

Vereinbarung zur Auftragsverarbeitung

Bei Fragen wenden Sie sich bitte an den Auftragsverarbeiter.

Datenschutzvereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen dem Verantwortlichen:

[[Firma]]

[[Strasse]]

[[Strasse2]]

[[PLZ]] [[Ort]]

[[Land]]

(nachstehend Auftraggeber genannt)

und dem Auftragsverarbeiter:

Just Software AG

Nobistor 16

22767 Hamburg

(nachstehend Auftragnehmer genannt)

wird folgende Vereinbarung geschlossen und ersetzt etwaige vorherige Vereinbarungen zur Auftragsverarbeitung zum gleichen Zweck:

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der in dieser Vereinbarung und der in **Anlage A** beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit der Dienstleistung in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

Einzelvereinbarungen in dieser Datenschutzvereinbarung gehen den Allgemeinen Geschäftsbedingungen (AGB) des Auftragnehmers vor.

§ 1 Definitionen

1. Personenbezogene Daten

Nach Art. 4 Abs. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder

identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

2. Auftragsverarbeiter

Nach Art. 4 Abs. 8 DS-GVO ist ein Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

3. Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Speicherung, Pseudonymisierung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete in der Regel schriftliche Anordnung des Auftraggebers. Die Weisungen werden vom Auftraggeber erteilt und können durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Die Weisungen des Auftraggebers sind schriftlich oder per E-Mail zu erteilen.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer erbringt im Auftrag des Auftraggebers Hosting-Leistungen in Form einer Software as a Service. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogenen Daten bekommt bzw. Kenntnis von diesen erlangt. Nach Art 28 DS-GVO ist daher der Abschluss einer Vereinbarung zur Verarbeitung im Auftrag erforderlich.
2. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 DS-GVO als Dienstleister ausgewählt. Voraussetzung für die Zulässigkeit einer Datenverarbeitung im Auftrag ist, dass der Auftraggeber dem Auftragnehmer den Auftrag schriftlich erteilt. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung i.S.d. Art 28 Abs. 3 DS-GVO und regelt die Rechte und Pflichten der Parteien zum Datenschutz im Zusammenhang mit der Erbringung der Software as a Service (SaaS) Leistungen.
3. Das Eigentum an den personenbezogenen Daten liegt ausschließlich beim Auftraggeber als "Verantwortlichem" im Sinne der DS-GVO. Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Berichtigung, Löschung, Sperrung und Herausgabe von personenbezogenen Daten verlangen.

§ 3 Gegenstand und Dauer des Auftrages

1. Der Gegenstand des Auftrages ist in **Anlage A** niedergelegt.
2. Diese Vereinbarung tritt mit ihrer Unterzeichnung durch beide Parteien in Kraft und endet im Regelfall mit Kündigung des zugrundeliegenden Hauptvertrages laut AGB. Weiterhin bleibt die vorliegende Vereinbarung über das Ende des Hauptvertrages hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat. Das Recht zur außerordentlichen Kündigung bleibt unberührt.

§ 4 Beschreibung der Verarbeitung, Daten und betroffener Personen

Umfang, Art und Zweck der Verarbeitung sind ebenso wie die Art der Daten und der Kreis der betroffenen Personen in **Anlage A** beschrieben.

§ 5 Technische und organisatorische Maßnahmen

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Wahrung der anzuwendenden Datenschutzvorschriften angemessen und erforderlich sind.

1. Da der Auftragnehmer den Betrieb der Software as a Service Leistungen für den Auftraggeber auch außerhalb der Geschäftsräume des Auftraggebers durchführt, sind vom Auftragnehmer zwingend die von ihm getroffenen technischen und organisatorischen Maßnahmen i.S.d. Art. 28 Abs. 3 lit. C DS-GVO, Art. 32 DS-GVO i.V.m. Art. 5 Abs. 1 und Abs. 2 DS-GVO hierzu zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Die Verarbeitung personenbezogener Daten durch Mitarbeitende des Auftragnehmers außerhalb der Betriebsstätte (z. B. im Homeoffice oder bei mobiler Arbeit) ist zulässig, sofern der Auftragnehmer durch geeignete technische und organisatorische Maßnahmen sicherstellt, dass die Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten gewährleistet bleibt.
2. Die Maßnahmen dienen der Datensicherheit und der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der mit diesem Auftrag in Zusammenhang stehenden Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.
3. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage B "Technische und organisatorische Maßnahmen zum Datenschutz"** dieser Vereinbarung 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 Vorwege 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. Dabei darf das Sicherheitsniveau der in der Anlage B „Technische und organisatorische Maßnahmen zum Datenschutz“ festgelegten Maßnahmen nicht unterschritten werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

