Vertrag über die Auftragsverarbeitung personenbezogener Daten

1. Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer, Auftragnehmer ist die iPrax Systems GmbH & Co. KG und der Auftraggeber ist das Unternehmen laut Bestellschein, (im Folgenden „Parteien" genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich" zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Gegenstand und Dauer der Verarbeitung

(1) Gegenstand: Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Hauptvertrag über die beauftragten Hauptleistungen zur Nutzung der iPrax-App samt Zusatzdienste (im Folgenden „Hauptvertrag").

(2) Dauer: Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages, sofern keine darüber hinaus gehenden Verpflichtungen direkt aus diesem Vertrag ergeben.

(3) Art und Zweck der Verarbeitung. Die Verarbeitung ist folgender Art: Datenverarbeitung im Rahmen der Bereitstellung einer Software zur Praxisverwaltung (Zweck): Erfassen, Organisation, Ordnen, Speicherung, Anpassung, Veränderung, Auslesen, Abfragen, Abgleich, Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten.

Es werden folgende Daten verarbeitet:

- Personenbezogene Daten
- Sensitive Daten (Art. 9 DSGVO: Besondere Arten personenbezogener Daten sind Angaben über Gesundheit)
- Personenstammdaten
- Behandlungsdaten (z. B. Text, Fotos und Videos)
- Kommunikationsdaten (z. B. Telefon, E-Mail)
- Vertragsstammdaten
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Rezeptabrechnungsdaten (gesetzlich und privat)
- Vertragsstammdaten zu Kostenträger (Krankenkassen)

(4) Kategorien der betroffenen Personen.
Von der Verarbeitung betroffen sind:

- Kundendaten des Auftraggebers
- Dritte, z. B. Interessenten
- Mitarbeiter des Auftraggebers
- Ansprechpartner
- Lieferanten
- Behörden
- Sozialversicherungsträger
- Kostenträger (Krankenversicherungen)
- Beschäftigte: Arbeitnehmerinnen und Arbeitnehmer; zu ihrer Berufsbildung Beschäftigte

3. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit und auf §203 StGB verpflichtet und wurden über die Strafbarkeit belehrt, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(6) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicher zu stellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

(10) Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

4. Technische und organisatorische Maßnahmen

(1) Die im Anlage 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Siedefinieren das vom Auftragnehmer geschuldete Minimum.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
(4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
(5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
(6) Die Verarbeitung von Daten in Privatwohnungen erfolgt nicht.
(7) Dedizierte Datenträger die vom Auftraggeber stammen, können vom Auftragnehmer nicht angenommen und verarbeitet werden.
(8) Der Auftragnehmer gewährleistet ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 lit. d DS-GVO.

5. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
(2) Entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

6. Unterauftragsverhältnisse

(1) Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmen mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmen bleiben unberührt. Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmen hinzuzieht. Vor Hinzuziehung oder Ersetzung des Subunternehmens informiert der Auftragnehmer den Auftraggeber.
(2) Der Auftraggeber hat das Recht innerhalb von zwei Wochen ab Kenntnis der Information über den Subdienstleister aus wichtigem Grund schriftlich beim Auftragnehmer Einspruch gegen den Einsatz des Subunternehmens einzulegen. Erfolgt kein Einspruch innerhalb der genannten Frist, gilt dies als Zustimmung des Auftraggebers zum Einsatz dieses Subdienstleisters. Der Auftragnehmer hat dafür Sorge zu tragen, die Pflichten dieses Vertrages auf den Subunternehmer zu übertragen und deren Einhaltung regelmäßig dokumentiert zu überprüfen. Der Auftragnehmer ha diese Dokumentation auf Anforderung vorzulegen. Subunternehmen sind vertraglich mindestens die Datenschutzverpflichtungen auferlegt, die denen in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
(3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmen wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmen durchzuführen oder durch Dritte durchführen zu lassen.
(4) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmens sind eindeutig voneinander abzugrenzen. Eine weitere Subbeauftragung durch das Subunternehmen ist nicht zulässig. Der Auftragnehmer wählt das Subunternehmen unter besonderer Berücksichtigung der Eignung der vom Subunternehmen getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus. Die Weiterleitung von im Auftrag verarbeiteten Daten an das Subunternehmen ist erst zulässig, wenn sich der Auftragnehmer dokumentiert, davon überzeugt hat, dass das Subunternehmen seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.
(5) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.
(6) Kommt das Subunternehmen seinen Datenschutzverpflichtungen nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

7. Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftragnehmer unterstützt angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen.
(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen schriftlich. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
(4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.
(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 4 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

8. Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle sind mitzuteilen. Die Mitteilung hat mindestens die Angaben nach Art. 33 Abs. 3 Datenschutz-Grundverordnung zu enthalten.
(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 32-36 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

9. Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
(2) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
(4) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

10. Beendigung des Auftrags

(1) Bei Beendigung des Auftragsverhältnisses hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben und sodann zu vernichten. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.
(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmen herbeizuführen.
(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

11. Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

12. Sonderkündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung"), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen, in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

(3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

(4) Der Auftragnehmer ist zur außerordentlichen Kündigung berechtigt, sofern der Auftraggeber der Beauftragung eines Subunternehmers gem. Kapitel 6 (2) dieses Vertrages widerspricht und keine Einigung erreicht werden kann.

13. Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist, stellt der Auftraggeber den Auftragnehmer auf erste Anforderung von sämtlichen Ansprüchen Dritter frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftragnehmer erhoben werden.

(3) Der Auftragnehmer haftet dem Auftraggeber gegenüber nur bei grober Fahrlässigkeit oder Vorsatz.

14. Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(3) Für Nebenabreden ist die Schriftform erforderlich.

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

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

—

Stand November 2026

Anlage 1: Technisch-organisatorische Maßnahmen

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

1. Zutrittskontrolle

Maßnahmen, die verhindern sollen, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Verarbeitung eigener Daten (insb. Vertrieb, Verwaltung, Personal): Die Verarbeitung eigener Daten erfolgt in geschützten Verwaltungsräumen, die durch eine Alarmanlage geschützt sind. Verarbeitung von Kundendaten im Rechenzentrum: Die Verarbeitung der Daten von iPrax Systems GmbH & Co. KG erfolgt in einem zertifizierten Hochsicherheitsrechenzentrum in München. Es besteht eine aktuelle Zertifizierung des Rechenzentrums nach ISO 27001 und ISO 9001. Ein rechtskonformer Vertrag im Rahmen der Auftragsdatenverarbeitung (Art. 28 DSGVO) mit erfolgter Erstkontrolle besteht. Überwachung der Außenhaut und Firmengelände:

- Glasbruchsensoren
- 24 x 7 Sicherheitsüberwachung durch Überwachungskameras auch in Infrarot
- Vergabe von Zutrittskarten nur über spezielles Freigabeverfahren mit Ausweiskontrolle
- Vollständig elektronisches Zutrittskontrollsystem basierend auf berührungslosen Zutrittskarten mit Foto und PIN Tastencodes
- Speicherung der Zutrittsdaten über 12 Monate, Kameraaufnahmen über mehrere Monate.

Überwachung im Rechenzentrum:

- 24 x 7 Sicherheitsüberwachung durch Überwachungskameras auch in Infrarot
- Vollständig elektronisches Zutrittskontrollsystem basierend auf berührungslosen Zutrittskarten mit Foto und PIN Tastencodes
- Biometrische Handflächenscanner bei der Colocationsfläche
- Verschlossene Colocation Suites mit berührungslosen Zutrittskarten mit Foto und PIN Tastencodes
- Verschlossene Serverschränke
- Einbruchsmeldesystem an Fluchtwegen und Notausgängen
- Speicherung der Zutrittsdaten über 12 Monate, Kameraaufnahmen über mehrere Monate.

Besucherzutritt: Besucher*innen dürfen sich nur in Begleitung von Mitarbeiter*innen im Unternehmen aufhalten. Der*die Besuchte hat die Verantwortung für den*die Besucher*in. Besucher*innen sind an der Tür von dem*von der Besuchten abzuholen, während des Aufenthalts im Unternehmen zu begleiten und zum Ausgang zu bringen.

