Auftragsverarbeitungsvertrag (AVV) gemäß Art 28 Abs 3 DSGVO

Diese Vereinbarung bildet eine Ergänzung bildet eine Ergänzung zu den AGBs vom _____ (nachfolgend "Hauptvertrag") und wird

zwischen

Kunde (nachfolgend "Verantwortlicher")

und

IDENTsmart GmbH (nachfolgend "Auftragsverarbeiter")

Carl-von-Ossietzky-Str. 3
83043 Bad Aibling
Deutschland

(beide Parteien gemeinsam nachfolgend "Vertragsparteien")

geschlossen.

Mit dem Abschluss dieser Vereinbarung gehen die Vertragsparteien ein Auftragsverarbeitungsverhältnis ein. In dieser Vereinbarung gelten die entsprechenden Begriffsdefinitionen der DSGVO (Datenschutz-Grundverordnung - Verordnung (EU) 2016/679). Wenn daher in diesem Vertragswerk etwa der Begriff „Daten“ verwendet wird, dann sind damit „personenbezogene Daten“ im Sinne der DSGVO gemeint. Falls sich diese Vereinbarung und der Hauptvertrag bezüglich der Verarbeitung von personenbezogenen Daten widersprechen, geht diese Vereinbarung im Zweifel dem Hauptvertrag vor.

§ 1: Vertragsgegenstand und Dauer des Vertrages

1.1.: Dieser Vertrag findet Anwendung auf all jene Verarbeitungen personenbezogener Daten, die sich aus dem Hauptvertrag zwischen den Vertragsparteien ergeben, sofern der Auftragsverarbeiter diese personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet.

1.2.: Der Auftragsverarbeitungsvertrag tritt ab dem Zeitpunkt der Unterfertigung durch beide Parteien in Kraft. Er gilt akzessorisch zum Hauptvertrag und bleibt jedenfalls für die Dauer der datenschutzrechtlich relevanten Leistungserbringung aus dem Hauptvertrag in Geltung. Bei vollständigem Wegfall des Hauptvertrages erlischt auch diese Vereinbarung automatisch. Es bedarf in diesem Fall keiner gesonderten Kündigung.

1.3.: Dieser Vertrag und somit das gesamte Auftragsverarbeitungsverhältnis kann von den Vertragsparteien zu jeder Zeit ohne Einhaltung einer Frist aufgekündigt werden, wenn die jeweils andere Partei schwerwiegend gegen diese Vereinbarung oder das einschlägige Datenschutzrecht verstößt.

Solch ein schwerwiegender Verstoß ist etwa dann gegeben, wenn der Auftragsverarbeiter die Pflichten, die sich aus dieser Vereinbarung und aus dem Art 28 DSGVO ergeben, nicht einhält. Weiters kann der Verantwortliche fristlos kündigen, wenn der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht befolgt, wenn der Auftragsverarbeiter die vertragsmäßig festgelegten Kontrollrechte des Verantwortlichen verweigert oder wenn der Auftragsverarbeiter zwingend notwendige oder vereinbarte Sicherheitsmaßnahmen unterlässt.

§ 2: Art und Zweck der Verarbeitung

2.1.: Die personenbezogenen Daten, die vom Verantwortlichen zur Verfügung gestellt werden, verarbeitet der Auftragsverarbeiter ausschließlich zur Erfüllung seiner vertraglichen Pflichten aus dem Hauptvertrag. Die Verarbeitung erfolgt daher aufgrund des Hauptvertrages, dieser Vereinbarung oder gemäß einer Weisung des Verantwortlichen. Dem Auftragsverarbeiter ist es untersagt personenbezogene Daten für eigene oder fremde Zwecke zu verarbeiten oder personenbezogene Daten, ohne vorherige schriftliche Weisung des Verantwortlichen an Dritte weiterzugeben. Die Duplizierung oder Kopie von personenbezogenen Daten durch den Auftragsverarbeiter ist nur so weit erlaubt, als diese im Vorhinein durch den Verantwortlichen genehmigt wurde oder diese für die Sicherstellung der ordnungsgemäßen Datenverarbeitung (Kopie zur Sicherung) oder zur Einhaltung gesetzlicher Pflichten (zB gesetzliche Aufbewahrungspflichten) unbedingt notwendig ist.

