Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

zwischen[1]

Städtische Wilhelm-Röntgen-Realschule München

Klabundstr. 8

81737 München

- Verantwortlicher –

und

FUJITSU Services GmbH

Mies-van-der-Rohe Straße 8

80807 München

- Auftragsverarbeiter -

Präambel

Der Auftragsverarbeiter stellt dem Verantwortlichen einen Messenger im Rahmen der Vergabe „Kommunikations- und Kollaborationstools 2022 („KoKo 2022“)“ als Software as a Service zur Verfügung, wartet diesen und bietet dem Verantwortlichen darüber hinaus diesbezügliche Zusatzleistungen wie Support, Anpassungs- sowie Beratungs- und Unterstützungsleistungen an. In diesem Zusammenhang verarbeitet er personenbezogene Daten im Auftrag des Verantwortlichen.

Diese Vereinbarung regelt die Verpflichtungen der Vertragsparteien nach Art. 28 Abs. 3 DSGVO und ergänzt insoweit den Vertrag des Auftragsverarbeiters mit dem Bayerischen Staatsministerium für Unterricht und Kultus (StMUK) vom 01.10.2022 (im Folgenden „Auftrag“ genannt). Sie findet Anwendung auf alle Verarbeitungen personenbezogener Daten, die mit dem Auftrag in Zusammenhang stehen und bei denen der Auftragsverarbeiter oder durch den Auftragsverarbeiter beauftragte Dritte personenbezogene Daten für den Verantwortlichen verarbeiten. Die in der vorliegenden

1 Zum Begriff der „Einrichtung“, bzw. auch „nutzungsberechtigten Einrichtung“ siehe Leistungsbeschreibung, Kapitel 3.3.2 als Teil des Auftrags.

Vereinbarung gewählten Begrifflichkeiten entsprechen den Begrifflichkeiten der DSGVO.

1. Gegenstand und Spezifizierung der Auftragsverarbeitung

1.1 Art, Zweck und Gegenstand der Verarbeitung

Zwecke der Verarbeitung

- **Bereitstellung des Messengers**:
  Zweck der Datenverarbeitung ist die Bereitstellung eines Messengers für nutzungsberechtigte Einrichtungen
  Der Messenger bietet insbesondere die Möglichkeit des Austausches von Chatnachrichten (ggfs. inkl. Dateianhängen) und Durchführung von Sprachanrufen zu schulischen bzw. behördlichen Zwecken in Einzel- und Gruppenchaträumen.
  Vgl. zur Bereitstellung insbesondere die Kapitel 4 und 6 der Leistungsbeschreibung als Teil des Auftrags.
- **Wartung des Messengers:**
  Gem. Ziffer 10.3 des EVB-IT Vertrags als Teil des Auftrags schuldet der Auftragnehmer die „Aufrechterhaltung der Betriebsbereitschaft des IT-Systems (vorbeugende Maßnahme)“.
  Hierbei kann der Zugriff auf die dafür erforderlichen personenbezogenen Daten im Rahmen der jeweils angemessenen Tätigkeit notwendig sein.
- **Support:**
  Der Auftragsverarbeiter stellt berechtigten Nutzern zum Support eine Hotline sowie einen E-Mail-Kanal für Supportanfragen zur Verfügung. Im Rahmen der Supportdienstleistung verarbeitet er ebenfalls personenbezogene Daten.
  U.U. wird der Support des Auftragsverarbeiters in ein bestehendes Supportsystem des StMUK eingebunden.
  Vgl. zum Support Ziffer 4.2.3.1 der Leistungsbeschreibung als Teil des Auftrags.
- **Anpassungsdienstleistungen:**
  Gem. Ziffer 10.11.2 des EVB-IT Vertrags als Teil des Auftrags schuldet der Auftragnehmer „[n]ach Bedarf und ausdrücklicher Beauftragung durch den Auftraggeber: Modifikation von Systemkomponenten sowie Weiterentwicklung und Anpassung“.
  Hierbei kann der Zugriff auf die dafür erforderlichen personenbezogenen Daten im

Rahmen der jeweils angemessenen Tätigkeit notwendig sein.

