Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO

zwischen

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

= 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, Materialen 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. DS-GVOerfüllt sind.

2. Art der Daten
   Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

   ---

3. Kategorien betroffener Personen
   Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

   ---

§ 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 Herr René Rautenberg bestellt:

   ER Secure GmbH
   Mr. René Rautenberg
   Geschäftsführer

   In der Knackenau 4
   82031 Grünwald

   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.

§ 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 beabsichtige 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, Wartung und Benutzerservice oder die Entsorgung von Datenträgern 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
Strato AG Berlin	Pascalstraße 10 10587 Berlin	Rechenzentrum: Datenspeicherung und Verarbeitung
Zeusware GmbH	Fähenweg 5 12527 Berlin	Servermanagement: Pflege und Wartung der easyfeedback Server

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 hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

2. Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
   die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
   die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
   aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
   eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

§ 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.

    1. 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

    2. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden

    3. 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

    4. die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung

    5. die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

§ 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 betroffener 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, Germany , den: _____

_____

Unterschrift, Funktion im Betrieb des Auftragsverarbeiter

Anlage 1: Konkretisierung der Auftragsverarbeitung

Anlage 2: Technische und organisatorische Maßnahmen

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 Leistung-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 Feedbackmanagement die Befragungssoftware des Auftragsverarbeiter:

1. Anlegen, erstellen und Durchführen von Umfragen
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 Strato AG, 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:** - Festlegung von Sicherheitsbereichen - Realisierung eines wirksamen Zutrittsschutzes - Festlegung zutrittsberechtigter Personen - Protokollierung des Zutritts - Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus - Begleitung von Besuchern und Fremdpersonal - Überwachung der Räume außerhalb der Betriebszeiten **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:** - Festlegung des Schutzbedarfs - Festlegung befugter Personen - Zugangsschutz (Authentisierung) - Umsetzung sicherer Zugangsverfahren, starke Authentisierung oder einfache Authentisierung je nach Schutzbedarf - Protokollierung des Zugangs - Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk - Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen - Automatische oder manuelle Zugangssperre - Durchführung von Datenkryptierungen bei Laptops **easyfeedback:** - Zuordnung von Benutzerrechten - Authentifikation mit Benutzername / Passwort - Richtlinien für Kennwortvergabe: min. 8 Zeichen, min. 1 Großbuchstabe, min. 1 Sonderzeichen, min. 1 Zahl - Alle 90 Tage Passwortwechsel - Protokollierung anhand von Log-Datein - Stets aktuelle sichere kryptografische Verfahren (SSL, TLS mit SHA246 Hash AES-GCM) - 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:** - Berechtigungskonzepte - Umsetzung von Zugriffsbeschränkungen - Vergabe minimaler Berechtigungen - Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen - Vermeidung der Konzentration von Funktionen **easyfeedback:** - Berechtigungskonzept mit differenzierten Berechtigungen - Stets aktuelle sichere kryptografische Verfahren (SSL, TLS mit SHA246 Hash AES-GCM) - Verwaltung der Rechte durch Systemadministrator - Anzahl der Administratoren auf das „Notwendigste“ reduziert - Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel - Einsatz von Aktenvernichtern - 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:** - Vorhandensein von Richtlinien und Arbeitsanweisungen - Vorhandensein von Verfahrensdokumentation - Umsetzung von Regelungen zur Programmierung - Regelungen zur System- und Programmprüfung - Umsetzung eines Abstimm- und Kontrollsystems **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:** - Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen - Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland - Sichere Datenübertragung zwischen Server und Client - Risikominimierung durch Netzseparierung - Implementation von Sicherheitsgateways an den Netzübergabepunkten - Härtung der Backendsysteme - Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder - Umsetzung einer Maschine-Maschine-Authentisierung - Sichere Ablage von Daten, inkl. Backups - Prozess zur Sammlung und Entsorgung - Einführung datenschutzgerechter Lösch- und Zerstörungsverfahren - Führung von Löschprotokollen **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:** - Protokollierung der Eingaben - Dokumentation der Eingabeberechtigungen **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 gesicherte Aufbewahrung der Log-Dateien - Speicherung von Protokolldateien

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:** - Vorhandensein und Umsetzung eines Konzeptes zur Durchführung von regelmäßigen Datensicherungen - Vorhandensein und regelmäßige Prüfung von Notstromaggregaten und Überspannungsschutzeinrichtungen - Überwachung der Betriebsparameter von Rechenzentren - Vorhandensein eines Notfallkonzeptes - Regelungen zur Aufnahme eines Krisen bzw. Notfallmanagements **easyfeedback:** - tägliches Backup 14-tägig Rückwirkend - 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 >** ER Secure Management System
- **Incident-Response-Management (IT Störungsmanagement) >** Notfallplan
- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) (Privacy by design / Privacy by default) >** Berechtigungskonzept, Möglichkeit der Datenportabilität, Löschbarkeit von Daten, Protrollierung von Eingabe, Änderung, Löschung von Daten