2.2.: Die konkreten Verarbeitungsarten (Art 4 Z 2 DSGVO) und Zwecke der Verarbeitung des Auftragsverarbeiters sind dem Hauptvertrag zu entnehmen.

§ 3: Art der personenbezogenen Daten, Kategorien betroffener Personen

Die durch den Auftragsverarbeiter verarbeiteten Arten personenbezogener Daten sowie die Kategorien der betroffenen Personen finden sich in Anhang 1. Der Anhang 1 stellt einen Teil dieser Vereinbarung dar.

§ 4: Rechte und Pflichten des Verantwortlichen

4.1.: Dem Verantwortlichen obliegt allein die Entscheidung über die Mittel und Zwecke der Verarbeitung von den von ihm zur Verfügung gestellten personenbezogenen Daten.

4.2.: Der Verantwortliche verpflichtet sich die EU-rechtlichen und nationalen Datenschutzbestimmungen sowie diese Vereinbarung einzuhalten. Er ist insbesondere dafür verantwortlich, die Rechtmäßigkeit der Verarbeitung personenbezogener Daten (Art 6 DSGVO) zu beurteilen und dass die Rechte der betroffenen Personen gemäß den Art 12 – 22 DSGVO gewahrt werden. Gleichzeitig obliegt die Entscheidung über die Beantwortung einer Anfrage einer betroffenen Person bezüglich ihrer Betroffenenrechte ausschließlich dem Verantwortlichen und die entsprechende Kommunikation erfolgt nur durch diesen.

4.3.: Der Verantwortliche ist berechtigt dem Auftragsverarbeiter Weisungen und Aufträge bezüglich Art und Umfang der Verarbeitung personenbezogener Daten zu erteilen.

Diese Aufträge und Weisungen sind durch den Verantwortlichen grundsätzlich auf eine dokumentierte und schriftliche oder elektronische Weise zu erteilen. Wenn Weisungen mündlich erteilt werden, sind diese schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Unter einer Weisung versteht dieses Vertragswerk eine Anordnung an den Auftragsverarbeiter bezüglich des Umgangs mit personenbezogenen Daten.

4.4.: Datenträger oder Datensätze, die der Verantwortliche dem Auftragsverarbeiter überlässt, verbleiben im Eigentum des Verantwortlichen. Der Verantwortliche ist jederzeit berechtigt dem Auftragsverarbeiter die Löschung, Berichtigung, Herausgabe, Anpassung oder Einschränkung der Datenverarbeitung anzuordnen.

4.5.: Der Verantwortliche meldet dem Auftragsverarbeiter unverzüglich Fehler und Auffälligkeiten, die ihm an Ergebnissen der Auftragsverarbeitung auffallen.

4.6.: Der Verantwortliche ist verpflichtet den Auftragsverarbeiter unverzüglich zu verständigen, wenn es zu einem Wechsel des Datenschutzbeauftragten kommt.

§ 5: Pflichten des Auftragsverarbeiters

5.1.: Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur aufgrund der dokumentierten Weisung des Verantwortlichen, sofern der Auftragsverarbeiter nicht durch das Recht der Union oder der Mitgliedstaaten hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2.: Der Auftragsverarbeiter ist verpflichtet personenbezogene Daten zu löschen, zu berichtigen, herauszugeben, anzupassen oder einzuschränken, wenn dies vom Verantwortlichen angeordnet wird.

5.3.: Der Auftragsverarbeiter hat zu gewährleisten, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.4.: Der Auftragsverarbeiter verpflichtet sich alle technischen und organisatorischen Maßnahmen (TOMs) im Sinne des Art 32 DSGVO, die für die Sicherheit der Verarbeitung von personenbezogenen Daten erforderlich sind, zu ergreifen. Die durch den Auftragsverarbeiter gesetzten TOMs sind im Anhang 2 näher beschrieben. Der Anhang 2 stellt einen Teil dieser Vereinbarung dar.

