# Vereinbarung über Auftragsverarbeitung

Anlage zu den *Allgemeinen Portalbedingungen der iX3 GmbH, Walldorf* (nachfolgend „APB“)

zwischen der

iX3 GmbH
Altrottstraße 31
69190 Walldorf
Deutschland

- nachfolgend " **Auftragsverarbeiter**" genannt -

und

dem Kunden
(d.h. Fragender / Antwortender als Vertragspartei des Hauptvertrages,
wie nachfolgend in Ziffer 2.1 definiert)

- nachfolgend "**Verantwortlicher** " genannt –

# Inhalt

## 1 Definitionen

Wenn in dieser Vereinbarung über Auftragsverarbeitung der Begriff „Daten“ verwendet wird, sind stets personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO gemeint. Im Übrigen sind die in dieser Vereinbarung über Auftragsverarbeitung verwendeten Begriffe so zu verstehen, wie sie in der DSGVO oder in anderen Gesetzen (z.B. § 2 BDSG) definiert sind.

## 2 Gegenstand und Dauer der Verarbeitung

2.1 Der Verantwortliche nutzt als Fragender oder Antwortender das Portal des Auftragsverarbeiters und hat zu diesem Zweck mit dem Auftragsverarbeiter über die APB einen Vertrag zur Portalnutzung abgeschlossen. Die vorliegende Vereinbarung über Auftragsverarbeitung bildet einen wesentlichen Bestandteil dieser APB. Der über die APB abgeschlossene Vertrag wird nachfolgend „Hauptvertrag“ genannt.

2.2 Der Auftragsverarbeiter ermöglicht dem Verantwortlichen nach Maßgabe des Hauptvertrages die Nutzung des Portals einschließlich der Verarbeitung von personenbezogenen Daten im Portal (nachfolgend zusammenfassend „Auftrag“ genannt). Dabei kann nicht ausgeschlossen werden, dass der Auftragsverarbeiter Zugriff auf personenbezogene Daten erhält und bei Erbringung der Leistungen solche Daten im Auftrag des Verantwortlichen verarbeitet. Der Auftragsverarbeiter verarbeitet die im Zusammenhang mit dem Auftrag stehenden personenbezogenen Daten ausschließlich im Rahmen der in dieser Vereinbarung über Auftragsverarbeitung getroffenen Bestimmungen. Der Auftragsverarbeiter verarbeitet die betreffenden personenbezogenen Daten für keine anderen und insbesondere nicht für eigene Zwecke.

2.3 Die Zwecke und Mittel der Verarbeitung bestimmt alleine der Verantwortliche. Änderungen des Verarbeitungsgegenstandes und Verarbeitungsänderungen sind gemeinsam abzustimmen und schriftlich durch Änderung dieser Vereinbarung über Auftragsverarbeitung festzulegen.

2.4 Die Dauer dieser Vereinbarung über Auftragsverarbeitung (Laufzeit) entspricht der Laufzeit des Hauptvertrages.

## 3 Konkretisierung des Auftrags

3.1 Der Inhalt des Auftrags wird in Bezug auf die Auftragsverarbeitung wie folgt konkretisiert:

| | |
|---|---|
| **Art und Zweck der Verarbeitung** | Art und Zweck der Verarbeitung ergeben sich aus dem Gegenstand des Hauptvertrages. Dies umfasst vor allem die Portalnutzung, wozu das Anlegen und Einsehen von Benutzerprofilen, das Stellen von Fragen, die Abgabe von Beantwortungsangeboten und das Abarbeiten erteilter Beauftragungen sowie Rechnungsstellung gehört. |
| **Art der personenbezogenen Daten** | Personenstammdaten, Kommunikationsdaten (z.B. Telefon, E-Mail), Vertragsstammdaten, Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Planungs- und Steuerungsdaten |
| **Kategorien der betroffenen Personen** | Kunden, Beschäftigte i. S. d. § 26 BDSG, Lieferanten, Interessenten |

## 4 Weisungsgebundenheit

4.1 Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen, sofern der Auftragsverarbeiter nicht durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung in Textform (z.B. per E-Mail oder Fax) mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die vorstehenden Regelungen gelten auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation.

