Vereinbarung zur Auftragsverarbeitung

Vereinbarung zwischen der

Xisi Meldecenter GmbH
Albrechtstraße 14b
10117 Berlin

-nachstehend **Auftragnehmer** genannt-

und

(Bitte tragen Sie hier Ihren Namen und Ihre Anschrift ein.)

-nachstehend **Auftraggeber** genannt-

-nachfolgend gemeinsam als die **“Parteien”** oder einzeln als die **“Partei”** bezeichnet -

Stand 12.01.2026

§1 Präambel

Diese Vereinbarung zur Auftragsverarbeitung (AVV) stellt eine ergänzende Regelung zur vertraglichen Beziehung dar, die durch die Allgemeinen Geschäftsbedingungen (AGBs) festgehalten sind. Sie dient der Einhaltung der datenschutzrechtlichen Vorgaben des Bundesdatenschutzgesetzes (BDSG) und der europäischen Datenschutz-Grundverordnung (DSGVO), insbesondere des Art. 28 Abs. 3 DSGVO. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien in Bezug auf die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer zur Erfüllung der AGBs bzgl. des Produkts “euBP-Senden”, denen beide Parteien zugestimmt haben.

§ 2 Gegenstand und Dauer des Auftrages

Der Auftragnehmer erbringt für den Auftraggeber Leistungen auf Grundlage des mit dem Auftraggeber geschlossenen Vertrages über die Nutzungsrechte an der euBP-Senden Webanwendung s. AGBs. Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO.

Die Bestimmungen dieses Vertrags finden Anwendung auf alle Tätigkeiten, die mit den AGBs in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit Auftraggeber-Daten in Berührung kommen oder für den Auftraggeber erhoben wurden. Die Dauer der Datenverarbeitung durch den Auftragnehmer richtet sich nach der Laufzeit, die in den AGBs aufgeführt wurde.

§ 3 Arten und Zwecke der Verarbeitungen

Die aufgrund dieser Vereinbarung getätigten Verarbeitungen von personenbezogenen Daten werden vom Auftragnehmer durchgeführt, um dem Auftraggeber das Übersenden einer elektronisch unterstützten Betriebsprüfung (euBP) über die Webanwendung zu ermöglichen.
Dem Zweckbindungsgrundsatz ist Rechnung zu tragen.
Die von diesem Auftrag umfassten Verarbeitungstätigkeiten ergeben sich aus den AGBs und dieser Vereinbarung zur Auftragsverarbeitung.
Eine davon abweichende oder darüber hinausgehende Verarbeitung von Auftraggeberdaten ist untersagt.

§ 4 Kategorien der betroffenen personenbezogenen Daten und Personen

Von der Verarbeitung bei Nutzung des Verfahrens “euBP” betroffen sind:

- Personenkategorien: Auftraggeber selbst, Beschäftigte (Arbeitnehmer), Kreditoren
- Datenkategorien: IP-Adressen, ggf. Angaben über Kreditoren (sofern solche Angaben gemacht worden sind)
- Empfängerkategorien**:** Rentenversicherung

§ 5 Rechte und Pflichten sowie Weisungen des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich.

5.1 Weisungsbefugnisse

Der Auftragnehmer darf die Daten von betroffenen Personen nur gemäß den dokumentierten Weisungen des Auftraggebers verarbeiten, d.h. der Auftragnehmer ist an die Weisungen des Auftraggebers gebunden. Der Auftragnehmer verarbeitet personenbezogene Daten im Rahmen der in den AGBs geregelten Dienste ausschließlich im Auftrag und gemäß den Weisungen des Auftraggebers, die in dieser Vereinbarung und den AGBs oder anderen Leistungsbeschreibungen hinsichtlich der Zwecke und des Umfangs bestimmt sind, es sei denn höherrangiges Recht gebietet eine anderweitige Verarbeitung durch den Auftragnehmer im Sinne des Art. 28 III lit. a) DSGVO. Verlangt das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, eine weitere Verarbeitung, teilt der Auftragnehmer dem Auftraggeber diese rechtliche Anforderung vor der Verarbeitung mit.

Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen im Hinblick auf die Berichtigung und Löschung von Auftraggeber-Daten sowie die Einschränkung der Verarbeitung von Auftraggeber-Daten. Die weisungsberechtigten Personen des Auftragnehmers ergeben sich aus **Anlage 2**.

