02/2025

Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO

zwischen

easyfeedback GmbH
Ernst-Abbe-Straße 4
56070 Koblenz, Deutschland

= Auftragsverarbeiter

und dem/der

= Verantwortlicher

Präambel

Der Verantwortliche beauftragt den Auftragsverarbeiter, durch die Lieferung einer Befragungssoftware zur Durchführung von Online-Befragungen, mit der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten (nachfolgend „Auftragsverarbeiter-Daten genannt). Um die Rechte und Pflichten aus dem Auftragsverhältnis gemäß der gesetzlichen Verpflichtungen zu konkretisieren, schließen die Vertragsparteien folgende Vereinbarung:

Soweit der Auftragsverarbeiter im Rahmen seiner o.g. Tätigkeiten im Unternehmen des Verantwortlichen Zugriff auf personenbezogene Daten sowie sonstige vertrauliche Informationen oder Betriebsgeheimnisse des Verantwortlichen erhält, so haben er und seine eingesetzten Mitarbeiter diese Daten und Informationen strikt vertraulich zu behandeln.

Personenbezogene Daten sind Angaben jedweder Art zu einer bestimmten oder bestimmbaren natürlichen Person, gleichgültig ob Mitarbeiter oder Kunde bzw. Lieferant. Auch Daten ohne direkten Personenbezug (z. B. ohne Namensangabe) können personenbezogene Daten sein, wenn aus ihnen auf die zugehörigen Personen geschlossen werden kann (z. B. Personalnummer, PC-Benutzerkennung, Kfz-Kennzeichen).

Vertrauliche Informationen im Sinne dieser Erklärung sind alle mündlichen oder schriftlichen Informationen, Daten, Unterlagen, Materialien und Angaben, die der Auftragsverarbeiter direkt oder indirekt von dem Verantwortlichen zur Abwicklung des Auftrages erhält oder in die er im Rahmen seiner Tätigkeiten Einsicht erhält. Dies gilt insbesondere, wenn diese Unterlagen, Materialien oder Informationen als vertraulich gekennzeichnet sind oder deren Vertraulichkeit sich aus ihrem Gegenstand oder sonstigen Umständen ergibt.

Die nachfolgenden Datenschutz- und Datensicherheitsbestimmungen finden daher Anwendung auf alle Leistungen der Auftragsverarbeitung, die der Auftragsverarbeiter gegenüber dem Verantwortlichen erbringt und auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragsverarbeiters oder durch den Auftragsverarbeiter beauftragte Dritte mit personenbezogenen Daten des Verantwortlichen in Berührung kommen können.

§ 1 Gegenstand und Dauer des Auftrags

1) Der Gegenstand der Nutzung ergibt sich aus den vom Verantwortlichen bestellten Leistungen und ist in Anlage 1 „Konkretisierung der Auftragsverarbeitung“ zu dieser Vereinbarung niedergelegt.

2) Die Dauer dieser Vereinbarung tritt mit Unterzeichnung beider Parteien in Kraft. Sie endet mit der Beendigung der Erhebung, Verarbeitung und/oder Nutzung der Daten des Verantwortlichen, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen des Auftragsverarbeiter ergeben.

§ 2 Konkretisierung des Auftragsinhalts

1) Art und Zweck der vorgesehenen Verarbeitung von Daten Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragsverarbeiters sind in Anlage 1 beschrieben.
Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen,

wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2) Art der Daten
Die Kategorien der personenbezogenen Daten, wie sie vom Auftraggeber bei der Erstellung der Umfragen im konkreten Fall festgelegt werden:

☐ Adressdaten	☐ Kontaktdaten	☐ Vertragsdaten
☐ Bankverbindungsdaten	☐ Kontodaten	☐ Abrechnungsdaten
☐ Leistungsdaten	☐ Finanzdaten	☐ Angebotsdaten
☐ Gesprächshistorie	☐ Transaktionsdaten	☐ Auskünfte
☐ Mitarbeiterdaten	☐ Personalverwaltung	☐ Qualifikationsdaten
☐ Videoaufzeichnungen	☐ Gesundheitsdaten	

