Klicken oder tippen Sie hier, um Text einzugeben.

Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung

zwischen

Link IT isi GmbH

Kleestraße 21-23

90461 Nürnberg

-**Auftragsverarbeiter**-

nachfolgend „Auftragnehmer“ genannt

und

parentcustomeridname

address1_line1

address1_postalcode address1_city

-**Verantwortlicher**–

nachfolgend „Auftraggeber“ genannt

Definitionen für ein einheitliches Verständnis

Für ein einheitliches Verständnis möchten wir vorangestellt auf einige Begrifflichkeiten näher eingehen, deren genaue Bedeutung im Rahmen der Auftragsverarbeitungsverträge von Relevanz ist.

Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, vgl. Art.4 Nr. 1 DSGVO.

Auftragsverarbeiter

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, vgl. Art.4 Nr. 8 DSGVO.

Datenverarbeitung im Auftrag

Es gibt keine Legaldefinition des Begriffs der Auftragsverarbeitung. In der DSGVO legt Art.28 lediglich die Anforderungen fest, die bei der arbeitsteiligen Datenverarbeitung bestehen. Demnach ist eine Datenverarbeitung im Auftrag die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter (Auftragnehmer) nach Weisung und im Auftrag des Auftraggebers.

Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt; der Auftraggeber hat ein Weisungsrecht im Rahmen dieser vereinbarten Leistung.

Subunternehmer / Unterauftragsverhältnis

Als Auftragnehmer des Auftragsverarbeiters im Sinne der DSGVO ist der Subunternehmer ein »weiterer Auftragsverarbeiter«, vgl. Art.28 Abs.4 DSGVO. Zur Vermeidung von Missverständnissen aufgrund der Erinnerung an § 11 Abs. 5 BDSG alt, sollte ein weiterer Auftragsverarbeiter nur bei der Teil- oder vollständigen Übernahme der Hauptleistung definiert werden.

Der Subunternehmer erbringt seine Leistung auf Basis eines Unterauftragsverhältnisses.

Dritter

Der Ausdruck »Dritter« bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem Auftraggeber, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Auftraggebers oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten (Art. 4 Nr. 10 DSGVO).

Datenübermittlung

Phase der Datenverarbeitung, in der personenbezogene Daten von dem Auftraggeber an andere Personen oder Stellen (Dritte) bekannt- oder weitergegeben werden; im BDSG definiert in § 3 Abs.4 Nr. 3. Die Bekanntgabe kann durch aktive Weitergabe, gleich in welcher Form, oder durch Einsicht eines Dritten oder Abruf der Daten durch einen Dritten erfolgen. Demgegenüber verwendet die DSGVO eine umfassendere, weniger differenzierte Begriffsbestimmung der Verarbeitung (Art.4 Nr. 2 DSGVO), der die Übermittlung umfasst.

Funktionsübertragung

Übertragung einer ganzen Funktion zur eigenverantwortlichen Wahrnehmung durch den Auftragnehmer (in Abgrenzung zur Datenverarbeitung im Auftrag). Mit diesem Begriff, der weder im BDSG, der RL 95/46 EG noch in der DSGVO definiert wird, wird seit seiner Erwähnung in einer Gesetzesbegründung zum BDSG im Jahr 1989 eine weisungsabhängige, primär technische Dienstleistung (Auftragsverarbeitung) von einer (weitgehend) weisungsfreien, dabei eigene Aufgaben erfüllende Leistungserbringung abgegrenzt. Der Dienstleister wird dabei auch wegen der eigenen verfolgten Zwecke damit zu einem Verantwortlichen (Beispiele: Rechtsanwalt, Steuerberater, Wirtschaftsprüfer oder auch Gutachter). Die Rechtmäßigkeitsgrundlage für die Übermittlung (Verarbeitung) der personenbezogenen Daten an solche Funktionsübernehmer ist meistens das überwiegende berechtigte Interesse (bisher nach § 28 Abs.1 Nr. 2 BDSG). Dieses Konstrukt ermöglicht auch die DSGVO in Art.6 Abs.1 lit. f DSGVO.

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand der Verarbeitung wird in der Anlage 1 beschrieben.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des SaaS-Vertrages.

§ 2 Konkretisierung des Auftragsinhalts:

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der Anlage 1 beschrieben.
Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in Deutschland statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers.

(2) Art der Daten

Die Art der personenbezogenen Daten, die für den Auftraggeber verarbeitet werden, sind in der Anlage 2 beschrieben.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen sind in Anlage 2 beschrieben.

§ 3 Technisch-organisatorische Maßnahmen

(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. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) 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 [Einzelheiten in Anlage 3].

(3) 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 und dem Auftraggeber mitzuteilen.

§ 4 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftraggeber kann jederzeit die Daten, die er im Auftrag verarbeiten lässt, eigenständig berichtigen, löschen oder deren Verarbeitung einschränken. 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 sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei Anfragen zur Datenportabilität im Rahmen seiner technischen Möglichkeiten.