Ist der Auftragnehmer der Auffassung, dass eine Weisung des Auftraggebers gegen diesen Vertrag, die DSGVO oder andere geltende datenschutzrechtliche Bestimmungen der Union oder der Mitgliedstaaten verstößt, hat er den Auftraggeber unverzüglich zu informieren (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Ausführung der betroffenen Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

5.2 Dokumentation der Weisungen

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Empfangsberechtigte Person ist der Datenschutzbeauftragte des Auftragnehmers.

5.3 Informationspflichten

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherheit der Daten und Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

§ 6 Rechte und Pflichten des Auftragnehmers

Der Auftragnehmer darf die Auftraggeber-Daten nur im Rahmen der AGBs und ausschließlich in Übereinstimmung mit den in diesem Vertrag enthaltenen Bestimmungen verarbeiten.

Die Verarbeitung der Auftraggeber-Daten für andere als die in den AGBs beschriebenen Zwecke bedarf der vorherigen schriftlichen Zustimmung durch den Auftraggeber. Der Auftragnehmer ist verpflichtet, auf Verlangen des Auftraggebers Änderungen dieser Festlegungen zuzustimmen, soweit er keinen sachlichen Grund zur Verweigerung dieser Zustimmung hat. Die Änderungen sind schriftlich festzulegen.

Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten. Er darf Auftraggeber-Daten nicht ohne vorherige schriftliche Zustimmung des Auftraggebers an Dritte weitergeben oder deren Zugriff aussetzen. Die Auftraggeber-Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von Auftraggeber-Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu.

Der Auftragnehmer darf Kopien oder Duplikate der Auftraggeber-Daten anfertigen, soweit und solange sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung, zur ordnungsgemäßen Erbringung der Leistungen gemäß den AGBs (einschließlich der Datensicherung) oder zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Beim Auftragnehmer ist der in **Anlage 1** aufgeführte betriebliche Datenschutzbeauftragte nach Art. 37 DSGVO (i.V.m. § 38 BDSG) bestellt .

Der Auftragnehmer gewährleistet, dass sich alle zur Verarbeitung der Auftraggeber-Daten befugte Personen (nachfolgend „**Mitarbeiter**“) vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 Satz 2 lit. b DSGVO). Die Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrags oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Der Auftragnehmer wird diese Verpflichtungen schriftlich dokumentieren und deren Einhaltung mit der gebotenen Sorgfalt sicherstellen.

Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer ergreift alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeber-Daten gem. Art. 32 DSGVO, insbesondere mindestens die in **Anlage 2** aufgeführten Maßnahmen (Art. 28 Abs. 3 Satz 2 lit. c DSGVO). Eine Änderung

der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Solche Änderungen wird der Auftragnehmer dokumentieren. Die Dokumentation ist für die Dauer dieses Vertrages aufzubewahren.

Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält, soweit hierzu eine gesetzliche Verpflichtung besteht. Der Auftragnehmer hat dem Auftraggeber auf Anforderung unverzüglich das Verzeichnis mit der aktuellen Aufstellung der Angaben zur Verfügung zu stellen.

Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgeabschätzung nach Art. 35 DSGVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO zu unterstützen.

Soweit Auftraggeberdaten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch eine Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, hat der Auftragnehmer den Auftraggeber darüber unverzüglich zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Im Rahmen dessen wird der Auftragnehmer alle zuständigen Stellen darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als “Verantwortlichem” im Sinne der DSGVO liegt.

6.1 Mitwirkungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und gesetzlichen Ansprüche der Betroffenen gem. Kapitel III, Art. 12 – 22 DSGVO.

Der Auftragnehmer unterstützt den Auftraggeber unter der Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen gem. Art. 28 Abs. 3 S. 2 lit. f DSGVO in einer angemessenen Art und Weise bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen.

6.2 Informationspflichten

Den Auftragnehmer trifft keinerlei Verpflichtung, Weisungen des Auftraggebers (datenschutz-)rechtlich zu prüfen. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden, Art. 33 Abs. 2 DSGVO.