3) Kategorien betroffener Personen
Die Kategorien betroffener Personen, die vom Auftraggeber bei der Erstellung der Umfragen im konkreten Fall festgelegt werden:

☐ Mitarbeiter	☐ Ruheständler	☐ Auszubildende
☐ Praktikanten	☐ Frühere Mitarbeiter	☐ Bewerber
☐ Unterhaltsberechtigte	☐ Angehörige	☐ Kunden
☐ Interessenten	☐ Lieferanten/Dienstleister	☐ Berater
☐ Makler	☑ Vermittler	☐ Mieter
☐ Gesellschafter	☐ Geschädigte	☐ Zeugen
☐ Kontaktpersonen	☐ Pressevertreter	

§ 3 Technische und organisatorische Maßnahmen

1) Der Auftragsverarbeiter 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 Verantwortlichen zur Prüfung zu übergeben. Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

2) Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 2].

3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 4 Berichtigung, Einschränkung und Löschung von Daten

1) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Als Datenschutzbeauftragter ist beim Auftragsverarbeiter bestellt:

heyData GmbH
Schützenstraße 5
10117 Berlin

www.heydata.eu
datenschutz@heydata.eu

Datenschutzkoordinator & Ansprechpartner
Dennis Wegner, Geschäftsführer
E-mail: datenschutz@easy-feedback.de

Ein Wechsel des Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen

2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragsverarbeiter 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 Auftragsverarbeiter und jede dem

Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

3) Der Auftragsverarbeiter verpflichtet sich, die im Rahmen des Auftragsverhältnisses zur Verfügung gestellten oder erarbeiteten Unterlagen und Daten sowie ihm sonst bekannt gewordene Informationen vertraulich zu behandeln und nur im Rahmen der Tätigkeit für dieses Vertragsverhältnis zu nutzen. Diese Verpflichtung besteht auch nach Ende des Vertragsverhältnisses fort.

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

5) Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

6) Die unverzügliche Information des Verantwortlichen 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 Auftragsverarbeiter ermittelt.

7) Soweit der Verantwortliche 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

8) Der Auftragsverarbeiter 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.

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

10) Für den Fall, dass der Auftraggeber unter das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland fällt, unterwirft sich auch der Auftragsverarbeiter gemäß § 30 Absatz 5 Satz 3 Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz; veröffentlicht in ABl. EKD 2017, S. 353) der kirchlichen Datenschutzaufsicht. Die Unterwerfung erstreckt sich auf die Aufgaben und Befugnisse der kirchlichen Datenschutzaufsicht nach §§ 43, 44 EKD-Datenschutzgesetz. Fällt der Auftraggeber nicht unter ein kirchliches Datenschutzgesetz, kann diese Klausel ignoriert werden.

§ 6 Unterauftragsverhältnisse

1) Der Auftragsverarbeiter ist nicht berechtigt, bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten des Verantwortlichen Unterauftragnehmer einzubeziehen ohne die vorherige schriftliche Zustimmung des Verantwortlichen. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich über die beabsichtigte Beauftragung eines Subunternehmers informieren. Lehnt der Verantwortliche nicht innerhalb einer Frist von 14 Tagen nach Eingang der Benachrichtigung eine Unterbeauftragung schriftlich (auch per E-Mail) ab, gilt die Zustimmung zur Unterbeauftragung als erteilt.