Registrierung: Besucher*innen haben sich in eine Besucherliste mit Name, Uhrzeit der Ankunft und Abfahrt, verantwortliche*r Besuchte*r einzutragen. Die Liste ist so zu gestalten, dass der*die Besucher*in keine Informationen anderer Besucher*innen bekannt werden.

2. Zugangskontrolle

Maßnahmen, die sicherstellen sollen, dass nur befugte Personen Zugang zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden. Verarbeitung eigener Daten: Die Verarbeitung eigener Daten findet in den Räumlichkeiten der iPrax Systems GmbH & Co KG statt, sowie für Präsentationen und Verwaltungszwecke auch auf Notebooks mit bestehender Datenverschlüsselung. Verarbeitung von Kundendaten im Rechenzentrum:

- Transport von Daten: Der Transport von Daten findet ausschließlich per Netzwerk statt. Alle hierbei eingesetzten Verbindungen sind per SSL/IP-Sec verschlüsselt. Es werden grundsätzlich keine mobilen Geräte für den Transport von Daten von Auftraggebern eingesetzt. Für die Administration eingesetzte Computer sind mittels Datenverschlüsselung gegen unbefugte Nutzung geschützt.
- Sicherheitsprotokolle: Es werden Security Logs der Systeme aufgezeichnet und automatisiert ausgewertet und ggf. eskaliert.
- Sicherung von Bildschirmarbeitsplätzen: An allen Arbeitsplätzen des Unternehmens setzt nach 900 Sekunden ohne Eingaben automatisch ein passwortgeschützter Bildschirmschoner ein. Diese Maßnahme ist soweit möglich technisch erzwungen.
- Schutz vor externem Zugriff: Die IT-Systeme sind durch Firewall, Intrusion Prävention Systeme und Netzwerksegmentierung gegen unbefugten Zugriff geschützt. Verschlüsselter Remote-Zugriff ist nur eigenen Mitarbeitern ermöglicht.
- Vernichtung von Datenträgern: Nicht mehr benötigte Daten werden sicher gelöscht, sofern keine anderen Weisungen der Auftraggeber bestehen. Die Standardzeit für die Löschung von personenbezogenen Daten beträgt 14 Tage bei Sozialdaten und 90 Tage bei personenbezogenen Daten nach der Vertragserfüllung. Defekte Datenträger werden fachgerecht unter Beachtung der datenschutzrechtlichen Anforderungen vernichtet.

3. Zugriffskontrolle

Maßnahmen, um sicherzustellen, dass berechtigte Personen nur auf solche personenbezogene Daten Zugriff erhalten, für die sie die Befugnis zur Einsichtnahme und zur Verarbeitung besitzen. Verarbeitung eigener Daten: Die Verarbeitung eigener Daten findet im Rahmen des bestehenden Berechtigungskonzeptes statt. Die Verteilung von Berechtigungen erfolgt nach dem Need-To-Know-Prinzip. Verarbeitung von Kundendaten im Rechenzentrum:

