

Vertrag zur Auftragsdatenverarbeitung

über die Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten
gemäß § 11 Bundesdatenschutzgesetz (BDSG)

zwischen

easyfeedback

Dennis Wegner

Ernst-Abbe-Straße 4

56070 Koblenz

= Auftragnehmer

verpflichtet sich gegenüber der

= Auftraggeber

Präambel

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

Soweit der Auftragnehmer im Rahmen seiner o.g. Tätigkeiten im Unternehmen des Auftraggebers Zugriff auf personenbezogene Daten sowie sonstige vertrauliche Informationen oder Betriebsgeheimnisse des Auftraggebers 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 bestimmbarer 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 Auftragnehmer direkt oder indirekt von dem Auftraggeber 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 Auftragsdatenverarbeitung i.S.d. § 11 Bundesdatenschutzgesetz (BDSG), die der Auftragnehmer gegenüber dem Auftraggeber erbringt und auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

§ 1 Gegenstand und Dauer des Auftrags

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

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

§ 2 Umfang, Art und Zweck der Datenverarbeitung, die Datenarten und der Kreis der Betroffenen

Der Auftragnehmer ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung (Anlage 1 „Konkretisierung des Auftrags“) zu verwenden. Dem Auftragnehmer ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemäßen Verarbeitung oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt. Dem Auftragnehmer ist nicht gestattet, personenbezogene Daten des Auftraggebers in Systeme Dritter einzuspielen. Auch nicht zu Testzwecken. Im Übrigen ist es dem Auftragnehmer nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Daten aus Adressbüchern und Verzeichnissen dürfen nur zur Kommunikation im Rahmen der Auftragserfüllung mit dem Auftraggeber verwendet werden. Eine anderweitige Nutzung und Übermittlung für eigene oder fremde Zwecke, einschl. Marketingzwecke, ist nicht gestattet.

Weitere Einzelheiten zu Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung sind unter Anlage 1 „Konkretisierung des Auftrags“ zu dieser Vereinbarung aufgeführt.

Die Art der personenbezogenen Daten sind unter Buchstabe B. der Anlage 1 aufgeführt. Der Kreis der Betroffenen ist unter den Buchstabe C. der Anlage 1 aufgeführt.

§ 3 Technische und organisatorische Maßnahmen

Die als Anlage 2 beigefügte Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG (Datenschutz- und Datensicherheitskonzept) werden Teil dieser Vereinbarung. Die hier festgelegten Maßnahmen müssen die personenbezogenen Daten vor der zufälligen oder unrechtmäßigen Zerstörung, vor dem zufälligen Verlust, der unberechtigten Änderung oder Weitergabe oder dem unberechtigten Zugang schützen. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2, S. 1 BDSG dem Auftraggeber zur Verfügung zu stellen.

§ 4 Berichtigung, Löschung und Sperrung von Daten

Der Auftragnehmer hat nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer diesen Antrag unverzüglich an den Auftraggeber weitergeben.

§ 5 Pflichten des Auftragnehmers gemäß § 11 Abs. 4 BDSG und vorzunehmende Kontrollen

Der Auftragnehmer wird zur Durchführung des Vertrages nur Mitarbeiter oder sonstige Erfüllungsgehilfen einzusetzen, die auf das Datengeheimnis nach § 5 BDSG verpflichtet und in geeigneter Weise mit den Anforderungen des Datenschutzes vertraut gemacht sind.

Ferner ist der Auftragnehmer verpflichtet, die einschlägigen Vorschriften zur Bestellung des Datenschutzbeauftragten gemäß §§ 4f, 4g BDSG zu erfüllen.

Der Auftragnehmer ist verpflichtet, technische und organisatorische Maßnahmen nach § 9 BDSG in einem angemessenen Verhältnis zum angestrebten Schutzzweck umzusetzen. Dabei hat er durch geeignete Kontrollen sicherzustellen, dass die im Auftrag zu verarbeitenden Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden, die übertragene Datenverarbeitung aufgabenbezogen getrennt von anderer Datenverarbeitung erfolgt und die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Er unterwirft sich eventuellen Kontrollmaßnahmen der Datenschutzaufsichtsbehörde und wird den Auftraggeber über eine eventuelle Kontrollmaßnahme unverzüglich informieren, wenn personenbezogene Daten des Auftraggebers betroffen sind.

