Peter-Behrens-Platz 9
4020 Linz/Austria
Tel. +43 (0)732/931-666-0
office@506.ai
www.506.ai

Vereinbarung über eine Auftragsverarbeitung nach Art 28 DSGVO

für die SaaS-Softwarelösung ***506 CompanyGPT*** der

506 Data & Performance GmbH
Peter-Behrens-Platz 9, 4020 Linz, Österreich
UID-Nr. ATU 74906257

nachstehend "Auftragnehmer" genannt.

Stand per Oktober 2023

Inhaltsverzeichnis

1	GEGENSTAND UND DAUER DER VEREINBARUNG	3
2	KONKRETISIERUNG DES AUFTRAGSINHALTS	3
3	TECHNISCH-ORGANISATORISCHE MASSNAHMEN	6
4	BERICHTIGUNG, EINSCHRÄNKUNG UND LÖSCHUNG VON DATEN	7
5	QUALITÄTSSICHERUNG UND SONSTIGE PFLICHTEN DES AUFTRAGNEHMERS	7
6	SUBAUFTRAGSVERHÄLTNISSE	8
7	KONTROLLRECHTE DES AUFTRAGGEBERS	10
8	MITTEILUNG BEI VERSTÖSSEN DES AUFTRAGNEHMERS	11
9	WEISUNGSBEFUGNIS DES AUFTRAGGEBERS	12
10	LÖSCHUNG UND RÜCKGABE VON PERSONENBEZOGENEN DATEN	12
11	HAFTUNG UND BEWEISLAST	12
12	SCHLUSSBESTIMMUNGEN	13

Präambel

Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien" genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der Datenschutz-Grundverordnung („DSGVO") zu verstehen.

1 GEGENSTAND UND DAUER DER VEREINBARUNG

1.1 Rollenverteilung

Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO. Der Auftragnehmer ist Auftragsverarbeiter des Auftraggebers.

1.2 Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Lizenzvereinbarung (dem SaaS-Vertrag) zwischen dem Auftragnehmer und dem Auftraggeber, auf die hier verwiesen wird (im Folgenden Lizenzvereinbarung) und die darin erwähnten Nutzungsbedingungen.

1.3 Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Lizenzvereinbarung.

2 KONKRETISIERUNG DES AUFTRAGSINHALTS

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: Es wird ein KI-basiertes Large Language Model (GPT) zur Verfügung gestellt, welches Useranfragen durch ein vortrainiertes Modell beantwortet. Das Modell wird in einem Rechenzentrum innerhalb der Europäischen Union betrieben und ist gänzlich von außen abgeschottet. Zu keinem Zeitpunkt werden Userdaten nach außen gegeben oder zum Training des Modells verwendet.

2.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien, Zutreffendes bitte ankreuzen)

x Berufliche Kontakt- und (Arbeits-) Organisationsdaten

zB Name, Vorname, E-Mailadresse

x IT-Nutzungsdaten

zB UserID, Rollen, Berechtigungen, Login-Zeiten, Rechnername, IP-Adresse

x Sonstige:

Daten, welche der Auftraggeber nach freier Wahl in das System einbringt, um dem Modell darüber Fragen zu stellen. Diese Daten werden nur flüchtig vorgehalten und nicht gespeichert. Die Auswahl über die Art und den Umfang der Daten kann vom Auftragnehmer nicht beeinflusst werden und liegt somit in der Verantwortung des Auftraggebers.

2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen (Zutreffendes bitte ankreuzen):

x Mitarbeiter (Mitarbeiter der eigenen Konzerngesellschaft)

zB Arbeitnehmer, Lehrlinge, Bewerber, ehemalige Beschäftigte

x Konzern-Mitarbeiter (Mitarbeiter anderer Konzerngesellschaften)

zB User ID, Rollen, Berechtigungen, Login-Zeiten, Rechnername, IP-Adresse

x Sonstige:

Daten in Datenkategorien, welche der Auftraggeber nach freier Wahl in das System einbringt, um dem Modell darüber Fragen zu stellen. Diese Daten werden nur flüchtig vorgehalten und nicht gespeichert. Die Auswahl über die Art und den Umfang der Daten und somit auch deren Datenkategorie kann von Auftragnehmer nicht beeinflusst werden und liegt somit in der Verantwortung des Auftraggebers.