§ 6 Verarbeitung von Daten

1. Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers. Er darf die Daten, die im Auftrag verarbeitet werden, beispielsweise nicht eigenmächtig berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber zur Freigabe weiterleiten.
2. Die Umsetzung von Löschung, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft sind nur nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

3. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
4. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens jedoch mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung spätestens jedoch bei Beendigung der Leistungsbeziehung vorzulegen.
5. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 7 Pflichten des Auftragnehmers

1. Eine Verarbeitung personenbezogener Daten, die sich nicht auf die Erbringung von SaaS-Leistungen oder Support bezieht, ist dem Auftragnehmer untersagt. Es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.
2. Der Auftragnehmer bestätigt, dass er – soweit dieser gesetzlich dazu verpflichtet ist – einen betrieblichen Datenschutzbeauftragten i.S.d. Artt. 38, 39 DS-GVO bestellt hat.
Der Auftragnehmer hat Carsten Knoop, audatis Consulting GmbH, Luisenstr. 1, 32052 Herford, datenschutz@just.social zum Datenschutzbeauftragten bestellt.
Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
3. Sofern der Auftraggeber dem Auftragnehmer nichts anderes mitteilt, sind die weisungsberechtigten Personen die bis zu vier Personen, für die der Auftragnehmer Support leistet. Der Auftraggeber hat die Pflicht, diese Personen zum Projektstart schriftlich zu benennen und den Auftragnehmer bei Änderungen unverzüglich zu informieren. Die Weisungsempfänger des Auftragnehmers sind die Mitarbeitenden des Customers Success Teams, die der Auftragnehmer ebenfalls zu Projektstart benennt und an den Auftraggeber kommuniziert.
4. 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.
5. Der Auftragnehmer hat die weisungsberechtigten Personen des Auftraggebers unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten des Auftraggebers zu unterrichten.
6. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung von dessen Pflichten zur Beantwortung von Anträgen betroffener Personen gemäß den Artikeln 12 bis 22 DSGVO. Der Auftragnehmer ist nicht berechtigt, Anfragen von betroffenen Personen direkt zu beantworten, es sei denn, der Auftraggeber hat ihn hierzu ausdrücklich schriftlich ermächtigt. Die Auftragnehmer leitet entsprechende Anfragen unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Eingang, schriftlich (z.B. E-Mail) an die weisungsberechtigten Personen des Auftraggebers weiter.
7. Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen, die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete personenbezogene Daten einer Verletzung des gesetzlichen Schutzes personenbezogener

Daten gem. Art. 33 DS-GVO (Datenschutzverstoß bzw. Datenpanne) unterliegen z.B. indem diese unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls bzw. der Vorfälle in Schriftform oder Textform via E-Mail zu informieren. Die Meldung an den Auftraggeber muss mindestens folgende Informationen enthalten:

- a. 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.
- b. Den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen.
- c. Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.
- d. Eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

8. Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO notwendigen Angaben zur Verfügung und führt als Auftragsverarbeiter selbst ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO.
9. Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der personenbezogenen Daten des Auftraggebers befassten Mitarbeiter gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO zur Wahrung der Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugriff auf personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in dieser Vereinbarung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Diese Vertraulichkeitsverpflichtung besteht auch nach Beendigung der Tätigkeit fort.
10. Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen. Zum Beispiel durch regelmäßige Auditierung und Zertifizierung durch ein externes Datenschutzunternehmen.
11. Des Weiteren verpflichtet sich der Auftragnehmer den Auftraggeber gemäß Art. 28 Abs. 3 lit. f DS-GVO bei der Einhaltung der in Artt. 32 - 36 DS-GVO genannten Pflichten zu unterstützen:
 - a. Im Rahmen seiner Informationspflicht gegenüber den betroffenen Personen und dem Auftraggeber in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
 - b. Bei der Durchführung seiner Datenschutz-Folgenabschätzung.
 - c. Im Rahmen einer vorherigen Konsultation mit der Aufsichtsbehörde.
12. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
13. Der Auftragnehmer hat den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, zu informieren. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

14. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung durch den Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
15. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

§ 8 Rechte und Pflichten des Auftraggebers

1. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Entwicklung, Pflege und Wartung von Software und/oder IT-Systemen gegenüber dem Auftragnehmer zu erteilen. Weisungen können schriftlich oder mündlich erfolgen. Der Auftraggeber soll mündliche Weisungen unverzüglich via E-Mail gegenüber dem Auftragnehmer bestätigen.
2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
3. Dem Auftraggeber obliegen die aus Art. 33 Abs. 1 DS-GVO resultierenden Meldepflichten.
4. Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten personenbezogenen Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.
5. Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang und die gesetzlichen Pflichten des Auftragnehmers hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen. Die Kosten betragen je angefangene Stunde 125 Euro (netto).

§ 9 Wahrung von Rechten der betroffenen Person

1. Der Auftraggeber ist für die Wahrung der Rechte der betroffenen Person verantwortlich.
2. Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Einschränkung, Datenübertragbarkeit oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.
3. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Löschung oder Einschränkung oder Datenübertragbarkeit seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

§ 10 Kontrollbefugnisse

1. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen sowie die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.
2. Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Abs. 1 erforderlich ist.

3. Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Abs. 1 in der Betriebsstätte des Auftragnehmers selbst oder durch von ihm beauftragte Prüfer zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden.
4. Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DS-GVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen.
5. Der Auftragnehmer erbringt den Nachweis technischer und organisatorischer Maßnahmen, die nicht nur den konkreten Auftrag betreffen. Dabei kann dies erfolgen durch:
 - a. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO.
 - b. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO.
 - c. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Datenschutzauditoren).
 - d. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001 oder BSI-Grundschutz).
6. Die Kosten für Aufwände einer Kontrolle beim Auftragnehmer gem. Abs. 3 und 4, die über die gesetzlichen Pflichten des Auftragnehmers hinausgehen, können gegenüber dem Auftraggeber geltend gemacht werden. Die Kosten betragen je angefangene Stunde 125 Euro (netto).
7. Sofern einschlägig, verpflichtet sich der Auftragnehmer den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

§ 11 Unterauftragsverhältnisse

1. Der Auftragnehmer nimmt für die Erbringung von SaaS-Leistungen im Auftrag des Auftraggebers keine Leistungen von Dritten in Anspruch, welche nicht in Abs. 2 genannt werden, die in seinem Auftrag Daten gem. Art. 28 DS-GVO verarbeiten ("Unterauftragnehmer").
2. Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen Unternehmen zur Leistungserfüllung heranzieht bzw. mit Leistungen unterbeauftragt. Aktuell handelt es sich um folgende Unternehmen:

Genehmigte Unterauftragnehmer bei durch Just Software AG gehosteten Diensten:

 - Netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe (Rechenzentrum)
 - Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen (Rechenzentrum)

In diesen beiden Rechenzentren werden die Just-Plattformen der Auftraggeber gehostet. Die Standorte der Rechenzentren sind in Deutschland (Nürnberg und Falkenstein).
3. Im Falle einer Beauftragung, hat der Auftragnehmer 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. 28 Abs. 3 lit. c, 32 DS-GVO i.V.m. Art. 5 Abs. 1, Abs. 2 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen

- hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i.S.d. Artt. 37-39 DS-GVO bestellt hat.
4. Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.
 5. Die Verpflichtung des Unterauftragnehmers muss grundsätzlich schriftlich erfolgen, sofern keine andere Form angemessen ist. Dem Auftraggeber ist die Verpflichtung auf Anfrage in Kopie zu übermitteln.
 6. Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 10 dieser Vereinbarung) 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. Nimmt der Auftragnehmer die Dienste eines neuen weiteren Auftragsverarbeiters (Hauptleistung) in Anspruch, so informiert er den Auftraggeber hierüber schriftlich und gibt ihm 30 Tage Zeit der Verarbeitung durch den neuen Auftragsverarbeiter zu widersprechen. Kann keine einvernehmliche Lösung erzielt werden, erfolgt eine Einschränkung oder Beendigung dieser Vereinbarung bzw. der Auftragsverarbeitung.
 8. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Unterauftragnehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Abschnitt vertraglich auferlegt wurden (Art. 28 Abs. 4 Satz 2 DSGVO).
 9. Eine Beauftragung von Unterauftragnehmer in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und der Auftraggeber vorab zustimmt.