- **Beratungs- und Unterstützungsleistungen**:
  Gem. Ziffer 10.13 des EVB-IT Vertrags als Teil des Auftrags schuldet der Auftragnehmer „[s]onstige Serviceleistungen“, insb. „Beratungs- und Unterstützungsleistungen“.
  Hierbei kann der Zugriff auf die dafür erforderlichen personenbezogenen Daten im Rahmen der jeweils angemessenen Tätigkeit notwendig sein.
- **Testzwecke zur Migration vom mebis IDM bzw. FIBS IDM auf das ByCS IDM**
  Gem. Kriterium BER-08 der Leistungsbeschreibung als Teil des Auftrags ist es dem Auftragsverarbeiter ausnahmsweise gestattet zu Testzwecken personenbezogene Daten aus dem Produktivsystem zu verwenden, soweit die Migration vom mebis IDM bzw. FIBS IDM auf das ByCS IDM getestet werden muss, da aufgrund der sehr hohen Komplexität für eine erfolgreiche Migration ein Vorabtests mit Echtdaten unerlässlich ist.
  Im Rahmen der Tests anfallende personenbezogene Daten sowie Testergebnisse mit Personenbezug sind unverzüglich nach endgültigem Abschluss des entsprechenden Tests zu löschen.

Art der verarbeiteten personenbezogenen Daten[2]

- **Stammdaten** wie in Nr. 3.1.1 in Abschnitt 7 Anlage 2 BaySchO genannt
- **Sichtbare Profilinformationen** wie in Nr. 3.1.2 in Abschnitt 7 Anlage 2 BaySchO genannt
- **Passwort** wie in Nr. 3.1.3 in Abschnitt 7 Anlage 2 BaySchO genannt
- **Inhaltsdaten** wie in Nr. 3.1.4 in Abschnitt 7 Anlage 2 BaySchO genannt
- **Sonstige Nutzungsdaten (Protokolldaten)** gem. 3.1.5 in Abschnitt 7 Anlage 2 BaySchO genannt
- **Video- und Bilddaten** für die Videonutzung wie in Nr. 3.2 in Abschnitt 7 Anlage 2 BaySchO genannt
- **Audiodaten** für die Nutzung von Ton bei Videonutzung oder Telefonie (bei Video- oder Telefonkommunikation) wie in Nr. 3.2 in Abschnitt 7 Anlage 2 BaySchO genannt
- **Gruppenbezogene Nutzungsdaten** wie in Nr. 3.3 in Abschnitt 7 Anlage 2 BaySchO genannt

2 Für nicht-schulische Einrichtungen handelt es sich bei den nachfolgenden Verweisen auf Abschnitt 7 Anlage 2 BaySchO um Rechtsfolgenverweisungen.

Ausgeschlossen ist die Verarbeitung von

- besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO), insbesondere Gesundheitsdaten und
- Daten, die einem besonderen strafrechtlichen Geheimnisschutz unterliegen,

soweit sie nicht durch Bekanntmachung des StMUK zugelassen wird, die die jeweiligen Anforderungen an die Datensicherheit festlegt.

<u>Kategorien der betroffenen Personen</u>

- Bei einer Nutzung des Messengers durch bayerische Schulen:
    - Pädagogisches Personal: Lehrkräfte, Betreuungspersonal förderbedürftiger Schülerinnen und Schüler, Studienreferendarinnen und Studienreferendare, Lehramtsstudierende im Schulpraktikum, weiteres pädagogisches Personal (z. B. Ganztagsbetreuung)
    - Verwaltungs- und Hauspersonal
    - Schülerinnen und Schüler
    - Gastnutzer
    - Weitere Personen, die von der Video- oder Tonübertragung erfasst werden (z. B. Schulbegleitungen)

- Bei einer Nutzung des Messengers durch nicht-schulische nutzungsberechtigte Einrichtungen:
    - Beschäftigte
    - Gastnutzer
    - Weitere Personen, die von der Video- oder Tonübertragung erfasst werden

1.2 Die in diesem Vertrag vereinbarten Leistungen und damit verbundene Datenverarbeitungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in einem Drittland, für welches ein gültiger Angemessenheitsbeschluss der Europäischen Kommission vorliegt (Art. 45 DSGVO), erbracht. Dies gilt unabhängig davon, ob diese von dem Auftragsverarbeiter selbst oder

weiteren Auftragsverarbeitern erbracht werden (siehe Ziffer 6 dieser Vereinbarung).