§ 6 Unterauftragsverhältnisse

Der Auftragnehmer ist berechtigt weitere Unterauftragnehmer einzubeziehen, wenn folgende Voraussetzungen vorliegen:

1. Der Auftragnehmer wird alle mit diesem Vertrag übernommenen Verpflichtungen dem Unterauftragnehmer selbständig auferlegen. Der Unterauftrag ist schriftlich zu fixieren. Die allgemeinen Vorschriften hinsichtlich des Verhältnisses zwischen dem Auftragnehmer und dem Unterauftragnehmer bleiben unberührt.
2. Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem Unterauftragnehmer so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
3. Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des § 11 BDSG i.V.m. Nr. 6 der Anlage zu § 9 BDSG beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

Der Auftraggeber erteilt mit Abschluss dieser Vereinbarung und vorbehaltlich der Erfüllung der Verpflichtungen gegenüber dem Unterauftragnehmer dem Auftragnehmer die Erlaubnis, die im Rahmen dieser Vereinbarung die in Anlage 3 aufgeführten Unternehmen als Unterauftragnehmer zu betrauen.

§ 7 Kontrollrechte des Auftraggebers und Mitwirkungspflichten des Auftragnehmers

Der Auftragnehmer räumt dem Auftraggeber und dessen Bevollmächtigten bezüglich der getroffenen Datenschutz- und Datensicherungsmaßnahmen ein jederzeitiges Besichtigungs- und Kontrollrecht, grundsätzlich nach vorheriger Ankündigung, ein. Der Auftragnehmer ist verpflichtet, im Falle von Auskünften und Einsichtnahmen die erforderliche Unterstützung bereitzustellen.

Unabhängig davon wird der Auftragnehmer den Nachweis der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen gemäß § 9 BDSG durch ein regelmäßiges, alle 3 Jahre zu erneuerndes Testat z. B. von einer anerkannten Wirtschaftsprüfungsgesellschaft, Revision oder von seinem betrieblichen Datenschutzbeauftragten oder ein anderes den gesetzlichen Anforderungen genügendes Dokument (z. B. aktualisierte Beschreibung der umgesetzten technischen und organisatorischen Maßnahmen) erbringen.

§ 8 Mitzuteilende Verstöße des Auftragnehmers

Bei begründetem Verdacht der Verletzung von in dieser Vereinbarung festgelegten Datenschutz- und Datensicherheitsbestimmungen durch den Auftragnehmer selbst, Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte ist der Auftragnehmer verpflichtet, den Auftraggeber unverzüglich zu benachrichtigen. Das Gleiche gilt auch bei Verstößen gegen die allgemeinen Vorschriften zum Schutz personenbezogener Daten. Dies gilt insbesondere, wenn personenbezogene Daten des Auftraggebers betroffen sind.

§ 9 Umfang der Weisungsbefugnisse

Der Auftraggeber ist für die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz sowie die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer verantwortlich. Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung (Anlage 1 „Konkretisierung des Auftrags“) ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen.

Falls der Auftragnehmer eine Weisung, gleich aus welchen Gründen, nicht einhalten kann, verpflichtet er sich, den Auftraggeber unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenweitergabe auszusetzen und/oder vom Vertrag zurückzutreten.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per Email bestätigen. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen das BDSG oder eine andere Vorschrift über den Datenschutz verstößt.