6.3 Zustimmung zur Telearbeit

Der Auftraggeber gestattet dem Auftragnehmer, unter Einhaltung der gesetzlichen Bestimmungen, zur Verarbeitung von personenbezogenen Daten dieses Auftrages auch Angestellte einzusetzen, die von Zuhause aus arbeiten.

§ 7 Kontrollrechte des Auftraggebers

Der Auftraggeber ist dazu berechtigt, jederzeit die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer einschließlich der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen und die Ordnungsmäßigkeit der Datenverarbeitungsprozesse und -programme des Auftragnehmers zu prüfen, um sich von der Einhaltung der Bestimmungen dieses Vertrags, der vom Auftraggeber erteilten Weisungen sowie der einschlägigen gesetzlichen Datenschutzbestimmungen zu überzeugen.

Zur Durchführung von Kontrollen kann der Auftraggeber z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen zur Verschwiegenheit verpflichteten sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht oder der Auftragnehmer anderweitige berechtigte Interessen gegen den Dritten vorbringt. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8 Rechte Betroffener

Macht der Betroffene seine Rechte gem. Art. 16-18 DSGVO geltend, ist der Auftragnehmer dazu verpflichtet, die betroffenen Auftraggeberdaten auf Weisung des Auftraggebers unverzüglich zu löschen oder einzuschränken. Der Auftragnehmer wird dem Auftraggeber die Löschung, Berichtigung bzw. Einschränkung der Daten auf Verlangen schriftlich nachweisen.

Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der

Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und wartet dessen Weisung ab.

§ 9 Löschung und Rückgabe von personenbezogenen Daten

Spätestens 3 Monate nach Abschluss der Erbringung der Verarbeitungsleistungen oder jederzeit nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche eventuell noch in seinem Besitz befindlichen personenbezogenen Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers dem Auftraggeber auszuhändigen oder datenschutzgerecht zu vernichten, soweit die Daten nicht gesetzlichen Aufbewahrungspflichten unterliegen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen. Trifft der Auftraggeber bis zum Ablauf der oben genannten Frist keine Wahl über Löschung oder Aushändigung, werden alle Daten i.S.d. S. 1 durch den Auftragnehmer datenschutzgerecht gelöscht.

Der Auftragnehmer wird über die Löschung bzw. die Vernichtung von Auftraggeber-Daten ein Protokoll erstellen, das dem Auftraggeber auf Verlangen vorzulegen ist. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter und zumutbarer Weise zu kontrollieren. Die in Punkt 7 aufgeführten Kontrollrechte gelten hierfür entsprechend.

§ 10 Haftung

Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen solchen Schaden gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung.

Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung entspricht.

Dies gilt auch im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

§ 11 Datenübermittlungen an einen Drittstaat

Die Datenverarbeitung durch den Auftragnehmer findet ausschließlich im Bereich der Bundesrepublik Deutschland statt. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

§ 12 Subauftragsverhältnisse

Als Subauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen und bei denen eine Verarbeitung von personenbezogenen Daten aus dem hier bestimmten Auftragsverhältnis stattfindet, diese aber nicht vom Auftraggeber persönlich erbracht wird. Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 3** genannten Subunternehmer durchgeführt. Der Auftraggeber stimmt hiermit der Hinzuziehung und Inanspruchnahme der Subunternehmer gemäß Anlage 3 zu.

Die Hinzuziehung weiterer oder die Ersetzung bestehender Subunternehmer zur Verarbeitung von Auftraggeber-Daten sind gem. Art. 28 Abs. 2 Satz 1 Alt. 2 DSGVO zulässig, soweit der Auftragnehmer eine solche Änderung dem Auftraggeber eine angemessene Zeit vorab on Kenntnis setzt und der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten an den neuen Subunternehmer schriftlich oder in Textform gegenüber dem Auftragnehmer Einspruch gegen die geplante Änderung erhebt (Art. 28 Abs. 2 Satz 2 DSGVO). Unterbleibt der Einspruch, gelten die neuen Subunternehmer als genehmigte Subunternehmer im Sinne dieses Vertrages.

Der Auftragnehmer wird den Subunternehmer nach dessen Zuverlässigkeit und unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählen.

Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten.
Der Auftragnehmer hat im Verhältnis zu seinen Subunternehmern (auch vertraglich) sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. 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).

Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

Der Auftragnehmer hat die Einhaltung der vertraglichen Verpflichtungen des Subunternehmers regelmäßig in geeigneter Form zu überprüfen und das Ergebnis der Prüfung zu dokumentieren. Der Auftraggeber bleibt berechtigt, die Ausübung der Kontrollbefugnisse durch den Auftragnehmer zu überwachen.

Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen, die Entsorgung von Datenträgern und Bewachungsdienste. 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. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Subunternehmers (Art. 28 Abs. 4 Satz 2 DSGVO).

§ 13 Technische und organisatorische Maßnahmen

Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass die Datensicherheit gem. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO nach allgemein anerkannten Regeln der Wissenschaft und Technik sichergestellt wird.

Die technischen und organisatorischen Maßnahmen (TOMs) zum angemessenen Schutz der im Auftrag des Auftraggebers verarbeiteten Daten für die Datensicherheit werden von dem Auftragnehmer eingerichtet und dokumentiert.

Die aktuellste Version der Maßnahmen zur Datensicherheit kann durch den Auftraggeber jederzeit angefordert werden und wird ihm durch den Auftragnehmer binnen vierzehn Tagen zur Verfügung gestellt.

Der Auftragnehmer darf die getroffenen Maßnahmen für die Datensicherheit jederzeit ändern, sofern sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftragnehmer unverzüglich.

§ 14 Schlussbestimmungen

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schrift- oder Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen der AGBs vor. Sollte eine Bestimmung oder Teile dieser Vereinbarung unwirksam sein oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam werden, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt. Die Parteien verpflichten sich, anstelle der unwirksamen Bestimmung eine der unwirksamen Bestimmung möglichst nahekommende, wirksame Bestimmung zu vereinbaren.

Diese Vereinbarung unterliegt dem deutschen Recht. Ausschließlicher Gerichtsstand ist Berlin, mithin der Sitz des Auftragnehmers.

Die nachfolgend aufgezählten Anlagen werden zum Bestandteil dieser Vereinbarung. Der Auftraggeber kann aktuelle Versionen dieser Anlagen auf Anfrage hin beim Auftragnehmer einsehen.

- Anlage Nr. 1 Weisungsberechtigte Personen und Datenschutzbeauftragter
- Anlage Nr. 2 Technische und organisatorische Maßnahmen des Auftragnehmers
- Anlage Nr. 3 Subunternehmer

Anlage 1 - Weisungsberechtigte Personen

1 Weisungsempfänger beim Auftragnehmer sind

Name	Funktion	E-Mail
Marcel Berschneider	CEO	marcel.berschneider@xisi.de
Fabian Bucher	Entwickler	fabian.bucher@xisi.de

2 Betriebliche Datenschutzbeauftragte beim Auftragnehmer ist

Name	Funktion	E-Mail
Fabian Rang	Datenschutzbeauftragter	datenschutz@xisi.de

Anlage 2 - Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1. 1 Zutrittskontrolle

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um den unbefugten Zutritt zu Datenverarbeitungsanlagen (insbes. Notebooks, Festplatten, IT-Server) zu sichern.

Nachfolgend sind die Maßnahmen des Subauftragnehmers "ACP IT Solutions AG" aufgeführt.

- ✔ Einbruchmeldeanlage mit Anschluss an eine Notrufzentrale vorhanden
- ✔ Sicherheits-Schließanlage
- ✔ Zutritts-Token werden protokolliert vergeben
- ✔ Brandmeldesystem
- ✔ Festlegung befugter Personen
- ✔ Unterteilung in verschiedene Sicherheitsbereich
- ✔ Videoüberwachung des Innen- und Außenbereichs
- ✔ Protokollierung der Schließvorgänge
- ✔ Sicherheitsdienst
- ✔ Anwesenheitsaufzeichnung von Besucherzutritten und Begleitung durch Mitarbeiter der ACP IT Solution AG
- ✔ Verschluss der Datenverarbeitungsanlagen
- ✔ Aufbewahrung der Server in verschlossenen Räumen

1.2 Zugangs- und Benutzerkontrolle

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um die unbefugte System Benutzung von Datenverarbeitungsanlagen zu sichern.