4.2 Der Verantwortliche hat das Recht, dem Auftragsverarbeiter im Rahmen des Auftragsgegenstandes (siehe Ziffer 2) Weisungen hinsichtlich der Art, des Umfangs und des Verfahrens der Verarbeitung der personenbezogenen Daten zu erteilen. Seine Weisungen kann er durch Einzelweisungen konkretisieren. Mündlich erteilte Weisungen sind vom Auftragsverarbeiter unverzüglich schriftlich oder

in Textform zu bestätigen. Als Weisung ist dabei die auf einen bestimmten datenschutzmäßigen Umgang (z.B. Anonymisierung, Berichtigung, Einschränkung der Verarbeitung, Löschung, Herausgabe) des Auftragsverarbeiters mit personenbezogenen Daten gerichtete Anordnung des Verantwortlichen zu verstehen.

4.3 Der Verantwortliche hat alle Weisungen, die er dem Auftragsverarbeiter erteilt, zu dokumentieren. Die Dokumentation stellt er dem Auftragsverarbeiter für jede erteilte Weisung zur Verfügung. Für die Dokumentation der Umsetzung der vom Verantwortlichen erteilten Weisungen ist dagegen der Auftragsverarbeiter verantwortlich.

4.4 Den entsprechenden Weisungen des Verantwortlichen hat der Auftragsverarbeiter jederzeit Folge zu leisten. Solange und soweit der Auftragsverarbeiter personenbezogene Daten aus dem Auftrag über das Auftragsende hinaus verarbeitet, gilt die Weisungsgebundenheit gegenüber dem Verantwortlichen auch nach der Beendigung dieser Vereinbarung über Auftragsverarbeitung weiter; Aufwendungen und Kosten, die dem Auftragsverarbeiter hierdurch entstehen, trägt der Verantwortliche.

4.5 Der Auftragsverarbeiter unternimmt alle erforderlichen Schritte, um sicherzustellen, dass die ihm unterstellten natürlichen Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

4.6 Falls Weisungen die in Ziffer 3 getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn vorher eine entsprechende Änderung dieser Vereinbarung über Auftragsverarbeitung in Text- oder Schriftform erfolgt ist.

4.7 Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich informieren, wenn eine vom Verantwortlichen erteilte Weisung nach Auffassung des Auftragsverarbeiters gegen gesetzliche Vorschriften und insbesondere gegen die DSGVO, das BDSG oder gegen andere anwendbare Datenschutzbestimmungen der Europäischen Union oder ihrer Mitgliedstaaten verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird. Sofern der Auftragsverarbeiter darlegen kann, dass eine Verarbeitung nach Weisung des Verantwortlichen zu einer Haftung des Auftragsverarbeiters nach Art. 82 DSGVO führen kann, steht dem Auftragsverarbeiter das Recht zu, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Vertragspartnern auszusetzen.

## 5 Verpflichtung zur Vertraulichkeit

5.1 Der Auftragsverarbeiter gewährleistet, dass er bei der Verarbeitung personenbezogener Daten nur Mitarbeiter beschäftigt, die er mit den für sie maßgebenden Bestimmungen des Datenschutzrechtes vertraut gemacht und schriftlich - auch über die Beendigung ihrer Tätigkeit hinaus - zur Vertraulichkeit verpflichtet hat; die Textform genügt nicht. Einer Verpflichtung bedarf es nicht, wenn Mitarbeiter einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.2 Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften durch die ihm unterstellten Personen, die Zugang zu personenbezogenen Daten haben. Seine mit der Verarbeitung von personenbezogenen Daten betrauten Mitarbeiter wird der Auftragsverarbeiter regelmäßig in angemessenem Umfang und in angemessenen Abständen schulen und für den Datenschutz sensibilisieren.