(3) Inhalte, die älter als 24 Monate sind, werden vom Auftragnehmer automatisiert gelöscht. Personenbezogene Daten der Betroffenen werden durch den Auftraggeber gelöscht. Hierzu stellt der Auftragnehmer dem Auftraggeber eine entsprechende Funktion in der Anwendung bereit.

§ 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:

(i) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

(ii) Die Wahrung der Vertraulichkeit 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 Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Diese Verpflichtung besteht auch nach Beendigung des Auftrages fort.

(iii) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 3].

(iv) Die Verarbeitung von Daten außerhalb der Betriebsräume des Auftragnehmers (z.B. Homeoffice) ist zulässig. Die hierfür erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Daten

sind vom Auftragnehmer festzulegen. Es muss sichergestellt sein, dass die Vertraulichkeit der Daten gegenüber Dritten gewahrt bleibt (z.B. Verhinderung der Kenntnisnahme oder des Zugriffs auf die Daten durch Dritte).

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

(vi) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

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

(viii) 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.

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

§ 6 Unterauftragsverhältnisse

(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 z.B.: Finanzberatung, Steuerberatung, Unternehmensberatung, Beratung durch Rechtsanwälte und Wirtschaftsprüfer, externe Betriebsärzte, Inkassobüros, Bankinstitut für den Geldtransfer, Postdienst für den Brieftransport, Installation und Wartung von Netzwerken, Hardware, Telefonanlagen als reiner technischer Support, Pflege von Software wie Betriebssystemen, Middleware oder Anwendungen, Programmentwicklungen, Programmanpassungen bzw. -umstellungen, Fehlersuche und Tests, Parametrisieren von Software, Telekommunikationsleistungen, Entsorgung von Datenträgern 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.

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

(3) Der Auftraggeber stimmt der Beauftragung der in der Anlage 4 genannten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO. Die in der Anlage 4 genannten Unterauftragnehmer werden in dem dort genannten Umfang beschäftigt und sind durch den Auftraggeber genehmigt.

(4) Die Auslagerung auf Unterauftragnehmer und der Wechsel des / der bestehenden Unterauftragnehmer sind zulässig, soweit folgende Bedingungen erfüllt sind:

(i) Der Auftragnehmer zeigt eine solche Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Unterauftragnehmer dem Auftraggeber 4 Wochen vorab schriftlich oder in Textform an.

(ii) Der Auftraggeber erhebt nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch.

(iii) Eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO wird zugrunde gelegt. Der Auftragnehmer hat sicherzustellen, dass seine vertraglichen Vereinbarungen mit Unterauftragnehmern so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer entspricht. Das gilt insbesondere im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen.

(iv) Dem Auftraggeber sind in der vertraglichen Vereinbarung mit dem Unterauftragnehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Auftraggeber berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den Inhalt des mit dem Unterauftragnehmer geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten.

(5) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(6) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU / des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Auch in diesem Fall bedarf es der vorherigen schriftlichen Zustimmung durch den Auftraggeber gem. § 6 Abs. 4. Es müssen die zusätzlichen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sein. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(7) Weitere Unterauftragsverhältnisse durch Unterauftragnehmer bedürfen der ausdrücklichen Zustimmung des Auftraggebers schriftlich oder in Textform. Der Auftragnehmer und der Unterauftragnehmer stellen sicher, dass sämtliche vertragliche Regelungen in der Vertragskette auch dem weiteren Unterauftragnehmer auferlegt werden.

(8) Kommt der Unterauftragnehmer seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragnehmers. Der Auftragnehmer hat in diesem Falle auf Verlangen des Auftraggebers die Beschäftigung des Unterauftragnehmers ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Unterauftragnehmer zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(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.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

(i) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;

(ii) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO; aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, InformaRevision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

(iii) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu informieren.

§ 8 Mitteilung bei Verstößen des Auftragnehmers

(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 u.a.

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 relevanten Informationen unverzüglich zur Verfügung zu stellen

iv) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

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

§ 9 Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Der bevorzugte Kanal zur Kommunikation ist Email.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften.

(3) Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(4) Die weisungsbefugten Personen des Auftraggebers sind in Anlage 5, die weisungsempfangsberechtigten Personen des Auftragnehmers sind in der Anlage 6 benannt und werden dort aktualisiert.

§ 10 Löschung und Rückgabe von personenbezogenen Daten

(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.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

(3) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(4) 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 Kündigungsrecht

Der Auftraggeber und der Auftragnehmer können den Vertrag jederzeit fristlos und außerordentlich kündigen, wenn ein wichtiger Grund vorliegt. Ein wichtiger Grund liegt insbesondere vor, wenn ein schwerwiegender Verstoß

(i) gegen die Bestimmungen dieses Vertrags und die Mindestanforderungen des Auftraggebers (A-Kriterien des Leistungsverzeichnisses)

oder

(ii) gegen die Bestimmungen der DSGVO, des BayDSG oder anderweitiger Datenschutzvorschriftenvorliegt und wenn die Einhaltung der Bestimmungen dieses Vertrages oder der gesetzlichen Bestimmungen trotz Abmahnung durch die andere Vertragspartei nicht mehr ausreichend erscheint.