- ✔ Authentifikation mittels Benutzer und Passwort
- ✔ Interne Applikations-Funktionen sind nur mit aktivem VPN möglich
- ✔ Einsatz von Anti-Viren-Software
- ✔ Einsatz von Firewalls
- ✔ Einsatz von VPN-Technologie

✔ Benutzerberechtigungen verwalten

✔ Protokollierung des Zugriffs

✔ Unmittelbare Löschung des Zugangs nach Ausscheiden des Mitarbeiters

✔ Verschlüsselung von Datenträgern in Laptops / Notebooks

✔ 2-Faktor-Authentifizierung beim Login durch Betreuer der Anwendung

✔ Schulung und Sensibilisierung der Mitarbeiter

1.3 Zugriffs, Daten- und Speicherkontrolle

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems zu verhindern.

✔ Einsatz von Aktenvernichtern zur Vernichtung und Entsorgung von Akten

✔ Anzahl der Administratoren ist auf das „Notwendigste“ reduziert

✔ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

✔ Verwaltung der Benutzerrechte durch definierte Systemadministratoren

1.4 Trennungsgebot & Trennbarkeit

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, sicherzustellen.

✔ Berechtigungskonzept vorhanden

✔ Trennung von Produktiv-und Testsystem

✔ Logische Mandantentrennung (softwareseitig)

1.5 Pseudonymisierung

Der Auftragnehmer setzt unter anderem die folgenden Maßnahmen ein, um sicherzustellen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Hierbei werden diese zusätzlichen Informationen gesondert aufbewahrt und unterliegen technischen und organisatorischen Maßnahmen.

✔ Wir verarbeiten die Daten zu den genannten Zwecken. Ein Zweck, bei dem eine Pseudonymisierung geboten wäre, liegt nicht vor.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport zu verhindern.

✔ Einrichtungen von VPN-Tunneln bzw. Standleitungen

✔ Verschlüsselte Datenübertragung im Internet (z.B. HTTPS, SFTP, etc.)

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Verfügbarkeitskontrolle

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen zum Schutz der Daten gegen zufällige oder mutwillige Zerstörung bzw. Verlust.

✔ Feuer- und Rauchmeldeanlagen vorhanden

✔ Automatisierte zyklische Durchführung einer Backup Routine

✔ Unterbrechungsfreie Stromversorgung (USV)

✔ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

✔ Systeme sind Redundant ausgelegt, gespiegelte Platten (RAID) bzw. HA-Cluster

✔ Backup- und Recoverykonzepts vorhanden

✔ Überwachung des Systemzustandes (Monitoring)

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

4.1 Auftragskontrolle

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um die weisungsgemäße Verarbeitung von Daten im Auftrag sicherzustellen.

✔ Dokumentation in einem Forums-System

✔ Eingesetzte Subunternehmen wurden auf Zuverlässigkeit und Eignung geprüft

✔ Mit eingesetzten Subunternehmen wurden Vereinbarungen zur Auftragsverarbeitung
(ADV) abgeschlossen.

✔ Verfahrensdokumentationen nach DSGVO vorhanden

4.2 Datenschutz-Management

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um die innerbetriebliche Organisation so zu gestalten, so dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

✔ Nachweise über durchgeführte Schulungen der Mitarbeiter zum Datenschutz

✔ Nachweise über Verpflichtungen auf die Vertraulichkeit

✔ Bestellung eines Datenschutzbeauftragten ist aufgrund der Mitarbeiterzahl gesetzlich
nicht notwendig

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um die Verarbeitung nur erforderlicher personenbezogener Daten durch Voreinstellung sicherzustellen.

✔ Die Löschfristen werden automatisch durch das System umgesetzt

4.4 Incident-Response-Management

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um die Meldepflicht bei IT-Sicherheitsvorfällen sicherzustellen.

✔ Interner Meldeprozess

✔ Meldeprozess an die Aufsichtsbehörde

✔ Cyber-Versicherung

Anlage Nr. 3 - Subauftragnehmer

Die Xisi Meldecenter GmbH beauftragt die Firma ACP IT Solutions AG mit dem Hosting von virtuellen Applikationsservern:

ACP IT Solutions AG / Carl-Jordan-Str. 18a / 83059 Kolbermoor / Tel.: 089 547274100 / Fax: 089 54727410 999 / E-Mail: gruppe@acp.de