2.4 Angemessenes Datenschutzniveau

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 Art 44 ff DSGVO erfüllt sind.

3 TECHNISCH-ORGANISATORISCHE MASSNAHMEN

3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben.

3.2 Wenn Datenträger des Auftraggebers benutzt werden, sind diese besonders zu kennzeichnen, aufzubewahren und nur befugten Personen zugänglich zu machen. Der Auftragnehmer hat in regelmäßigen Abständen den Nachweis der Erfüllung seiner Pflichten, also insbesondere technischen und organisatorischen Maßnahmen und deren Wirksamkeit unaufgefordert zu erbringen. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.3 Der Auftragnehmer hat die Sicherheit gem Art 28 Abs 3 lit c, 32 DSGVO insbesondere in Verbindung mit Art 5 Abs 1, Abs 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der 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 DSGVO zu berücksichtigen.

3.4 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

3.5 Die Beschreibung der technischen und organisatorischen Maßnahmen hat so detailliert zu erfolgen, dass für einen sachkundigen Dritten der Leistungsinhalt zweifellos zuordenbar ist. Die aktuelle Liste der technischen und organisatorischen Maßnahmen sind an diese Auftragsverarbeitungsvereinbarung angehängt.

3.6 Die im Auftrag verarbeiteten Daten sind von sonstigen Datenbeständen des Auftragsnehmers strikt zu trennen und es dürfen keinerlei Duplikate oder Kopien erstellt werden, sofern diese nicht technisch notwendige, bloß temporäre Vervielfältigungen beinhalten und ohne Beeinträchtigung des vereinbarten Datenschutzniveaus erfolgen. In jedem Fall ist der Auftraggeber von Kopien oder Duplikaten zu verständigen.

4 BERICHTIGUNG, EINSCHRÄNKUNG UND LÖSCHUNG VON DATEN

4.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers 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 weiterleiten.

4.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5 QUALITÄTSSICHERUNG UND SONSTIGE PFLICHTEN DES AUFTRAGNEHMERS

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

Der Auftragnehmer wird durch folgenden externen Datenschutzbeauftragten vertreten:

EY Law
Pelzmann Gall Größ
Rechtsanwälte GmbH
Wagramer Straße 19, IZD-Tower
1220 Wien

Als Ansprechpartner beim Auftragnehmer wird Herr Gerhard Kürner, CEO, T: +43 732 931 666, M: +43 650 4466777, E: gdpr@506.ai benannt.

Die Wahrung der Vertraulichkeit erfolgt gemäß Art 28 Abs 3 S 2 lit b, 29, 32 Abs 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der dokumentierten Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

Die Verpflichtung zur Vertraulichkeit gilt auch über das Vertragsende hinaus und bleibt hinsichtlich der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung der Tätigkeit bzw. Ausscheiden beim Auftragnehmer aufrecht.

Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art 28 Abs 3 S 2 lit c, 32 DSGVO.

Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem gerichtlichen Verfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

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.

Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6 SUBAUFTRAGSVERHÄLTNISSE

6.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer zB. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2 Der Auftragnehmer darf Subauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw dokumentierter Zustimmung des Auftraggebers beauftragen.

(i) □ Eine Subbeauftragung ist generell unzulässig.

(ii) x Der Auftraggeber stimmt der Beauftragung der nachfolgenden Subauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art 28 Abs 2-4 DSGVO zu:

Firma	Adresse	Leistung
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18	Hosting des Large Language Models im Azure-Cloudrechenzentrum in Frankfurt am Main. Der Subunternehmer hat weder Zugriff auf Daten, noch ist er in irgendeiner Art und Weise mit operativen Tätigkeiten betraut.