§ 10 Löschung der Daten nach Beendigung des Auftrags

Der Auftragnehmer ist verpflichtet, die personenbezogenen Daten nach Abschluss der Arbeiten bzw. bei Beendigung/ Kündigung des Vertrages - nach den Vorgaben des Auftraggebers - vollständig datenschutzgerecht zu löschen (einschließlich der verfahrens- oder sicherheitstechnisch notwendigen Kopien) oder an den Auftraggeber zurückzugeben. Das gleiche gilt auch für Test- und Ausschussmaterial, das bis zur Löschung oder Rückgabe unter datenschutzgerechtem Verschluss zu halten ist. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

§ 11 Besondere Sicherheitsbedingungen

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

- der Zutritt des Auftragnehmers in den Räumen des Auftraggebers erforderlich ist,
 - eigene Systeme des Auftraggebers genutzt werden oder
 - Zugriffe auf das interne Netz des Auftraggebers von außen stattfinden (z. B. Fernwartung).
1. Der Auftragnehmer unterliegt in den Gebäude- und Grundstücksbereichen des Auftraggebers den Kontrolleinrichtungen des Auftraggebers (Zutritts-, Zugangs- und Zugriffskontrolle).
 2. Für die Dauer der notwendigen Maßnahmen wird durch den Auftraggeber ggf. ein verschlüsselter/ zugriffsgeschützter Verbindungsaufbau frei geschaltet.
 3. DV-Dienstleistungen, die außerhalb der Kontrolleinrichtungen des Auftraggebers erbracht werden, protokolliert der Auftragnehmer. Die Aufzeichnungen sind 2 Jahre zu Kontrollzwecken aufzubewahren und auf Verlangen vorzuzeigen.
 4. Dem Auftragnehmer ist es nicht gestattet, EDV-Geräte, die nicht vom Auftraggeber zur Verfügung gestellt werden, ohne vorherige Genehmigung des Auftraggebers an das interne Netz bzw. die Telekommunikations-einrichtungen des Auftraggebers anzuschließen.

_____, den _____

Unterschrift, Funktion im Betrieb des Auftraggebers

_____, den _____

Unterschrift, Funktion im Betrieb des Auftragnehmers

- Anlage 1:** Konkretisierung des Auftrags
A. Ergänzungen zu § 2 Umfang, Art und Zweck der Datenverarbeitung
B. Ausführung der Art der Daten gemäß § 2
C. Kreis der Betroffenen gemäß § 2

Anlage 2: Technische und organisatorische Maßnahmen gemäß § 3

Anlage 3: Bestehende Unterauftragsverhältnisse

Anlage 1: Konkretisierung des Auftrags

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

Dem Auftraggeber stehen 4 Umfrage-Pakete (Leistungspakete) zur Auswahl, welche sich in der Anzahl Umfragen, Funktionen und Laufzeit unterscheiden. Die Leistungen der Umfrage-Pakete sind auf der Website von easyfeedback definiert.

Die Laufzeit der einzelnen Umfrage-Pakete und dieser Vereinbarung endet automatisch nach 3, 6 oder 12 Monaten, wenn keine Verlängerung beauftragt wird.

A. Zu § 2 Ergänzung zu Umfang, Art und Zweck der Datenverarbeitung

Der Auftraggeber verwendet im folgenden Umfang und zum Zwecke des Feedbackmanagement die Befragungssoftware des Auftraggebers:

1. Anlegen, erstellen und durchführen von Umfragen
2. Einladen von Teilnehmern
3. Auswerten und herunterladen von Umfrageergebnissen

B. Zu § 2 Art der personenbezogenen Daten

(maßgebliche Datenarten sind angekreuzt)

- | | | |
|---|---|--|
| <input type="checkbox"/> Adressdaten | <input type="checkbox"/> Kontaktdaten | <input type="checkbox"/> Vertragsdaten |
| <input type="checkbox"/> Bankverbindungsdaten | <input type="checkbox"/> Kontodaten | <input type="checkbox"/> Abrechnungsdaten |
| <input type="checkbox"/> Leistungsdaten | <input type="checkbox"/> Finanzdaten | <input type="checkbox"/> Angebotsdaten |
| <input type="checkbox"/> Gesprächshistorie | <input type="checkbox"/> Transaktionsdaten | <input type="checkbox"/> Auskünfte |
| <input type="checkbox"/> Mitarbeiterdaten | <input type="checkbox"/> Personalverwaltung | <input type="checkbox"/> Qualifikationsdaten |
| <input type="checkbox"/> Videoaufzeichnungen | <input type="checkbox"/> Gesundheitsdaten | |