§ 12 Datengeheimnis und Geheimhaltungspflichten

1. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnischutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnischutzregeln mitzuteilen.
2. Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist.
3. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieser Vereinbarung 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 oben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.
4. 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.

§ 13 Haftung

Es wird auf die Haftungsregelungen des Art. 82 DS-GVO verwiesen.

§ 14 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die personenbezogenen Daten des Auftraggebers beim Auftragnehmer oder bei Unterauftragnehmern durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den personenbezogenen Daten ausschließlich beim Auftraggeber als "Verantwortlichem" im Sinne der DS-GVO liegen.
2. Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
3. Bei Unwirksamkeit einer Bestimmung in diesen Vertragsbedingungen bleiben die übrigen Bestimmungen gleichwohl wirksam. Die Vertragsparteien verpflichten sich, eine unwirksame Bestimmung oder eine planwidrig fehlende Bestimmung nach Treu und Glauben durch eine Bestimmung zu ersetzen, die dem gemeinsam verfolgten Zweck der Vertragsparteien am nächsten kommt.
4. Im Übrigen wird soweit rechtlich zulässig als Gerichtsstand Hamburg vereinbart und es gilt deutsches Recht.
5. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

[[Ort]], 18.05.2026

gez. *[[Name]]* (Vertretungsberechtigter des Auftraggebers)

Hamburg, 18.05.2026

gez. *Dr. Thomas Kreye* (Vorstand, Just Software AG)

[Diese Vereinbarung ist ohne Unterschrift gültig]

Anlage A: Details zum Auftrag

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

Wartung und Pflege der Social Software „Just“

Zugriffe auf die IT-Systeme (speziell Social Software „Just“) des Auftraggebers per Fernwartung.

Bereitstellung der Social Software „Just“ als gehostete Software im Rechenzentrum des Auftragnehmers oder eines Subunternehmers.

Anlage A: Details zum Auftrag

Der Umfang der Verarbeitung und damit die Menge der eingesetzten Daten sind variabel und richtet sich nach der Nutzungsintensität durch den Auftraggeber. Der Zweck dient zur Verwaltung der Aufgaben und Maßnahmen im Datenschutz und Dokumentation von digitalen bzw. digitalisierten Dokumenten sowie zu durchgeführten Schulungsmaßnahmen einzelner Beschäftigter des Auftraggebers. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Bei der Auftragsleistung handelt es sich um folgende Arten der automatisierten Verarbeitung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen:

- Verändern (z.B. durch Änderungen der Benutzer an den Datensätzen)**
- Übermitteln (z.B. durch Übermittlung per E-Mail von Nachrichten)**
- Speichern (z.B. durch Sicherung und Archivierung auf Festplatten, anderen Speichersystemen oder Datenträgern)**
- Löschen (z.B. durch Löschen von Datensätzen oder Vernichten von Datenträgern)**
- Einschränken (z.B. durch Deaktivierung von einzelnen Datensätzen)**
- Nutzen (z.B. durch Durchführung von Auswertungen)
- Erheben (z.B. durch Einlesen von Mitarbeiterlisten und anderen Daten)

Anlage A: Details zum Auftrag

- Beschäftigtendaten (z.B. Fotos, Namen, Kontaktdaten, Position, Geburtstag).**
- Nutzungsdaten (z.B. Protokollierung der Nutzeraktivitäten, Log-Files).**

Anlage A: Details zum Auftrag

- Beschäftigte und ehemalige Beschäftigte des Auftraggebers**
- Beschäftigte und ehemalige Beschäftigte von verbundenen Unternehmen des Auftraggebers
- Kunden
- Vereinsmitglieder
- Externe Personen

