# Vertrag über die Verarbeitung von Daten im Auftrag

zwischen

***Name:***
***Straße:***
***PLZ & Stadt:***

**- Auftraggeber -**

und

***Kurabu GmbH***
***Friedrich-Ebert-Straße 36***
***14469 Potsdam***

**- Auftragnehmer –**

## 1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

## 2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

## 3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 3 das Recht zu,

den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(6) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

## 4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer wird die Datenverarbeitung im Auftrag grundsätzlich in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchführen. Dem Auftragnehmer ist eine Datenverarbeitung auch außerhalb von EU oder EWR erlaubt, wenn entsprechende Unterauftragnehmer im Drittland unter Einhaltung der Voraussetzungen von Ziff. 9 eingesetzt werden und die Voraussetzungen der Art. 44-48 DSGVO erfüllt sind bzw. eine Ausnahme i.S.d. Art. 49 DSGVO vorliegt.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange

auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

## 5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

## 6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen,

der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

– eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

## 7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 12 dieses Vertrages.

(2) Der Auftragnehmer unterstützt bei der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

## 8. Regelung zu mobilen Arbeitsplätzen

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen außerhalb der Geschäftsräume des Auftragnehmers erlauben.

(2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch bei der Nutzung von mobilen Arbeitsplätzen der Beschäftigten des Auftragnehmers gewährleistet ist. Abweichungen von einzelnen vertraglich vereinbarten technischen und organisatorischen Maßnahmen sind vorab mit dem Auftraggeber abzustimmen und von diesem in Textform zu genehmigen.

(3) Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere am Ort des jeweiligen mobilen Arbeitsplatzes befindliche Personen keinen Zugriff auf diese Daten erhalten.

(4) Der Auftragnehmer ist verpflichtet, Sorge dafür zu tragen, dass eine wirksame Kontrolle der Verarbeitung personenbezogener Daten im Auftrag an mobilen Arbeitsplätzen durch den Auftraggeber möglich ist.

(5) Sofern auch bei Unterauftragnehmern Beschäftigte an mobilen Arbeitsplätzen eingesetzt werden sollen, gelten die Regelungen der Absätze 1 bis 4 entsprechend.

## 9. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenen Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.

(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 3 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments i.S.d. Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils

zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

(6) Die Parteien sind sich darüber einig, dass die Kontrollmaßnahmen bei einer Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen zur Wahrung der Persönlichkeitsrechte von weiteren Personen an diesen mobilen Arbeitsplätzen primär durch eine Kontrolle der Sicherstellung der vom Auftragnehmer nach Ziff. 8 Abs. 2 und 3 zu treffenden Maßnahmen erfolgt. Anlassbezogen ist dem Auftraggeber auch eine Kontrolle des mobilen Arbeitsplatzes von Beschäftigten durch den Auftragnehmer zu ermöglichen.

## 10. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, die in der **Anlage 2** zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 2 genannten Voraussetzungen zulässig.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 2 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen zwei Wochen nach Zugang der „Information“ zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information“ erfolgt, gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat, sofern der Unterauftragnehmer zur Benennung eines Datenschutzbeauftragten gesetzlich verpflichtet ist.

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 9 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(7) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

## 11. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

(2) Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

## 12. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

## 13. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen. Diese Verpflichtung gilt nicht, soweit eine gesetzliche Pflicht zur Offenlegung gegenüber Behörden, insbesondere von Datenschutzaufsichtsbehörden, besteht.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

## 14. Vergütung

Etwaige Regelungen zu einer Vergütung von Leistungen sind zwischen den Parteien gesondert zu vereinbaren.

