Vereinbarung zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO

zwischen

_____

_____

_____

_____

nachfolgend «**Auftraggeber**» genannt

und

enuvo GmbH
Seefeldstrasse 25
8008 Zürich
Schweiz

nachfolgend «**Auftragnehmer**» genannt

1. Gegenstand der Vereinbarung

Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

Wird die vertraglich vereinbarte Dienstleistung nicht in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht, darf die Verarbeitung in einem Drittstaat nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2. Dauer der Vereinbarung

Diese Vereinbarung wird auf unbestimmte Zeit geschlossen.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten Pflichten stellt einen schweren Verstoß dar.

3. Art und Zweck der Verarbeitung; Art der Daten und Kreis der Betroffenen

Der Auftragnehmer bietet dem Auftraggeber die Möglichkeit Online-Umfragen durchzuführen. Solche Umfragen können durch den Auftraggeber beliebig gestaltet werden. Die Fragen können frei formuliert werden und die Umfrageteilnehmer werden durch den Auftraggeber selbst bestimmt. Der Auftragnehmer stellt sicher, dass die Umfrage via Internet erreichbar ist und dass die Antworten von Umfrageteilnehmern sicher gespeichert werden. Der Auftragnehmer ermöglicht dann dem Auftraggeber die Umfrageresultate einzusehen und zu analysieren.

Der Auftraggeber hat die Möglichkeit, Umfragen zu beliebigen Themen durchzuführen. Dies können Mitarbeiterbefragungen, Kundenzufriedenheitsumfragen, Befragungen von Website-Besuchern, Marktforschungsumfragen, und viele mehr sein. Entsprechend vielfältig gestaltet sich die Art der Daten, die durch solche Befragungen gesammelt werden können. Generell sind es jedoch Antworten von Umfrageteilnehmern auf Fragen, die durch den Auftraggeber formuliert werden. Oft werden dabei auch personenbezogene Daten übermittelt, wie Name, E-Mail-Adresse, Postadresse, Telefonnummer, Beruf, Alter und sonstige Informationen, die es in Kombination mit anderen Daten ermöglichen können, eine natürliche Person zu identifizieren. Die Art der personenbezogenen Daten, die gesammelt werden, wird durch den Auftraggeber bestimmt.

Je nach Umfrageart können die Umfrageteilnehmer ganz unterschiedliche Personen sein, wie zum Beispiel Mitarbeitende, Kunden, Website-Besucher, oder auch zufällige Personen, die gewillt sind an der Umfrage teilzunehmen (beispielsweise im Rahmen einer Marktforschungsumfrage). Der Kreis der Betroffenen wird durch den Auftraggeber bestimmt.

4. Pflichten des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DSGVO ergriffen hat. Die entsprechenden Technischen und Organisatorischen Maßnahmen (TOM) sind als **Anlage 1** Bestandteil dieser Vereinbarung.

Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, in dessen Auftrag zu vernichten. Die Speicherung und Archivierung von Daten gemäß gesetzlicher Pflicht bleibt unberührt.

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

6. Mitteilungspflichten des Auftragnehmers bei Datenpannen und Verstößen

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern

Der Auftragnehmer kann Sub-Auftragsverarbeiter hinzuziehen. Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters rechtzeitig zu verständigen, so dass er allenfalls Einspruch erheben kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art. 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

Zurzeit sind für den Auftragnehmer diverse Subunternehmer mit der Verarbeitung von personenbezogenen Daten beauftragt. In **Anlage 1** kann eine vollständige Liste aller Subunternehmer eingesehen werden. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

8. Ort der Durchführung der Datenverarbeitung

Der Auftragnehmer weist darauf hin, dass die von ihm als Service zur Verfügung gestellte Software vollständig extern bei Amazon Web Service, Inc. (kurz «AWS») betrieben wird. Der Betrieb der Hard- und Software erfolgt in Rechenzentren dieses Unterauftragnehmers innerhalb der EU (Region Irland und/oder Frankfurt).