§ 12 Sonstiges

(1) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung, durch ein Konkurs- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Alle Daten des Auftraggebers sind in diesem Zusammenhang rechtzeitig vor Eintritt dieser Maßnahmen von den betroffenen Systemen zu entfernen.

Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt.

(3) Jede Anlage zu diesem Vertrag kann zur Arbeitserleichterung beider Vertragsparteien durch neue Versionen ersetzt werden, ohne den Vertrag selbst anzupassen. Mit der Vereinbarung einer neuen Version einer Anlage verliert jede ältere Version dieser Anlage an Gültigkeit und wird von der neuen Version ersetzt.

(4) Um den Administrationsaufwand zu reduzieren, vereinbaren Auftraggeber und Auftragnehmer die Aktualisierung von Inhalten dieses Vertrages oder seiner Anlagen im elektronischen Format (z.B. PDF-Version einer überarbeiteten Anlage zur elektronischen Signatur) vorgenommen werden dürfen.

§ 13 Salvatorische Klausel

Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Anlagenübersicht

Anlage 1: Verarbeitungsgegenstand

Anlage 2: Verarbeitete personenbezogene Daten

Anlage 3: Technisch-organisatorische Maßnahmen

Anlage 4: Genehmigte Unterauftragsnehmer

Anlage 5: Weisungsbefugte Personen des Auftraggebers

Anlage 6: Weisungsempfangsberechtigte Personen des Auftragnehmers

Anlage 7: Ansprechpartner Datenschutz

cr5f5_konfanlageheader

Sebastian Kopp

Nürnberg, den 10. November 2022 Unterschrift Link IT isi GmbH

address1_city, den Unterschrift parentcustomeridname

Anlage 1: Verarbeitungsgegenstand
Version: 10.11.2022

(1) Der Auftragnehmer stellt dem Auftraggeber sowie dessen Kunden für die Dauer des Vertragsverhältnisses eine Austauschplattform für Einrichtungen des Auftraggebers zur Nutzung zur Verfügung. Die Daten auf der Austauschplattform werden auf Servern von deutschen Rechenzentren gehalten, betrieben und gewartet. Der Auftraggeber entscheidet, welche von der in der Anwendung bereitgestellten Funktionen er in seiner Einrichtung seinen Kunden anbieten möchte. Eine Anpassung ist jederzeit möglich und kann vom Auftraggeber selbständig vorgenommen werden.

(2) Zugriff und Nutzung der Austauschplattform durch den Auftraggeber erfolgen über das Internet unter Verwendung eines Internet-Browsers. Die Austauschplattform ist über die Domain cr5f5_domain erreichbar. Alternativ erfolgt der Zugriff über eine Anwendung auf Mobiltelefonen mit den Betriebssystemen Android oder iOS („Apps“), die in den jeweiligen Verkaufsplattformen der Hersteller zu beziehen sind.

(3) Die Austauschplattform ist eine Anwendung zur Vernetzung von Kunden des Auftraggebers und Mitarbeitenden des Auftraggebers sowie Kunden des Auftraggebers untereinander bzw. Mitarbeitende/Organisation untereinander. Zu den wesentlichen Funktionen der Austauschplattform gehören unter anderem:

- Individuelle, geschlossene Gruppen anlegen,
- Benachrichtigungsfunktion,
- Veranstaltungsplanung mit Kalenderfunktion,
- Aufgabenverwaltung,
- Umfragen,
- Datenverwaltung,
- News-Feed und Push-Nachricht,
- Übersetzungsfunktion,
- Film und Fotogalerie,
- Dateiverwaltung,
- Unterstützung bei administrativen Tätigkeiten
  (z.B. Entwicklungsdokumentation, Kantinenverwaltung, Abwesenheitsmeldung, Festhalten der Bring- und Abholzeiten, Schlaf-, Wickel- und Essensprotokoll)
- Videokonferenzmöglichkeit,
- Information über meldepflichtige Infektionskrankheit,
- Dokumentation von Covid19-Testnachweis.

(4) Darüber hinaus möchte der Auftragnehmer die angebotene Dienstleistung fortwährend optimieren. Es können daher zukünftig weitere Dienstleistungen hinzukommen, die der Auftragnehmer dem Auftraggeber zusätzlich zur aktuellen Leistung zur Verfügung stellen kann, die zum Zeitpunkt des Vertragsabschlusses

noch nicht bekannt sind. Eine Anpassung des Vertrages ist bei einer (unentgeltlichen) Erweiterung der Leistungen durch den Auftragnehmer nicht vorgesehen.

(5) Die Nutzung der Plattform sind auf die vom Auftraggeber autorisierten Mitarbeiter gemäß Anlage 5, die vom Auftraggeber angelegten Nutzer sowie die Administratoren des Auftragnehmers beschränkt.