- Sicherheitsstufen: Die iPrax-Plattform wird durch mehrere Sicherheitsstufen geschützt.
- Zugriffskontrolle:Im iPrax Büro sind gesicherte Zugänge gewährleistet. Der Zugang zu den iPrax Systemen durch das Unternehmen selbst erfordert einen Benutzernamen und ein Passwort (d. h. personalisierter Nutzer). Benutzernamen können bis zu 50 Zeichen lang sein. Passwörter sind mindestens 12 Zeichen lang. Die Applikation im jeweiligen mobilen Apple Gerät in der Praxis baut auf einer SQlite-Datenbank Infrastruktur auf. Nur der authorisierte Nutzer kann Zugang zur Anwendung erhalten. Der Zugang zur iPrax-Software erfordert einen Benutzernamen und ein Passwort (d.h. personalisierter Nutzer). Benutzernamen können bis zu 10 Zeichen lang sein. Passwörter des mobilen Apple Geräts sind maximal 4 Zeichen lang. Darüber hinaus findet eine weitere Identifizierung über die Kundennummer, die Geräte-ID und den Praxisschlüssel statt. Zusätzlich wird über eine Zwei-Faktor-Authentifizierung eine zusätzliche Gerätebindung des Zugangs hergestellt.
- Zeitliche Sitzungsbeschränkung: Sessions mit der iPrax Plattform sind zeitlich beschränkt. Offene Sessions, die länger als 30 Minuten inaktiv sind, werden beendet.
- Kommunikations-Sicherheit: Die Kommunikation mit der Datenbank im Rechenzentrum ist TLS-verschlüsselt. SSL-Zertifikate sichern Verbindung zwischen Servern und Ihren Benutzern ab.
- Sicherheit auf Datenebene (Data Security Layer): Die Serverumgebung speichert Informationen in einer Datenbank und in einem Dateisystem. Der Zugang zur Datenbank im Rechenzentrum ist passwortgeschützt, unter Verwendung von einer Authentifizierung.
- Berechtigungskonzept: Im Unternehmen besteht ein definiertes Berechtigungskonzept für a) Administration, b) Softwareentwicklung, c) Usermanagement und d) Benutzer.
- Nutzerkennungen: Es existiert eine zentrale Administration für die eingesetzten Serversysteme. Die zentrale Administration nimmt keine Tätigkeiten außer der technischen Verwaltung der Sicherheits- und Serversysteme vor (seperation of duty). Die zentrale Kundenverwaltung vergibt und überwacht die individualisierten Zugänge für Kunden und sonstige Berechtigungen zum Zugriff auf eingesetzte Systeme. Der Zugriff auf die iPrax-App ist passwortgeschützt. Der Zugriff der iPrax-App auf die Datenbank im Rechenzentrum ist zum einen durch die Kunden-ID und zum anderen durch die Verschlüsselung der gesendeten Daten mit dem Praxisschlüssel gesichert. Für die Praxen und Mitarbeiter werden ebenfalls individuelle Kennungen vergeben. Initialpasswörter hat der Inhaber unmittelbar nach Empfang zu ändern. Alle Passwörter sind individuell und geheim. Die Übermittlung der Passwörter im Rahmen einer Nutzeranmeldung erfolgt getrennt auf einem anderen Medium, als die Übermittlung des Benutzer Accounts. Alle Berechtigungen orientieren sich am tatsächlichen Bedarf der Nutzergruppen und sind entsprechend so restriktiv wie möglich ausgestaltet.

- Begrenzung/Protokollierung der Fehlversuche bei der Anmeldung: Erfolgreiche und verweigerte Anmeldeversuche werden über den Server protokolliert und im Bedarfsfall eskaliert.
- Administrationszugriff: Der verschlüsselte Remote-Zugriff auf die eingesetzten Server-Systeme ist nur für folgende Personen freigeschaltet: a) Administrator, b) Entwickler
- Administratortätigkeiten: Administrative Tätigkeiten werden überwacht, als Changelog gespeichert und nachvollziehbar gemacht. Es erfolgt eine regelmäßige Prüfung dieser Logdateien.
- Protokollierung: Dateizugriffe werden überwacht und ggf. (z. B. verweigerter Zugriff) protokolliert. Auffälligkeiten, wie mehrfach fehlgeschlagene Anmeldeversuche zur Nutzung von Hard- oder Software oder andere Abweichungen werden ebenfalls protokolliert. Die Auswertung der Protokolle erfolgt soweit möglich automatisch.

4. Trennungskontrolle

Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten auch nur getrennt verarbeitet werden. Verarbeitung eigener Daten: Innerhalb des Verwaltungssystems findet keine Verarbeitung von Auftragsdaten statt.