Der Auftragnehmer hat mit AWS eine separate Auftragsdatenverarbeitungsvereinbarung (ADV) geschlossen, namentlich «AWS DATA PROCESSING ADDENDUM», die den Standardvertragsklauseln (auch als Modellklauseln bezeichnet) entsprechen, welche von der Europäischen Kommission definiert und genehmigt wurden. Die Vereinbarung mit AWS stellt einen integralen Bestandteil der TOM des Auftragnehmers dar.

Weiterführende Informationen zu AWS und der Einhaltung von EU-Datenschutzrichtlinien können hier abgerufen werden: https://aws.amazon.com/de/compliance/eu-data-protection/

9. Sonstiges

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen dieser Vereinbarung hiervon nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmungen tritt eine Regelung, die dem wirtschaftlichen Zweck der unwirksamen oder undurchführbaren Bestimmungen so nahe wie möglich kommt. Gleiches gilt im Fall von Regelungslücken.

Etwaige Vereinbarungen über eine Auftragsverarbeitung, die zuvor zwischen den Parteien getroffen wurden, werden ab dem 25. Mai 2018 durch diese Vereinbarung ersetzt. Ansonsten tritt diese Vereinbarung per sofort in Kraft.

Mit nachfolgenden Unterschriften erkennen Auftraggeber und Auftragnehmer die Regelungen dieser Vereinbarung an:

Auftragnehmer

enuvo GmbH
Seefeldstrasse 25
8008 Zürich
Schweiz

Datenschutzbeauftragter:
Lionel Marbot
lionel.marbot@enuvo.ch

Ort und Datum

Zürich, 24.05.2018

Unterschrift

Lionel Marbot

Auftraggeber

Name der/des Verantwortlichen:

_____

Funktion der/des Verantwortlichen:

_____

Ort und Datum

_____

Unterschrift

_____

Anlage 1: Technische und Organisatorische Maßnahmen (TOM)

Technische und organisatorische Maßnahmen

Die enuvo GmbH (nachfolgend auch «Auftragnehmer», «wir», «uns», o.ä. genannt) ist die Betreiberin der Online-Befragungsplattform «Umfrage Online». Der Sitz des Unternehmens liegt in Zürich in der Schweiz. Dieser Standort enthält nur Büroräumlichkeiten, welche dem Support sowie der Weiterentwicklung der Plattform dienen.

Daten, die via den Auftragnehmer gesammelt werden (Teilnehmerantworten, etc.), werden ausschließlich in europäischen Rechenzentren (Irland und/oder Deutschland) von Amazon Web Services (AWS) gespeichert und verarbeitet. In Zürich werden Daten jeweils nur temporär, zur Erfüllung von Support-Anfragen des Auftraggebers, verarbeitet.

1. Pseudonymisierung und Verschlüsselung

Wir bieten Zugang zu unserer Software ausschließlich verschlüsselt über SSL an. Unverschlüsselte Aufrufe via http:// werden automatisch zu https:// weitergeleitet.

Jeglicher Datentransfer von unseren Rechenzentren zum Support-Team in Zürich erfolgt verschlüsselt via HTTPS (SSL). Dies ist dieselbe Verschlüsselung, die die Auftraggeber (Umfrageersteller) und deren Endkunden (Umfrageteilnehmer) für den Zugriff zu Umfrage Online verwenden.

Sämtliche Passwörter, wie auch Token (bspw. um das Passwort zurückzusetzen), die in der Datenbank gespeichert werden, sind sicher «gesalzen» und «gehashed» und somit für niemanden in Klartext lesbar, auch nicht für Systemadministratoren. Dieses Verfahren ist unumkehrbar.

Sämtliche Daten sind ausschließlich durch authentisierte und autorisierte Zugriffe erreichbar. Zudem sind alle Datenbanken inkl. Sicherungskopien (Backups) durch Port- und IP-Filter auf Netzwerk-Ebene geschützt. Bei Wartungsarbeiten an einer Datenbank durch den Auftragnehmer wird kurzzeitig die IP-Adresse des Auftragnehmers freigeschaltet. Der Zugang zur Datenbank ist dann für den Auftragnehmer möglich, jedoch immer noch nur nach erfolgreicher Authentisierung und Autorisierung. Dritte können die Datenbanken sowie Sicherungskopien nie über das Internet erreichen.