2. Rechte und Pflichten des Auftragsverarbeiters

2.1 Der Auftragsverarbeiter verarbeitet Daten von betroffenen Personen ausschließlich im Rahmen der getroffenen Vereinbarungen und der dokumentierten Weisungen des Verantwortlichen sowie entsprechend den datenschutzrechtlichen Regelungen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder der Mitgliedstaaten der Europäischen Union, dem der Auftragsverarbeiter unterliegt, verpflichtet ist. In letzterem Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 Buchst. a DSGVO). Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen Daten für keine anderen und insbesondere nicht für eigene Zwecke. Kopien der Daten werden, ohne dass sie im Auftrag oder in diesem Vertrag geregelt sind, nicht erstellt.

Sofern Weisungen des Verantwortlichen zunächst mündlich erfolgen, sind sie unverzüglich schriftlich oder elektronisch zu bestätigen.

Soweit der Auftraggeber eine Einrichtung in Trägerschaft der katholischen oder evangelischen Kirche ist, unterwirft sich der Auftragnehmer der jeweiligen kirchlichen Datenschutzaufsicht (vgl. § 29 Abs. 4 lit. h, § 32 KDG bzw. § 30 Abs. 5 Satz 3 DSG-EKD).

2.2 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Ist die Rechtmäßigkeit einer Weisung zweifelhaft, ist der Auftragsverarbeiter berechtigt, die Durchführung der Weisung so lange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird. Stehen schwere Persönlichkeitsrechtsverletzungen im Raum oder nimmt der Auftragsverarbeiter bei weisungsgemäßem Handeln das Risiko einer strafbaren Handlung auf sich, darf er die Umsetzung der Weisung darüber hinaus aussetzen, bis die Parteien eine einvernehmliche Lösung gefunden haben.

2.3 Der Auftragsverarbeiter gestaltet seine innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft insbesondere geeignete

technische und organisatorische Maßnahmen, um einen dem Risiko angemessenen Schutz der Daten des Verantwortlichen zu gewährleisten (Art. 32 Abs. 1 DSGVO). Er trifft diese technischen und organisatorischen Maßnahmen so, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sind. Die entsprechenden technischen und organisatorischen Maßnahmen ergeben sich aus der Anlage 1. Änderungen der getroffenen Maßnahmen durch den Auftragsverarbeiter sind nur zulässig, wenn sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind dem Verantwortlichen mitzuteilen und mit diesem abzustimmen.

2.4 Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte (Art. 28 Abs. 3 Buchst. e DSGVO) und unterstützt den Verantwortlichen unter Berücksichtigung der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, wie etwa bei erforderlichen Datenschutz-Folgenabschätzungen (Art. 28 Abs. 3 Satz 2 Buchst. f DSGVO).

2.5 Der Auftragsverarbeiter gewährleistet, dass es den mit der Verarbeitung der Daten des Verantwortlichen befassten Beschäftigten und anderen für den Auftragsverarbeiter tätigen Personen nach Maßgabe des Art. 29 DSGVO untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragsverarbeiter, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

2.6 Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn ihm im Rahmen des Auftragsverhältnisses Verletzungen des Schutzes personenbezogener Daten des Verantwortlichen bekannt werden. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

2.7 Der Auftragsverarbeiter nennt dem Verantwortlichen Ansprechpartner für im Rahmen des Vertrages anfallende Weisungen sowie einen etwaigen Datenschutzbeauftragten. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem

Verantwortlichen die Kontaktdaten eines neuen, zuständigen Ansprechpartners bzw. etwaigen Datenschutzbeauftragten unverzüglich anzuzeigen.

Ansprechpartner des Auftragsverarbeiters:

Name: Robert Schmid

Funktion: Service Manager

Telefon: +49 89 62060 2667

E-Mail: robert.schmid3@fujitsu.com und bycs-msg.sdm@fujitsu.com

Datenschutzbeauftragter des Auftragsverarbeiters

Name: Strobel, Stefan

Funktion: Datenschutzbeauftragter

Anschrift: Mies-van-der-Rohe-Str. 8, 80807 München

Telefon: +49 89 62060 2111

E-Mail: datenschutzbeauftragter@ts.fujitsu.com

2.8 Der Auftragsverarbeiter berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Verantwortliche dies anweist und dies vom Weisungsrahmen umfasst ist, es sei denn, die Weisung widerspricht etwaigen gesetzlichen Aufbewahrungspflichten.