(6) Der Auftragnehmer stellt dem Auftraggeber den zur uneingeschränkten vertragsgemäßen Nutzung erforderlichen Speicherplatz für die vom Auftraggeber und den zugelassenen Kunden des Auftraggebers durch Nutzung der Austauschplattform erzeugten und/oder die zur Nutzung der Austauschplattform erforderlichen Daten zur Verfügung. Der Auftragnehmer trifft hinsichtlich dieser Kundendaten keine Verwahrungs- und Obhutspflichten, sofern diese nicht nach anderen Verträgen zwischen den Parteien ausdrücklich vereinbart sind.

(7) Nicht zum Vertragsgegenstand sind insbesondere folgende Leistungen des Auftragnehmers zu zählen:

– Prüfung der Inhalte der Kommunikation auf der Plattform,

– Benutzerberechtigung: Auftraggeber schaltet seine Kunden selbst frei,

– keine Zurverfügungstellung von Inhalts- und Bildscannern,

– Datenauswertungen,

– Support für Kunden des Auftraggebers.

Anlage 2: Verarbeitete personenbezogene Daten
Version: 10. November 2022

(1) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenkategorien und -arten unterschieden, nach den personenbezogenen Daten, die zwingend vorausgesetzt werden oder die abhängig von der Nutzung des Funktionsumfangs durch den Auftraggeber festgelegt werden können.

a) Pflichtangaben:

Lfd. Nr.	Bezeichnung der Kategorie	Datenarten, die verarbeitet werden
(i)	Name und Funktion	Name
(ii)	Kontaktinformation	Emailadresse

b) Optionale Angaben in Abhängigkeit des vom Auftraggeber genutzten Funktionsumfangs:

Lfd. Nr.	Bezeichnung der Kategorie	Datenarten, die verarbeitet werden
(iii)	Name und Funktion	Namen, User Name, Verantwortungsebene, Beruf, Kontobezeichnung sozialer Medien, Berufsbezeichnung
(iv)	Kontaktinformation	Straße, Postleitzahl, Telefonnummer, Device ID, IP Adresse
(v)	Persönliche Eigenschaften	Geschlecht, Nationalität, Alter
(vi)	Aus- und Weiterbildung	Studiengang, Berufliche Qualifikationen, Akademischer Grad, Schulische Ausbildung
(vii)	Datumswerte	Geburtsdatum, Eintrittsdatum, Kalendereinträge, Ankunfts- und Abholzeit, Abwesenheit, Schlaf- Wickel- und Esszeit
(viii)	Physikalische und elektronische Verfolgung	Audio- und Videoaufzeichnung

(ix)	Andere	Dokumentation des Entwicklungsfortschrittes, Fragebogen-Antworten
(x)	Religion	Stellung oder Aufgabe in einer Kirche, Synagoge oder anderer Kultstätte, Teilnehmer religiöser Zeremonien, Kirchenmitgliedschaften, religiöse Einstellung, religiöse Praktiken
(xi)	Kommunikationsinhalte	Kommunikationsinhalte
(xii)	Krankheitsdaten	Gesundheitsinformationen, Krankmeldungen, Dokumentation von Testnachweisen
(xiii)	Zahlungsinformation	Kontonummer, Gläubiger-Identifikationsnummer

c) Bei der Nutzung über ein Smartphone oder Tablet:

Lfd. Nr.	Bezeichnung der Kategorie	Datenarten, die verarbeitet werden
(xiv)	Geräte- und Kartenkennungen	Gerätenummer [International Mobile Equipment Identity "IMEI" oder Unique Device ID "UDID"], Kartennummer [International Mobile Subscriper Identity "IMSI"], Netzwerk-Adapter-Adresse [Media AccessControl-Adresse "MAC-Adresse"], Mobilfunknummer [Mobile Subscriber ISDN-Number "MSISDN"], benutzerdefinierter Name des Smartphones), Standortdaten, biometrische Erkennungsverfahren (Fingerabdruck, Gesichts- und Iriserkennung

Dem Auftraggeber steht es frei, den vollen Funktionsumfang der Anwendung einzuschränken oder zu erlauben. Erlaubt der Auftraggeber die Nutzung einer Funktion, so hat der Benutzer die Möglichkeit, diese zu nutzen. Nur im Falle einer tatsächlichen Nutzung werden die unter Buchstabe b) ausgeführten personenbezogenen Daten verarbeitet.

Der Auftragnehmer ermöglicht die Nutzung von Teilen der angebotenen Leistung über Mobiltelefone mit den Betriebssystemen von Apple ("iOS") und Google ("Android") bereitstellen (beide Betriebssysteme zusammengefasst "Smartphones"). Diese Smartphones bieten den Kunden und Mitarbeitenden des Auftragsgebers die Möglichkeit, über Programme ("Apps") komfortabler und sicherer auf die dort

bereitgestellten Leistungen des Auftragnehmers zurückzugreifen. Dabei erheben die Smartphones personenbezogene Daten (Artikel 2, Absatz 2 (xiv)), die nicht vom Auftragnehmer genutzt werden. Der Auftragnehmer hat keinen Einfluss, welche personenbezogenen Daten das Smartphone zu diesem Zweck an den Betreiber des Betriebssystems weiterleitet.