2) 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 Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen oder Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

3) Der Verantwortliche stimmt der Beauftragung der nachfolgenden Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma, Rechtsform	Anschrift	Beschreibung von Art und Umfang der Beauftragung
Cronon GmbH	Otto-Ostrowski-Straße 7 10249 Berlin	Rechenzentrum: Datenspeicherung und Verarbeitung

Folgende Dienstleister kommen nur zum Einsatz bei der Nutzung der separaten „Chatumfragen“ und der „AI-Analyse im Result STUDIO“ und sind optional zu sehen:

sci-an GmbH	Bergheimer Straße 104 D-69115 Heidelberg	Bereitstellung der Technologie Chatumfragen inkl. Analyse der Ergebnisse mittels dem KI-Sprachmodell „OpenAI“ (folgend)

OpenAI OpCo, LLC	1960 Bryant Street, San Francisco, CA 94110	Bereitstellung künstlicher Intelligenz zur Analyse von Daten: Für die Analyse der Umfrageergebnisse wird das Sprachmodell der Firma „OpenAI“ in der Professional-Variante genutzt. Alle an die Firma OpenAi gelieferten Daten werden somit nicht für Trainingszwecke verwendet und nach 30 Tagen automatisch gelöscht. Die Daten werden nur für Abrechnungszwecke 30 Tage aufbewahrt. Jeder gesendete Datensatz steht für sich alleine und kann nicht mit anderen Daten/Teilnahmen in Verbindung gebracht werden. Folgende Daten werden für die AI-Analyse übermittelt: - Fragetitel, Antwortoptionen - Prozentualer Anteil der gewählten Antwortoption - Häufigkeitsverteilung der gewählten Antworten - ø-Werte - Freitextantworten Daten werden immer anonym an die Firma OpenAI gesendet. Ein Personenbezug zu einem Teilnehmer, zu dem Absender der Umfrage oder dem Unternehmen ist nicht möglich. Wenn ein Teilnehmer in einer Freitextantwort einen Namen nennt, wird dieser übermittelt – außer Sie anonymisieren die Freitextantwort vor der Übermittlung.

Die Auslagerung auf Unterauftragsverarbeiter oder der Wechsel des bestehenden Unterauftragsverarbeiters sind zulässig, soweit eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

4) Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

5) Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen gemäß Art. 45, 46 DSGVO sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

6) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragsverarbeiter aufzuerlegen

§ 7 Kontrollrechte des Verantwortlichen

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

2) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen 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 Auftragsverarbeiters erforderlich sind.

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

§ 8 Mitteilung bei Verstößen des Auftragsverarbeiters

1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) 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

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden

c) die Verpflichtung, dem Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

2) Für darüber hinausgehende Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht

auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen. In einem solchen Fall informiert der Auftragsverarbeiter den Verantwortlichen über das Entstehen von Kosten.

§ 9 Weisungsbefugnis des Verantwortlichen

1) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen verarbeiten. Der Verantwortliche entscheidet allein über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten. Eine Verarbeitung für andere Zwecke, insbesondere für eigene Zwecke des Auftragsverarbeiters, ist nicht zulässig.

2) Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mind. Textform).

3) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

§ 10 Löschung und Rückgabe von personenbezogenen Daten

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

3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

§ 11 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragsverabeiter, wird der Auftragsverarbeiter die betroffene Person an den Verantwortlichen verweisen, sofern eine Zuordnung an den Verantwortlichen nach Angaben der betroffenen Person möglich ist. Der Auftragsverarbeiter informiert den Verantwortlichen und leitet den Antrag der betroffenen Person unverzüglich weiter. Er unterstützt den Verantwortlichen weiterhin bei der Erfüllung seiner Pflichten nach Kapitel III DS-GVO im erforderlichen Umfang.

§ 12 Haftung und Schadenersatz

Der Verantwortliche und der Auftragsverarbeiter haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelungen.

§ 13 Besondere Sicherheitsbedingungen

Folgende Klauseln gelten nur dann und insoweit, falls im Rahmen der Auftragsverarbeitung:

- der Zutritt des Auftragsverarbeiters in den Räumen des Verantwortlichen erforderlich ist,
- eigene Systeme des Verantwortlichen genutzt werden oder
- Zugriffe auf das interne Netz des Verantwortlichen von außen stattfinden (z. B. Fernwartung).

