

Auftragsverarbeitungsvertrag

Vertrag zur Auftragsverarbeitung
zwischen

Podigee UG
Am Walde 2
56249 Herschbach

als Auftragsverarbeiter (hier bezeichnet als „Podigee“ oder wir)
und
Klaus, Backhaus
als Verantwortlicher (hier bezeichnet als „Kunde“ oder du)

Vertrag generiert am 2018-04-25

Präambel

Wir sind ein Podcast-Hosting-Dienst. Wir bieten ein komplettes Rundum-sorglos-Paket für die Veröffentlichung und Verbreitung von Podcasts.

Du möchtest Podigee mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Damit wir diese Vorgaben einhalten, schließen wir mit dir den folgenden Vertrag:

1. Wichtige Begriffe

Damit du diesen Vertrag besser verstehst klären wir zunächst einmal die wichtigsten Begriffe:

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

D.h. jeder der Podigee und die zur Verfügung gestellten Leistungen nutzen möchte ist „Verantwortlicher“. Um die Leistungen von Podigee nutzen zu können, ist es erforderlich, dass personenbezogene Daten der Kunden von dir auf der Plattform von Podigee verarbeitet werden können.

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

Du entscheidest selbst, welche Leistungen du von Podigee im Einzelnen in Anspruch nehmen möchtest. Podigee verarbeitet dann in deinem Auftrag die Daten, um dir Analysen etc. zur Verfügung stellen zu können. [1] [2] Wenn du unseren Premium Dienst nutzt, verarbeiten wir u.a.

auch E-Mails von deinen Hörern, die für deinen Podcast Content bezahlen.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(5) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

2. Vertragsgegenstand

(1) Wir erbringen für dich Leistungen im Bereich Podcast Hosting auf der Grundlage unserer Allgemeinen Nutzungsbedingungen in der jeweils aktuellen Fassung. („Hauptvertrag“). Dabei erhalten wir Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung von dir.

Umfang und Zweck der Datenverarbeitung durch uns ergeben sich immer aus dem Hauptvertrag und den Leistungen, die du in Anspruch nimmst. Dem Kunden obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Um die datenschutzrechtlichen Rechte und Pflichten zwischen dir und uns zu regeln, wird dieser Auftragsverarbeitungsvertrag geschlossen und geht im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der wir, unsere Beschäftigten oder durch uns Beauftragte mit personenbezogenen Daten in Berührung kommen, die von dir stammen oder für dich erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages.

3. Weisungsrecht

(1) Podigee darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen in diesem Vertrag von dir erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. [3] [4] Werden wir durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilen wir dir diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen von dir werden durch diesen Vertrag festgelegt und können von dir danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Du bist zu jeder Zeit berechtigt, eine solche Weisung zu erteilen. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Bitte richte deine Anfragen an datenschutz@podigee.com oder privacy@podigee.com zu

richten.

(3) Du solltest bitte eventuelle Weisungen dokumentieren und speichern- wir werden dieses ebenfalls machen.

Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Sind wir der Ansicht, dass deine Weisung gegen datenschutzrechtliche Bestimmungen verstößt, werden wir dich darauf hinweisen.

Wir sind berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch dich bestätigt oder geändert wird.

Die Durchführung einer offensichtlich rechtswidrigen Weisung dürfen wir ablehnen.

4. Art der verarbeiteten Daten und Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhalten wir Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten. Diese Daten umfassen keine besonderen Kategorien personenbezogener Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist ebenfalls in Anlage 1 dargestellt.

5 Unsere Schutzmaßnahmen

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

(2) Wir gestalten unseren Verantwortungsbereich und unsere innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Wir treffen alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten von dir (Auftraggebers gem. Art. 32 DS-GVO) insbesondere mindestens die in Anlage 3 aufgeführten Maßnahmen der

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Trennungskontrolle
5. Eingabekontrolle
6. Verfügbarkeitskontrolle
7. Überprüfungs-kontrolle[5]

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt uns vorbehalten, wobei sichergestellt wird, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Unser Ansprechpartner für den Datenschutz ist Mateusz Sojka (datenschutz@podigee.com) Wir veröffentlichen die Kontaktdaten des Ansprechpartners für Datenschutz auf unserer Internetseite.

