standort, Logbuch, Rechtlicher Inhalt und Kontaktinhalt, Dokumente, eigene Videos) • https://www.ideracorp.com/legal/Froala
Amazon Web Services, Inc.	Amazon Web Services, Inc. 410 Terry Ave North Seattle, W A 98109-5210, US	Hosting von Backenddaten (Alle Dokumente, wie PDFs, Bilder und eigene Videos). Diese liegen als AWS S3 Bucket in Frankfurt/Deutschland • https://aws.amazon.com/de/security/

UploadCare, Inc.	2711 Centerville Road, Suite 400 City of Wilmington, County of New Castle, 19808, USA	Hosting von Backenddata (Bilder von Newsartikeln, Kategorien, Teams, Standorten, Profilbilder und Dokumente die über den Chat hochgeladen werden) ➔ Aktueller Unterauftragnehmer ist Uploadcare Neuer Unterauftragnehmer bis Ende Quartal 2 2023 ist Amazon Web Service in Frankfurt/Deutschland. • https://uploadcare.com/about/gdpr/ • https://aws.amazon.com/de/security/
Cloudflare	101 Townsend St, San Francisco, CA 94107 USA	*KURABU* Domain auf Cloudflare app.kurabu Verteilt die Inhalte der Website auf CloudFlare Server weltweit, sodass die Website beschleunigt ausgeliefert wird, Website erhält DDOS Schutz, zusätzliche Firewall wird vor die Website geschaltet. ➔ Aktueller Unterauftragnehmer ist Cloudflare Neuer Unterauftragnehmer bis Ende Q2 2023 ist Amazon Web Services (CloudFront) in Frankfurt/Deutschland. • https://www.cloudflare.com/de-de/gdpr/introduction/ • https://aws.amazon.com/de/cloudfront/?nc1=h_ls
Mailjet SAS (Global HQ) et	13-13 bis, rue de l'Aubrac, 75012 Paris, France	E-Mail Versand / Kundenkommunikation (Alle E-Mails ID's und Vornamen von den Administratoren und den Mitgliedern, um die automatischen Standardemails von *KURABU* zu erhalten.) • https://www.mailjet.de/sicherheit-datenschutz/
OneSignal, Inc.	2850 S Delaware St #201, San Mateo, CA 94403, United States	Versendung von Push-Nachrichten für Chats und Newsartikel (Alle user-ID's, user-emails der Mobile App Nutzer) • https://onesignal.com/privacy

ANLAGE 2 – Technisch-organisatorische Maßnahmen

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Der Auftragsverarbeiter oder die verwendetet Drittanbieter erfüllen diesen Anspruch durch die nachfolgenden Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Alarmanlage	☒ Schlüsselregelung / Liste
☒ Automatisches Zugangskontrollsystem	☒ Empfang / Rezeption / Pförtner
☒ Biometrische Zugangssperren	☒ Besucherbuch / Protokoll der Besucher

☒ Chipkarten / Transpondersysteme	☒ Mitarbeiter- / Besucherausweise
☒ Sicherheitsschlösser	☒ Besucher in Begleitung durch Mitarbeiter
☒ Schließsystem mit Codesperre	☒ Sorgfalt bei Auswahl des Wachpersonals
☒ Absicherung der Gebäudeschächte	☒ Sorgfalt bei Auswahl Reinigungsdienste
☒ Türen mit Knauf Außenseite	
☒ Klingelanlage mit Kamera	
☒ Videoüberwachung der Eingänge	
☒ Videoüberwachung der Eingänge	

Weitere Informationen sind hier verlinkt:

- https://aws.amazon.com/de/compliance/data-center/controls/
- https://aws.amazon.com/de/security/
- https://devcenter.heroku.com/articles/gdpr
- https://www.cloudflare.com/de-de/privacypolicy/
- https://www.mailjet.de/av-vertrag/
- https://documentation.onesignal.com/docs/handling-personal-data
- https://uploadcare.com/about/gdpr/

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung

von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Login mit biometrischen Daten	☒ Erstellen von Benutzerprofilen
☒ Anti-Viren-Software Server	☒ Richtlinie „Sicheres Passwort“
☒ Anti-Virus-Software Clients	☒ Richtlinie „Löschen / Vernichten“
☒ Anti-Virus-Software mobile Geräte	☒ Richtlinie „Clean desk“
☒ Firewall	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit
☒ Mobile Device Management	☒ Mobile Device Policy
☒ Verschlüsselung von Datenträgern	☒ NDA – Non-Disclosure Agreement
☒ Verschlüsselung Smartphones	☒ Anleitung „Manuelle Desktopsperre“
☒ BIOS Schutz (separates Passwort)	☒ NDA – Non-Disclosure Agreement
☒ Automatische Desktopsperre	
☒ Verschlüsselung von Notebooks / Tablet	

Weitere Informationen sind hier verlinkt:

- https://aws.amazon.com/de/compliance/data-center/controls/
- https://aws.amazon.com/de/security/
- https://devcenter.heroku.com/articles/gdpr
- https://www.cloudflare.com/de-de/privacypolicy/
- https://www.mailjet.de/av-vertrag/
- https://documentation.onesignal.com/docs/handling-personal-data
- https://uploadcare.com/about/gdpr/

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Aktenschredder (mind. Stufe 3, cross cut)	☒ Einsatz Berechtigungskonzepte
☒ Physische Löschung von Datenträgern	☒ Minimale Anzahl an Administratoren
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒ Datenschutztresor
	☒ Verwaltung Benutzerrechte durch Administratoren