5.3 Der Verantwortliche ist verpflichtet, alle im Rahmen des Auftrags erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen sowie Daten- und andere IT-Sicherheitsmaßnahmen des Auftragsverarbeiters, insbesondere die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters, streng vertraulich zu behandeln und diese weder weiterzugeben noch auf sonstige Art zu verwerten oder zu offenbaren. Dies gilt gegenüber jeglichen unbefugten Dritten, d.h. auch gegenüber eigenen unbefugten Mitarbeitern, sofern die Weitergabe bzw. sonstige Verwertung oder Offenbarung von solchen Informationen nicht zur ordnungsgemäßen Erfüllung der vertraglichen oder gesetzlichen Verpflichtungen des Verantwortlichen erforderlich ist. In Zweifelsfällen ist der Verantwortliche verpflichtet, vor einer solchen Weitergabe bzw. sonstigen Verwertung oder Offenbarung die schriftliche Zustimmung des Auftragsverarbeiters einzuholen.

5.4 Ungeachtet der in Ziffer 5.3 vereinbarten Verschwiegenheitspflichten des Verantwortlichen, darf dieser technische und organisatorische Maßnahmen des Auftragsverarbeiters, die den Auftrag betreffen, im Rahmen der dem Verantwortlichen gesetzlich auferlegten Rechenschaftspflicht gegenüber berechtigten Personen und Stellen (z.B. Aufsichtsbehörden) offenbaren, soweit er dazu gesetzlich verpflichtet ist.

## 6 Technische und organisatorische Maßnahmen

6.1 Der Auftragsverarbeiter setzt für den Auftrag unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Vereinbarung erfolgt.

6.2 Die als Anhang 1 (Technische und organisatorische Maßnahmen) beigefügten Datenschutzvorkehrungen des Auftragsverarbeiters, die die Festlegungen gemäß Art. 32 DSGVO enthalten, werden für die Durchführung des Auftrags als verbindliches Minimum festgelegt, das zu keiner Zeit unterschritten werden darf. Der Auftragsverarbeiter verpflichtet sich zur Einhaltung der in Anhang 1 niedergelegten technischen und organisatorischen Maßnahmen.

6.3 Stellt der Verantwortliche während der Laufzeit des Auftrages fest, dass sich die Risiken für die Rechte und Freiheiten der Betroffenen verändert haben, teilt er dies dem Auftragsverarbeiter unverzüglich mit, damit der Auftragsverarbeiter seine technischen und organisatorischen Maßnahmen so anpassen kann, dass das für den Auftrag erforderliche Datenschutzniveau weiterhin gewährleistet bleibt; die dem Auftragsverarbeiter durch die Anpassung entstehenden einmaligen und wiederkehrenden Aufwendungen und Kosten trägt der Verantwortliche. Sobald der Auftragsverarbeiter in Anhang 1 die aktualisierten technischen und organisatorischen Maßnahmen festgelegt hat, ersetzt dieser neue Anhang 1 den bis dahin gültigen Anhang 1. Sollte eine entsprechende Anpassung der technischen und organisatorischen Maßnahmen dem Auftragsverarbeiter nicht möglich, nicht zumutbar oder gar für ihn unzulässig sein, stellt dies für beide Vertragspartner einen wichtigen Grund dar, der zur außerordentlichen Kündigung des Hauptvertrages einschließlich der vorliegenden Vereinbarung über Auftragsverarbeitung berechtigt.

6.4 Der Auftragsverarbeiter stellt sicher, dass die im Auftrag verarbeiteten personenbezogenen Daten von sonstigen Datenbeständen strikt getrennt werden. Nähere Anforderungen und Maßnahmen zur Trennung sind in den technischen und organisatorischen Maßnahmen in Anhang 1 festgelegt.

6.5 Wenn und soweit der Auftragsverarbeiter gegenüber dem Verantwortlichen zum Nachweis der getroffenen technischen und organisatorischen Maßnahmen verpflichtet ist, kann er Nachweise über die Einhaltung genehmigter Verhaltensregelungen gemäß Art. 40 DSGVO oder über aktuelle Zertifizierung gemäß Art. 42 DSGVO vorlegen, um seinen Nachweis zu stützen. Des Weiteren kann er diesen Nachweis auch über aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch ein Informationssicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, als Bestandteil einer ISO 27001-Zertifizierung) führen.