Anlage B: Beim Auftragsverarbeiter umgesetzte Maßnahmen

Massnahme	Schutzziel
Audits	Vertraulichkeit, Integrität, Verfügbarkeit
Bestellung eines Datenschutzbeauftragten	Vertraulichkeit, Integrität, Verfügbarkeit
Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten	Vertraulichkeit, Integrität, Verfügbarkeit
Schriftlicher Vertrag zur Auftragsverarbeitung gem. Art. 28 DS-GVO mit Regelungen zu den Rechten und Pflichten des Auftragnehmers	Vertraulichkeit, Integrität, Verfügbarkeit
Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen.	Vertraulichkeit, Integrität, Verfügbarkeit
Softwaregestützte Tools	Vertraulichkeit, Integrität, Verfügbarkeit
Verpflichtung auf die Vertraulichkeit gem. Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO	Vertraulichkeit, Integrität, Verfügbarkeit
Alarmanlage	Vertraulichkeit
Automatisches Zugangskontrollsystem	Vertraulichkeit
Besucherbuch / Protokoll der Besucher	Vertraulichkeit
Besucherkontrolle	Vertraulichkeit
Bewegungsmelder	Vertraulichkeit
Chipkarten / Transpondersysteme	Vertraulichkeit
Die Backups der privaten Cloudserver werden vor der Übertragung verschlüsselt und per SSH/SCP auf getrennte Backupserver übertragen und dort gespeichert.	Vertraulichkeit
Differenzierte Berechtigungen	Vertraulichkeit
Dokumentation von Berechtigungen	Vertraulichkeit
Empfang / Rezeption / Pförtner	Vertraulichkeit
Getrennte Systeme (logische Mandantentrennung)	Vertraulichkeit
Getunnelte Datenfernverbindungen (VPN=Virtual Private Network)	Vertraulichkeit
Ggf. zusätzliche Absicherung durch einen VPN-Tunnel	Vertraulichkeit
Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)	Vertraulichkeit

Manuelles Schließsystem	Vertraulichkeit
Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk	Vertraulichkeit
Profile- und Rollenkonzept	Vertraulichkeit
Schlüsselverwaltung	Vertraulichkeit
Sichere Übertragung der Daten im Internet durch SSL-Verschlüsselung (https) oder SSH Verbindung	Vertraulichkeit
Sollte der Auftragsnehmer auf Wunsch des Auftraggebers Exporte oder andere Daten vom Server ziehen, so findet die Übertragung und lokale Speicherung ausschließlich verschlüsselt statt.	Vertraulichkeit
Sorgfalt bei Auswahl Reinigungsdienste	Vertraulichkeit
Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)	Vertraulichkeit
SSH mit personalisierten SSH-Keys für die Wartung der Server	Vertraulichkeit
SSL(https) / TLS >= 1.2 für die Nutzung der Software	Vertraulichkeit
Trennung Kontaktdaten	Vertraulichkeit
Trennung Stammdaten	Vertraulichkeit
Trennung von Test- und Entwicklungssystemen	Vertraulichkeit
Türen mit Knauf Außenseite	Vertraulichkeit
Verschluss des Arbeitslaptops im Homeoffice	Vertraulichkeit
Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren.	Vertraulichkeit
Verwaltung von Berechtigungen	Vertraulichkeit
Verwendung von Kennziffern für Kunden oder Personal anstatt Namen	Vertraulichkeit
Videoüberwachung der Eingänge	Vertraulichkeit
Zugriffsberechtigungen	Vertraulichkeit
Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Login Daten	Integrität
Systemseitige Protokollierungen	Integrität

Zugriffsrechte	Integrität
(USV) Unterbrechungsfreie Stromversorgung	Verfügbarkeit
Aufbewahrung von Datensicherung auf einem ausgelagerten Server im Rechenzentrum	Verfügbarkeit
Backup-Verfahren	Verfügbarkeit
IT-Notfallpläne und Wiederanlaufpläne	Verfügbarkeit
Klimaanlage in Serverräumen	Verfügbarkeit
Regelmäßige und dokumentierte Datenwiederherstellungen	Verfügbarkeit
Spiegeln von Festplatten	Verfügbarkeit

18.05.2026