(4) Den bei uns beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Wir werden alle Personen, die von uns mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-

GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen werden so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und uns bestehen bleiben. Dir sind die Verpflichtungen auf Anfrage nachzuweisen.[6]

6. Unsere Informationspflichten

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch uns, bei uns im Rahmen des Auftrags beschäftigten Personen oder durch Dritte werden wir dich unverzüglich in Schrift- oder Textform informieren. Dasselbe gilt für Prüfungen von Podigee durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

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

(2) Wir treffen unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informieren dich hierüber.

(3) Wir sind darüber hinaus verpflichtet, dir jederzeit Auskünfte zu erteilen, soweit deine Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 werden wir dich zeitnah unterrichten.

(5) Wir führen ein Verzeichnis zu allen Kategorien von im Auftrag von dir durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält.

7. Kontrollrechte des Kunden

(1) Wir verpflichten uns, dir auf dessen schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen erforderlich sind.

(2) Auf Wunsch stellen wir dir ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(3) Auf Anfrage weisen wir dir die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf nach.

8 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 4 genannten Subunternehmer durchgeführt.

Wir sind im Rahmen unserer vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Wir setzen dich davon in Kenntnis.

Wir wählen jeden Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit aus. Wir

achten darauf, dass wir unsere Verpflichtungen dir gegenüber auch (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen können. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat Podigee sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Podigee wird dem Kunden auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn wir Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die wir für dich erbringen und Bewachungsdienste.

9. Anfragen und Rechte Betroffener

(1) Wir unterstützen dich nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung deiner Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber uns geltend, so reagiert wir nicht selbstständig, sondern verweisen den Betroffenen an dich und wartet dessen Weisungen ab.

10. Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, bist im Innenverhältnis zu uns alleine du gegenüber dem Betroffenen verantwortlich.

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

11. Beendigung des Hauptvertrags

(1) Wir werden dir nach Beendigung des Hauptvertrags oder jederzeit auf deine Anforderung alle Daten zurückgeben oder – auf deinen Wunsch hin, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen durch uns oder unsere Subunternehmer. Wir haben hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(2) Wir verpflichten uns, auch über das Ende des Hauptvertrags hinaus die im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie wir über personenbezogene Daten verfügen, die uns von dir zugeleitet wurden oder die wir für diesen erhoben haben.

12. Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen Textform.

Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

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

(3) Diese Vereinbarung unterliegt deutschem Recht unter Ausschluss des in Deutschland geltenden UN-Kaufrechts. Ausschließlicher Gerichtsstand ist Herschbach.

Anlagen

Anlage 1 – Beschreibung der Datenkategorien/ Beschreibung der Betroffenen/Betroffenengruppen

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3 – Genehmigte Subunternehmer

Anlage 1: Beschreibung der angebotenen Leistungen[7] [8] [9] [10] [11]

Standard & Business-Kunden

- Bereitstellung von Audio-Inhalten im RSS-Feed
- Bereitstellung von Audio- und Text-Inhalten auf einer Podcast-Webseite
- Sammlung und Auswertung von Statistiken mit geographischen Informationen
- Technischer Support und Beratung

Podigee-Premium

- Verkauf von Premium Inhalten
- Speichern von E-Mail-Adressen der Premium-Abonnenten (der Premium-Produzent kann E-Mail-Adressen von Premium-Hörern einsehen)
- Technischer Support für Podcast-Produzenten und Podcast-Hörer
- Zahlungsformular zum Verkauf von Premium-Inhalten
- Verwaltung von Benutzerkontos

Anlage 2 Datenkategorien und der gespeicherten Daten

1. Art der Daten (Datenkategorie):

- Personenstammdaten (Name, Vorname, Adresse)
- Kommunikationsdaten (E-Mail)
- Rechnungsdaten
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) Anonymisierte IP-Adressen um geographische Daten ermitteln zu können.

Zahlungsdaten werden beim Dienstleister extern und sicher gespeichert (PCI-konform).

2. Zweck der Datenverarbeitung

- Vertragsabwicklung zur Erfüllung der bei uns durch den Kunden gebuchten Leistungen –

siehe Beschreibung unter Anlage 1

- Anonymisierte IP-Adressen für Hörer-Statistiken

3. Betroffene Personen

- Kunden
- Podcast-Produzenten (Kontaktdaten, E-Mail, Rechnungsadresse)
- Podcast-Hörer (anonyme IP-Adressen)
- Zahlende Podcast-Hörer (anonyme IP-Adressen, Kontaktdaten, E-Mail, Rechnungsadresse)

Anlage 3: Technische und organisatorische Maßnahmen[12]

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Das Büro von Podigee befindet sich in einem Wohnhaus. Das Büro wird durch einen Beauftragten von Podigee während und außerhalb der Bürozeiten überwacht.