1. Der Auftragsverarbeiter unterliegt in den Gebäude- und Grundstücksbereichen des Verantwortlichen den Kontrolleinrichtungen des Verantwortlichen (Zutritts-, Zugangs- und Zugriffskontrolle).
2. Für die Dauer der notwendigen Maßnahmen wird durch den Verantwortlichen ggf. ein verschlüsselter/zugriffsgeschützter Verbindungsaufbau frei geschaltet.
3. DV-Dienstleistungen, die außerhalb der Kontrolleinrichtungen des Verantwortlichen erbracht werden, protokolliert der Auftragsverarbeiter. Die Aufzeichnungen sind 2 Jahre zu Kontrollzwecken aufzubewahren und auf Verlangen vorzuzeigen.
4. Dem Auftragsverarbeiter ist es nicht gestattet, EDV-Geräte, die nicht vom Verantwortlichen zur Verfügung gestellt werden, ohne vorherige Genehmigung des Verantwortlichen an das interne Netz bzw. die Telekommunikationseinrichtungen des Verantwortlichen anzuschließen.

_____ , den: _____

_____

Unterschrift, Funktion im Betrieb des Verantwortlichen

Koblenz, Deutschland , den: _____

_____

Unterschrift, Funktion im Betrieb des Auftragsverarbeiter

Anlage 1: Konkretisierung der Auftragsverarbeitung

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 3: Vertraulichkeitsvereinbarung (NDA)

Anlage 1: Konkretisierung der Auftragsverarbeitung

Der Auftragsverarbeiter stellt über seine Website www.easy-feedback.de und www.easy-feedback.com eine onlinebasierte Befragungssoftware (Software as a Service) zur Verfügung, über diese online Befragungen durchgeführt und ausgewertet werden können.

Dem Verantwortlichen stehen unterschiedliche Leistungs-Tarife zur Auswahl, welche sich in der Anzahl Umfragen, Funktionen und Laufzeit unterscheiden. Die Leistungen der Tarife sind auf der Website von easyfeedback definiert.

Die Laufzeit der einzelnen Leistungs-Tarife und dieser Vereinbarung endet mit der Kündigung automatisch. Die Kündigung der Leistungs-Tarife kann je nach gewähltem Abrechnungszeitraum monatlich oder jährlich erfolgen.

Ergänzung zu § 2, Abs. 1 Umfang, Art und Zweck der Datenverarbeitung

Der Verantwortliche verwendet im folgenden Umfang und zum Zwecke des Feedbackmanagements die Befragungssoftware des Auftragsverarbeiter:

1. Anlegen, erstellen und Durchführen von Umfragen online Fragebögen, Formularen oder Informationsinhalten
2. Einladen von Teilnehmern
3. Auswerten und Herunterladen von Umfrageergebnissen

Anlage 2: Technische und organisatorische Maßnahmen

Kontrollziele und Beschreibung der technischen und organisatorischen Maßnahmen im Rechenzentrum der Cronon GmbH, nachfolgend**„Rechenzentrum“** , genannt, und der easyfeedback GmbH, nachfolgend **„easyfeedback“** genannt.

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

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
1. Zutrittskontrolle (Räume und Gebäude) Zielbeschreibung: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.	**Rechenzentrum:** - Empfangs- und Sicherheitsdienst - Individuelle, dokumentierte und rollenabhängige Zutrittsberechtigungen (Karten, Transponder und Schlüssel) - Mitarbeiter- und Besucherausweise - Besucher dürfen sich grundsätzlich nur in Begleitung eines Mitarbeiters im Gebäude aufhalten - Alarm- und Einbruchmeldeanlage - Büroräume sind außerhalb der Arbeitszeit verschlossen **easyfeedback:** - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude - Zutrittsregelung für betriebsfremde Mitarbeiter - Namensscharfe Dokumentierung der Schlüsselvergabe