6.6 Die technischen und organisatorischen Maßnahmen müssen im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Dazu werden die im Anhang 1 vereinbarten technischen und organisatorischen Maßnahmen vom Verantwortlichen und vom Auftragsverarbeiter im Lichte der Ziffer 6.1 sowie unter Berücksichtigung des Stands der Technik mindestens einmal im Kalenderjahr überprüft. Aus solchen Überprüfungen resultierende Änderungen sind schriftlich festzulegen. Stellt der Auftragsverarbeiter während der Laufzeit des Auftrages von sich aus fest, dass die von ihm getroffenen Maßnahmen die Risiken für die Rechte und Freiheiten der Betroffenen nicht oder nicht mehr angemessen abdecken, benachrichtigt er den Verantwortlichen. Für die Anpassung des Anhangs 1 gelten die in Ziffer 6.3 vereinbarten Bestimmungen entsprechend.

## 7 Einbeziehung weiterer Auftragsverarbeiter

7.1 Der Verantwortliche erteilt hiermit seine allgemeine Zustimmung zur Inanspruchnahme weiterer Auftragsverarbeiter.

7.2 Im Falle der Beauftragung von weiteren Auftragsverarbeitern (Kettenauftragsverarbeitung) oder der Ersetzung von weiteren Auftragsverarbeitern wird der Auftragsverarbeiter den Verantwortlichen informieren. Will der Verantwortliche gegen derartige Änderungen in Übereinstimmung mit Ziffer 7.2 Einspruch erheben, hat er diesen gegenüber dem Auftragsverarbeiter innerhalb von zwei (2) Wochen nach Zugang der Information bzw. unverzüglich nach Kenntniserlangung von einem sich später ergebenden Einspruchsgrund schriftlich zu erklären. Die Bestimmungen dieser Ziffer 7 gelten entsprechend für jede Hinzuziehung bzw. Ersetzung von weiteren Auftragsverarbeitern im Rahmen einer mehrstufigen Kettenauftragsverarbeitung.

7.3 Der Auftragsverarbeiter erlegt weiteren Auftragsverarbeitern im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats im Wesentlichen dieselben Datenschutzpflichten auf, die in dieser Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind. Dabei ist sicherzustellen, dass geeignete technische und organisatorische Maßnahmen auch von dem weiteren Auftragsverarbeiter so durchgeführt werden, dass die Verarbeitung den gesetzlichen Anforderungen des Datenschutzrechtes entspricht.

7.4 Bei Abschluss dieser Vereinbarung über Auftragsverarbeitung hat der Verantwortliche der Inanspruchnahme der in Anhang 2 (Weitere Auftragsverarbeiter) mit Namen und konkretisiertem Auftragsinhalt bezeichneten weiteren Auftragsverarbeitern mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang zugestimmt.

7.5 Der Verantwortliche kann gegen den Einsatz eines weiteren Auftragsverarbeiters durch den Auftragsverarbeiter nur dann Einspruch erheben, wenn er begründete Zweifel daran hat, dass der weitere Auftragsverarbeiter die datenschutzrechtlichen Bestimmungen oder die Bedingungen dieser Vereinbarung über Auftragsverarbeitung einhalten wird. Erhebt der Verantwortliche gegen einen weiteren Auftragsverarbeiter in zulässiger Weise Einspruch, wird der Auftragsverarbeiter zumutbare Anstrengungen unternehmen, um die Verarbeitung personenbezogener Daten durch den beanstandeten weiteren Auftragsverarbeiter zu vermeiden, ohne den Verantwortlichen unangemessen zu belasten. Wenn der Auftragsverarbeiter nicht in der Lage ist oder es ihm nicht zumutbar ist, eine solche Änderung innerhalb eines angemessenen Zeitraums, der dreißig (30) Tage nicht überschreiten darf, zur Verfügung zu stellen, kann jeder Vertragspartner nach billigem Ermessen (i) den Hauptvertrag nur in Bezug auf diejenigen Leistungen, die vom Auftragsverarbeiter nicht ohne den Einsatz des beanstandeten weiteren Auftragsverarbeiters erbracht werden können, oder (ii) den gesamten Hauptvertrag außerordentlich kündigen.

7.6 Nicht als Inanspruchnahme weiterer Auftragsverarbeiter im Sinne dieser Ziffer 7 sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Reinigungskräfte, Telekommunikationsleistungen und Postdienste.