Die Netzwerk-Einstellungen für den Zugriff auf die Datenbanken können durch den designierten Systemadministrator angepasst werden. Dieser Administrations-Zugang zu AWS ist derzeit nur einer Person (Lionel Marbot, Inhaber) möglich. Der Zugang ist mit einer Zwei-Faktor-Authentifizierung geschützt.

Aufgrund des oben beschriebenen, hohen Sicherheitsniveaus wird derzeit auf eine übrige Verschlüsselung der Daten verzichtet.

Personenbezogene Daten, die durch den Auftraggeber gesammelt werden, sind nicht strukturiert, sondern können sich überall in Teilnehmerantworten wiederfinden. Aus diesem Grund ist eine Pseudonymisierung dieser Daten nicht möglich.

2. Gewährleistung der Vertraulichkeit

Büroräumlichkeiten für Kunden-Support und Software-Entwicklung, Zürich, Schweiz

Die Büroräumlichkeiten sind nur mit einem entsprechenden Schlüssel zugänglich. Jeder Mitarbeitende hat einen persönlichen Schlüssel, um zu seinem Arbeitsplatz zu gelangen. Relevant für die Arbeit ist der Zugriff auf Umfrage Online, welcher ausschließlich mit persönlichen Zugangsdaten (Benutzername und Passwort) möglich ist. Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist gestattet, sofern die Maßnahmen nach Art. 32 DS-GVO auch in diesem Fall sichergestellt sind.

Jeder Mitarbeitende muss sich bei Umfrage Online anmelden, um arbeiten zu können. Mitarbeitende haben dabei persönliche, nur ihnen selbst bekannte Zugangsdaten. Jedem Mitarbeitenden werden dem Tätigkeitsgebiet entsprechende Benutzerrechte zugeteilt. Alle Mitarbeitenden sind zudem angewiesen, auch beim kurzzeitigen Verlassen ihres Arbeitsplatzes, den Computer zu sperren.

Alle Computer sind passwortgeschützt, verfügen über sichere Anti-Viren-Software und stehen hinter einer Hardware-Firewall.

Es werden keine personenbezogenen Daten von Auftraggebern in Zürich gespeichert. Auch auf den Entwicklungs-Umgebungen wird nicht mit produktiven Daten gearbeitet.

Rechenzentren, Europa (Irland und Deutschland)

Die durch den Auftragnehmer als Service zur Verfügung gestellte Software wird vollständig extern bei Amazon Web Service, Inc. (kurz «AWS») betrieben. Der Betrieb der Hard- und Software erfolgt in einem Rechenzentrum dieses Unterauftragnehmers innerhalb der EU (Region Dublin und/oder Frankfurt). Die von Umfrage Online gesammelten Daten werden zu keinem Zeitpunkt außerhalb der EU gespeichert oder verarbeitet.

Für die Gewährleistung der Vertraulichkeit und für die DSGVO-Konformität von AWS als Unterauftragnehmer wird auf Absatz 8, Subunternehmern, verwiesen.

3. Gewährleistung der Integrität

Umfrage Online wird als SaaS – Software as a Service – betrieben. Alle Kundendaten werden auf derselben Infrastruktur gelagert und verarbeitet. Alle Kunden identifizieren sich gegenüber unserem Service mittels ihrer persönlichen Zugangsdaten. Durch die logische Mandantentrennung (softwareseitig) kann somit jeder Auftraggeber ausschließlich auf seinen eigenen Kundendaten zugreifen. Es ist nicht möglich, auf Daten anderer Kunden zuzugreifen.

Auf Seite des Auftragnehmers verfügen nur die für den Kunden-Support zuständigen Mitarbeitenden über das Recht zur Eingabe, Änderung und Löschung von Daten. Die Mitarbeitenden besitzen nur die Berechtigungen, welche Sie zur Ausübung Ihrer Tätigkeit benötigen. Dabei kommt der Grundsatz „so viel wie nötig, so wenig wie möglich“ zur Anwendung. Die Rechte werden ausschließlich durch den Systemadministrator verwaltet.