Der Zugang erfolgt über eine Klingelanlage. Es erfolgt eine Sichtkontrolle. Zugang zu den Büros haben nur die beiden Eigentümer, sowie der Beauftragte. Mit diesem besteht eine Vertraulichkeitsvereinbarung. Die mobile Hardware wird außerhalb der Geschäftszeiten in einem geschlossenem Raum aufbewahrt.[13]

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Die Berechtigungen zum Zugang zu Daten und Systemen werden ausschließlich durch die beiden Firmengründer Benjamin Zimmer und Mateusz Sojka erteilt. Die Erteilung erfolgt immer individuell und nach Bedarf.

Die Erteilung und der Entzug von Zugängen werden dokumentiert.

Einmal pro Quartal erfolgt eine Überprüfung, ob die Berechtigungen noch aktuell sind. Dazu werden verknüpfte Dienste analysiert und individuelle Berechtigungen hinterfragt.

Die Passwörter, die verwendet werden, haben folgende Mindestanforderungen:

50 Zeichen pro Passwort mind. 2 Zahlen und 2 Sonderzeichen (da wo es technisch möglich ist).

Alle Passwörter bei der Nutzung von Podigee müssen mindestens

8 Zeichen lang sein. Die Länge des Passworts wird hierbei technisch erzwungen (sowohl im

Client als auch in der Datenbank)

Auf der eingesetzten Hardware werden Festplattenverschlüsselungen eingesetzt. Die mobilen Endgeräten sind Secure Enclave gesichert.

Alle Datenträger werden mittels einer Festplattenverschlüsselung abgesichert.

Als Betriebssysteme werden nur sichere, wie MacOS und Linux eingesetzt.

Sämtliche Zugriffe auf die IT-Systeme von Podigee werden dokumentiert. Zudem werden Logins über SSH-Zertifikate eingesetzt.

Jeder externe Dienstleister wird individuell durch Podigee ausgesucht und auf DSGVO-Konformität geprüft. Es werden nur die wesentlichen Dienste eingesetzt.

3. Zugriffskontrolle

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

Berechtigungen werden individuell und pro Bereich / Tätigkeit vergeben.

Alle 6 Monate werden die Berechtigungen überprüft.

Beim Wechsel der Aufgabenzuständigkeit oder dem Ausscheiden aus dem Unternehmen, werden sämtliche Zugänge dieser Person gesperrt und gelöscht. Passwörter, die mit der betroffenen Person geteilt wurden, werden ebenfalls ersetzt.

Die Administratorenrechte werden sehr restriktiv vergeben. Die Firmeninhaber übernehmen die Vergabe höchstpersönlich.

Zugriffe auf Anwendungen und Daten werden durch Logging und Audits protokolliert.

Die Vernichtung nicht mehr genutzter Datenträger erfolgt durch das Ändern der Passwörter und anschließende physikalisch vernichten.

Es wird keinerlei Papier verwendet, so dass entsprechend auch keine Sicherheitsvorkehrungen getroffen werden müssten.

4. Trennungskontrolle

Um sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können verwendet Podigee verschiedene Tabellen in der Datenbank, und trennt die Abläufe mithilfe von dedizierten Backend-Modells.

Die Daten von unseren Kunden werden immer gesondert verarbeitet- ein Zugriff von einem Kunden auf den anderen ist ausgeschlossen. - Wie wird sichergestellt, dass Daten verschiedener Kunden getrennt von einander

Podigee setzt dafür Industriestandards ein. Es werden Sessions (Cookies) und Auth-Tokens

verwendet, die pro Kunde unterschiedlich sind.

Das Testsystem verwendet andere Zugriffsparameter und Zugriffsdaten als das Produktivsystem.

Bei der Sammlung von IP-Adressen für die Podcast-Analytics (die Statistiken von gehörten / abgespielten Inhalten) wird der Range der IP-Adressen auf /24 gesetzt. So wird aus der IP-Adresse „123.123.123.123“ (/32) die folgende Adresse „123.123.123.0“ (/24). Dies ermöglicht die Auswertung von geographischen Daten, ohne personenbezogene IP-Adressen zu sammeln.