2.9 Nach Auftragsende sind Daten, Datenträger sowie sonstige Materialien auf Verlangen und nach Wahl des Verantwortlichen entweder zurückzugeben oder zu löschen, sofern nicht nach dem Recht der Europäischen Union oder dem Recht der Mitgliedstaaten der Europäischen Union eine Verpflichtung zur weiteren Speicherung der personenbezogenen Daten besteht.

2.10 Im Falle einer Inanspruchnahme des Verantwortlichen durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftragsverarbeiter, den Verantwortlichen bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

3. Rechte und Pflichten des Verantwortlichen

3.1 Der Verantwortliche ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Beurteilung der Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO, die Datenweitergabe an den Auftragsverarbeiter sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

3.2 Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, falls er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3.3 Im Falle einer Inanspruchnahme des Auftragsverarbeiters durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Verantwortliche, den Auftragsverarbeiter bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

3.4 Der Verantwortliche nennt dem Auftragnehmer im Rahmen eines vom StMUK zur Verfügung gestellten, digitalen Portals zur Unterzeichnung solcher Vereinbarungen (im Folgenden: AVV Portal, siehe dazu Kapitel 4.1.5 der Leistungsbeschreibung als Teil des Auftrags) weisungsberechtigte Personen für im Rahmen des Vertrages anfallende Weisungen sowie den Datenschutzbeauftragten. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Auftragnehmer unverzüglich die Kontaktdaten eines neuen, zuständigen Ansprechpartners bzw. Datenschutzbeauftragten anzuzeigen.

<u>Weisungsberechtigte Personen des Verantwortlichen</u>

Leiter(in) der Einrichtung

Name:

RSDin Sandra Kranz

Telefon:

E-Mail: sandra.kranz@muenchen.de

Administrator der Einrichtung

E-Mail: Tarenz, Ralph, ; Schächer, Lisa,

Behördlicher Datenschutzbeauftragte(r) des Verantwortlichen

LH München, Referat für Bildung und Sport

Anschrift: Bayerstraße 28; 80335 München

E-Mail: datenschutz.rbs@muenchen.de

Telefon: 089-23383978

3.5 Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen. Die Befugnisse der Aufsichtsbehörden – insbesondere nach Art. 58 Abs. 1 DSGVO – bleiben hiervon unberührt.

4. Anfragen betroffener Personen

Macht eine betroffene Person ihre Rechte gemäß Art. 15 ff. DSGVO gegenüber dem Auftragsverarbeiter geltend, wird dieser die betroffene Person an den Verantwortlichen verweisen, sofern eine Zuordnung an den Verantwortlichen auf Basis der Angaben der betroffenen Person möglich ist. Gemäß Nr. 2.4 dieser Vereinbarung unterstützt der Auftragsverarbeiter den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen.

5. Kontrollrechte des Verantwortlichen

5.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung (Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO).

5.2 Sofern einschlägig, verpflichtet sich der Auftragsverarbeiter, den Verantwortlichen 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.

5.3 Der Verantwortliche ist berechtigt, sich vor Beginn und während der Verarbeitung von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen. Dies und Maßnahmen nach Nr. 5.4 werden nicht durch die Vorlage von Nachweisen nach Nr. 5.1 ausgeschlossen.

5.4 Inspektionen durch den Verantwortlichen oder durch einen von diesem beauftragten Prüfer werden grundsätzlich nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlauffrist zu den üblichen Geschäftszeiten durchgeführt. Der Auftragsverarbeiter hat die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung abhängig zu machen, wenn die Möglichkeit besteht, dass der Verantwortliche oder ein von diesem beauftragter Prüfer im Rahmen seiner Inspektion auch Kenntnis von Daten erlangt, die der Auftragsverarbeiter im Auftrag eines anderen Verantwortlichen verarbeitet. Der Verantwortliche stellt sicher, dass ein von ihm beauftragter Prüfer in keinem Wettbewerbsverhältnis zu dem Auftragsverarbeiter steht.

6. Subunternehmer (weitere Auftragsverarbeiter)

6.1 Ein Subunternehmerverhältnis liegt vor, wenn der Auftragsverarbeiter weitere Auftragsverarbeiter mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt.