Es steht jedem Betroffenen frei, auf die Nutzung einer App zu verzichten. Die Funktionalität ist vollumfänglich und ohne Verarbeitung personenbezogener Daten des Artikel 2, Absatz 2 (xiv) auf herkömmlichen Computern verfügbar.

Die verarbeiteten personenbezogenen Daten werden benötigt, um einen neuen Benutzer auf der Plattform anzulegen und die Funktionen, die der Auftragnehmer bereitstellt, zu nutzen.

Wenn der Benutzer über die Services des Auftragnehmers sogenannte Push-Benachrichtigungen abonniert (also Mitteilungen, die dem Benutzer auch dann auf ihr Mobilgerät gesendet werden, wenn sie unsere App nicht benutzen), speichert der Auftragnehmer eine Device ID. Der Benutzer kann diese Push-Benachrichtigungen in den Einstellungen in dem Browser des Computers ein- und ausschalten. Beim Aktivieren der Push-Mitteilungen wird eine eindeutige, durch Software des Auftragnehmers generierte Kennnummer des Mobilgeräts (Device ID) an den Dienst kommuniziert, der bei dem Anbieter der Push Notification die Push-Funktionalität bereitstellt (bei Chrome: Firebase Cloud Messaging, bei Firefox: Mozilla Cloud Services und bei Edge: Windows Push Notification Service). Dieser Dienst liefert einen sogenannten Identifier („Push Notification Identifier“) zurück, der keine Rückschlüsse mehr auf die Device ID und somit auf den Benutzer zulässt. Die Kommunikation mit dem Push-Server des Auftragnehmers erfolgt danach immer mit diesem Identifier.

Die Device ID wird darüber hinaus nicht verwendet. Mit jedem Deaktivieren / Aktivieren ändert sich die Device ID. Der Auftragnehmer hat keinen Einfluss auf die Art und Weise der Benutzung der übermittelten Daten durch die Anbieter der Push Notification Dienste. Der Auftragnehmer kann nicht ausschließen, dass der Anbieter der Push Notification personenbezogene Daten ins Ausland übermittelt.

Der Subauftragnehmer speichert IP Adressen, um die Auslastung auf dem Server steuern zu können, sowie Hackerangriffe erkennen und unterbinden zu können. Eine über diesen Zweck hinausgehende Auswertung erfolgt vom Auftragnehmer nicht. IP Adressen werden vom Auftragnehmer nicht weitergegeben.

(2) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

(i) Kunden des Auftraggebers,

(ii) Interessenten des Auftraggebers,

(iii) Mitarbeitende des Auftraggebers und des Auftragnehmers,

(iv) Lieferanten des Auftraggebers,

(v) Ansprechpartner des Auftraggebers,

(vi) Kinder der Kunden oder Interessenten des Auftraggebers.

Anlage 3: Technisch-organisatorische Maßnahmen
Version: 10. November 2022

Hier sind die technischen und organisatorischen Maßnahmen nach Artikel 32 DSGVO (nachfolgend „TOM“) beschrieben. Die TOM können unabhängig vom Vertrag verändert werden. Dies dient dazu, administrativen Aufwand zu reduzieren. § 3 Absatz 3 dieser Vereinbarung zur Auftragsverarbeitung ist hierbei zu beachten.

Allgemein

Die informationsverarbeitenden Systeme des Auftragnehmers liegen in einem modernen Rechenzentrumsgebäude, das sehr hohen Schutz durch moderne Sicherheitstechnik gewährleistet. Bei der Auswahl des Rechenzentrums durch den Auftragnehmer ist das Sicherheitsniveau neben der bedarfsgerechten Performance das Hauptkriterium.

Der Betrieb erfolgt bei dem in der Anlage 4 genannten Rechenzentrum.

Der Betreiber des Rechenzentrums veröffentlicht seine eigenen technischen und organisatorischen Maßnahmen, die von dem Auftragnehmer kritisch geprüft wurden, bevor eine Verarbeitung aufgenommen wird. Die beschriebenen Maßnahmen des Rechenzentrums können dem Auftraggeber jederzeit bereitgestellt oder in den Geschäftsräumen des Auftragnehmers eingesehen werden.

Die technischen und organisatorischen Maßnahmen des Rechenzentrums werden in den TOM des Auftragnehmers nicht wiederholt.

Der Auftragnehmer behält es sich jederzeit vor, das Rechenzentrum zu verlegen. Dies kann insbesondere aufgrund technischer Entwicklungen sowie wirtschaftlichen oder performancebedingten Gründen notwendig werden. Die Abstimmung erfolgt nach den Vorgaben des § 6 der Auftragsverarbeitung.