## 8 Unterstützung des Verantwortlichen

8.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei dessen Pflicht, Anträge auf Wahrnehmung der in Art. 12 bis 22 DSGVO sowie in §§ 32 bis 37 BDSG genannten Rechte der betroffenen Person zu bearbeiten und zu beantworten. Dazu wird er dem Verantwortlichen auf Anfrage alle zweckdienlichen Informationen bereitstellen, die dem Auftragsverarbeiter im Einzelfall vorliegen. Wendet sich ein Betroffener mit Anträgen auf Wahrnehmung der in Art. 12 bis 22 DSGVO und in §§ 32 bis 37 BDSG genannten Rechten unmittelbar an den Auftragsverarbeiter, wird dieser den Betroffenen an den Verantwortlichen verweisen.

8.2 Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen.

8.3 Der Auftragsverarbeiter ergreift geeignete technische und organisatorische Maßnahmen, um den Verantwortlichen gemäß Ziffer 8.1 unterstützen zu können.

8.4 Des Weiteren unterstützt der Auftragsverarbeiter mit den ihm zur Verfügung stehenden Informationen den Verantwortlichen bei dessen Einhaltung der ihm gemäß Art. 32 bis 36 DSGVO obliegenden Pflichten.

8.5 Der Verantwortliche hat dem Auftragsverarbeiter alle Aufwendungen und Kosten zu erstatten, die dem Auftragsverarbeiter im Rahmen der Unterstützung des Verantwortlichen entstehen.

## 9 Rückgabe und Löschung von Daten

9.1 Nach Beendigung der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche im Zusammenhang mit dem Auftrag in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungsergebnisse, die personenbezogene Daten enthalten, sowie alle im Rahmen der Erbringung der Leistungen verarbeiteten personenbezogenen Daten ohne vorherige Übergabe datenschutzgerecht zu löschen. Der Verantwortliche kann vom Auftragsverarbeiter jedoch verlangen, dass dieser ihm vor der Löschung die Unterlagen, Arbeitsergebnisse und personenbezogenen Daten übergibt und erst danach die Löschung des beim Auftragsverarbeiter verbliebenen Rests der personenbezogenen Daten durchführt. Die vorstehende Übergaberegelung ist so zu verstehen, dass der Verantwortliche nach erfolgter

Übergabe über alle personenbezogenen Daten aus und im Zusammenhang mit dem Auftrag verfügt. Der Auftragsverarbeiter hat dem Verantwortlichen die Vernichtung bzw. Löschung zu bestätigen.

9.2 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Gleiches gilt, soweit nach dem Unionsrecht oder dem vom Auftragsverarbeiter anzuwendenden Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

9.3 Entstehen dem Auftragsverarbeiter nach Beendigung der vertraglichen Arbeiten zusätzliche Aufwendungen oder Kosten durch die Rückgabe, Vernichtung oder Löschung von personenbezogenen Daten, so trägt diese der Verantwortliche.

## 10 Nachweis der Einhaltung der datenschutzrechtlichen Pflichten

10.1 Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anforderung alle erforderlichen Informationen zum Nachweis der Einhaltung der in dieser Vereinbarung niedergelegten Pflichten zur Verfügung.

10.2 Außerdem ermöglicht und unterstützt der Auftragsverarbeiter Überprüfungen einschließlich Inspektionen und Untersuchungen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer oder von Aufsichtsbehörden durchgeführt werden. Der Auftragsverarbeiter erklärt sich insbesondere damit einverstanden, dass der Verantwortliche oder ein von diesem beauftragter Prüfer im Regelfall nach angemessener Vorankündigung berechtigt ist, während der üblichen Bürozeiten des Auftragsverarbeiters die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen dieser Vereinbarung über Auftragsverarbeitung im erforderlichen Umfang und ohne Störung des Betriebsablaufs des Auftragsverarbeiters vor Ort zu kontrollieren.

10.3 Sollte der durch den Verantwortlichen beauftragte Prüfer in einem unmittelbaren Wettbewerbsverhältnis zu dem Auftragsverarbeiter stehen, hat der Auftragsverarbeiter gegen diesen Prüfer ein Einspruchsrecht.