Andere sensitive Daten gemäß § 3 Abs. 9 BDSG:

Sonstige:

C. Zu § 2 Kreis der Betroffenen

- | | | |
|---|--|--|
| <input checked="" type="checkbox"/> Mitarbeiter | <input type="checkbox"/> Ruheständler | <input type="checkbox"/> Auszubildende |
| <input type="checkbox"/> Praktikanten | <input type="checkbox"/> Frühere Mitarbeiter | <input type="checkbox"/> Bewerber |
| <input type="checkbox"/> Unterhaltsberechtigte | <input type="checkbox"/> Angehörige | <input checked="" type="checkbox"/> Kunden |
| <input checked="" type="checkbox"/> Interessenten | <input type="checkbox"/> Lieferanten/Dienstleister | <input type="checkbox"/> Berater |
| <input type="checkbox"/> Makler | <input type="checkbox"/> Vermittler | <input type="checkbox"/> Mieter |
| <input type="checkbox"/> Gesellschafter | <input type="checkbox"/> Geschädigte | <input type="checkbox"/> Zeugen |
| <input type="checkbox"/> Kontaktpersonen | <input type="checkbox"/> Pressevertreter | |

Sonstige:

(maßgebliche Personengruppen sind angekreuzt)

Anlage 2: Datenschutz gemäß §9 BDSG

Kontrollziele gemäß Anlage §9 BDSG und Beschreibung der technischen und/oder organisatorischen Sicherungsmaßnahmen im Rechenzentrum der Strato AG, nachfolgend „Rechenzentrum“ genannt, und easyfeedback, Inh. Dennis Wegner, nachfolgend „easyfeedback“ genannt.

| Kontrollziele bezüglich Umgang mit personenbezogenen Daten | Maßnahmen |
|---|--|
| <p>1. Zutrittskontrolle (Räume und Gebäude)</p> <p>Zielbeschreibung: Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.</p> | <p>Rechenzentrum:</p> <ul style="list-style-type: none"> - 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 <p>easyfeedback:</p> <ul style="list-style-type: none"> - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude - Zutrittsregelung für betriebsfremde Mitarbeiter - Namensscharfe Dokumentierung der Schlüsselvergabe |
| <p>2. Zugangskontrolle (IT-Systeme, Anwendungen)</p> <p>Zielbeschreibung: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.</p> | <p>Rechenzentrum:</p> <ul style="list-style-type: none"> - 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 <p>easyfeedback:</p> <ul style="list-style-type: none"> - Richtlinien für Kennwortvergabe: min. 8 Zeichen, min. 1 Großbuchstabe, min. 1 Sonderzeichen, min. 1 Zahl - Alle 90 Tage Passwortwechsel - Protokollierung anhand von Log-Dateien - SSL-Verschlüsselung - Bildschirmsperre mit Passwortschutz |

