

Vereinbarung zur Auftragsverarbeitung

zwischen _____
_____ (Name + Adresse)

als Verantwortlicher (hier bezeichnet als „Auftraggeber“)

und

dem Digitalcourage e.V., vertreten durch den Vorstand, Marktstraße 18, 33602
Bielefeld

als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“).

Präambel

Der Auftragnehmer stellt das quelloffene Terminfindungs- und Umfragetool „Nuudel“ seinen Nutzern kostenlos zur Verfügung. Der Auftraggeber möchte dieses Tool für sein Unternehmen nutzen. Da im Rahmen der Termin- und Entscheidungsfindung auch personenbezogene Daten eingetragen werden können, kann die Verarbeitung personenbezogener Daten nicht gänzlich ausgeschlossen werden. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 2 Gegenstand der Verarbeitung

Gegenstand dieser Vereinbarung ist ausschließlich das Terminfindungs- und Umfragetool „Nuudel“, dessen Nutzung für den jeweiligen Nutzer kostenlos ist.

§ 3 Weisungsrecht

(1) Der Auftragnehmer darf Daten gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich

darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen Nutzung von „Nuudel“ erhält der Auftragnehmer in der Regel Zugriff auf folgende personenbezogene Daten:

- Name (falls angegeben)
- E-Mail-Adresse (falls angegeben)
- IP-Adresse (soweit technisch notwendig)
- In Freitextfeldern angegebene Informationen, die ggf. personenbezogen sein und zudem in die besondere Kategorie nach Art. 9 DSGVO fallen können.

(2) Der Kreis der von der Datenverarbeitung Betroffenen sind die Kund.innen (ggf. Patient.innen oder Mandant.innen) und Mitarbeiter.innen des Auftraggebers, sowie andere Personen, denen der Auftraggeber die Nutzung von Nuudel ermöglicht.

§ 5 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in Anlage 1 aufgeführten Maßnahmen der

- a) Zutrittskontrolle
- b) Zugangskontrolle

- c) Zugriffskontrolle
- d) Weitergabekontrolle
- e) Eingabekontrolle
- f) Auftragskontrolle
- g) Verfügbarkeitskontrolle
- h) Trennungskontrolle

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Ansprechpartnerin für den Datenschutz beim Auftragnehmer ist Nils Büschke (Datenschutzbeauftragter, c/o Digitalcourage e.V., Marktstr. 18, 33602 Bielefeld).

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen sind so gefasst, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 6 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragneh-

mers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
- b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des betrieblichen Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

(7) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig, nach vorheriger Ankündigungen, von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

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

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

teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

§ 8 Einsatz von Subunternehmern

(1) Derzeit sind im Rahmen der Bereitstellung des Dienstes „Nuudel“ keine Subunternehmer involviert und es werden zukünftig keine Subunternehmer aus Drittländern beauftragt. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern eine Genehmigung der Auftraggeber einzuholen und die Subunternehmen entsprechend den Regelungen dieser Vereinbarung zu verpflichten. Dabei ist sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann.

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

§ 9 Anfragen und Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DSGVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 10 Haftung

(1) Für die Haftung gelten die Regelungen der DSGVO, insbesondere Artikel 28 Absatz 4 Satz 2 DSGVO und Artikel 82 DSGVO.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(3) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 11 Beendigung der Nutzung

(1) Der Auftragnehmer wird die Umfrage, inkl. den dazugehörigen Daten automatisch nach 720 Tagen nach dem letzten Termin der Abstimmung löschen, oder an dem vom Auftraggeber vorgegebenen Löschdatum. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757-1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

§ 12 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Bielefeld.

Anlage 1 – Technische und organisatorische Maßnahmen des Auftragnehmers

Ort, Datum, Unterschrift (Auftraggeber)

Bielefeld, 09.03.2023

Ort, Datum, Unterschrift (Auftragnehmer)

Anlage 1 – Technische und organisatorische Maßnahmen

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

1.1 Zutrittskontrolle

Die Serverinfrastruktur für nuudel.de ist im Rechenzentrum von Individual Network Berlin e.V. (im folgenden: Provider) untergebracht. Der Provider hat folgende Maßnahmen eingeführt, mit denen Unbefugten der Zutritt zu Räumen verwehrt wird, in denen die betreffenden Datenverarbeitungsanlagen untergebracht sind:

- Festlegung von Sicherheitszonen
- Realisierung eines wirksamen Zutrittsschutzes
- Protokollierung des Zutritts
- Festlegung zutrittsberechtigter Personen
- Verwaltung von personengebundenen Zutrittsberechtigungen
- Begleitung von Dritten

1.2 Zugangskontrolle

Der Zugang zur Serverinfrastruktur für nuudel.de ist nur für besonders benannte Mitarbeitende von Digitalcourage e.V. möglich. Der Zugang ist mit einer starken Authentisierung gesichert und erfolgt nur von Endgeräten mit verschlüsselten Speichermedien. Logins und andere sicherheitsrelevante Ereignisse werden protokolliert.

1.3 Zugriffskontrolle

Es kann nur auf die Daten zugegriffen werden, für die eine Zugriffsberechtigung besteht.