2. Zugangskontrolle (IT-Systeme, Anwendungen) Zielbeschreibung: Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.	**Rechenzentrum:** - Formale Benutzer- und Berechtigungsverfahren - Login nur mit Benutzername, Passwort und wo erforderlich 2-Faktor-Authentifizierung - Systemisch forcierte Passwortrichtlinien - VPN bei Remotezugriff und durch vom Verantwortlichen verwaltete Geräte - Mobile Device Management - Mobile Datenträger sind verschlüsselt - Automatische Sperre von Desktops nach wenigen Minuten Inaktivität - Clean Desk-Policy **easyfeedback:** - Zuordnung von Benutzerrechten - Authentifikation mit Benutzername / Passwort / 2FA - Richtlinie Passwortverfahren inkl. Passwortlänge, Passwortwechsel - Protokollierung anhand von Log-Dateien - Stets aktuelle sichere kryptografische Verfahren (SSL, TLS mit SHA256 Hash AES-GCM) - Richtlinie kryptografische Maßnahmen - Bildschirmsperre mit Passwortschutz

3. Zugriffskontrolle (auf Daten) Zielbeschreibung: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.	**Rechenzentrum:** - Führen von Assetregistern und Ableitung von Maßnahmen anhand der Datenklassifikation - Nutzung kryptografischer Verfahren (z.B. Verschlüsselung) - Umsetzung von Berechtigungskonzepten nach dem Need-to-Know-Prinzip - Trennung von Anwendungs- und Administrationszugängen - Protokollierung von Zugriffsversuchen - Einrichtung von Administratorarbeitsplätzen - Minimale Anzahl an Administratoren - Nutzung von Dokumentenvernichtung **easyfeedback:** - Berechtigungskonzept mit differenzierten Berechtigungen - Stets aktuelle sichere kryptografische Verfahren (SSL, TLS mit SHA256 Hash AES-GCM) - Richtlinie kryptografische Maßnahmen - AES-256 Verschlüsselung der Daten in der Datenbank - Verwaltung der Rechte durch Systemadministrator - Anzahl der Administratoren auf das „Notwendigste“ reduziert (Need to know) - Richtlinie Passwortverfahren inkl. Passwortlänge, Passwortwechsel - Einsatz von Aktenvernichtern Sicherheitsstufe 5 - Richtlinie/Verbot zur privaten Nutzung von externen Datenträgern Alle befugten Personen, haben jeweils nur auf die für Sie relevanten Daten Zugriff und sind zur Einhaltung der datenschutzrechtlichen Gesetze und Regelungen verpflichtet und entsprechend geschult.
4. Trennungskontrolle (zweckbezogen) Zielbeschreibung: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing.	**Rechenzentrum:** - Trennung von Entwicklungs-, Test- und Produktivumgebung - Personenbezogene Daten dürfen nicht für Testzwecke verwendet werden - Mandantenfähigkeit / logische Trennung von Daten bei relevanten Anwendungen: Separate Datenbanken, Schema-Trennung in Datenbanken, Berechtigungskonzepte und/oder strukturierte Dateiablage **easyfeedback:** - Trennung von Datensätzen - Logische Mandantenfähigkeit (softwareseitig) - Erstellung eines Berechtigungskonzepts - Getrennte Test- und Produktionsumgebung

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

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
5. Weitergabekontrolle (von Daten) Zielbeschreibung: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.	**Rechenzentrum:** - Bereitstellung von Daten über verschlüsselte Verbindungen (z.B. SFTP) - Weitergabe von personenbezogenen Daten im Sinne des Need-to-Know / Need-to-Do Prinzips - Personenbezogene Daten werden nach ihrem Schutzbedarf klassifiziert, wobei vertrauliche Daten nur über sichere Kommunikationswege übertragen werden dürfen - Wo möglich wird E-Mailverschlüsselung eingesetzt - Wo möglich werden personenbezogene Daten nur in pseudonymisierter oder anonymisierter Form übermittelt - Dokumentation der Weitergabe von physischen Speichermedien - Weitergabe von Papierdokumenten mit personenbezogenen Daten in einem verschlossenen undurchsichtigen Umschlag **easyfeedback:** - SSL Verschlüsselung SHA256 (SSL 3.0 Fallback deaktiviert) der Datenübertragung auf Speichermedien - Richtlinie/Verbot zur privaten Nutzung von externen Datenträgern - Schulung der betroffenen Personen zur Einhaltung und Verpflichtung der datenschutzrechtlichen Gesetze