## 11 Verfahrensverzeichnisse

Der Auftragsverarbeiter führt das gemäß Art. 30 Abs. 2 DSGVO von ihm zu führende Verzeichnis und stellt dieses der Aufsichtsbehörde auf Anfrage zur Verfügung.

## 12 Sonstige Pflichten des Auftragsverarbeiters

12.1 Der Auftragsverarbeiter arbeitet auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

12.2 Ist für eine geplante Verarbeitung personenbezogener Daten eine Datenschutz-Folgeabschätzung erforderlich, unterstützt der Auftragsverarbeiter den Verantwortlichen auf Anforderung und gegen Vergütung seines damit verbundenen Aufwandes bei der Abschätzung und stellt ihm alle erforderlichen Dokumentationen und zweckdienlichen Informationen zur Verfügung.

12.3 Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Art. 58 DSGVO sowie über Ermittlungen, die eine zuständige Behörde nach Art. 83 DSGVO und §§ 42, 43 BDSG beim Auftragsverarbeiter durchführt, informieren, soweit diese Kontrollhandlungen, Maßnahmen oder Ermittlungen Bezüge zur Auftragsverarbeitung aufweisen.

## 13 Mitzuteilende Verstöße

13.1 Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich, wenn ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird. Meldungen erfolgen in Textform und müssen mindestens die in Art. 33 Abs. 3 DSGVO aufgezählten Informationen umfassen.

13.2 Dem Auftragsverarbeiter ist bekannt, dass nach Art. 33 und 34 DSGVO Melde- und Benachrichtigungspflichten im Falle der Verletzung des Schutzes personenbezogener Daten gegenüber der Aufsichtsbehörde und den betroffenen Personen bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Verantwortlichen mitzuteilen. Der Auftragsverarbeiter hat in Abstimmung mit dem Verantwortlichen angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

13.3 Soweit den Verantwortlichen Pflichten nach Art. 33 und 34 DSGVO treffen, hat der Auftragsverarbeiter ihn hierbei gegen Vergütung des für den Auftragsverarbeiter damit verbundenen Aufwandes zu

unterstützen. Die Vergütungspflicht besteht nicht, wenn eine Unterstützung aufgrund eines Verstoßes des Auftragsverarbeiters gegen seine Pflichten als Auftragsverarbeiter erforderlich wird. Ungeachtet dessen bleibt der Verantwortliche für die Erfüllung der ihn gemäß Art. 33 und 34 DSGVO treffenden Melde- und Benachrichtigungspflichten selbst verantwortlich.

## 14 Anhänge

Die folgenden Anhänge bilden einen wesentlichen Bestandteil dieser Vereinbarung über Auftragsverarbeitung und haben im Fall von Widersprüchen oder Unklarheiten Vorrang vor den Bestimmungen der vorliegenden Vereinbarung über Auftragsverarbeitung:

Anhang 1: Technischen und organisatorische Maßnahmen

Anhang 2: Weitere Auftragsverarbeiter

# Anhang 1: Technische und organisatorische Maßnahmen / TOM

# I. iX³ GmbH Walldorf

### 1 Pseudonymisierung und Verschlüsselung

1.1 Ziel: Die Zuordnung von personenbezogenen Daten zu einer identifizierbaren Person durch Unberechtigte soll erschwert oder verhindert werden.

1.2 Ergriffene technische und organisatorische Maßnahmen:

- Pseudonymisierungsverfahren werden nicht angewendet, weil im Rahmen der Wartung der Plattform, insbesondere im Supportfall, regelmäßig Datensätze benötigt oder eingesehen werden, die stets in Bilder oder Dokumente eingebettete Echtdaten enthalten.
- Technische Verschlüsselungsverfahren finden auf allen Desktop-PCs sowie Laptops Anwendung.
- Verschlüsselte Datenspeicherung (z.B. Dateiverschlüsselung nach AES256 Standard)
- Verschlüsselte Datenübertragung (verschlüsselte Internetverbindungen mittels TLS/SSL)

### 2 Zutrittskontrolle

2.1 Ziel: Unbefugten ist der physische Zugang zu Räumlichkeiten, Gebäuden oder Räumen, in denen sich Datenverarbeitungssysteme befinden, die personenbezogene Daten verarbeiten, zu verwehren; Unbefugte sind unbefugt, wenn ihre Tätigkeit nicht den ihnen zugewiesenen Aufgaben entspricht. Ausnahmen können Dritten zum Zweck der Prüfung der Einrichtungen gewährt werden, solange sie vom Auftragsverarbeiter beaufsichtigt werden und keinen Zugang zu den personenbezogenen Daten selbst erhalten.