Der Auftragsverarbeiter trägt bei der Auswahl eines Subunternehmers insbesondere Sorge dafür, dass dieser hinreichende Garantien dafür bietet, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung personenbezogener Daten entsprechend den Anforderungen der Datenschutz-Grundverordnung erfolgt.

Nicht als Subunternehmerverhältnis im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice (wenn ein Zugriff auf personenbezogene Daten des Verantwortlichen ausgeschlossen ist), Reinigungskräfte und Prüfer. Der Auftragsverarbeiter trifft mit diesen Dritten im erforderlichen Umfang schriftliche Vereinbarungen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen

zu gewährleisten und behält sich Kontrollmaßnahmen vor, um den Schutz und die Sicherheit der Daten des Verantwortlichen zu gewährleisten.

6.2 Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO). In dem Vertrag mit dem Subunternehmer sind dieselben datenschutzrechtlichen Pflichten aus der vorliegenden Vereinbarung dem Subunternehmer wirksam aufzuerlegen. Insbesondere muss der Verantwortliche berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

6.3 Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragsverarbeiter im Einklang mit dem vorliegenden Abschnitt vertraglich auferlegt wurden.

6.4 Der Auftragsverarbeiter nimmt keinen Subunternehmer ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung in Anspruch. Der Auftragsverarbeiter teilt dem Verantwortlichen die bereits bei Abschluss dieses Vertrags bestehenden Subunternehmer vorab mit. Die bei Vertragsbeginn bestehenden Subunternehmer wurden vom Auftragsverarbeiter im Rahmen seines Angebots in der Anlage 2 benannt. Diese gelten als von Beginn des Auftrages an genehmigt.

6.5 Gemäß den vorgenannten Regelungen erteilt der Verantwortliche dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 Abs. 2 DSGVO in Anspruch zu nehmen (Art. 28 Abs. 2 Satz 1 Alt. 2, Satz 2 DSGVO). Der Auftragsverarbeiter informiert den Verantwortlichen frühzeitig, wenn er Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Verantwortliche kann gegen derartige Änderungen Einspruch erheben. Der Einspruch ist innerhalb von einem Monat nach Zugang der Information über die Änderungen schriftlich gegenüber dem Auftragsverarbeiter einzulegen. Kann keine einvernehmliche Lösung erzielt werden, erfolgt eine Einschränkung oder Beendigung der Auftragsverarbeitung.

6.6 Eine Beauftragung von Subunternehmern mit Sitz in Drittländern außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums darf nicht erfolgen. Dies gilt nicht, wenn für das betreffende Drittland ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt (Art. 45 DSGVO).

7. Haftung und Schadensersatz

Die Vertragsparteien haften entsprechend den einschlägigen gesetzlichen Bestimmungen bzw. gegenüber betroffenen Personen gemäß Art. 82 DSGVO.

8. Schlussbestimmungen

8.1 Die Laufzeit der vorliegenden Vereinbarung entspricht der Laufzeit des Auftrags.

8.2 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn die Daten des Verantwortlichen durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter beim Auftragsverarbeiter gefährdet werden. Der Auftragsverarbeiter informiert in diesem Fall alle Beteiligten unverzüglich darüber, dass das Eigentum an den Daten ausschließlich beim Verantwortlichen liegt.

8.3 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen oder in einem elektronischen Format abgefassten Vereinbarung, die den ausdrücklichen Hinweis darauf enthält, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt.

8.4 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so ist die Wirksamkeit der übrigen Regelungen hiervon nicht betroffen. In diesem Falle werden die Parteien einvernehmlich eine neue Regelung oder Ergänzung der bestehenden Regelung vereinbaren, die die unwirksame oder undurchführbare Regelung in einer Art und Weise ersetzt bzw. ergänzt, die der ursprünglich von den Parteien bei Abfassung dieser Anlage beabsichtigten Regelung am nächsten kommt, hätten sie denn die Unwirksamkeit oder Undurchführbarkeit bedacht. Dies gilt auch für Regelungslücken.