Zutrittskontrolle

Mit der Zutrittskontrolle soll verhindert werden, dass unberechtigte Personen Zutritt zu den informationsverarbeitenden Systemen des Auftragnehmers bekommen.

Organisatorische Maßnahmen

Schlüsselvergabe

Der Zugang zu den Räumen mit Zugang zu informationsverarbeitenden Systemen des Auftragnehmers ist ausschließlich den Mitarbeitern im Rahmen ihrer Aufgabenerfüllung vorbehalten.

Die Räume sind durch Türschlösser gesichert. Die Schlüssel stehen nur den Mitarbeitenden sowie dem Empfangspersonal des Gebäudes zur Verfügung.

Die Schlüsselausgabe und -rücknahme werden zentral protokolliert, so dass jederzeit bekannt ist, wer sich zu den Räumen des Auftragnehmers Zutritt verschaffen kann.

Gäste haben keinen Zutritt zu den Räumen mit Zugang zu den informationsverarbeitenden Systemen.

Technische Maßnahmen

Das Gebäude mit den Räumen des Auftragnehmers ist durch Videokameras geschützt.

Zugangskontrolle

Die Zugangskontrollen sollen ein Eindringen unberechtigter Personen in die Informationsverarbeitenden Systeme des Auftragnehmers anhand technischer und organisatorischer Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung verhindern.

Organisatorische Maßnahmen

Benutzer- und Berechtigungsverfahren

Benutzer, die im Rahmen ihrer Aufgabenerfüllung Zugang zu einem System erlangen sollen, müssen diese Berechtigungen über einen dokumentierten Benutzer- und Berechtigungsprozess beantragen.

Die Anforderungen zur Benutzer- und Berechtigungsvergabe sind durch die internen Sicherheitsrichtlinien beschrieben.

Berechtigungen von Benutzern werden gesperrt, sobald diese aus dem Unternehmen ausscheiden oder diese Berechtigungen zur Aufgabenerfüllung nicht mehr benötigt werden.

Technische Maßnahmen

Authentisierungsverfahren

Zugangsberechtigungen werden restriktiv nur so vergeben, wie sie zur Aufgabenerfüllung benötigt werden.
Die Zugangskontrollverfahren gelten für alle Mitarbeitenden des Auftragnehmers gleichartig.
Alle Systeme sind durch zweistufige Authentisierungsverfahren (Benutzer-ID und Passwort) geschützt, die unberechtigten Zugriffe unterbinden.

Werden im Rahmen des Authentisierungsverfahrens Passwörter eingesetzt, müssen diese den internen Passwortrichtlinien für Mitarbeitenden und Systeme entsprechen. Passwörter, die nach den Richtlinien nicht der Qualität entsprechen, sind nicht erlaubt.
Die Systeme werden nach einer bestimmten Zeit der Inaktivität automatisch gesperrt.

Verschlüsselung

Der Zugriff auf die Server im Rechenzentrum erfolgt über verschlüsselte Datenübertragung durch HTTPS. Diese wird sichergestellt durch „Permanent SEO-safe 301 redirect from HTTP to HTTPS". Dabei wird auf ein unter der Marke „Let's Encrypt" von der Firma Internet Security Research Group (ISRG), 1 Letterman Drive, Suite D4700, San Francisco, CA 94129 ausgestelltes SSL/TLS-Zertifikat genutzt.

Die Passwortverschlüsselung in den Datenbanken erfolgt durch Hash mit SHA512 + Whirlpool und zusätzlichem Salt.

Der Schutz des Servers und der Datenbanken wird durch sichere Passwörter (Zeichenlänge mindestens 8 Zeichen inkl. Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) untermauert, die hohe Sicherheit gegen Brute-force-Attacken bieten.

Zugriffskontrolle

Die Maßnahmen dienen zur Überwachung und Protokollierung der Zugriffe.

Berechtigungsvergabe

Die Systeme wurden in der Weise konfiguriert, dass ein regulärer Zugriff mit administrativen Rechten nur für entsprechend autorisierte, interne Mitarbeitende möglich ist. Hier wurden bedarfsorientierte Berechtigungskonzepte ausgestaltet, die die Zugriffsrechte, sowie deren Überwachung und Protokollierung definieren. Die Berechtigungsvergabe erfolgt durch die Zuweisung von Rollen und Profilen der Benutzer mit den entsprechenden Berechtigungen.

Auswertungen

Zugriffe auf System-IDs werden auf einem zentralen Server protokolliert. Die Protokollierung schließt die autorisierten Administratoren ein. Beim auffälligen Zugriffsversuch wird zusätzlich eine Alarmierung (Security Monitoring) an den Datenschutzbeauftragten und die Geschäftsführung ausgelöst.

Löschung

Das Löschen von Benutzerberechtigungen (z.B. nach dem Austritt eines Mitarbeitenden) erfolgt innerhalb eines Arbeitstages.