| | |
|--|---|
| <p>3. Zugriffskontrolle (auf Daten)</p> <p>Zielbeschreibung: Es ist zu 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.</p> | <p>Rechenzentrum:</p> <ul style="list-style-type: none"> - Berechtigungskonzepte - Umsetzung von Zugriffsbeschränkungen - Vergabe minimaler Berechtigungen - Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen - Vermeidung der Konzentration von Funktionen <p>easyfeedback:</p> <ul style="list-style-type: none"> - Berechtigungskonzept mit differenzierten Berechtigungen - SSL-Verschlüsselungsverfahren SHA256 (SSL 3.0 Fallback deaktiviert) <p>Alle befugten Personen, haben jeweils nur auf die für Sie relevanten Daten Zugriff und sind gemäß BDSG zur Einhaltung der datenschutzrechtlichen Gesetze und Regelungen verpflichtet und entsprechend geschult.</p> |
| <p>4. Eingabekontrolle (in Datenverarbeitungssysteme)</p> <p>Zielbeschreibung: Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden.</p> | <p>Rechenzentrum:</p> <ul style="list-style-type: none"> - Protokollierung der Eingaben - Dokumentation der Eingabeberechtigungen <p>easyfeedback:</p> <ul style="list-style-type: none"> - Protokollierung anhand von Log-Dateien - SSL SHA256 (SSL 3.0 Fallback deaktiviert) gesicherte Aufbewahrung der Log-Dateien <p>Über Log-Dateien wird der Aufruf jeder einzelnen Seite (Kunden-Login, Control-Panel-Engine und Serveradministration) dokumentiert und kann anhand von Signaturen einer Person (User) zugeordnet werden.</p> |
| <p>5. Weitergabekontrolle (von Daten)</p> <p>Zielbeschreibung: Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports 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.</p> | <p>Rechenzentrum:</p> <ul style="list-style-type: none"> - 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 <p>easyfeedback:</p> <ul style="list-style-type: none"> - SSL Verschlüsselung SHA256 (SSL 3.0 Fallback deaktiviert) der Datenübertragung auf Speichermedien - Namensscharfe Dokumentation bei Übertragung der Speichermedien auf eine Person - Schulung der betroffenen Personen zur Einhaltung und Verpflichtung der datenschutzrechtlichen Gesetze |

| | |
|--|---|
| <p>6. Verfügbarkeitskontrolle (von Daten)</p> <p>Zielbeschreibung: Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.</p> | <p>Rechenzentrum:</p> <ul style="list-style-type: none"> - 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 <p>easyfeedback:</p> <ul style="list-style-type: none"> - tägliches Backup 14-tägig Rückwirkend - Notfallplan - Brandmelder - Firewall/Virenschutz |
| <p>7. Datentrennungskontrolle (zweckbezogen)</p> <p>Zielbeschreibung: Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.</p> | <p>Rechenzentrum:</p> <ul style="list-style-type: none"> - Vorhandensein von Richtlinien und Arbeitsanweisungen - Vorhandensein von Verfahrensdokumentation - Umsetzung von Regelungen zur Programmierung - Regelungen zur System- und Programmprüfung - Umsetzung eines Abstimm- und Kontrollsystems <p>easyfeedback:</p> <ul style="list-style-type: none"> - Logische Trennung von Datensätzen - Interne Mandantenfähigkeit - Getrennte Test- und Produktionsumgebung |
| <p>8. Auftragskontrolle</p> <p>Zielbeschreibung: Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.</p> | <p>Rechenzentrum:</p> <ul style="list-style-type: none"> - Abschluss eines Vertrags zur Auftragsdatenverarbeitung (ADV) - Protokollierung der Auftragsausführung durch den Auftragnehmer <p>easyfeedback:</p> <p>Personenbezogene Daten werden nur weisungsgebunden verarbeitet (s. §9). Sofern easyfeedback Subunternehmen mit Aufgaben betraut, gelten für diesen die gleichen Regelungen und Bestimmungen wie für easyfeedback selbst.</p> |

easyfeedback, Dennis Wegner · Ernst-Abbe-Str. 4, 56070 Koblenz, Germany · Tel.: +49 (0)261 960987 51 · kontakt@easy-feedback.de · www.easy-feedback.de

Datenschutzbeauftragter: ER Secure · ER Secure ist eine Marke der René Rautenberg GmbH · Rupert-Mayer-Straße 44 · 81369 München · Tel.: 089 - 552 94 87 0 · rene.rautenberg@er-secure.de · www.er-secure.de

Anlage 3: Bestehende Unterauftragsverhältnisse

Gemäß § 6, Abs. 4 dieser Vereinbarung stimmt der Auftraggeber der Beauftragung folgender Unterauftragsverhältnisse zu:

| 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 |
| | | |
| | | |
| | | |