5.5.: Der Verantwortliche erklärt sich mit den im Anhang 3 gelisteten weiteren Auftragsverarbeitern (nachfolgend „Sub-Auftragsverarbeiter) einverstanden. Diese gelisteten Sub-Auftragsverarbeiter sind zur Erfüllung des Hauptvertrages erforderlich. Ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung nimmt der Auftragsverarbeiter keine weiteren Auftragsverarbeiter in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Sub-Auftragsverarbeiter zu informieren. Der Verantwortliche hat dann die Möglichkeit gegen die Änderung innerhalb einer angemessenen Frist Einspruch zu erheben.

5.6.: Mit beauftragten Sub-Auftragsverarbeitern wird durch den Auftragsverarbeiter eine vertragliche Vereinbarung geschlossen, die zumindest das gleiche Datenschutzniveau wie dieser Vertrag zwischen dem Verantwortlichen und Auftragsverarbeiter gewährleistet. Dabei werden alle gesetzlichen und vertraglichen Vorgaben berücksichtigt, insbesondere die technischen und organisatorischen Maßnahmen gemäß Art 32 DSGVO.

5.7.: Verstößt ein Sub-Auftragsverarbeiter gegen seine datenschutzrechtlichen Pflichten, haftet der Auftragsverarbeiter dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters. Der Verantwortliche kann im Falle eines Verstoßes gegen datenschutzrechtliche Pflichten durch den Sub-Auftragsverarbeiter den Auftragsverarbeiter anweisen die Beschäftigung des Sub-Auftragsverarbeiters ganz oder teilweise zu beenden.

5.8.: Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit, damit dieser die Rechte der betroffenen Person nach Kapitel III der DSGVO innerhalb der gesetzlichen Fristen erfüllen kann. Dafür ergreift der Auftragsverarbeiter technische und organisatorische Maßnahmen. Wird ein Antrag irrtümlicherweise an den Auftragsverarbeiter gestellt und ist es ersichtlich, dass er eigentlich an den Verantwortlichen gestellt werden hätte sollen, so leitet der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiter und benachrichtigt diesen auch.

5.9.: Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der in 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-Folgenabschätzung, vorherige Konsultation der Aufsichtsbehörde).

5.10.: Der Auftragsverarbeiter verpflichtet sich nach Erbringung der Verarbeitungsleistungen oder davor nach Anordnung des Verantwortlichen, spätestens mit Beendigung des Hauptvertrages alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben und vorhandene Kopien zu löschen.

Der Auftragsverarbeiter ist berechtigt Dokumentationen, unter Berücksichtigung der einschlägigen Aufbewahrungsfristen, für den Nachweis der auftrags- und ordnungsgemäßen Datenvereinbarung auch nach Beendigung des Vertragsverhältnisses aufzubewahren.

5.11.: Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche selbst oder durch Dritte Überprüfungen und Inspektionen bezüglich der Einhaltung der Vorschriften über Datenschutz und Datensicherheit beim Auftragsverarbeiter durchführt. Der Auftragsverarbeiter stellt alle dafür erforderlichen Informationen zur Verfügung und wirkt unterstützend mit. Der Verantwortliche hat für diese Überprüfungen und Inspektionen grundsätzlich einen Termin zu vereinbaren. Der Verantwortliche darf seine Kontrollrechte nur in einem angemessenen und erforderlichen Umfang ausüben.

5.12.: Der Auftragsverarbeiter informiert den Verantwortlichen umgehend, wenn es zu schwerwiegenden Störungen des Betriebsablaufes kommt, wenn er der Ansicht ist, dass eine Weisung gegen gesetzliche Datenschutzbestimmungen verstößt, es zu Verstößen durch Mitarbeiter oder Sub-Auftragsverarbeiter kommt oder wenn sich Unregelmäßigkeiten im Zuge der Verarbeitung der Daten des Verantwortlichen ergeben. Der Auftragsverarbeiter kann die Durchführung von Weisungen, die gegen gesetzliche Datenschutzbestimmungen verstoßen, aussetzen, bis sie durch den Verantwortlichen bestätigt oder abgeändert wurden.

