

Vertrag über die Auftrags-verarbeitung gemäß Art. 28 Datenschutzgrundverordnung (DSGVO)

zwischen

dem Kunden der Dr. Clip GmbH

nachfolgend: „Auftraggeber“-

und

Dr. Clip GmbH, Jenischstr. 62, 22609 Hamburg

nachfolgend: „Auftragnehmer“

nachfolgend gemeinsam: „Parteien“

Präambel

Die Parteien haben einen Vertrag über die Erbringung von Leistungen im Zusammenhang mit personenbezogenen Daten geschlossen (nachfolgend „Hauptvertrag“). Dieser Vertrag konkretisiert die Verpflichtungen der Parteien zum Datenschutz, die sich aus dem Hauptvertrag ergeben. Er findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer, Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

1. Gegenstand der Verarbeitung (Art. 28 Abs. 3 S. 1 DSGVO)

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers zur Erfüllung seiner vertraglichen Pflichten gegenüber dem Auftraggeber.

☐ Der Gegenstand der Verarbeitung ergibt sich aus dem Hauptvertrag.

☒ Der Gegenstand der Verarbeitung ergibt sich aus Anlage 1.

☐ Gegenstand der Verarbeitung ist:

2. Dauer der Verarbeitung (Art. 28 Abs. 3 S. 1 DSGVO)

☒ Die Dauer der Verarbeitung ergibt sich aus dem Hauptvertrag.

☐ Die Dauer der Verarbeitung beträgt:

3. Art und Umfang der Verarbeitung (Art. 28 Abs. 3 S. 1 DSGVO)

☐ Art und Umfang der Verarbeitung ergibt sich aus dem Hauptvertrag.

☒ Art und Umfang der Verarbeitung ergeben sich aus Anlage 1.

☐ Art und Umfang der Verarbeitung ist:

4. Zweck der Verarbeitung (Art. 28 Abs. 3 S. 1 DSGVO)

5. Art der personenbezogenen Daten (Art. 28 Abs. 3 S. 1 DSGVO)

☐ Die Arten der personenbezogenen Daten ergeben sich aus dem Hauptvertrag.

☒ Die Arten der personenbezogenen Daten ergeben sich aus Anlage 1.

☐ Die Verarbeitung betrifft folgende Arten personenbezogener Daten:

6. Kategorien betroffener Personen (Art. 28 Abs. 3 S. 1 DSGVO)

☐ Die Kategorien betroffener Personen ergeben sich aus dem Hauptvertrag.

☒ Die Kategorien betroffener Personen ergeben sich aus Anlage 1.

☐ Die Verarbeitung betrifft folgende Kategorien von Personen:

7. Pflichten und Rechte des Auftraggebers (Art. 28 Abs. 3 S. 1 DSGVO)

Die Pflichten und Rechte des Auftraggebers ergeben sich aus dem Hauptvertrag und diesem Vertrag.

8. Verarbeitung personenbezogener Daten nur auf dokumentierte Weisung (Art. 28 Abs. 3 S. 2 lit. a DSGVO)

Der Auftragnehmer verarbeitet und übermittelt personenbezogene Daten des Auftraggebers nur auf dokumentierte Weisung des Auftraggebers. Das gilt insbesondere für die Übermittlung personenbezogener Daten des Auftraggebers an einen Empfänger in einem Drittland oder an eine internationale Organisation. Eine solche Übermittlung ist nur zulässig, wenn eine entsprechende Weisung vorliegt und die Voraussetzungen nach Kapitel V DSGVO erfüllt sind.

Die Weisungen werden anfänglich durch diesen Vertrag und den Hauptvertrag festgelegt und können vom Auftraggeber danach in Textform (auch per E-Mail) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden.