München ,den 31.07.2023

Ort Datum

gez. Bastian Ligniez

- Verantwortlicher -

München, den 31.07.2023

Ort Datum

- Auftragsverarbeiter -

Anlage 1 - Technische und organisatorische Maßnahmen

Die Anlage 1 dient dem Nachweis der nach Art. 32 DSGVO genannten, seitens des Auftragsverarbeiters getroffenen Maßnahmen zur Datensicherheit. (S. 3.2 der vorliegenden Vereinbarung). Der Auftragsverarbeiter hat dabei auf alle Unterpunkte der folgenden Gliederung einzugehen und jeweils ***alle tatsächlich vorhandenen*** *technischen und/oder organisatorischen Maßnahmen zu benennen.*

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

1.1 Zutrittskontrolle

1.2 Zugangskontrolle

1.3 Zugriffskontrolle

1.4 Trennungskontrolle

2. Pseudonymisierung und Verschlüsselung nach Art. 32 Abs. 1 lit. a DSGVO
3. Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO
4. Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

4.1 Weitergabekontrolle

4.2 Eingabekontrolle

5. Verfügbarkeit gem. art. 32 Abs. 1 lit. b DSGVO

6. Belastbarkeit gem. Art. 32 Abs. 1 lit. b DSGVO

7. Wiederherstellung gem. Art. 32 Abs. 1 lit. c DSGVO

8. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d DSGVO

Auftragnehmer Technische und organisatorische Maßnahmen zur Lösung

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

11 Zutrittskontrolle

Maßnahmen, die dazu dienen, Unberechtigten den Zutritt zu Systemen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Gebäude/Gelände • Alarmanlage (Einbruch-, Kontaktmelder für Zugänge - Fenster, Türen) **Kameraüberwachung** • der Gebäudezugänge • der Zugänge zum Rechenzentrumsraum • der Zugänge zu sensiblen Infrastrukturräumen **Zutrittsmanagement** • Automatisches Zugangskontrollsystem • Chipkarten-/Transponder-Schließsystem • Manuelles Schließsystem mit Sicherheitsschlössern • Sichere Schlüsselaufbewahrung / Schlüsseltresor	**Personenkontrolle** • Anwesenheitszeit von Personen im Sicherheitsbereich wird protokolliert • Einteilung in Sicherheitszonen / Sperrbereiche • Gruppierung der Zutrittsbefugnisse nach Aufgaben- und Zuständigkeitsgebiet • Regelmäßige Kontrollrundgänge • Personenkontrolle durch Empfang / Pförtner / Werkschutz • Protokollierung von Besuchern **Rechte Management** • Prozess zur Vergabe/Entzug von Zutrittsrechten und -token • Regelmäßige Überprüfung von vergebenen Zutrittsrechten • Schlüsselregelung **Dienstleister Management** • Begleitung von Dienstleistern in Sicherheitsbereichen • Sorgfältige Auswahl von Reinigungspersonal

	• Sorgfältige Auswahl von Sicherheitspersonal • Tragepflicht von Mitarbeiter-/ Gastausweisen **Zutrittsmanagement** • Zutritt in sensitive Infrastrukturbereiche ist streng limitiert • Zutritt in Rechenzentrumsräume streng limitiert • Zutrittsregelung schriftlich fixiert

12 Zugangskontrolle

Maßnahmen, die verhindern sollen, dass Systeme von Unberechtigten genutzt werden können.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Verschlüsselung von Notebooks / Laptops	Berechtigungskonzept für Zugänge zu IT-Systemen
Authentifizierung mit personifizierten Zugangsdaten	Erstellen von Benutzerprofilen
Automatische und kennwortgeschützte PC-Bildschirmsperre	Passwortrichtlinie und geschützte Passwortvergabe
Automatische Sperrung bei fehlgeschlagenen Anmeldeversuchen	Protokollierung von fehlgeschlagenen Zugriffsversuchen
Einsatz von Anti-Viren-Software	Prozess zur Rechtevergabe / zum Rechteentzug
Einsatz von Firewalls	Rechtevergabe durch geschultes Personal
Einsatz von VPN bei Remote-Zugriffen auf IT-Systeme	Regelmäßige Überprüfung von Richtlinien auf Aktualität und Wirksamkeit
	Regelmäßige Überprüfung von Zugangsrechten