6. Eingabekontrolle (in Datenverarbeitungssysteme) Zielbeschreibung: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.	**Rechenzentrum:** - Technische Protokollierung der Eingabe, Änderung und Löschung von personenbezogenen Daten sowie Kontrolle der Protokolle - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen) - Rollenbasiertes Berechtigungskonzept (Lese-, Schreib-, und Löschrechte) - Protokollierung von administrativen Änderungen **easyfeedback:** - Protokollierung der Eingabe, Änderung und Löschung von Daten - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts - SSL SHA256 (SSL 3.0 Fallback deaktiviert) gesicherte Aufbewahrung der Log-Dateien

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

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
7. Verfügbarkeitskontrolle (von Daten) Zielbeschreibung: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; onsite/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO).	**Rechenzentrum:** - Einsatz von Hardware- und Softwarefirewalls - Intrusion Detection Systeme - Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag - Unterbrechungsfreie-Stromversorgung (USV) - Notfallhandbücher für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust - Durchführung von Wiederherstellungstests - Wo notwendig Nutzung redundanter Systeme (z.B. RAID) - Regelmäßiger Test von Datensicherungen - Externe Audits und Sicherheitstests **easyfeedback:** - Tägliches verschlüsseltes Backup rückwirkend für 14 Tage aktiviert - Notfallplan, Master Recovery - Brandmelder - Firewall/Virenschutz - Redundante EDV-Dienste

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

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
8. Auftragskontrolle Zielbeschreibung: Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Verantwortlichen, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.	**Rechenzentrum:** - Abschluss eines Vertrags zur Auftragsdatenverarbeitung (ADV) - Protokollierung der Auftragsausführung durch den Auftragsverarbeiter **easyfeedback:** - Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) - Schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag) - Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis nach §53 Bundesdatenschutzgesetz - Laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten - Nachweis eines Datenschutz Management Systems nach EU DS-GVO

Weitere Verfahren zur Auftragskontrolle:

Datenschutz Management

- Datenschutzbeauftragte und ein Informationssicherheitsbeauftragter sind benannt
- Etablierung einer Datenschutz- und Informationssicherheitsorganisation
- Alle Mitarbeiter sind auf die Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet und werden auf das Telekommunikationsgeheimnis hingewiesen
- Mitarbeiter sind im Umgang mit personenbezogenen Daten sensibilisiert
- Neue Mitarbeiter erhalten Informationsmaterial bezüglich dem Umgang mit personenbezogenen Daten
- Ein Verzeichnis von Verarbeitungstätigkeiten wird gepflegt und Datenschutzfolgenabschätzungen werden bei Bedarf durchgeführt
- Prozesse zur Wahrnehmung von Betroffenenrechten sind etabliert

Auftragskontrolle

- Daten die im Auftrag verarbeitet werden, werden nur nach Weisungen des Auftraggebers verarbeitet
- Auftragnehmer werden im Hinblick auf getroffene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten sorgfältig ausgewählt
- Weisungen zum Umgang mit personenbezogenen Daten werden in Textform dokumentiert
- Sofern erforderlich werden Auftragsverarbeitungsvereinbarungen bzw. geeignete Garantien zur Übermittlung von Daten an Drittländer geschlossen

Datenschutzfreundliche Voreinstellungen

- Es wird prozessual sichergestellt, dass Systeme und Produkte datenschutzfreundlich entwickelt werden
- Es werden nur diejenigen personenbezogenen Daten erhoben, die für den jeweiligen Zweck erforderlich sind

Incident-Response-Management

- Dokumentierter Prozess zur Erkennung, Meldung und Dokumentation von Datenschutzverletzungen unter Einbindung des Datenschutzbeauftragten
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen unter Einbindung des Informationssicherheitsbeauftragten

Anlage 3: Vertraulichkeitsvereinbarung (NDA)

Zur Geheimhaltung und zur Sicherung bzw. zum Schutz wichtiger und als geheimhaltungsbedürftig bzw. vertraulich gekennzeichneter Informationen (nachfolgend insgesamt als „Vertrauliche Informationen“ bezeichnet) vereinbaren der Verantwortliche und der Auftragsverarbeiter - zusammen nachfolgend „Partei“ bzw. „Parteien“ genannt - nachfolgende Vereinbarung:

1. Definitionen

"**Dritte**" sind verbundene Unternehmen einer Partei und die im Auftrag für eine Partei oder ihre verbundenen Unternehmen tätigen Berater.