Verarbeitung von Kundendaten im Rechenzentrum:

- Mandantentrennung: Alle personenbezogenen Daten werden innerhalb des DV-Systems, sowohl a) im Empfang der Daten, b) Verarbeitung, als auch in der c) Auslieferung auftragsbezogen getrennt gespeichert. Für jeden Kunden werden eigene Accounts angelegt, die logisch und auf Berechtigungsebene von anderen Kunden getrennt sind.
- Trennung von Entwicklungs-, Test- und Produktionsprogrammen: Entwicklungs- und Produktionsdaten werden voneinander getrennt auf den jeweils dafür eingesetzten DV-Anlagen gespeichert.

5. Pseudonymisierung

Die gem. Art. 32 Abs. 1 lit. a DSGVO und Art. 25 Abs. 1 DSGVO zu erfolgenden Maßnahmen wie Pseudonymisierung und Verschlüsselungwerden gewährleistet, um für ein dem Risiko angemessenes Schutzniveau zu sorgen. Dabei erfolgt 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.

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

1. Weitergabekontrolle

Maßnahmen, die verhindern, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Zudem soll überprüft und festgestellt werden können, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen der Datenübertragung vorgesehen ist.

Verarbeitung eigener Daten: Die Weitergabe eigener Daten darf nur im Rahmen der Richtlinien zur Kommunikationssicherheit erfolgen. Sensible personenbezogene Kunden- oder Sozialdaten im Rahmen von iPrax dürfen nur verschlüsselt weitergegeben werden.

Verarbeitung von Kundendaten im Rechenzentrum:

- Regelung für den Eingang von personenbezogenen Daten: Auftragsbezogene personenbezogene Daten erreichen iPrax Systems GmbH & Co. KG ausschließlich per verschlüsselter Datenfernübertragung. Es werden keine physikalischen Datenträger zum Transport eingesetzt.
- Protokollierung von Dateneingängen: Dateneingänge werden über ein Monitoring erfasst und die Server-Protokolle zu Kontrollzwecken gespeichert. Die Löschung der Protokolldaten erfolgt, wenn der Auftragszweck erfüllt ist und keine steuerrechtlichen oder anderen gesetzlichen Archivierungspflichten mehr bestehen.
- Authentisierung bei Aufträgen des Auftraggebers:
  Im Bereich der iPrax-Plattform initiieren die Benutzer die Übertragung der personenbezogenen Daten selbst durch passwortgeschützte Anmeldung und anschließender Verwendung der Software. Bei Verwendung der iPrax Software werden Daten ausschließlich verschlüsselt übertragenen.
- Datenschutzgerechte Verträge mit Dritten:
  Soweit eine Beauftragung von Dritten erfolgt, erfolgt dies transparent gegenüber dem Auftraggeber. Es werden nur datenschutzrechtlich erforderlichen Verträge geschlossen, die mindestens den Anforderungen der Verträge zwischen Auftraggeber und Auftragnehmer dieses Vertrages entsprechen. Dokumentierte Erstprüfungen und laufende Prüfungen der Auftragnehmer erfolgen.
- Verpflichtung der Mitarbeiter auf das Datengeheimnis:
  Alle Mitarbeiter des Auftragnehmers sind datenschutzrechtlich zur Verschwiegenheit verpflichtet.
  Es bestehen folgende Verpflichtungserklärungen im Unternehmen:
- Verpflichtungserklärung/Vertraulichkeitserklärung Datenschutz. Es wird im Sinne des Art. 28 Abs. 3 lit b) DSGVO gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben.
- Verpflichtungserklärung Vertraulichkeitserklärung Telekommunikationsgeheimnis gem. § 3 TDDDG Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz);
- Verpflichtungserklärung Vertraulichkeitserklärung Geschäftsgeheimnis (Gesetz zum Schutz von Geschäftsgeheimnissen – GeschGehG);
- Verpflichtungserklärung Sozialgeheimnis § 35 SGB I (Sozialgesetzbuch I)

2. Eingabekontrolle

Maßnahmen, um zu ermöglichen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungsanlagen eingegeben, verändert oder entfernt worden sind. Verarbeitung eigener Daten: Die Eingabekontrolle beim Serversystem erfolgt über Changelogs. Änderungen innerhalb des Dateisystems werden sichergestellt.