13 Zugriffskontrolle

Maßnahmen, die sicherstellen sollen, dass die Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Technische Maßnahmen	Organisatorische Maßnahmen
Berechtigungsebenen nach Abteilungen und Zugriffserfordernissen	Berechtigungskonzept mit Minimalprinzip etabliert
Automatische und kennwortgeschützte PC-Bildschirmsperre	Clean-Desk- und Clean-Screen-Richtlinie
Verschlossene Entsorgungstonnen von zertifizierten Datenvernichtern	Etablierter Datenvernichtungs-/ Datenlösch-Prozess
Protokollierung von Zugriffen	Es werden zeitnah im Rahmen der Rechenzentrumswartung Software und Security Updates durchgeführt. Außerhalb dieses Rahmens wird in Abstimmung mit dem Auftraggeber für kritische Sicherheitsschwachstellen ein Out-of-Band Patchprozess zur Verfügung gestellt.
Einsatz von Aktenvernichtern oder Entsorgungstonnen	Etablierter Rückbauprozess bei Produktkündigungen
Löschung von Datenträgern vor deren Wiederverwendung	Klassifizierung von Informationen nach vorgegebener Richtlinie
	Passwortrichtlinie
	Regelmäßige Überprüfung der Richtlinien und Prozesse auf Aktualisierung
	Sichere Aufbewahrung von Datenträgern
	Verwaltung der Benutzerrechte durch geschulte Systemadministratoren

14 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Technische Maßnahmen	Organisatorische Maßnahmen

Der Auftragnehmer setzt hierzu im Bereich der Separierung von Netz und Netzsegmenten die VLAN Technologie ein.	Festlegung von Datenbankrechten
Logische Mandantentrennung	Es ist durch den Auftragnehmer und dessen technische Konzeption sichergestellt, dass unterschiedliche Auftraggeber (unabhängig ihrer Berechtigung für das Rollenkonzept und Usermanagement auf Applikationsebene) keinen Zugriff auf fremde Daten nehmen oder erhalten können. Diese Mandantentrennung wird im Berechtigungsmanagement fortgeführt (Prinzip der minimalen Rechte)
Versehen der Datensätze mit Zweckattributen / Datenfeldern	

2. Pseudonymisierung und Verschlüsselung nach Art. 32 Abs. 1 lit. a DSGVO

Technische Maßnahmen	**Organisatorische Maßnahmen**
Der Zugriff auf Auftraggebersysteme erfolgt grundsätzlich nur mit Protokollen, welche eine verschlüsselte Kommunikation sicherstellen (z.B. SSH, RDP). Ausnahmen bestehen insbesondere bei Produkten, welche eine Konfiguration dahingehend nicht zulassen.	
Der Fernzugriff (insbesondere für den Bereitschaftsdienst) erfolgt über VPN und ist verschlüsselt. Der Auftragnehmer setzt hierbei anerkannte Maßnahmen zur Verschlüsselung ein.	
Einsatz von Verschlüsselung bei Web-Übertragung (HTTPS)	

3. Datenminimierung

Die Datenminimierung nach Art. 5 Abs. 1 lit. C DSGVO wird durch ein Löschkonzept gewährleistet.

4. Integrität gem. Art. 32 Abs. 1 lit. B DSGVO

41 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten nicht unberechtigt verarbeitet werden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Einsatz von VPN bei Remote-Zugriffen auf IT-Systeme	Klassifizierung von Informationen nach vorgegebener Richtlinie
Einsatz von Verschlüsselung bei Web-Übertragung (flächendeckender Einsatz von HTTPS)	Der Umgang mit Druckern, Kopierern und Multifunktionsgeräten ist in der Benutzerrichtlinie geregelt.
Protokollierung von Zugriffen	Etablierter Datenvernichtungs-/ Datenlösch-Prozess
Einsatz von Aktenvernichtern oder Entsorgungstonnen	
Löschung von Datenträgern vor deren Wiederverwendung	
Elektronische Kommunikation, welche über öffentliche Leitungen erfolgt, wird generell verschlüsselt	
Eine Elektronische Datenübermittlung erfolgt in der Rechenzentrumsinfrastruktur ausschließlich über dedizierte Leitungen, die nicht von Dritten genutzt werden können	

42 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft werden kann, ob und von wem Daten verarbeitet wurden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Protokollierung von Zugriffen	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes

	Der Auftragnehmer gewährleistet durch eine entsprechende Verpflichtung seiner Arbeitnehmer und die Umsetzung ausreichender Zutritts-/, Zugangs- und Zugriffskontrolle, dass schützenswerte Daten nicht von unbefugten Dritten oder Arbeitnehmern / Organen von Auftragnehmer eingegeben bzw. verändert werden.
	Änderungen durch den Auftragnehmer werden nach entsprechenden Service Managementprozessen (Change und Incident) dokumentiert.