Der Auftragnehmer darf personenbezogene Daten des Auftraggebers auch verarbeiten und übermitteln, wenn er hierzu durch das Recht der Europäischen Union oder eines Mitgliedstaats verpflichtet ist. In diesem Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

9. Verpflichtung eingeschalteter Personen (Art. 28 Abs. 3 S. 2 lit. b DSGVO)

Der Auftragnehmer verpflichtet zur Verarbeitung der personenbezogenen Daten eingesetzte oder befugte Personen vorab zur Vertraulichkeit und Wahrung des Datengeheimnisses oder stellt sicher, dass sie einer angemessenen gesetzlichen Verschwiegenheitspflicht in Bezug auf die personenbezogenen Daten unterliegen.

10. Technische und organisatorische Maßnahmen (Art. 28 Abs. 3 S. 2 lit. c DSGVO)

Der Auftragnehmer gestaltet seine innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers, die den datenschutzrechtlichen Anforderungen genügen. Diese ergeben sich insbesondere aus Art. 32 DSGVO. Die konkret getroffenen Maßnahmen sind in Anlage 2 dokumentiert.

Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieser Verarbeitung sind die technischen und organisatorischen Maßnahmen durch den Auftragnehmer fortlaufend an die Anforderungen dieser Verarbeitung anzupassen und

weiterzuentwickeln. Das hier und in Anlage 2 vereinbarte Schutzniveau darf dabei nicht unterschritten werden.

11. Einschaltung von Unterauftragnehmern (Art. 28 Abs. 3 S. 2 lit. d DSGVO)

Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer für die Verarbeitung personenbezogener Daten des Auftraggebers die in Anlage 3 aufgezählten Unterauftragnehmer einsetzt.

- ☐ Der Auftragnehmer beauftragt weitere Unterauftragnehmer nur nach individueller schriftlicher Genehmigung des Auftraggebers.
- ☒ Der Auftraggeber gestattet die Beauftragung weiterer Unterauftragnehmer ohne vorherige gesonderte Genehmigung. Der Auftragnehmer informiert den Auftraggeber vorab über jede beabsichtigte Beauftragung weiterer Unterauftragnehmer oder die Änderung bestehender Beauftragungen. Der Auftraggeber hat gegen die Beauftragung neuer Unterauftragnehmer oder die Änderung bestehender Beauftragungen ein Recht zum Einspruch. Die Mitteilung muss so rechtzeitig erfolgen, dass der Auftraggeber dieses Einspruchsrecht mit angemessener Überlegungsfrist vor der beabsichtigten Änderung ausüben kann.

Nimmt der Auftragnehmer die Dienste eines in Anlage 3 genannten oder eines weiteren Unterauftragnehmers für die Verarbeitung personenbezogener Daten des Auftraggebers in Anspruch, so erlegt er dem Unterauftragnehmer vorab vertraglich oder durch ein anderes anwendbares Rechtsinstrument nach dem Recht der Europäischen Union oder des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auf, die zwischen ihm und dem Auftraggeber in diesem Vertrag oder durch ein anderes anwendbares Rechtsinstrument des Rechts der Europäischen Union festgelegt sind. Er stellt dabei insbesondere sicher, dass der Unterauftragnehmer hinreichende Garantien bietet, dass geeignete technische und organisatorische Maßnahmen getroffen sind und so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des Datenschutzrechts und dieses Vertrags erfolgt. Der Auftragnehmer haftet dem Auftraggeber für die Einhaltung dieser Datenschutzpflichten durch den Unterauftragnehmer.

12. Unterstützung des Auftraggebers bei der Erfüllung datenschutzrechtlicher Pflichten (Art. 28 Abs. 3 S. 2 lit. e und f DSGVO)

Der Auftragnehmer unterstützt den Auftraggeber nach seinen Möglichkeiten bei der Beantwortung von Anfragen betroffener Personen, der Information von betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten und der Umsetzung der Rechte der betroffenen Personen in Bezug auf die verarbeiteten Daten. Der Auftragnehmer beantwortet Auskunftsanfragen und andere Begehren von betroffenen Personen nicht selbst, sondern verweist die betroffenen Personen insoweit an den Auftraggeber.