2.2 Ergriffene technische und organisatorische Maßnahmen:

- Besucherprotokollierung - Protokollierung der Besucher
- Bewegungsmelder - Bewegungsmelder
- Chipkarten - Chipkarten-/Transponder-Schließsystem
- Am Empfang findet eine Besucherkontrolle sowie Eintrag ins Besucherbuch statt.
- Videoüberwachung - Videoüberwachung der Zugänge

### 3 Zugangskontrolle

3.1 Ziel: Das Eindringen Unbefugter in die IT-Systeme ist zu verhindern.

3.2 Ergriffene technische und organisatorische Maßnahmen:

- Authentifikation mit Benutzer und Passwort - Authentifikation mit Benutzer und Passwort
- Benutzerberechtigungen - Benutzerberechtigungen verwalten (bei Eintritt, Änderung, Austritt)
- Firewall - Einsatz von Firewalls zum Schutz des Netzwerkes
- Sorgfältige Personalauswahl - Sorgfältige Auswahl von Reinigungspersonal und Sicherheitspersonal
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren

### 4 Zugriffskontrolle

4.1 Ziel: Personen, die zur Nutzung eines Datenverarbeitungssystems berechtigt sind, erhalten nur Zugang zu den Daten, auf die sie ein Zugriffsrecht haben, und personenbezogene Daten dürfen im Verlauf der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

4.2 Ergriffene technische und organisatorische Maßnahmen:

- Berechtigungskonzept - Erstellen und Einsatz eines Berechtigungskonzepts

- Datenlöschung - Sichere Löschung von Datenträgern vor deren Wiederverwendung (z.B. durch mehrfaches Überschreiben)
- Einsatz von Aktenvernichtern - Einsatz von Aktenvernichtern (min. Sicherheitsstufe 3 und Schutzklasse 2)
- Einsatz von Dienstleistern - Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit DIN 66399 Zertifikat)
- Passwortlichtlinien - Passwortrichtlinie inkl. Länge, Komplexität und Wechselhäufigkeit
- Sichere Aufbewahrung - sichere Aufbewahrung von Datenträgern
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren

**5 Weitergabekontrolle**

5.1 Ziel: Außer soweit dies für die Erbringung der Dienstleistungen gemäß dem Hauptvertrag erforderlich ist, dürfen personenbezogene Daten während der Übertragung oder Speicherung nicht unbefugt gelesen, kopiert, geändert oder entfernt werden, und es muss möglich sein, zu überprüfen, an wen personenbezogene Daten übertragen wurden.

5.2 Ergriffene technische und organisatorische Maßnahmen:

- SSL / TLS Verschlüsselung - Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet

**6 Eingabekontrolle**

6.1 Ziel: Es muss möglich sein, im Nachhinein zu prüfen und festzustellen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, geändert oder entfernt worden sind.

6.2 Ergriffene technische und organisatorische Maßnahmen:

- Personalisierte Benutzernamen - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Protokollierung - Protokollierung der Eingabe, Änderung und Löschung von Daten
- Zugriffsrechte - personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe

**7 Auftragskontrolle**

7.1 Ziel: Personenbezogene Daten, die im Auftrag verarbeitet werden, werden ausschließlich in Übereinstimmung mit dem Hauptvertrag und den damit verbundenen Anweisungen des für die Verarbeitung Verantwortlichen verarbeitet. Der Auftragsverarbeiter erbringt die Dienstleistungen und insbesondere die Datenverarbeitungsdienste für personenbezogene Daten nur in Übereinstimmung mit den Anweisungen des für die Verarbeitung Verantwortlichen.