§ 6: Vertraulichkeit

Die Vertragsparteien verpflichten sich, alle Kenntnisse von betriebsinternen Geheimnissen oder datenschutzrechtlicher Sicherheitsmaßnahmen der jeweils anderen Vertragspartei vertraulich zu behandeln und nicht an Dritte weiterzugeben. Diese Verpflichtung gilt auch nach Beendigung des Vertrages weiterhin.

§ 7: Schriftlichkeit bei Änderungen

Jegliche Änderungen oder Ergänzungen dieser Vereinbarung bedürfen für Ihre Wirksamkeit der Schriftform. Dies gilt auch für Änderungen dieser Schriftformklausel.

§ 8: Haftung

Etwaige im Hauptvertrag geregelten Haftungsprivilegierungen finden auf diese Vereinbarung keine Anwendung. Für nachteilige Folgen von Verletzungen datenschutzrechtlicher Pflichten im Rahmen des vertraglich und gesetzlich bestimmten eigenen Verantwortungsbereichs haftet jede Vertragspartei im Innenverhältnis allein und uneingeschränkt. In diesem Zusammenhang verpflichten sich sowohl der Verantwortliche als auch der Auftragsverarbeiter den jeweils anderen bei einer Inanspruchnahme durch Dritte vollumfänglich schad- und klaglos zu halten.

Davon sind insbesondere auch behördliche Geldbußen umfasst, die über eine Vertragspartei aufgrund des der anderen Vertragspartei zuzurechnenden Verhaltens verhängt wurden.

§ 9: Rechtswahl und Gerichtsstand

Diese Vereinbarung unterliegt deutschem Recht sowie dem sachlich relevanten Unionsrecht, insbesondere der DSGVO. Ausschließlicher Gerichtsstand ist der Sitz des Auftragsverarbeiters.

§ 10: Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages undurchführbar oder unwirksam sein, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt.

.....
Datum, Ort (Auftragsverarbeiter)

.....
Unterschrift (Auftragsverarbeiter)

.....
Vorname, Nachname, Funktion (Auftragsverarbeiter)

Anhang 1: Datenverarbeitungsspezifikationen

Begriffserklärungen zur Art der Datenverarbeitung

	Beschreibung zur Datenverarbeitung
Benutzerkonten	Anmeldedaten, Passwörter, Nutzername
Persönliche Identifikationsdaten	Name, Titel, (private und berufliche) Adresse, frühere Adressen, (private, berufliche) Telefonnummer, von der für die Verarbeitung verantwortliche Person zugeteilte Kennnummern.
Keine personenbezogenen Daten	
Zahlungsdaten	Höhe, Datum...
Finanzgeschäfte	Von der betroffenen Person geschuldete und gezahlte Beträge, eingeräumter Kredit, Bürgschaften, Zahlungsmethoden, Überblick über die Zahlungen, Einlagen und andere Garantien.
Finanzidentifikationsdaten	Bankidentifikation und Bankkontonummer, Kredit- und Lastschriftkartennummern, Geheimcodes.
Anwesenheit und Disziplin	Überblick über die Anwesenheit, Motive für die Abwesenheit, Disziplinarmaßnahmen. Urlaub, Zeitausgleich, Krankenstand
Berufliche Tätigkeiten	Art der von der betroffenen Person genutzten bzw. gelieferten Tätigkeiten, Güter oder Dienstleistungen, Geschäftskontakte.