Weitere Informationen sind hier verlinkt:

- https://aws.amazon.com/de/compliance/data-center/controls/
- https://aws.amazon.com/de/security/
- https://devcenter.heroku.com/articles/gdpr
- https://www.cloudflare.com/de-de/privacypolicy/
- https://www.mailjet.de/av-vertrag/
- https://documentation.onesignal.com/docs/handling-personal-data
- https://uploadcare.com/about/gdpr/

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☒ Mandantenfähigkeit relevanter Anwendungen	☒ Datensätze sind mit Zweckattributen versehen

Weitere Informationen sind hier verlinkt:

- https://aws.amazon.com/de/compliance/data-center/controls/
- https://aws.amazon.com/de/security/
- https://devcenter.heroku.com/articles/gdpr
- https://www.cloudflare.com/de-de/privacypolicy/
- https://www.mailjet.de/av-vertrag/
- https://documentation.onesignal.com/docs/handling-personal-data
- https://uploadcare.com/about/gdpr/

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

Weitere Informationen sind hier verlinkt:

- https://aws.amazon.com/de/compliance/data-center/controls/
- https://aws.amazon.com/de/security/
- https://devcenter.heroku.com/articles/gdpr
- https://www.cloudflare.com/de-de/privacypolicy/
- https://www.mailjet.de/av-vertrag/
- https://documentation.onesignal.com/docs/handling-personal-data
- https://uploadcare.com/about/gdpr/

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

2.1. Weitergabekontrolle

Maßnahmen, die 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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind

Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Email-Verschlüsselung	☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☒ Protokollierung der Zugriffe und Abrufe	☒ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☒ Weitergabe in anonymisierter oder pseudonymisierter Form
	☒ Persönliche Übergabe mit Protokoll

Weitere Informationen sind hier verlinkt:

- https://aws.amazon.com/de/compliance/data-center/controls/
- https://aws.amazon.com/de/security/
- https://devcenter.heroku.com/articles/gdpr
- https://www.cloudflare.com/de-de/privacypolicy/
- https://www.mailjet.de/av-vertrag/
- https://documentation.onesignal.com/docs/handling-personal-data
- https://uploadcare.com/about/gdpr/

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☒ Klare Zuständigkeiten für Löschungen

Weitere Informationen sind hier verlinkt:

- https://aws.amazon.com/de/compliance/data-center/controls/
- https://aws.amazon.com/de/security/
- https://devcenter.heroku.com/articles/gdpr
- https://www.cloudflare.com/de-de/privacypolicy/
- https://www.mailjet.de/av-vertrag/
- https://documentation.onesignal.com/docs/handling-personal-data
- https://uploadcare.com/about/gdpr/

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

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)
☒ Feuerlöscher Serverraum	☒ Kontrolle des Sicherungsvorgangs

☒ Serverraumüberwachung Temperatur und Feuchtigkeit	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☒ Serverraum klimatisiert	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ USV	☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☒ Schutzsteckdosenleisten Serverraum	☒ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
☒ Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	☒ Getrennte Partitionen für Betriebssysteme und Daten
☒ RAID System / Festplattenspiegelung	
☒ Videoüberwachung Serverraum	
☒ Alarmmeldung bei unberechtigtem Zutritt zum Serverraum	

Weitere Informationen sind hier verlinkt:

- https://aws.amazon.com/de/compliance/data-center/controls/
- https://aws.amazon.com/de/security/
- https://devcenter.heroku.com/articles/gdpr
- https://www.cloudflare.com/de-de/privacypolicy/
- https://www.mailjet.de/av-vertrag/
- https://documentation.onesignal.com/docs/handling-personal-data
- https://uploadcare.com/about/gdpr/

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Software-Lösungen für Datenschutz-Management im Einsatz	☒ Interner / externer Datenschutzbeauftragter
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
☒ Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	☒ Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich
☒ Anderweitiges dokumentiertes Sicherheits-Konzept	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
☒ Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

Weitere Informationen sind hier verlinkt:

- https://aws.amazon.com/de/compliance/data-center/controls/
- https://aws.amazon.com/de/security/
- https://devcenter.heroku.com/articles/gdpr
- https://www.cloudflare.com/de-de/privacypolicy/
- https://www.mailjet.de/av-vertrag/
- https://documentation.onesignal.com/docs/handling-personal-data
- https://uploadcare.com/about/gdpr/

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Einbindung von ☒ DSB und ☒ ISB in Sicherheitsvorfälle und Datenpannen
☒ Intrusion Detection System (IDS)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☒ Intrusion Prevention System (IPS)	

Weitere Informationen sind hier verlinkt:

- https://aws.amazon.com/de/compliance/data-center/controls/
- https://aws.amazon.com/de/security/
- https://devcenter.heroku.com/articles/gdpr
- https://www.cloudflare.com/de-de/privacypolicy/
- https://www.mailjet.de/av-vertrag/
- https://documentation.onesignal.com/docs/handling-personal-data
- https://uploadcare.com/about/gdpr/

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
☒ Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	

Weitere Informationen sind hier verlinkt:

- https://aws.amazon.com/de/compliance/data-center/controls/
- https://aws.amazon.com/de/security/
- https://devcenter.heroku.com/articles/gdpr
- https://www.cloudflare.com/de-de/privacypolicy/
- https://www.mailjet.de/av-vertrag/
- https://documentation.onesignal.com/docs/handling-personal-data
- https://uploadcare.com/about/gdpr/