## 15. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Kommt eine Einigung über wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der Daten beeinträchtigen könnten, nicht zustande, sind beide Parteien berechtigt, den Vertrag mit einer Frist von einem Monat zum Monatsende zu kündigen. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

## 16. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

## 17. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren.

(2) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

## 18. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Für den **Auftraggeber**:

_____, _____

Ort, Datum

_____

[Unterschrift einfügen]

_____

[Name/Position des Unterzeichnenden]

# ANLAGE 1 - Gegenstand des Auftrags

## 1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

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 Teilnehmer (siehe Punkt 3) bereit. Dies erfolgt zu den Zwecken ser digitalen Verwaltung des Vereins sowie der Verwaltung von Vereinsmitgliedern, Beiträgen, Veranstaltungen, Kommunikation, Dokumente und Spenden. Dazu zählt insbesondere die Bereitstellung folgender Funktionen und Teildienste:

- Rollen- & Rechteverwaltung, Anlage und Verwaltung von Administratoren und sonstigen Nutzern,
- Teilnehmerverwaltung (siehe Punkt 3), Rechnungsstellung,
- Protokoll- und Anwesenheitslisten,
- Erstellung und Verwaltung von Teamveranstaltungen, Events & Platzbuchungen,
- Erstellung, Versendung und Empfang von E-Mail- und Push-Nachrichten (standardisiert und personalisiert).

Nähere Informationen hinsichtlich Gegenstand, Art und Zweck finden sich im Hauptvertrag.

## 2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Titel, Name, Vorname, Position (optional), ggf. Teamleiterstatus,
- Geburtsdatum, Geschlecht, Profil-Bild,
- Anschrift, Telefonnummer, E-Mail-Adresse, Rechnungsanschrift,
- Vereinszugehörigkeit (Mitglied seit/bis), Beitragsinformationen & Bankdaten
- Veranstaltungsdaten (Anmeldungen, Anwesenheiten)
- Kommunikationsdaten

Gesundheitsdaten i.S.d. Art. 9 Abs. 1 DSGVO werden von *KURABU* standardmäßig nicht verarbeitet; der Verein kann jedoch eigenständig entsprechende Datenfelder anlegen und über

frei konfigurierbare Textfelder gesundheitsbezogene Angaben (z. B. Krankenkasse, Gesundheits-/Reha-Maßnahmen) erfassen, die dann, sofern angelegt, als besondere Kategorien personenbezogener Daten im Auftrag verarbeitet werden.

## 3. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

- Vereinsleitung,
- Betreuung/Teamleitung,
- Vereinsmitglieder,
- GastbucherInnen,
- alle im Mitgliederbereich angelegten Datensätze.

## ANLAGE 2 - Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“). Dabei handelt es sich um nachfolgende(s) Unternehmen:

| **Name Unterauftrag-nehmer** | **Anschrift/ Land** | **Standort des genutzten Servers** | **Beschreibung der Datenverarbeitung** |
|---|---|---|---|
| Amazon Web Services EMEA SARL | 38 Avenue John F. Kennedy, L-1855, Luxemburg | Europäische Union / Deutschland / Frankfurt | Hosting von Backenddaten (Mitgliederdaten, Beschreibungen, Daten des Vereins), Hosting von Backenddata (Bilder von Newsartikeln, Abteilungen, Teams, Standorten, Profilbilder und Dokumente die über den Chat hochgeladen werden), Hosting von Backenddaten (Alle Dokumente, wie PDFs, Bilder und eigene Videos). Diese liegen alle **verschlüsselt** in Frankfurt/Deutschland<br>• https://aws.amazon.com/de/security/ |
| Cloudflare, Inc. | 101 Townsend St, San Francisco, CA 94107 USA | Europäische Union<br><br>Zertifizierung beim Data Privacy Framework | *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.<br>• https://www.cloudflare.com/de-de/cloudflare-customer-dpa/ |
| Mailjet SAS (Global HQ) et | 4 rue Jules Lefebvre 75009 Paris, France | Europäische Union / Deutschland / Frankfurt & Belgien / Saint-Ghislain | 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.)<br>• https://www.mailjet.de/sicherheit-datenschutz/ |
| OneSignal, Inc. | 201 S. B Street, Suite 200, San Mateo, CA 94401, USA | Europäische Union / Niederlande<br><br>Zertifizierung beim Data Privacy Framework | Versendung von Push-Nachrichten für Chats und Newsartikel (Alle user-ID’s, user-emails der Mobile App Nutzer)<br>• https://onesignal.com/privacy |

| | | | |
|---|---|---|---|
| Yousign SAS | Rue De Suède Av Pierre Berthelot 14000 - CAEN, France | Europäische Union / Frankreich | Mit diesem Service können bei Aktivierung alle Dokumente (Rechnungen, Bestätigungen und Co.) digital unterzeichnet werden.<br>• https://yousign.com/de-de/datenverarbeitung |