Bereich: 01 Zeiterfassung

Verarbeitung	01.01 Accounterstellung, Login und Loginverwaltung
Zweck der Verarbeitung	Sowohl die Accounterstellung, der Login als auch die Loginverwaltung von Benutzern werden über Auth0 abgehandelt.
Art der Datenverarbeitung	• Benutzerkonten • Persönliche Identifikationsdaten
Empfänger	• Auth0

Verarbeitung	01.02 Hosting
Zweck der Verarbeitung	Sowohl das Frontend als auch das Backend sind bei Google Cloud gespeichert. Die Server stehen dabei ausschließlich in Europa. Auch Backups werden in der Google Cloud gespeichert.
Art der Datenverarbeitung	• Keine personenbezogenen Daten
Empfänger	• Google Cloud EMEA Limited

Verarbeitung	01.03 Zahlungsabwicklung
Zweck der Verarbeitung	Für die Zahlungsabwicklung besteht die Möglichkeit eine Kreditkarte zu hinterlegen. Die Zahlungen werden dann über einen Zahlungsdienstleister abgewickelt.
Art der Datenverarbeitung	• Zahlungsdaten • Finanzgeschäfte • Finanzidentifikationsdaten
Empfänger	• Stripe, Inc.

Verarbeitung	01.04 Versand von Einladungslinks und Reports
Zweck der Verarbeitung	Einladungslink und Reports werden über einen
Art der Datenverarbeitung	• Persönliche Identifikationsdaten
Empfänger	• twilio sendgrid

Verarbeitung	01.05 Arbeitszeiterfassung

Zweck der Verarbeitung	Im Rahmen der Zeiterfassung müssen Mitarbeiter im ersten Schritt durch Benutzer des Systems angelegt werden. Verpflichtend sind dabei die Angabe des Vor- und Nachnamens, sowie der RFID Token Nummer. Angaben über Adresse, E-Mailadresse, Telefonnummer, Geburtsdatum sowie Personalnummer sind optional. Verarbeitet und gespeichert werden Arbeitszeiterfassungen, Überstunden, Krankmeldungen sowie Urlaubsanträge und -zeiten.
Art der Datenverarbeitung	• Anwesenheit und Disziplin • Persönliche Identifikationsdaten • Berufliche Tätigkeiten
Empfänger	-

Anhang 2: Technisch organisatorische Maßnahmen (Art 32 Abs 1 DSGVO)

Schutzart: 1.1.1 Vertraulichkeit: Zutrittskontrolle

Bezeichnung	Letztes Audit
1.1.1.04 Eingangstüren zu Unternehmensgebäuden oder Räumen sind durch eine genormte Schließanlage gesichert (Sicherheitsschlösser, Chipkarten, Transponder, Codeschloss)	08.03.2022
1.1.1.06 Die Vergabe, Verlust und Rückgabe von Schlüsseln, Transpondern, Chipkarten oder Codes an Personen wird dokumentiert	08.03.2022
1.1.1.07 Der Einsatz von Chipkarten, Transpondern oder die Verwendung von Zugangscodes wird protokolliert (zb. Zeitpunkt, Ort der Verwendung, Key)	08.03.2022
1.1.1.08 Es ist sichergestellt, dass Personen nur dort Zutritt erhalten, wo Sie für die Erfüllung Ihrer Aufgaben auch Zutritt benötigen	08.03.2022
1.1.1.14 Besucher oder Personal von Fremdfirmen werden von Mitarbeitern begleitet	08.03.2022
1.1.1.19 Lichtschranken oder Bewegungsmelder lösen die Außenbeleuchtung von Unternehmensgebäuden aus	08.03.2022

Schutzart: 1.1.2 Vertraulichkeit: Zutrittskontrolle (sensible Räume)

Bezeichnung	Letztes Audit
1.1..2.04 Personalakten werden in verschließbaren Aktenschränken aufbewahrt	08.03.2022
1.1.2.01 Personaldaten werden in gesonderten Räumlichkeiten verarbeitet (zb. Personalbüro)	08.03.2022
1.1.2.03 Die Eingangstür zu Räumen in denen Personaldaten verarbeitet werden,verfügen über einen automatischen Schließ- und Sperrmechanismus oder werden beim Verlassen versperrt	08.03.2022
1.1.2.05 Bildschirme auf denen Personaldaten verarbeitet werden sind von außen (Fenster) oder innen (Glastüre oder Glasfront) nicht einsehbar	08.03.2022

Schutzart: 1.2 Vertraulichkeit: Zugangskontrolle

Bezeichnung	Letztes Audit
1.2.02 Laptops oder Smart Devices (Ipad etc.) werden nach Dienstende versperrt aufbewahrt oder werden mit nach Hause genommen	08.03.2022