1.4 Verwendungszweck-/Trennungskontrolle

Für nuudel.de gilt besondere Datensparsamkeit: Es werden nur die vom Benutzer eingetragenen Daten gespeichert, die technisch notwendig sind. Insbesondere werden keine IP-Adressen in Log-Dateien erfasst. Verschiedene Datensätze werden nicht miteinander verknüpft. Es erfolgt keine Weiterverwendung der gespeicherten Daten über den Zweck der Anwendung nuudel.de hinaus.

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

Beim Erstellen einer neuen Umfrage ist vermerkt, dass keine reale E-Mailadresse eingegeben werden muss. Der Versand von E-Mails findet somit nur statt, wenn dies bei der Erstellung der Umfrage ausdrücklich gewünscht wird.

Es werden keine weiteren Daten gespeichert, als für den Zweck erforderlich. Damit können Daten, die zur Erreichung des Verwendungszwecks nicht erforderlich sind,

nur durch eine Aktion der betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.

1.6 Verschlüsselung

Die Übertragung von Daten zwischen Client und Server bei der Eingabe und Anzeige erfolgt ausschließlich über verschlüsselte Verbindungen.

1.7 Anonymisierung

Auf die Möglichkeit anonymer Umfragen wird ausdrücklich hingewiesen.

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

2.1 Weitergabekontrolle

Der Zugang zu einer Umfrage ist über die zufällig erzeugte URL gesichert, die nur den Beteiligten der Umfrage bekannt ist. Nur die Beteiligten können die angezeigten Daten auf ihren lokalen PC exportieren. Nur wer Zugriff auf die bei Erstellung der Umfrage zufällig festgelegte Admin-URL zu der Umfrage hat, kann die Stammdaten der Umfrage einsehen und ändern oder veranlassen, sich Informationen zu den Umfragen an die ggf. selbst eingetragene E-Mail-Adresse schicken zu lassen.

Eine sonstige Weitergabe an Dritte findet nicht statt.

2.2 Löschung der Daten

Umfragen werden bei Erreichen des Löschdatums vollständig gelöscht. Das Löschdatum ist im Normalfall 720 Tage nach Erstellung der Umfrage, kann aber bei Erstellung der Umfrage und später auf ein beliebiges früheres Datum geändert werden. Außerdem kann die Löschung mit sofortiger Wirkung ausgelöst werden.

2.3 Datensicherungen

Die Daten des Servers werden in einem regelmäßigen Backup gesichert. Der Backup-Server befindet sich in den Geschäftsräumen von Digitalcourage, die Übertragung der Daten erfolgt über eine Ende-zu-Ende-verschlüsselte Verbindung, und die Sicherung erfolgt auf verschlüsselte Speichermedien. Der Zugriff des Backups ist mit starker Authentisierung abgesichert.

2.4 Eingabekontrolle

Der Zugriff auf die in nuudel.de eingetragenen Daten ist grundsätzlich für jede Person möglich, die Zugriff auf die URL's mit den Zugängen zur Umfrage bzw. zum Admin-Zugang hat. Eine Protokollierung findet aus Gründen der Datensparsamkeit nicht statt.

3. Verfügbarkeit und Belastbarkeit, Disaster Recovery

Der Server ist mit redundanter Stromversorgung und redundantem Massenspeicher (RAID1) versehen und in das Monitoring-System der von Digitalcourage e.V. betriebenen Serverinfrastruktur eingebunden. Der Server verfügt über die üblichen Verfahren zur Abwehr von systembelastendem Missbrauch. Für den Fall eines Serverausfalls gibt es ein Recovery-Verfahren zum Einspielen eines Backups.

Der Provider verfügt über einen Notfallplan für das Rechenzentrum, der die folgenden Aspekte umfasst:

- Redundanz der Stromversorgung
- Redundanz der Kommunikationsverbindungen
- Regelmäßige Prüfung der Notfalleinrichtungen
- Definition der Maßnahmen bei Eintritt von Notfallbedingungen
- Individual Network Berlin e.V. - Auftragsverarbeitungsvertrag, Version 20180524 Seite 9/114 Datenschutzorganisation

4. Datenschutzorganisation

Die Serverinfrastruktur von Digitalcourage e.V. ist ausschließlich für die Mitglieder des Admin-Teams von Digitalcourage e.V. zugänglich. Alle IT-Administratoren sind angemessen geschult für die verantwortliche Wahrnehmung ihrer Aufgaben und auf Vertraulichkeit und Fernmeldegeheimnis verpflichtet. Es bestehen Regelungen zur Aufgabenverteilung sowie zur Vertretungsregelung.

5. Auftragskontrolle

Durch die Auftragskontrolle wird gewährleistet, dass personenbezogene Daten die im Auftrag verarbeitet werden nur entsprechend der Weisungen des Auftraggebers verarbeitet werden können. Für alle Fremdaufträge liegen Verträge zur Auftragsverarbeitung (AVV) vor.

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

Es bestehen Verfahrensregelungen zu folgenden Aspekten:

- Informationssicherheitsmanagement
- Prozess zur Evaluation der Technischen und Organisatorischen Maßnahmen
- Sicherheitsvorfall-Management
- Durchführung von technischen Überprüfungen
- Durchführung von Softwareaktualisierungen