# ANLAGE 3 - Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

## 1. Vertraulichkeit

**Zutrittskontrolle**

| Technische Maßnahme | Organisatorische Maßnahme |
|---|---|
| Manuelles Schließsystem (Schlüsselvergabe mit dokumentierter Schlüsselliste) | Personal und Reinigungspersonal wurde zur Vertraulichkeit verpflichtet |
| Alarm System | Clean-Desk-Policy |
| | Physische Sicherheit in Rechenzentren durch Hosting-Provider gemäß dessen TOMs |

**Zugangskontrolle**

| Technische Maßnahme | Organisatorische Maßnahme |
|---|---|
| Authentifizierung mit Passwort | Passwortrichtlinie (u.a. Mindestlänge 12 Zeichen, Kombination von kleinen und großen Buchstaben, Zahlen und Sonderzeichen, Rotation nur anlassbezogen) |
| Sperrung externer Schnittstellen | Zuweisung von Administratorrechten an eine minimale Anzahl von Personen |
| Protokollierung von Anmeldevorgängen | MFA verpflichtend für alle externen und administrativen Zugriffe |

**Zugriffskontrolle**

| Technische Maßnahme | Organisatorische Maßnahme |
|---|---|
| Datenverschlüsselung (AES-256 für ruhende Daten (Datenbanken, Backups, Endgeräte); TLS 1.2/1.3 für Datenübertragungen) | Differenzierung der administrativen Aufgaben (SoD, Vier-Augen-Prinzip) |
| Protokollierung von Zugriffen | Rollenbasiertes Berechtigungskonzept (RBAC) mit Rollen-/Rechte-Matrix, Least |

| | |
|---|---|
| | Privilege, Regelmäßige (jährlich) Prüfung auf Aktualität und Notwendigkeit von Zugriffen |
| Kontosperrung nach mehrfachen falschen Passworteingaben | Acceptable Use Policy (Regeln für die Nutzung von IT-Systemen, Anwendungen und Daten) |
| Zertifikatbasierte Authentifizierung der Datenquelle | |

**Trennungskontrolle**

| Technische Maßnahme | Organisatorische Maßnahme |
|---|---|
| Strikte Trennung von Produktions- und Testsystemen in separaten Cloud-Accounts/Projekten und Netzsegmenten (VPCs) | Produktiv-Daten werden nicht zu Testzwecken eingesetzt (ausschließlich synthetische oder anonymisierte Testdaten) |
| Getrennte Zugänge/Rollen für Produktions- und Testsysteme | Freigabeprozess für Deployments und Änderungen |
| Logische Mandantentrennung auf Anwendungs-/Datenebene (Zugriff beschränkt nach Mandant/Rolle) | |

**Pseudonymisierung und Verschlüsselung**

| Technische Maßnahme | Organisatorische Maßnahme |
|---|---|
| Verschlüsselung von ruhenden Daten in der Datenbank (AES-256) sowie verschlüsselte Backups | Frühzeitige Pseudonymisierung personenbezogener Daten |
| Pseudonymisierung von Daten während der weiteren Verarbeitung oder Übermittlung | |

## 2. Integrität

**Eingabekontrolle**

| Technische Maßnahme | Organisatorische Maßnahme |
|---|---|
| Protokollierung von Änderungen oder Korrekturen gespeicherter Daten | Sofortige Korrektur fehlerhafter Daten |

| | |
|---|---|
| Protokollierung der Eingabe während der Erhebung und Hinzufügung von Daten | Änderungs-/Freigabeprozess (Ticket/Change-Mgmt) |
| Automatische Auswertung von Protokolldaten | |
| Revionssichere Audit-Logs | |