5. Verfügbarkeit gem. Art. 32 Abs. 1 lit. b DSGVO

Technische Maßnahmen	**Organisatorische Maßnahmen**
Monitoring aller relevanten Infrastruktur- und IT-Systeme	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
Feuer- und Rauchmeldeanlagen	Regelmäßige Backups und Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
Feuerlöscher im Serverraum vorhanden	Serverräume über der Wassergrenze, oder ausreichendes Pumpensystem vorhanden
Feuerlöscher in Büros und Infrastrukturräumen vorhanden	
Feuerlöschanlage (Argon/Stickstoff) im Serverraum vorhanden	
Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	
Klimaanlage für Serverräume	
Netzwerkanbindung über zwei separate Zuleitungen	
Netzwerkanbindung über mind. zwei unterschiedliche Carrier	

Autonome Stromversorgung über eigene Trafostation	
Netzersatzanalage vorhanden (Diesel-Aggregat)	
Stromanbindung in Serverracks über zwei separate Zuführungen	
Stromversorgung der Rechen-zentrumsräume über zwei Zuleitungen	
Unterbrechungsfreie Stromversorgung - USV-Anlage für Serverräume	
Unterbrechungsfreie Stromversorgung für relevante Infrastruktur- und IT-Systeme	
Einsatz von Datenspiegelung (RAID) für relevante IT-Systeme	

6. Belastbarkeit gem. Art 32 Abs. 1 lit. b DSGVO

Technische Maßnahmen	**Organisatorische Maßnahmen**
Siehe Maßnahmen unter Ziffer 5 („Verfügbarkeit“)	Siehe Maßnahmen unter Ziffer 5 („Verfügbarkeit“)

7. Wiederherstellung gem. Art. 32 Abs. 1 lit. c DSGVO

Technische Maßnahmen	**Organisatorische Maßnahmen**
Datensicherung und Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort	Notfallkonzept für relevante Infrastruktur- und IT-Systeme vorhanden
	Regelmäßige Tests der Datenwieder-herstellung

8. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d DSGVO

Technische Maßnahmen	**Organisatorische Maßnahmen**

	Überprüfung der Maßnahmen im Rahmen der Wirksamkeitskontrolle des Informationssicherheitsmanagement-systems (ISMS - gemäß DIN ISO/IEC 27001)
	Kontinuierlicher Verbesserungsprozess im Rahmen des ISMS

Anlage 2 - Liste der Subunternehmer (weitere Auftragsverarbeiter)

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer (weitere Auftragsverarbeiter) im Sinne der Nr. 6.4 der Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 Abs. 3 DSGVO.

Firma/Adresse	**Kontaktdaten/Ansprechpartner**	**Leistung**
PlusServer GmbH Hohenzollernring 72 50672 Köln	Büttner, Jens Key Account Manager Tel.: +49 2203 1045 3221 E-Mail: Jens.Buettner@plusserver.com	Die PlusServer GmbH stellt Ressourcen für das Hosting der Messenger-Lösung zur Verfügung.
Sdui GmbH Universitätsstr. 3 56070 Koblenz	Jan Luca Pulst Head of Engineering / Product Tel: +49 1578 7437625 E-Mail: jan-luca.pulst@sdui.de	Die Sdui GmbH stellt einen den Anforderungen entsprechenden Messenger, Sprach- und Videotelefonie, sowie anteilige Betriebs- und Supportleistungen zur Verfügung.
Friendly Captcha GmbH Am Anger 3-5 82237 Woerthsee	Benedict Padberg Geschäftsführer Tel.: ++49 89 21 54 8 11 80 E-Mail: ben@emessage.friendlycaptcha.com	Die Friendly Captcha GmbH stellt einen DSGVO konformen Captcha Dienst bereit. Der Dienst wird genutzt, um die Registrierung von Gastnutzern für den Messenger Dienst abzusichern.
• Klicken um Text einzugeben..	• Klicken um Text einzugeben.	• Klicken um Text einzugeben..