(iii) Die Auslagerung auf Subauftragnehmer oder

der Wechsel des bestehenden Subauftragnehmers

sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Subauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

6.3 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Subbeauftragung gestattet.

6.4 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit gemäß Art. 44 bis 50 DSGVO durch entsprechende Maßnahmen sicher.

6.5 Eine weitere Auslagerung durch den Subauftragnehmer

□ ist nicht gestattet;

□ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (Email);

x sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Subauftragnehmer aufzuerlegen.

6.6 Der Subauftragnehmer übernimmt alle Datenschutzpflichten mit mindestens gleichem Schutzniveau, die Verantwortlichkeiten von Auftragnehmer und Subauftragnehmer sind eindeutig voneinander abzugrenzen. Rechte des Auftraggebers dürfen auch gegenüber dem Subauftragnehmer ausgeübt werden, wobei der Auftragnehmer für die Einhaltung der Pflichten zu regelmäßigen Kontrollen verpflichtet ist bzw für etwaige Pflichtverletzungen nach Art 82 DSGVO haftet. Die Kontrollrechte des Auftraggebers gelten in gleicher Weise gegenüber dem Subauftragsnehmer.

7 KONTROLLRECHTE DES AUFTRAGGEBERS

7.1 Der Auftraggeber hat das Recht, Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich insbesondere durch unangekündigte Stichprobenkontrollen, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (zB Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit.

8 MITTEILUNG BEI VERSTÖSSEN DES AUFTRAGNEHMERS

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören unter anderem

(i) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

(ii) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;

(iii) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

(iv) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung; sowie

(v) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8.2 Die Mitteilung der Verletzung des Schutzes personenbezogener Daten (= Data Breach bzw Datenpanne) an den Auftraggeber hat jedenfalls die Art der Verletzung, die Angabe der Kategorien und ungefähre Zahl der betroffenen Personen, der betroffenen Kategorien und ungefähren Zahl der betroffenen personenbezogenen Datensätze zu umfassen, Namen und Kontaktdaten des etwaigen Datenschutzbeauftragen sowie Maßnahmen zur Abmilderung der Folgen der Datenschutzverletzung. Des Weiteren sind auch erhebliche Störungen der Auftragserledigung sowie Verstöße von Mitarbeitern des Auftragnehmers unverzüglich an den Auftraggeber mitzuteilen. Der Auftragnehmer kennt die für den Auftraggeber geltende Meldepflicht nach Art 33 DSGVO, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei entsprechenden Meldepflichten unterstützen.

9 WEISUNGSBEFUGNIS DES AUFTRAGGEBERS

9.1 Mündliche Weisungen bestätigt der Auftragnehmer unverzüglich, die Bestätigung der Weisung erfolgt an eine vom Auftraggeber zu nennende Email-Adresse.

9.2 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10 LÖSCHUNG UND RÜCKGABE VON PERSONENBEZOGENEN DATEN

10.1 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.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Lizenzvereinbarung – 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 vorzulegen.

10.3 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.

11 HAFTUNG UND BEWEISLAST

Der Auftragnehmer trägt die Beweislast, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung. Die Ersatzpflichten gelten nicht, sofern der Schaden trotz korrekter Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber nachweislich erteilten Weisung entstanden ist.

12 SCHLUSSBESTIMMUNGEN

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

12.2 Für Nebenabreden ist die Schriftform erforderlich.

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

12.4 Diese Vereinbarung und die Verhältnisse zwischen den Parteien (soweit sie sich direkt oder indirekt auf diese Vereinbarung beziehen) unterliegen hinsichtlich des anwendbaren Rechts und des Gerichtsstandes den Bestimmungen der Lizenzvereinbarung.