**Übertragungskontrolle**

| Technische Maßnahme | Organisatorische Maßnahme |
|---|---|
| Inhaltsverschlüsselte Datenübertragung (TLS 1.2/1.3) | Übermittlung von Daten in pseudonymisierter Form wenn möglich |
| Protokollierung aller Datentransfers | Übermittlung von Daten in anonymisierter Form wenn möglich |

## 3. Verfügbarkeit und Belastbarkeit

| Technische Maßnahme | Organisatorische Maßnahme |
|---|---|
| Automatisierte Erstellung von Datensicherungen | Backup- und Wiederherstellungskonzept |
| Loadbalancing der Server | Notfallplan für den Neustart von Servern und Diensten |
| Loadbalancing der Dienste | Notfallplan im Falle eines Datenschutz- oder IT-Sicherheitsvorfalls (Interne Richtlinie umgesetzt, unverzügliche Benachrichtigung des Verantwortlichen, Erkennung und Eindämmung des Vorfalls) |
| Regelmäßige Überprüfung der Datenwiederherstellung (quartalsweise) | Notfallplan bei Datenverlust |
| | Automatisches Notrufsystem |
| | Festplattenspiegelung (RAID) |

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

| Technische Maßnahme | Organisatorische Maßnahme |
|---|---|
| Protokollierung aller Administratoraktivitäten | Bestellung eines Datenschutzbeauftragten |
| Protokollierung von Löschvorgängen | Möglichkeit zur Beantragung einer Korrektur durch elektronische Anwendung |
| Protokollierung fehlgeschlagener Zugriffsversuche | Datenschutz durch Voreinstellung |
| Automatisches Benachrichtigungssystem bei maximaler Auslastung | Datenschutz durch Technikgestaltung |
| Automatische Skalierung virtueller Systeme | Definition automatisierter Löschzyklen |
| Sperrung externer Schnittstellen (z.B. USB) | Definition verbindlicher Löschfristen |
| IT-Komponenten haben eine klar definierte Leistung | Dokumentation von Vertrags- und Unterauftragsverhältnissen |
| Sicherung der Protokolldaten gegen Veränderung und Verlust | Dokumentation der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung |
| Vernichtung von Datenträgern gemäß DIN 66399 | Dokumentation der getroffenen Sicherheitsmaßnahmen (im Verzeichnis der Verarbeitungstätigkeiten) |
| | Dokumentation der bestehenden IT-Infrastruktur |
| | Dokumentation der verwendeten Programme und Anwendungen |
| | Einrichtung eines Verfahrens zur Berichtigung von Daten auf Anfrage |
| | Unabhängige elektronische Korrektur von Daten durch die betroffene Person |
| | Verpflichtung der Mitarbeiter zur Einhaltung der Anforderungen der DSGVO |
| | Veröffentlichung von Informationen über die Verarbeitung personenbezogener Daten (z.B. online oder als Hinweis) |
| | Stichproben zur Überprüfung der Wirksamkeit bestimmter Maßnahmen |

| | |
|---|---|
| | Regelmäßige manuelle Auslösung der Löschung nicht benötigter Daten |
| | Regelungen beim Verlassen von Mitarbeitern |
| | Definierte Verantwortlichkeiten für Datensicherung |
| | Führen eines Verarbeitungsverzeichnisses |
| | Drittanbieter Management Richtlinie (Umgang mit neuen Dienstleistern und Kriterien für den Einsatz, Lieferanten-Prüfung inkl. DPA, TIA, SCC/DPF; jährliche Re-Bewertung) |

## 5. Mobile Arbeitsplätze / Remote Work

| Technische Maßnahme | Organisatorische Maßnahme |
|---|---|
| Firmenendgeräte mit Festplattenverschlüsselung (Bitlocker/FileVault) | Remote Work Richtlinie (u.a. keine Speicherung sensibler Daten lokal, Clean Desk) |
| Automatische Sicherheits-/OS-Updates | Heim-WLAN mind. WPA2/WPA3, keine Nutzung offener Netze |
| Antivirus verpflichtend | Keine Cloud-Drittdienste ohne Freigabe |
| Bildschirmsperre nach 5 Minuten | |