Verarbeitung von Kundendaten im Rechenzentrum:

- Protokollierung von Dateneingaben: Soweit personenbezogene Daten im Auftrag des Auftraggebers empfangen und verarbeitet werden, wird dies über das bestehende Monitoring erfasst und protokolliert. Die Löschung der Protokolldaten erfolgt, wenn der Auftragszweck erfüllt ist und keine steuerrechtlichen oder anderen gesetzlichen Archivierungspflichten mehr bestehen.
- Protokollierung von Datenveränderungen: Veränderungen in den Datenbanken werden protokolliert. Die Löschung der Protokolldaten erfolgt, wenn der Auftragszweck erfüllt ist und keine steuerrechtlichen oder anderen gesetzlichen Archivierungspflichten bestehen.
- Definierte Abläufe für den IT-Betrieb: Über bestehende Prozesse, die die Tätigkeiten insb. der Entwickler vorgeben, sind die Aufgaben und Vorgehensweisen für jede Rolle im Rahmen der IT- Betreuung geregelt.

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

1. Verfügbarkeitskontrolle

Maßnahmen, mit denen personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden. Verarbeitung eigener Daten: Die Sicherung eigener Daten erfolgt im Rahmen eines bestehenden Backup- und Archivierungskonzeptes. Verschlüsselte Datensicherungsträger werden aus den Verwaltungsräumen regelmäßig ausgelagert. Verarbeitung von Kundendaten im Rechenzentrum: Das gesamte Rechenzentrum des eingesetzten Dienstleisters ist auf höchste Verfügbarkeit ausgelegt.