"**Verbundene Unternehmen**" einer Partei sind gemäß § 15 AktG verbundene Unternehmen.

"**Vertrauliche Informationen**" sind

1.1) Sämtliche Unterlagen, Spezifikationen, Entwürfe, Pläne, Zeichnungen, Softwarematerialien, Daten, Muster oder Prototypen in schriftlicher, mündlicher oder elektronisch aufgezeichneter Form sowie

1.2) Unkörperliche Informationen wie Geschäftsidee oder Konzepte, die von einer Vertragspartei im Zusammenhang mit den oben erwähnten Gesprächen offenbart werden sowie

1.3) Die Tatsache, dass die Parteien Gespräche führen werden.

Die Pflicht zur Vertraulichkeit gilt unabhängig davon, ob die betreffende Information von der offenbarenden Partei ausdrücklich als vertraulich gekennzeichnet wurde oder nicht.

2. Geheimhaltung

Jede Partei verpflichtet sich, alle erhaltenen vertraulichen Informationen

2.1) ausschließlich für den in der Präambel genannten Zweck zu verwenden

2.2) nur denjenigen ihrer Mitarbeiter und Mitarbeitern von Dritten zugänglich zu machen, die die vertraulichen Informationen zu dem vorgesehenen Zweck benötigen, vorausgesetzt, diese Mitarbeiter sowie die jeweiligen Dritten sind schriftlich verpflichtet, die vertraulichen Informationen in einer dieser Vereinbarung mindestens gleichwertigen Weise zu behandeln und

2.3) geheim zu halten und dabei die gleiche Sorgfalt wie hinsichtlich eigener Informationen und Daten von ähnlicher Bedeutung anzuwenden, mindestens jedoch ein angemessenes Maß an Sorgfalt.

3. Ausnahmen

Die in Ziffer 2 dieser Vereinbarung enthaltenen Verpflichtungen gelten nicht für vertrauliche Informationen, die

3.1) der empfangenden Partei bereits vor deren Überlassung ohne Verpflichtung zur Geheimhaltung rechtmäßig bekannt waren

3.2) öffentlich zugänglich sind oder werden, ohne dass dies die empfangende Partei oder die Dritten, denen die vertraulichen Informationen von der empfangenden Partei zugänglich gemacht wurden, zu vertreten haben

3.3) der empfangenden Partei von einer dritten Person rechtmäßig und ohne Geheimhaltungsverpflichtung zugänglich gemacht werden, vorausgesetzt die dritte Person verletzt - nach Kenntnis der empfangenden Partei – beim Zugänglich machen der Informationen keine eigene Geheimhaltungsverpflichtung

3.4) von der empfangenden Partei unabhängig entwickelt worden sind oder

3.5) von der überlassenden Partei schriftlich freigegeben worden sind.

Die Beweislast für das Vorliegen obiger Ausnahmen trägt die Partei, die sich darauf beruft. Die empfangende Partei darf vertrauliche Informationen der überlassenden Partei offenbaren, soweit die empfangende Partei hierzu aufgrund einer behördlichen oder richterlichen Anordnung oder zwingender rechtlicher Vorschriften verpflichtet ist, vorausgesetzt, dass die empfangende Partei die überlassenden Partei darüber zwecks Wahrnehmung ihrer Rechte unverzüglich schriftlich informiert und dass die empfangende Partei das ihr Zumutbare unternimmt, um sicherzustellen, dass die vertraulichen Informationen vertraulich behandelt werden.