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen (1) bei der Implementierung und Umsetzung technischer und organisatorischer Maßnahmen des Auftraggebers, (2) im Falle von Datenschutzverletzungen, bei der ggf. gesetzlich erforderlichen Meldung an die Datenschutzaufsichtsbehörden und der ggf. gesetzlich erforderlichen Benachrichtigung von betroffenen Personen, (3) bei gesetzlich erforderlichen Pflichten zur Datenschutz-Folgenabschätzung und (5) bei gesetzlich erforderlichen Abstimmungen mit der Datenschutzaufsichtsbehörde.

13. Löschung oder Rückgabe von Daten nach Abschluss der Verarbeitung (Art. 28 Abs. 3 S. 2 lit. g DSGVO)

Nach Wahl des Auftraggebers löscht der Auftragnehmer die Daten des Auftraggebers oder gibt diese zurück, wenn die Verarbeitung abgeschlossen ist. Nur sofern und solange eine entsprechende Rechtspflicht besteht, darf der Auftragnehmer die Daten davon unabhängig speichern.

14. Datenschutzrechtliche Pflichten des Auftragnehmers, Nachweis der Einhaltung und Kontrollrechte (Art. 28 Abs. 3 S. 2 lit. h DSGVO)

Der Auftraggeber kann sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den getroffenen technischen und organisatorischen Maßnahmen des Auftragnehmers überzeugen. Hierfür kann er insbesondere Auskünfte des Auftragnehmers einholen, sich vorhandene Testate eines Sachverständigen vorlegen lassen und zur Verarbeitung seiner Daten eingesetzte Datenverarbeitungsanlagen prüfen oder durch beauftragte Dritte prüfen lassen.

Der Auftragnehmer kontrolliert regelmäßig die getroffenen technischen und organisatorischen Maßnahmen und bestellt einen Datenschutzbeauftragten, soweit er gesetzlich dazu verpflichtet ist.

Der Auftragnehmer führt das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO und stellt dies dem Auftraggeber auf Anforderung zur Verfügung.

Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung seiner vertraglichen und gesetzlichen Pflichten als Auftragsverarbeiter zur Verfügung. Er gestattet und ermöglicht dem Auftraggeber und von ihm beauftragten Prüfern entsprechende Überprüfungen einschließlich Inspektionen und trägt in zweckmäßigem Maß dazu bei.

15. Information über datenschutzwidrige Weisungen (Art. 28 Abs. 3 S. 3 DSGVO)

Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt.

16. Berichtigung, Löschung und Sperrung von Daten

Der Auftragnehmer berichtigt, löscht oder sperrt personenbezogene Daten des Auftraggebers, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

17. Mitteilung von Verstößen (Art. 33 Abs. 2 DSGVO)

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei unrechtmäßiger Kenntniserlangung der personenbezogenen Daten durch Dritte oder bei sonstigen schwerwiegenden Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder in diesem Vertrag getroffene Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

18. Weitere Pflichten und Schlussbestimmungen

Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren, durch Verlangen nach Offenlegung im Zusammenhang mit gerichtlichen Verfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im datenschutzrechtlichen Sinne liegen.

Änderungen oder Ergänzungen dieses Vertrags bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrags den Regelungen des Hauptvertrages und anderen vertraglichen Regelungen vor.

Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit dieses Vertrags im Übrigen nicht.

Bei Widersprüchen zwischen der deutschen und der englischen Version dieses Vertragstextes gilt die deutsche Version.

Es gilt deutsches Recht.