Anlage
Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

der 506 Data & Performance GmbH

Stand per 04.04.2023

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

Die og. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

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

1.1. Zutrittskontrolle

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

Technische Maßnahmen	**Organisatorische Maßnahmen**
x Alarmanlage	☐ Schlüsselregelung / Liste
x Automatisches Zugangskontrollsystem	x Empfang / Rezeption / Pförtner
☐ Biometrische Zugangssperren	☐ Besucherbuch / Protokoll der Besucher
x Chipkarten / Transpondersysteme	☐ Mitarbeiter- / Besucherausweise
☐ Manuelles Schließsystem	x Besucher in Begleitung durch Mitarbeiter
x Sicherheitsschlösser	x Sorgfalt bei Auswahl Reinigungsdienste
☐ Schließsystem mit Codesperre	☐
x Absicherung der Gebäudeschächte	☐
x Türen mit Knauf Außenseite	☐
☐ Klingelanlage mit Kamera	☐
☐ Videoüberwachung der Eingänge	☐
☐	☐
☐	☐
☐	☐

Weitere Maßnahmen bitte hier beschreiben:

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.
Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten" Passworts).

Technische Maßnahmen	**Organisatorische Maßnahmen**
x Login mit Benutzername + Passwort	x Verwalten von Benutzerberechtigungen
☐ Login mit biometrischen Daten	x Erstellen von Benutzerprofilen
x Anti-Viren-Software Server	☐ Zentrale Passwortvergabe
x Anti-Virus-Software Clients	x Richtlinie „Sicheres Passwort"
x Anti-Virus-Software mobile Geräte	x Richtlinie „Löschen / Vernichten"
x Firewall	x Richtlinie „Clean desk"
☐ Intrusion Detection Systeme	x Allg. Richtlinie Datenschutz und / oder Sicherheit
x Mobile Device Management	x Mobile Device Policy
☐ Einsatz VPN bei Remote-Zugriffen	x Anleitung „Manuelle Desktopsperre"
☐ Verschlüsselung von Datenträgern	☐
☐ Verschlüsselung Smartphones	☐
☐ Gehäuseverriegelung	☐
x BIOS Schutz (separates Passwort)	☐
☐ Sperre externer Schnittstellen (USB)	☐
x Automatische Desktopsperre	☐
x Verschlüsselung von Notebooks / Tablet	☐
☐	☐
☐	☐

Weitere Maßnahmen:
506 betreibt keine lokalen, eigenen Server. Alle Unternehmensdaten und alle Kundendaten liegen auf verschlüsselten Cloudservern in zertifizierten Rechenzentren innerhalb der Europäischen Union.

596 verwendet als Clients bis auf wenige Ausnahmen Geräte von Apple, welche betriebssystemseitig hochwertigen Virenschutz bieten. Die wenigen Nicht-Apple-Geräte sind mit entsprechender Virus-Software ausgestattet.

1.3. Zugriffskontrolle

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

Technische Maßnahmen	**Organisatorische Maßnahmen**
x Aktenschredder (mind. Stufe 3, cross cut)	x Einsatz Berechtigungskonzepte
☐ Externer Aktenvernichter (DIN 32757)	x Minimale Anzahl an Administratoren
x Physische Löschung von Datenträgern	☐ Datenschutztresor
x Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	x Verwaltung Benutzerrechte durch Administratoren
☐	☐
☐	☐

Weitere Maßnahmen:
506 betreibt keine lokalen, eigenen Server. Alle Unternehmensdaten und alle Kundendaten liegen auf verschlüsselten Cloudservern in zertifizierten Rechenzentren innerhalb der Europäischen Union.