4. Ausschluss von Rechten & Haftung

4.1) Lizenzen oder sonstige Rechte, gleich welcher Art, werden durch diese Vereinbarung weder eingeräumt, noch ergibt sich hieraus eine entsprechende Pflicht, derartige Rechte einzuräumen. Die empfangende Partei ist nicht dazu berechtigt, mit den vertraulichen Informationen Patente oder andere gesetzliche Schutzrechte anzumelden. Die Überlassung der vertraulichen Informationen begründet für die empfangende Partei keine Vorbenutzungsrechte.

4.2) Die Zugänglichmachung der vertraulichen Informationen erfolgt unentgeltlich. Eine Gewährleistung oder Haftung hinsichtlich der Richtigkeit, Fehlerfreiheit, Freiheit von Schutzrechten dritter Personen, Vollständigkeit und/oder Verwendbarkeit der vertraulichen Informationen, wird - soweit gesetzlich zulässig - ausgeschlossen.

4.3) Für die unberechtigte Weitergabe oder Offenlegung von vertraulichen Informationen durch einen Dritten, dem die empfangende Partei vertrauliche Informationen zugänglich gemacht hat, haftet die empfangende Partei gegenüber der überlassenden Partei so, als handelte es sich um eigene Handlungen oder Unterlassungen der empfangenden Partei.

5. Laufzeit & Rückgabe

5.1) Diese Vereinbarung erlischt 5 Jahre nach Beendigung des Hauptvertrages und der Erhebung und Verarbeitung von Daten über den Auftragsverarbeiter. Die sich aus dieser Vereinbarung ergebenden Verpflichtungen bleiben jedoch für jede Partei für die Dauer von 4 Jahren nach Ende dieser Vereinbarung bestehen.

5.2) Empfangene vertrauliche Informationen sind auf Verlangen der überlassenden Partei nach Wahl der empfangenden Partei zurückzugeben oder zu vernichten. Hiervon ausgenommen sind routinemäßig angefertigte Sicherungskopien des elektronischen Datenverkehrs und Kopien, die einer weitergehenden Aufbewahrungspflicht nach zwingendem Recht unterliegen, vorausgesetzt, dass diese vertraulichen Informationen von der empfangenden Partei und Dritten gemäß der Bestimmung dieser Vereinbarung unbefristet geheim gehalten werden. Die Erfüllung der Verpflichtungen aus dieser Ziffer 5.2 sind der überlassenden Partei auf Wunsch schriftlich zu bestätigen.

6. Schlussbestimmungen

6.1) Auf alle sich aus oder aufgrund dieser Vereinbarung ergebenden Streitigkeiten findet ausschließlich deutsches Recht Anwendung. Ausschließlicher Gerichtsstand ist dabei der Sitz der easyfeedback GmbH in Koblenz

6.2) Diese Vereinbarung schließt keine Veränderungen in der Art und Anzahl der Mitarbeiter der Partei, welche die Informationen erhält, aus.

6.3) Durch diese Vereinbarung wird weder eine Teilhaber- schaft noch ein Joint Venture zwischen den Parteien begründet.

6.4) Keine der Parteien kann diese Vereinbarung oder einzelne Rechte oder Verpflichtungen aus dieser Vereinbarung ohne schriftliche Zustimmung der anderen Partei auf dritte Personen übertragen.

6.5) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Auf dieses Schriftformerfordernis kann nur schriftlich verzichtet werden.

6.6) Sofern eine Bestimmung dieser Vertraulichkeitsvereinbarung unwirksam wird oder undurchführbar werden sollte, so wird hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Das gleiche gilt, soweit die Vertraulichkeitsvereinbarung eine Regelungslücke enthält. Anstelle der unwirksamen oder undurchführbaren Bestimmung soll eine dem Vertragszweck und den wirtschaftlichen Interessen der Parteien entsprechende angemessene Regelung getroffen werden. Eine Regelungslücke kann nur durch eine Regelung ersetzt werden, die die Parteien getroffen hätten, wenn sie diese Regelungslücke von vornherein gekannt und bedacht hätten.