(Unterschrift Dr. Clip)

Datum (date), Unterschrift (signature) – Auftraggeber (Controller)

Anlage 1

Angaben zur Verarbeitung

Gegenstand, Art und Umfang der Verarbeitung

Betrieb der Dr. Clip Software

Speicherung der Daten

Zwecke der Verarbeitung

Vertragserfüllung: Bereitstellung des Dienstes Dr. Clip

Art der personenbezogenen Daten

Stammdaten /Adressdaten des Kunden Arztes:

-Name Anschrift

-Kommunikationsstammdaten

Stammdaten des Patienten:

-Name Anschrift

-Kommunikationsstammdaten

Befunddaten des Patienten

Behandlungsvorschläge

Kategorien betroffener Personen

Kunde (Arzt)

Patienten

Anlage 2

Technische und organisatorische Maßnahmen des Auftragnehmers

Zutrittskontrolle

Bei der Zutrittskontrolle handelt es sich um Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu den Datenschutzverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Automatisches Zugangskontrollsystem
- Bewegungsmelder
- Schlüsselregelung
- Transponderzutrittssystem
- Manuelles Schließsystem
- Sicherheitsschlösser
- Sorgfältige Auswahl von Reinigungskräften

Zugangskontrolle

Bei der Zugangskontrolle handelt es sich um Maßnahmen, die geeignet sind, zu verhindern,

dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Zuordnung von Benutzerrechten
- Passwortvergabe komplexer Passwörter
- Authentifikation Benutzername / Passwort
- Schlüsselregelung
- Erstellen von Benutzerprofilen
- Sicherheitsschlösser
- Einsatz einer Firewall

Zugriffskontrolle

Bei der Zugriffskontrolle handelt es sich um Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Erstellung von Berechtigungskonzepten

- Anzahl der Administratoren auf das Notwendigste reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung oder auch Löschung von Daten
- Physische Löschung von Datenträgern vor Wiederverwendung
- Einsatz von Aktenvernichtern (nach DIN)
- Verschlüsselung von Datenträgern

Weitergabekontrolle

Bei der Weitergabekontrolle handelt es sich um Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Beim physischen Transport erfolgt eine sorgfältige Auswahl des Transportunternehmens
- Zugriff auf alle datenhaltende Systeme über verschlüsselte Verbindungen, ebenso Übertragung aller personenbezogener Informationen (SSL) Eingabekontrolle

Bei der Eingabekontrolle handelt es sich um Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Nachvollziehbarkeit der Eingabe, Änderung und Löschung der Daten auf Basis eines Berechtigungskonzeptes
- Vergabe von Rechten zur Eingabe, Änderung und Löschung auf Basis des oben genannten Konzeptes

Auftragskontrolle

Bei der Auftragskontrolle handelt es sich um Maßnahmen, welche gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

- **Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart**

Verfügbarkeitskontrolle

Bei der Verfügbarkeitskontrolle handelt es sich um Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- **Feuer- und Rauchmeldeanlagen**
- **Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort**
- **Erstellen eines Backup- / Recoverykonzepts**

Trennungsgebot

Bei dem Trennungsgebot handelt es sich um Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- **Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern**
- **Erstellung eines Berechtigungskonzepts**

Anlage 3 / Annex 3

Unterauftragnehmer

Unterauftragnehmer / Sub-Processors	Kontaktdaten / Contact Details	Gegenstand der Verarbeitung / Subject Matter of the Processing
9elements GmbH	Kortumstraße 19-21 44787 Bochum, Germany +49 234 689 4188	Erstellung und Überwachung der Plattform
Amazon Web Services	Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy 1855 Luxemburg	Hosting der Software, Speicherung der Daten
Teamviewer	TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen Deutschland	Technisch / administrative Supportleistung, nur zum Zwecke der Fehlerbeseitigung / Wartung

Kontakt zum Datenschutzbeauftragten:

Sebastian Biermann
Datenschutzbeauftragter (TÜV)
c/o ANKA Rechtsanwaltsgesellschaft mbH
Kaninenberghöhe 50, 45136 Essen

Email: dsb@anka.eu