1.2.05 Die Anmeldung an einem Client erfolgt durch personenbezogene Benutzeraccounts (Benutzername und Passwort oder ähnliche Verfahren (Gesichtserkennung, Fingerprint etc.))	08.03.2022
1.2.06 Der Benutzer am Client Rechner hat keine Administrator Rechte bzw. für die tägliche Arbeit wird mit einem Benutzer ohne Administratorrechten gearbeitet	08.03.2022
1.2.09 Auf jedem Client Rechner ist eine Antiviren Software installiert, diese wird täglich bzw. bei einer Neuanmeldung aktualisiert	08.03.2022
1.2.11 Eingehende Mails werden online am Mail Server (Hoster) auf Spam geprüft	08.03.2022
1.2.14 Der Zugang zum internen Netzwerk (WLAN) ist mit einem eigenen Passwort gesichert	08.03.2022
1.2.15 Der Zugang zu Systemen (Server, Software) von außerhalb des Unternehmens erfolgt über verschlüsselte Verbindungen (VPN, Zugriff via Citrix)	08.03.2022

Schutzart: 1.3 Vertraulichkeit: Zugriffskontrolle

Bezeichnung	Letztes Audit
1.3.01 Die Anzahl der Administratoren für Server und zentrale Software ist auf das „Notwendigste“ reduziert	08.03.2022
1.3.05 Passwörter von Benutzern weisen eine ausreichende Komplexität auf (beinhalten Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern und weisen eine Mindestlänge von 8 Stellen auf)	08.03.2022
1.3.06 Die Verwaltung von Benutzerrechten für genutzte Software erfolgt zentral über festgelegte Systemadministratoren	08.03.2022
1.3.08 Jeder Benutzer erhält auf Basis des "need to know" Prinzip, nur die Zugriffsrechte (auf Daten, Systeme, Software, Dateiablagesysteme) die er für seine Tätigkeit auch zwingend benötigt	08.03.2022
1.3.09 Beim Ausscheiden eines Benutzers aus dem Unternehmen ist sichergestellt, dass seine Zugriffsberechtigungen umgehend entfernt und der Benutzer nach Ablauf einer gewissen Frist auch gelöscht wird.	08.03.2022
1.3.11 Fällt die Notwendigkeit eines oder mehrerer Zugriffsrechte bei einem Benutzer weg, dann werden ihm die Rechte auch zeitnah entzogen	08.03.2022

Schutzart: 1.4 Vertraulichkeit: Trennungsgebot

Bezeichnung	Letztes Audit

1.4.02 Bei Softwareapplikationen die personenbezogene Daten verarbeitet existiert eine Trennung in Test- und Produktivsystem	08.03.2022
1.4.03 Der Zugriff auf Daten in Datenbanken ist geregelt	08.03.2022
1.4.05 Softwareapplikationen und Dateiablagen auf die mehrere Benutzer Zugriff haben, sind mit einem Berechtigungssystem ausgestattet.	08.03.2022
1.4.06 Die Verarbeitung von personenbezogenen Daten erfolgt nur zu den festgelegten Zwecken	08.03.2022
1.4.07 Die Weitergabe von personenbezogenen Daten erfolgt nur zu den festgelegten Zwecken	08.03.2022

Schutzart: 1.6 Vertraulichkeit: Verschlüsselung

Bezeichnung	Letztes Audit
1.6.04 Zur Datenweitergabe werden verschlüsselte Verbindungen wie https (Webseite) oder sftp (FTP Server) genutzt	08.03.2022
1.6.06 Es wird die aktuellste Version des TLS Verschlüsselungsprotokolls verwendet	08.03.2022

Schutzart: 2.1 Integrität: 1. Eingabekontrolle

Bezeichnung	Letztes Audit
2.1.01 Dokumente oder Formulare in denen sensible Daten erhoben werden, werden aufbewahrt sofern diese automatisch weiterverarbeitet werden, um Datenfehlübernahmen korrigieren zu können.	08.03.2022
2.1.03 Die Eingabe, Änderung und Löschung von Daten durch individuelle Benutzer (nicht Benutzergruppen) kann nachvollzogen werden	08.03.2022