Die Mitarbeitenden sind vertraglich verpflichtet, sich an das Datengeheimnis sowie die Sorgfaltspflicht zu halten. Die Arbeitnehmer und deren Tätigkeiten werden dabei laufend überprüft.

Der Auftragnehmer bestätigt, dass er die gesetzlichen Vorgaben zum Datenschutz und zum Datengeheimnis jederzeit einhält und deren Einhaltung durch seine Mitarbeiter und Erfüllungsgehilfen ausbildet und regelmäßig kontrolliert.

4. Gewährleistung der Verfügbarkeit

AWS stellt weltweit diverse „Regionen“ zur Verfügung, in welchen deren Services genutzt werden können. Jede Region hat mindestens zwei, voneinander unabhängige Rechenzentren, auf denen man die Services ebenfalls aufteilen kann, zwecks erhöhter Ausfallsicherheit.

Wir nutzen für unsere Services die Region «Irland» und haben unsere Server und Datenbanken auf drei Rechenzentren in Irland repliziert. Somit wird gewährleistet, dass im unwahrscheinlichen Falle eines Systemausfalls innerhalb eines Rechenzentrums, automatisch auf eines der zwei weiteren Rechenzentren Rückgriff genommen wird. Dieses automatische «Fail-Over» Verfahren ermöglicht uns den Betrieb einer redundanten und hochverfügbaren Software.

Für unsere Datenbanken werden automatisch rollende Backups der letzten 35 Tage gemacht. Bei größeren Software-Updates erstellen wir zudem manuelle Backups, die nicht automatisch verfallen.

Sicherungskopien von Datenbanken werden allesamt in diesen europäischen Rechenzentren erstellt und aufbewahrt. Der Zugriff auf solche Sicherungskopien ist wie in Absatz 1, Pseudonymisierung und Verschlüsselung, für Dritte nicht möglich. In Zürich werden keine Sicherungskopien gespeichert.

5. Gewährleistung der Belastbarkeit der Systeme

Die Sicherheit von Kundendaten steht für den Auftragnehmer an oberster Stelle. Mitarbeitende werden laufend zu verschiedensten Themen der Datensicherheit weitergebildet und erhalten genügend Zeit und Ressourcen, um dieses Wissen in Ihrer Arbeit einfließen zu lassen. Dies betrifft nicht nur die technische Sicherheit der Software, sondern auch die Vermeidung von Social Engineering, wie z.B. Phishing-Versuche, etc.

Unsere Applikation wurde zudem einem ausgiebigem Penetration-Test durch Protect7 (www.protect7.com) unterzogen und Mängel wurden umgehend behoben. Im Falle einer grundlegenden Software-Erneuerung würden wir neue Tests durchführen lassen.

Die physikalische Belastbarkeit der Systeme in den Rechenzentren wir durch den Unterauftragnehmer AWS gewährleistet, siehe Absatz 8, Subunternehmern.

6. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Die in Absatz 4, Gewährleistung der Verfügbarkeit, beschriebenen Sicherungskopien unserer Datenbanken lassen sich auf jeden beliebigen Zeitpunkt zurücksetzen, innerhalb der letzten 35 Tage. Für den unwahrscheinlichen Fall eines Totalausfalls, der nicht durch die redundante IT-Infrastruktur automatisch gelöst wird, besteht ein internes Konzept, um mittels Sicherungskopien den Betrieb und Zugang zur Software und deren Daten wiederherzustellen.

7. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Im täglichen Betrieb unserer Software kommt es, wie mit jedem System, immer wieder zu natürlichen, kleineren Störungen. Dank unserer redundanten IT-Infrastruktur werden solche Störungen automatisch via Fail-Over mit null Ausfallzeit behoben («Zero Down-Time»). Jeder Vorfall stellt einen erfolgreichen Test unserer technischen Maßnahmen unter Realbedingungen dar.

Des Weiteren gibt es immer wieder Kunden (Arbeitgeber), die aus Versehen eigene Daten von unserem System löschen. Wir können diese Daten dann wiederherstellen, in dem wir eine Komplettwiederherstellung einer Sicherungskopie durchführen. Eine solche Wiederherstellung ist die gleiche, die notwendig wäre, um das gesamte System wiederherzustellen. Somit wird die Systemwiederherstellung regelmäßig überprüft und optimiert.