Weitergabekontrolle

Im Rahmen der Weitergabekontrolle werden Maßnahmen beim Transport, der Übertragung und Übermittlung, sowie bei der nachträglichen Überprüfung von personenbezogenen Daten definiert.

Organisatorische Maßnahmen

Schulungsmaßnahmen

Alle Mitarbeiter des Auftragnehmers sind auf das Datengeheimnis hin verpflichtet worden (Art. 32 Abs. 4 DSGVO). Neue Mitarbeiter erhalten bei Eintritt eine Sicherheitsschulung.

Klassifizierung der Informationen

Vertrauliche Informationen werden zum Schutz der Informationen entsprechend klassifiziert und nicht auf Datenträger außerhalb des Rechenzentrums gespeichert.

Technische Maßnahmen

Zugriffs-und Transportsicherung

Grundsätzlich können auf die Systeme, die personenbezogene Daten verarbeiten, nur autorisierte Nutzer zugreifen. Die Übertragung von Daten erfolgt ausschließlich durch das System selbst an autorisierte Empfänger über gesicherte Wege.

Um das System vor unberechtigten Zugriffen von Rechnern der Mitarbeitenden und somit vor einer unautorisierten Weitergabe von Daten zu schützen, gelten die internen Sicherheitsrichtlinien für Mitarbeiter des Auftragnehmers.

Um Datenverlust zu verhindern, dürfen arbeitsrelevante Daten ausschließlich auf Servern gespeichert werden. Diese Daten werden regelmäßig gemäß den definierten Backup-Konzepten gesichert, sodass einem Datenverlust vorgebeugt ist.

Die von Mitarbeitenden des Auftragnehmers eingesetzten Notebooks, Laptops, Tablets oder anderen mobilen Geräten arbeiten nach gängigen Sicherheitsstandards, die einen Schutz vor Datenmissbrauch bieten. Die Kommunikation findet ausschließlich über VPN-Verbindungen mit dem Rechenzentrum statt. Die Festplatten der Notebooks und Laptops sind verschlüsselt. Alle Geräte sind mit einem Kennwortschutz vor Zugriff geschützt. Auf allen Notebooks und Laptops werden Virenscanner eingesetzt.

Eingabekontrolle

Um eine Nachvollziehbarkeit und Dokumentation der Datenverwaltung und –pflege zu gewährleisten, werden Protokolle zur nachträglichen Überprüfung, von wem welche Daten eingegeben, verändert oder gelöscht worden sind, implementiert.

Protokollierungs- und Protokollauswertung

Durch die Einhaltung der oben aufgeführten Regeln zu Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle wurde die Grundlage für die Eingabekontrolle der Systeme geschaffen, die personenbezogene Daten verarbeiten.

Analysen der Protokolle werden bei Bedarf von den Systemadministratoren, dem betrieblichen Datenschutzbeauftragten oder der Geschäftsführung vorgenommen, insbesondere wenn Auffälligkeiten vermutet oder erkannt wurden.

Auftragskontrolle

Alle Weisungen des Auftraggebers zum Umgang mit personenbezogenen Daten werden dokumentiert und an zentraler Stelle bereitgestellt.

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen dieser getroffenen Vereinbarungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach den Weisungen des Auftraggebers. Abweichende Verarbeitungen erfolgen nur nach schriftlicher Einwilligung des Auftraggebers.

Der Datenschutzbeauftragte des Auftraggebers hat das jederzeitige Recht, nach Absprache die Umsetzung seiner Weisungen bei des Auftragnehmers zu kontrollieren. Der Auftragnehmer wird den Auftraggeber bei der Durchführung von Kontrollen durch den Auftraggeber unterstützen und an der vollständigen Abwicklung der Kontrolle mitwirken.

Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach ihrer Einschätzung gegen gesetzliche Regelungen verstößt, sowie dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und / oder die erteilten Weisungen des Auftraggebers unverzüglich mitteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist.

Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses unterworfen (Art. 32 Abs. 4 DSGVO). Sie verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien werden innerhalb einer ungekündigten Vertragslaufzeit erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet.

Mit der Kündigung des Hauptvertrages hat der Kunde 3 Monate über das Vertragsende hinaus das Recht, unentgeltlich seine erfassten Daten herunterzuladen und für eigene Zwecke außerhalb der informationsverarbeitenden Systeme des Auftragnehmers zu nutzen. Danach werden die Daten des Auftraggebers nach Ablauf einer gegebenenfalls bestehenden Aufbewahrungspflicht durch den Auftragnehmer datenschutzgerecht vernichtet.

Verfügbarkeitskontrolle

Organisatorische Maßnahmen

Notfallhandbücher und Backup-Verfahren

Die Notfallhandbücher legen Verantwortlichkeiten (z.B. Notfallverantwortliche) sowie Eskalations-, Informations- und Alarmierungsprozesse, fest.