- Stromversorgung: Die externe Stromversorgung erfolgt redundant über zwei selbständige Trassen von unterschiedlichen Umspannwerken. Auch intern sind alle Löschabschnitte ebenfalls redundant versorgt und räumlich getrennt (Power Distribution Units an gegenüberliegenden Gebäudeseiten). Die Verfügbarkeit der Stromversorgung liegt bei 99.99 %. Sollte dennoch eine Störung eintreten, so wird die unterbrechungsfreie Stromversorgung sofort durch USV's auf Basis von Batterien sichergestellt. Nach einer Minute Stromausfall übernehmen Dieselgeneratoren die Stromversorgung. Deren Treibstoffreserven erlauben 24 Stunden Betrieb bei Volllast. Bei Absinken des Vorrats unter 75 % wird automatisch aufgefüllt. Hierfür bestehen Verträge mit ortsansässigen Lieferanten, die jederzeitige Versorgung sicherstellen.
- Klimatisierung: Die ausreichend dimensionierte Klimatisierung des Rechenzentrums (Kühlleistung aktuell 3 Megawatt) ist redundant ausgelegt. Derzeit existieren 12 Central Cooling Units, von denen mindestens zwei den Rechenzentrumsbereich des RZ-Dienstleisters versorgen.
- Wartung und Überwachung der IT-Infrastruktur: Monitoringsysteme melden permanent den Zustand der IT-Infrastruktur. Bei ungewöhnlichem Verhalten wird die Problemanalyse und -Lösung, auch teils unter Hinzunahme von externen Spezialdienstleistern, vorgenommen. Hinsichtlich der RZ-Infrastruktur werden nach den Wartungsrichtlinien quartalsweise, halbjährliche und jährliche Funktionstest einzelner Systeme durchgeführt. Bei den Dieselgeneratoren erfolgt z. B. ein monatlicher Testlauf gegen eine Lastbank, der die Funktion der Notstromaggregate bei Volllast prüft. Tests und Testergebnisse werden fortlaufend dokumentiert. Es finden automatisierte, permanente elektronische Tests der Core IT-Systeme statt, die die Funktion und Leistungsfähigkeit (z. B. den Durchsatz) prüfen. Jährlich viermal werden proaktiv Soft- und Hardwareupdates der zentralen Systeme evaluiert. Bugfixreports der Lieferanten garantieren darüber hinaus eine Prävention von Hard- und Softwarefehlern. Die Stabilität einer Hard-/Software hat Vorrang vor Featurevielfalt, wenn die Entscheidung für ein Update getroffen werden soll.
- Umwelteinflüsse, Notfallprävention, insb. Brandschutz: Das gesamte Rechenzentrum wird über ein zentrales Gebäudemanagementsystem überwacht. Es existieren automatische Meldeeinrichtungen für Wassereinbruch, Temperaturanstieg, Brandfrüherkennung und sonstige betriebsrelevanten Störungen. Auch Bereiche mit Unterbodenleitungen werden automatisch überwacht. Die Meldeeinrichtungen werden regelmäßig gewartet und auf Funktion getestet. Die Feuerlösch- und Rauchabzugsanlage wird automatisch beim Eintreten von kritischen Situationen durch mehrfach vorhandene Brandmeldeanlagen ausgelöst. Die zusätzliche optische Überwachung und die damit gegebene Möglichkeit des manuellen Eingreifens schützt die im Rechenzentrum befindlichen Systeme bestmöglich vor Beschädigungen im Brandfall. Im Gebäude werden soweit wie möglich nicht entflammbare und raucharme Materialien verwendet. Das Gebäude ist in mehrere selbständige Brandabschnitte unterteilt. Innerhalb des eigentlichen Rechenzentrumsbereichs erfolgt keine Lagerung, insbesondere von entflammbaren Materialien. Brandschutzwartungen erfolgen nach geltender Brandschutzverordnung. Betriebsrelevante Systeme wie z. B. Gebäudetechnik, USV/UPS inkl. Batterie und Generatortechnik, Klimatechnik werden nach Richtlinien der Hersteller gewartet. Notfallübungen werden im Zuge der Wartungen durchgeführt. Zusätzlich wird ein jährlicher „Black Building"-Test zur Simulation eines totalen Stromausfalls durchgeführt. Tatsächliche Störungsmeldungen werden zentral außerhalb des Rechenzentrums gesammelt und rund um die Uhr ausgewertet. Je nach Art der Störung erfolgt eine sofortige Benachrichtigung der Mitarbeiter vor Ort per E-Mail (Ticketsystem) oder telefonisch.
- Netzwerkanbindung: Glasfaser- und Kupferleitungen sind jeweils in höchstwertigen eigenen Leitungsschächten verlegt. Die Anbindung des Rechenzentrums an das Internet erfolgt mehrfach redundant über verschiedene 1 und 10 Gbit/s Ethernet Carrieruplinks sowie Peerings mit anderen Internet Service Providern und Rechenzentren. Momentan bestehen 7 Anbindungen. Die Verfügbarkeit der Anbindung liegt bei 99,95 %. Backbonestörungen sind innerhalb von maximal 4 Stunden zu beheben. Internetverbindungen bestehen standardmäßig mit 1 Gbit/s, optional sind auch 10 Gbit/s möglich. Diese Bandbreiten sind garantiert bis zu den Backbones anderer Betreiber.
- Bedienter Betrieb: Der bediente Betrieb 7x24 wird gewährleistet. Sowohl für die RZ Grundleistungen wie auch für die Netzwerksysteme steht ein 7x24 Stundensupport zur Verfügung, der die Verfügbarkeit und Leistung der Systeme überwacht. Eine 24 Stundenhotline für den Kunden ist vorhanden.
- Gebäudewartung: Geplante Wartungen und andere notwendige Maßnahmen – z. B. Veränderungen an der RZ Infrastruktur – werden hinsichtlich der Beeinträchtigung verschiedenen Klassifizierungsstufen (PSA no, low und high) zugeordnet. Der Auftragnehmer wird über eine geplante und voraussichtlich Servicebeeinträchtigende Maßnahme vier Wochen im Voraus durch den RZ-Betreiber informiert.
- Datensicherung: Die Sicherung der Systeme beim beauftragten Dienstleister erfolgt in mindestens 14 Generationen. Eine Rücksicherung der Daten im Rahmen des erfolgten Backups zurückgehend durch den Dienstleister wird garantiert. Die garantierte Verfügbarkeit der Systeme beträgt im Jahresmittel mindestens 99 %.
- Notfallkonzept: Der Dienstleister hat ein bestehendes Notfallkonzept in dessen Rahmen regelmäßige Test der Infrastruktur (Internetanbindung, Storage, Serverinfrastruktur) dokumentiert durchgeführt werden.
- Updates: Der Administrator versorgt alle Server und Software regelmäßig mit aktuellen Sicherheits- und sonstigen notwendigen Updates. Der Einsatz von Sicherheitsupdates erfolgt nach Tests auf separaten Testsystemen.
- Virenschutz: Im Rahmen der Gateway Security werden übertragene Daten auf den eingesetzten Servern auf Schadsoftware überwacht. Die Software hält sich selbst automatisch auf aktuellem Stand (Programm und Signaturen). Verdächtige Dateien werden automatisch in ein Quarantäne-Verzeichnis verschoben Eine rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) wird durch die Rücksicherung der Daten im Rahmen von Backups gewährleistet.