Schutzart: 2.2. Integrität: 2. Weitergabekontrolle

Bezeichnung	Letztes Audit
2.2.03 Auf Rechner wird mittels Fernwartung nur nach Zustimmung des Benutzers zugegriffen. Ausgenommen davon sind Update und Konfigurationsvorgänge am Rechner mit Hilfe automatischer Installationstools.	08.03.2022
2.2.05 Sonstige Datenträger (USB Sticks, mobile Festplatten, ausgebaute Festplatten) werden vor deren internen oder externen Weitergabe gelöscht, formatiert oder physisch zerstört	08.03.2022

2.2.06 Bei Druckern oder Faxgeräten werden deren interne Datenträger vor der externen Weitergabe gelöscht, formatiert, physisch zerstört oder nach Vorgaben des Herstellers gelöscht	08.03.2022

Schutzart: 3.1 Verfügbarkeit und Belastbarkeit: Verfügbarkeitskontrolle

Bezeichnung	Letztes Audit
3.1.01 Auf Clients und Servern werden Updates und Sicherheitspatches regelmäßig eingespielt	08.03.2022
3.1.06 Räumlichkeiten in denen personenbezogene Daten verarbeitet werden, sind mit einer Feuer- und Rauchmeldeanlage ausgestattet	08.03.2022
3.1.07 Räumlichkeiten in denen personenbezogene Daten verarbeitet werden, verfügen leicht erreichbar, über geeignete Löschmittel zur Brandbekämpfung (zB. Feuerlöscher)	08.03.2022
3.1.10 Über oder durch Räume in denen Server stehen, laufen keine Gas oder Wasser führenden Leitungen	08.03.2022

Schutzart: 4.1 Verfahren zur Überprüfung: Datenschutz-Management

Bezeichnung	Letztes Audit
4.1.01 Es wurde ein interner oder externer Datenschutz Beauftragter bestellt	08.03.2022
4.1.02 Es wird ein Verzeichnis der Verarbeitungstätigkeiten geführt und laufend aktualisiert	08.03.2022
4.1.03 Eine Audit/ Überprüfung der Wirksamkeit der technisch organisatorischen Maßnahmen findet jährlich statt	08.03.2022
4.1.04 Es existieren Abläufe zur Erfüllung der Rechte von betroffenen Personen	08.03.2022
4.1.05 Eine Datenschutz Management Software ist im Einsatz	08.03.2022
4.1.06 Die Informationspflichten (Datenschutzerklärung) werden regelmäßig geprüft	08.03.2022
4.1.07 Es existiert ein Löschkonzept in dem festgelegt ist, wann, welche Daten zu löschen sind. Die Löschung von Daten wird stichprobenartig oder regelmäßig überprüft.	08.03.2022
4.1.10 Alle Mitarbeiter sind auf Vertraulichkeit und Datengeheimnis verpflichtet	08.03.2022

Schutzart: 4.2 Verfahren zur Überprüfung: Incident-Response-Management

Bezeichnung	Letztes Audit

4.2.01 Fehlerhafte Login Versuche führen zu einer automatischen Sperre des Benutzer Logins. Die Sperre bleibt für einen definierten Zeitraum (siehe Passwort Richtlinie) bestehen.	08.03.2022
4.2.02 Ein Ablauf zur Meldung von Sicherheitsverletzungen an die Datenschutz Behörde und betroffene Personen existiert	08.03.2022
4.2.07 Verarbeitungen werden hinsichtlich einer Datenschutz Folgeabschätzung geprüft. Eine solche wird bei Bedarf auch durchgeführt und dokumentiert	08.03.2022

Anhang 3: Subunternehmen (weitere Auftragsverarbeiter)

Bezeichnung	Land	Übermittlung Drittland
Auth0	USA	Drittland
Google Cloud EMEA Limited	Irland	EU
Stripe, Inc.	USA	Drittland
twilio sendgrid	Irland	EU