7.2 Ergriffene technische und organisatorische Maßnahmen:

- Auswahl - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- AV-Vertrag - Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO
- Laufende Überprüfung - laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Schulung - Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen
- Verpflichtung - Verpflichtung auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO

**8 Verfügbarkeitskontrolle**

8.1 Ziel: Personenbezogene Daten sind vor Offenlegung, versehentlicher oder unbefugter Zerstörung oder Verlust zu schützen.

8.2 Ergriffene technische und organisatorische Maßnahmen

- Antivirensoftware - Einsatz von Antivirensoftware zum Schutz vor Malware

- Auslagerung Datensicherung - Aufbewahrung von Datensicherung an einem sicheren Ort.
- Backup- & Recoverykonzept - Erstellen eines Backup- & Recoverykonzepts
- Brandmeldeanlagen - Feuer- und Rauchmeldeanlagen

### 9 Verfahren zur regelmäßigen Überprüfung der Wirksamkeit

9.1 Ziel: Es muss ein Verfahren implementiert werden, um die Wirksamkeit der technischen und organisatorischen Maßnahmen, die vom Verarbeiter zur Gewährleistung der Sicherheit der Verarbeitung ergriffen werden, regelmäßig zu testen, zu bewerten und auszuwerten.

9.2 Ergriffene technische und organisatorische Maßnahmen

- Software Voreinstellungen - Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO)

## II. randevu

Die zum Zeitpunkt des Abschlusses dieser Vereinbarung über Auftragsverarbeitung für randevu Software Services geltenden technischen und organisatorischen Maßnahmen sind zu finden in „randevu Technical and organizational measures“ unter https://randevu.tech/wp-content/uploads/2023/09/randevu_iX3_Data_Processing_Agreement.pdf.

## III. Microsoft

Die zum Zeitpunkt des Abschlusses dieser Vereinbarung über Auftragsverarbeitung für Microsoft 365 und Microsoft Azure-Dienste geltenden technischen und organisatorischen Maßnahmen sind zu finden in Microsoft's DPA (Datenschutznachtrag zu den Produkten und Services von Microsoft) unter https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14.

## IV. Stripe

Die zum Zeitpunkt des Abschlusses dieser Vereinbarung über Auftragsverarbeitung für Stripe Payments Europe, Limited geltenden technischen und organisatorischen Maßnahmen sind zu finden in Stripe’s Data Processing Agreement unter https://stripe.com/de/legal/dpa.

# Anhang 2: Weitere Auftragsverarbeiter

| Name / Firma, Anschrift | Auftragsinhalt | Umfang der Auftragsverarbeitung |
|---|---|---|
| Microsoft Ireland Operations Limited,<br>1 Microsoft Place,<br>South County Business Park,<br>Leopardstown<br>Dublin 18,<br>Ireland | Skalierbare Infrastruktur<br>Der Auftragsverarbeiter hat für den Betrieb seiner verwalteten Infrastruktur bei Microsoft die Region "Germany West Central" beauftragt. | Nutzung der skalierbaren Cloud-Services zur Umsetzung der in Ziffer 3.1 dieser Vereinbarung über Auftragsverarbeitung beschriebenen Auftragskonkretisie-rung. Verarbeitet werden Verträge und andere Anhänge als pdf-Dateien sowie User-Login-Daten. |
| randevu GmbH,<br>Samariterstraße 13,<br>10247 Berlin,<br>Deutschland | Digitale B2B Plattform | Randevu stellt eine iX³ spezifische B2B Plattform für die digitale Beratung von Geschäftspartnern zur Verfügung.<br>In diesem Zusammenhang werden die anfallenden Stammdaten digital verwaltet, Geschäftsprozesse digital abgewickelt und die erforderliche Kommunikation digital abgewickelt. |
| Stripe Payments Europe, Limited (SPEL),<br>1 Grand Canal Street Lower,<br>Grand Canal Dock,<br>Dublin D02 H210,<br>Irland | Digitale B2B Zahlungsabwicklung (Geschäftspartner innerhalb der EU) | Stripe wickelt die über die AQUGA Plattform initiierten Zahlungsein- und -ausgänge für die iX³ ab.<br>In diesem Zusammenhang werden die anfallenden Stammdaten digital verwaltet. |