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

1. Incident-Response-Management

Bei Sicherheitsvorfällen kann auf einen bestehenden Vorfallreaktionsplan zurückgegriffen werden. Alle verantwortlichen Personen werden auf mögliche Vorfälle vorbereitet. Dies umfasst die Identifikation des Vorfalls, die Eindämmung des Schadens, die Entfernung der betroffenen Systeme und die Wiederherstellung des Status Quo. Gewonnene Erkenntnisse werden dokumentiert und analysiert, so dass künftige Reaktionen verbessert werden können.

2. Datenschutzfreundliche Voreinstellungen

Datenschutzfreundliche Voreinstellungen gem. Art. 25 Abs. 2 DS-GVO werden proaktiv und frühzeitig implementiert, um das Schutzniveau für personenbezogene Daten in der DS-GVO zu gewährleisten. Dabei werden vor allem Zweck, Umfang, Speicherfrist und Zugänglichkeit von personenbezogenen Daten berücksichtigt. Die getroffenen Maßnahmen stellen insbesondere sicher, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

3. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur gemäß den Weisungen des Auftraggebers verarbeitet werden können. Verarbeitung eigener Daten: Die Verarbeitung eigener Daten findet in den Büroräumen statt. Verarbeitung von Kundendaten im Rechenzentrum: Die Verarbeitung personenbezogener Daten im Auftrag erfolgt ausschließlich im Rahmen der zugrundeliegenden Vereinbarung, entsprechend der gesetzlichen Vorschriften und nach Weisung des Auftraggebers. Soweit eine Beauftragung von Dritten erfolgt, erfolgt dies transparent gegenüber dem Auftraggeber. Es werden nur datenschutzrechtlich erforderliche Verträge geschlossen, die mindestens den Anforderungen der Verträge zwischen Auftraggeber und Auftragnehmer dieses Vertrages entsprechen. Dokumentierte Erstprüfungen und laufende Prüfungen der Auftragnehmer erfolgen.

—

Stand April 2026

Anlage 2: Liste der Subdienstleister

Subdienstleister/Firmierung	Kurzbeschreibung/Tätigkeit	Garantie bei Drittlandtransfer
SumUp Koppenstr. 8, Berlin 10243 Deutschland	Finance/Zahlungsdienstleistung	
Collmex Lilienstraße 37, 66119 Saarbrücken Deutschland	Buchhaltung	
Telekom Landgrabenweg 149, 53227 Bonn Deutschland	IT-Dienstleister / Erbringung von Kommunikationsdienstleistungen	
Marketcircle 30 Centurian Drive, Unit 201, Markham Kanada	IT-Dienstleister / Zurverfügungstellung Daylite als Verwaltungsprogramm	Angemessenheitsbeschluss der EU-Kommission
Fiskaly Mariahilfer Str. 36, 1070 Wien Österreich	IT-Dienstleister	
Atlassian 341 George Street, Sydney NSW 2000 Australien	IT-Dienstleister / Atlassian Data Processing Addendum bezüglich Erwerb von Atlassian Produkte: Confluence und Jira	Standardvertragsklauseln (SCC)