5. Eingabekontrolle

Darunter sind alle Maßnahmen zu verstehen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Protokollierung dieser Art von Daten werden durch einen externen Dienstleister gespeichert.

\- Wie lange speichert ihr die Nachweise dieser Eingaben, Änderungen und Löschungen („Protokolle“)?

So lange, wie es der konkrete Dienstleister vorsieht.

Alleinigen Zugriff auf diese Protokolle haben Benjamin Zimmer und Mateusz Sojka.

Personenbezogene Daten zwischen Kunden und Podigee werden über einen privaten Kundenbereich in der eigenen Webapplikation übertragen.

Zahlungsmethoden werden wegen PCI-compliance nicht zu den Servern von Podigee übertragen, sondern direkt zum Zahlungsprovider.

Während der Übertragung erfolgt eine SSL / HTTPS Verschlüsselung.

Die Daten werden nach einem Lösungskonzept gelöscht.

6. Verfügbarkeits- und Belastbarkeitskontrolle

Sämtliche Daten werden über Cloud-Dienstleister angeboten. Es gelten dann deren technische und organisatorische Maßnahmen.

Das Datensicherungs- und Wiederherstellungskonzept richtet sich nach PGDump / PGRestore / AWS S3- Die Datensicherungen sind verschlüsselt und es gibt einen Notfallplan.

Die Datensicherungen erfolgen bei Hetzner (siehe Anlage 4 Subunternehmer).

Eine schnelle Datenwiederherstellung wird durch Point-in-time Recovery gewährleistet.

7. Überprüfungskontrolle

Wir bei Podigee übernehmen als Unternehmensleitung Verantwortung für Datenschutz und Informationssicherheit.

Unsere Beschäftigten werden zum Datenschutz regelmäßig geschult.

Es werden mit allen Beschäftigten Vertraulichkeitsvereinbarungen getroffen.

Ansprechpartner für den Datenschutz ist Mateusz Sojka.

Wir bei Podigee verwenden und speichern nur die wesentlichen Daten um unseren Dienst überhaupt zu ermöglichen.

Wir überwachen alle Prozesse um Datenschutzverstöße zu erkennen. Zudem halten wir uns durch unsere Rechtsanwältin auf dem aktuellsten Stand was das Datenschutzrecht angeht.

Anfragen von Betroffenen werden umgehend bearbeitet.

Ein Verzeichnis der Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO liegt vor. Um die datenschutzrechtlichen Vorgaben einzuhalten, haben wir ein Audit durchgeführt und alle irrelevanten Tracker- und Analysetools entfernt.

Anlage 4 – Genehmigte Subunternehmer

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer im Sinne der Nr. 8:

HelpScout, Inc,
131 Tremont Street
3rd Floor
Boston, MA 02111-1338
USA

(AV-Vetrag vorhanden)

Funktion: Kundenbetreuung und Ticketing-System für den Tech-Support

Stripe

Stripe Payments Europe, Ltd., a private limited company organized under the laws of Ireland with company number 513174 and offices at The One Building, 1 Grand Canal Street Lower, Dublin 2, Ireland

(AV-Vetrag vorhanden)

Funktion: Zahlungsdienstleister

Quaderno (Rechnungen)

Recrea Systems, SLU ('Recrea'), with company registration number B35635648 and headquartered at Fernando Guanarteme 111 - 35010 Las Palmas, Spain

(AV-Vetrag vorhanden)

Funktion: Rechnungen und Angebote

Google LLC

Google Ireland Limited

Gordon House, Barrow Street, Dublin, D04 E5W5, Dublin
Irland

Funktion: Datenspeicher für Rechnungen (Google Drive)

(AV-Vetrag vorhanden)

Slack Technologies Limited

One Park Place, Hatch Street, Dublin 2, Ireland

Funktion: Interne Kommunikation und Benachrichtigungsdienst (z.B beim Empfang von Support-Anfragen oder Registrierung von Neukunden)

(AV-Vetrag vorhanden)

Hetzner Online GmbH

Industriestr. 25

91710 Gunzenhausen

Deutschland

Funktion: Server-Infrastruktur und Backup-Datenspeicher

Es werden keine personenbezogenen Daten von Hetzner verarbeitet.