1.4. Trennungskontrolle

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

Technische Maßnahmen	**Organisatorische Maßnahmen**
x Trennung von Produktiv- und Test-umgebung	x Steuerung über Berechtigungskonzept
x Physikalische Trennung (Systeme / Datenbanken / Datenträger)	x Festlegung von Datenbankrechten
x Mandantenfähigkeit relevanter Anwendungen	☐ Datensätze sind mit Zweckattributen ver-sehen
☐	☐
☐	☐

Weitere Maßnahmen:

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

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

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

Weitere Maßnahmen:

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

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
x Email-Verschlüsselung (TLS) ☐ Email-Signatur (S/MIME / PGP)	☐ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☐ Einsatz von VPN	☐ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☐ Protokollierung der Zugriffe und Abrufe	☐ Weitergabe in anonymisierter oder pseudonymisierter Form
☐ Sichere Transportbehälter	☐ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
x Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☐ Persönliche Übergabe mit Protokoll
☐ Nutzung von Signaturverfahren	☐
☐	☐
☐	☐

Weitere Maßnahmen:
Es werden keine Daten physisch weitergegeben. Alle Daten der 506 befinden sich grundsätzlich verschlüsselt auf Cloudspeichern in zertifizierten Rechenzentren der Europäischen Union.

Mails werden TLS verschlüsselt gesendet. Jeglicher Zugriff auf 506-Seiten und auf Kunden-Seiten erfolgt verschlüsselt.

2.2. Eingabekontrolle

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

Technische Maßnahmen	**Organisatorische Maßnahmen**
x Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☐ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☐ Manuelle oder automatisierte Kontrolle der Protokolle	x Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
☐	x Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☐	x Aufbewahrung von Formularen, von denen Daten in automatisierte Verar-beitungen übernommen wurden
☐	x Klare Zuständigkeiten für Löschungen

Weitere Maßnahmen:

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

3.1. Verfügbarkeitskontrolle

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

Technische Maßnahmen	**Organisatorische Maßnahmen**
x Feuer- und Rauchmeldeanlagen	x Backup & Recovery-Konzept (ausformuliert)
☐ Feuerlöscher Serverraum	x Kontrolle des Sicherungsvorgangs
☐ Serverraumüberwachung Temperatur und Feuchtigkeit	x Regelmäßige Tests zur Datenwiederher-Herstellung und Protokollierung der Ergebnisse
☐ Serverraum klimatisiert	☐ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☐ USV	☐ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☐ Schutzsteckdosenleisten Serverraum	☐ Existenz eines Notfallplans (z.B. BSI IT Grundschutz 100-4)
☐ Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quell-dichtung etc.)	☐ Getrennte Partitionen für Betriebs-systeme und Daten
☐ RAID System / Festplattenspiegelung	☐
☐ Videoüberwachung Serverraum	☐
☐ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	☐
☐	☐
☐	☐
☐	☐

Weitere Maßnahmen:
506 betreibt keine lokalen, eigenen Server. Alle Unternehmensdaten und alle Kundendaten liegen auf verschlüsselten Cloudservern in zertifizierten Rechenzentren innerhalb der Europäischen Union und werden auch dort gesichert.

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

4.1. Datenschutz-Management

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

Weitere Maßnahmen:

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
x Einsatz von Firewall und regelmäßige Aktualisierung	x Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
x Einsatz von Spamfilter und regelmäßige Aktualisierung	☐ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
x Einsatz von Virenscanner und regelmäßige Aktualisierung	x Einbindung von DSB in Sicherheitsvorfälle und Datenpannen
☐ Intrusion Detection System (IDS)	x Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☐ Intrusion Prevention System (IPS)	x Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvor-fällen und Datenpannen
☐	☐
☐	☐
☐	☐

Weitere Maßnahmen:

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

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
x Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	x Einfache Ausübung des Widerrufrechts des Betroffenen durch organisatorische Maßnahmen
☐	☐
☐	☐
☐	☐

Weitere Maßnahmen:

4.4. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	Organisatorische Maßnahmen
☐	x Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
☐	x Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
☐	x Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
☐	x Schriftliche Weisungen an den Auftragnehmer
☐	x Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
☐	x Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
☐	x Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☐	☐ Regelung zum Einsatz weiterer Subunternehmer
☐	x Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐	☐ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Weitere Maßnahmen:

Ausgefüllt für die Organisation durch

Ing. Mag. Karl Mitteregger
COO / CTO
karl.mitteregger@506.ai

Linz, 04.04.2023