Alle Daten werden in regelmäßigen Intervallen bedarfsgerecht gesichert. Der Zugang auf die Backup-Software ist limitiert auf Mitarbeitenden mit der entsprechenden Zuständigkeit. Die Häufigkeit von Datenbackups richtet sich nach der Kritikalität der Informationen.

Technische Maßnahmen

Firewall und Virenschutz

Die Netze und Entwicklungs- und Testsysteme des Auftragnehmers sind mit einer Firewall gegen Hackerangriffe geschützt, die regelmäßig von autorisierten Systemadministratoren gewartet und aktualisiert werden. Alle Internetverbindungen sind durch eine Firewall geschützt.

Brandschutz

In den Räumen des Auftragnehmers sind Brandmelder, in einigen Bereichen darüber hinaus Handmelder eingebaut.
Zur ersten Bekämpfung von Bränden sind Handfeuerlöscher installiert.

Trennungskontrolle

Produktivsysteme werden strikt getrennt von den Entwicklungs- und Testsystemen betrieben.

Personenbezogene Daten aus Produktivsystemen dürfen nur anonymisiert als Kopie für Testzwecke verwendet werden.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management

Die Rückmeldungen der Anwender sowie eigene Erkenntnisse fließen fortwährend in die Produktentwicklung ein. Die Einhaltung des Datenschutzes ist parallel zur Performance als die oberste Zielsetzung definiert.

Incident-Response-Management

Sollte wider Erwarten ein Datenverlust eintreten, erfolgt die Mitteilung durch alle Mitarbeitenden an den Datenschutzbeauftragten des Auftragnehmers. Dieser wird sowohl die Geschäftsführung des Auftragnehmers als auch die / den Datenschutzbeauftragte(n) des Auftraggebers informieren.

Sollten bei einem Datenverlust personenbezogene Daten betroffen sein, wird sich der Auftragnehmer vorrangig bemühen, den Schaden für den oder die Betroffenen zu minimieren und danach in Abstimmung mit der / dem Datenschutzbeauftragte(n) des Auftraggebers notwendige Meldungen an Betroffene und die zuständigen Aufsichtsbehörden vornehmen.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO):

Die Anwendungen des Auftragnehmers sind grundsätzlich so eingestellt, dass eine Datensparsamkeit gewährleistet ist.

Die technische Integration des Datenschutzes ist weitest möglich vorgenommen. Dazu zählen beispielsweise eine Benutzeradministration auf Basis einer bestehenden Emailadresse, die den Versand nur an diese hinterlegte Adresse ermöglicht.

Der Auftragnehmer kann jedoch trotz der zuvor beschriebenen Maßnahmen sowie den Schutzmaßnahmen auf den Geräten des Auftraggebers oder seiner Kunden nicht verhindern, dass Kunden und / oder Mitarbeiter des Auftraggebers Daten bereitstellen, die für die Verarbeitung nicht benötigt werden.

Anlage 4: Genehmigte Unterauftragnehmer
Version: 10. November 2022

Firma **Unterauftragnehmer**	**Anschrift /** **Land**	**Leistung**
noris network AG	Thomas-Mann-Straße 16 – 20 90471 Nürnberg Deutschland	• Ausgelagertes Rechenzentrum • Auslagerung der Backup-Sicherheitsspeicherung und anderen Archivierungen
IBM Deutschland GmbH	IBM-Allee 1 71139 Ehningen Deutschland	Übersetzungsdienstleistungen; Der Benutzer hat die Möglichkeit, sich einen angezeigten Text in einer anderen Sprache anzeigen zu lassen.
verbaneum GmbH	Forchheimer Str. 8 90425 Nürnberg Deutschland	Kompetente zentrale Anlaufstelle für Anliegen des Auftraggebers in Form persönlicher Kommunikation

Anlage 5: Weisungsbefugte Personen des Auftraggebers
Version: 10. November 2022

Name: fullname

Tel: telephone1

Email: emailaddress1

Name: new_vornamecr5f5_nachname_5

Tel: cr5f5_telweisungsbefugt2

Email: cr5f5_email_5

Anlage 6: Weisungsempfangsberechtigte Personen des Auftragnehmers
Version: 10. November 2022

Name: Sebastian Kopp

Tel.: +49 176 41651166

Email: *sebastian.kopp@link-it-isi.de*

Name: Stefan Teschner

Tel.: +49 173 3775570

Email: *stefan.teschner@link-it-isi.de*

Anlage 7: Ansprechpartner Datenschutz
Version: 10. November 2022

Auftragnehmer:

Auf Seiten des Auftragnehmers ist eine dezidierte Emailadresse für die Kommunikation mit dem Datenschutzbeauftragten eingerichtet.

Nachfolgend die vereinbarten Kontaktdaten der Datenschutzbeauftragten:

Name: Thomas Bischoff

Tel.: +49 172 6607532

Email: *datenschutz@link-it-isi.de*

Auftraggeber:

Name: new_dataprotection_fullname

Tel: address2_telephone1

Email: emailaddress2

cr5f5_konfanlageheader

Version: 10. November 2022

cr5f5_konfanlageav