8. Subunternehmern

Der Auftragnehmer hat mit allen nachfolgenden Sub-Auftragsverarbeitern die erforderlichen Vereinbarungen im Sinne des Art. 28 Abs. 4 DSGVO abgeschlossen.

Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, WA 89109-5210, USA

Sämtliche personenbezogenen Daten werden in europäischen Rechenzentren unseres Unterauftragnehmers Amazon Web Services (AWS) gespeichert und verarbeitet.

enuvo hat mit AWS eine Vereinbarung zur Auftragsverarbeitung (ADV) geschlossen, namentlich «AWS DATA PROCESSING ADDENDUM», die den Standardvertragsklauseln (auch als Modellklauseln bezeichnet) entsprechen, welche von der Europäischen Kommission definiert und genehmigt wurden. Die Vereinbarung mit AWS stellt einen integralen Bestandteil dieser technischen und organisatorischen Maßnahmen dar. Aufgrund eines integrierten Geheimhaltungsabkommen kann diese Vereinbarung nicht durch Dritte eingesehen werden.

AWS ist DSGVO-konform und ist unter anderem ISO 27001, 27017 und 27018 zertifiziert. ISO 27018 ist ein Verhaltenskodex für den Schutz persönlicher Daten in der Cloud. Er basiert auf dem Informationssicherheitsstandard ISO 27002 und dient als Leitfaden für die Implementierung von ISO 27002-Steuerungen, die für personenbezogene Daten, anhand derer eine Person eindeutig identifiziert werden kann, in der öffentlichen Cloud gelten. Der Standard bietet zusätzliche Kontrollen und Richtlinien für die Schutzanfoderungen von personenbezogenen Daten, die von den aktuellen Kontrollen des ISO 27002 nicht berücksichtigt werden.

Durch die Einhaltung dieses Standards verfügt AWS über ein System von Steuerungsmechanismen, die sich speziell mit dem Datenschutz der Inhalte beschäftigen. Durch die Einhaltung dieses international anerkannten Leitfadens und ihre unabhängige Überprüfung zeigt AWS seine Verpflichtung zum Datenschutz der Kundeninhalte.

Weitere Information zu unserem Unterauftragnehmer und deren Zertifizierungen können hier abgerufen werden: https://aws.amazon.com/de/compliance/gdpr-center/

Hostpoint AG, Neue Jonastrasse 60, 8640 Rapperswil-Jona, Schweiz

Hostpoint ist ein Schweizer Hosting-Provider, den wir für kleinere Projekte und Webseiten nutzen. Dieses Hosting kann unter Umständen verwendet werden, um temporär Dateien zu hosten (bspw. für den Download), die personenbezogene Daten enthalten könnten.

Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Betreibt mit “G Suite” unsere E-Mail-Infrastruktur (Gmail), die wir nutzen um den Kundensupport zu gewährleisten und intern zu kommunizieren. Sollten Sie uns bspw. eine E-Mail senden, dann wird diese E-Mail von Gmail verarbeitet.

Der Versand von Umfrage-Einladungen, etc., wird jedoch nicht via Google verarbeitet, sondern via Amazon Web Services. Google verarbeitet keine Umfragedaten, ausser diese werden durch den Support via E-Mail versandt.

Trello, Inc., 55 Broadway, 25th Floor, New York, NY 10006, USA

Trello ist eine online Software, die wir für die interne Projektverwaltung nutzen. Wir nutzen diesen Service hauptsächlich im Zusammenhang mit der Weiterentwicklung unserer eigenen Software. Beim Erfassen von neuen Kundenanforderungen an unsere Software kann es sein, dass wir bspw. den Inhalt einer Kunden-E-Mail ebenfalls in Trello speichern.

Slack Technologies, Inc., 500 Howard Street, San Francisco, CA 94105, USA

Slack ist ein online Messenger, den wir für die interne Kommunikation nutzen. Es kann sein, dass wir im Rahmen unserer internen Kommunikation auf Kunden verweisen (bspw. anhand der Kunden-E-Mail-Adresse).