DIVERA 24/7

Allgemeine Geschäftsbedingungen Datenschutz zur Auftragsverarbeitung

der

DIVERA GmbH, Vohwinkeler Str. 58, 42329 Wuppertal

-Auftragnehmer-

PRÄAMBEL

Dieser Vertrag beschreibt die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den Verträgen der Parteien ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit einem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

1. Anwendungsbereich und Verantwortlichkeit

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im jeweiligen Vertrag und ggf. in der Leistungsbeschreibung konkretisiert sind.

Gegenstand dieses Vertrages ist die Bereitstellung der SaaS Anwendung DIVERA 24/7, einer cloudbasierten Lösung zur Darstellung von Verfügbarkeiten von Rettungs- und Sicherheitskräften und deren Alarmierung im Einsatzfall.

Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus den Nutzungsbedingungen (https://www.divera247.com/nutzungsbedingungen.html).

Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

Die datenschutzrechtlichen Pflichten des Auftragnehmers sind durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

Die Art der zu verarbeitenden Daten und die Kategorien der betroffenen Personen ergeben sich aus den Leistungsbeschreibungen der jeweils vom Kunden beauftragten DIVERA 24/7-Leistungen sowie aus den ***Anhang 1***.

Die Laufzeit dieses AV-Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

Die Verarbeitung der Daten findet ausschließlich in einem Mitgliedsstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in einem Drittland mit einem in ***Anhang 4*** beschriebenen angemessenen Datenschutzniveau statt.

Der Auftragnehmer wird personenbezogene Daten nur mit vorheriger dokumentierter Zustimmung des Auftraggebers in ein anderes Drittland übermitteln und unter der weiteren Voraussetzung, dass der Auftragnehmer Maßnahmen zur Sicherung eines angemessenen Datenschutzniveaus gem. Art. 44 ff. DS-GVO ergriffen hat.

In diesem Fall wird der Auftragnehmer eine Dokumentation dieser Maßnahmen in Form einer überarbeiteten Version der Anhang 1 zur Unterschrift durch beide Parteien vorlegen.

2. Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

Weisungsempfänger beim Auftragnehmer sind:

- Geschäftsführung: Sébastien Thommes, info@divera.gmbh, 0202 25 13 98 39
- Der für den Auftrag verantwortliche Mitarbeiter des Auftragnehmers, erreichbar über dessen Kontaktdaten oder allgemein: support@divera247.com, 0202 25 13 10 91

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt

und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Die Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass ein angemessenes oder vertraglich vereinbartes Schutzniveau nicht unterschritten wird.

Eine Beschreibung der technisch-organisatorischen Maßnahmen des Auftragnehmers findet sich im ***Anhang 2*** an diese Bedingungen.

3. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten.

4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisungen zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

6. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter/als Ansprechpartner für den Datenschutz

Herr Dipl. Inform. Olaf Tenti

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

als externer Datenschutzbeauftragter

Körnerstr. 45

58095 Hagen

Tel.: +49 (0) 2331 / 356832-0

Fax: +49 (0) 2331 / 356832-1

E-Mail: info@gdi-mbh.eu

bestellt. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

7. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

8. Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle Unterlagen, Daten und Datenträger, die aus der Auftragsverarbeitung stammen, zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen oder vernichten. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Falls eine im ersten Satz beschriebene Verpflichtung zur Speicherung besteht, sind alle Unterlagen, Daten und Datenträger, die aus der Auftragsverarbeitung stammen und der Verpflichtung unterliegen, zurückzugeben, zu löschen oder zu vernichten, sobald diese Verpflichtung wegfällt. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

3. Pflichten des Auftraggebers

1.Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

2. Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt § 2 Abs. 10 entsprechend.

3. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

4. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

5. Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Bedingung niedergelegten Pflichten mit geeigneten Mitteln nach.

2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

6. Subunternehmer (weitere Auftragsverarbeiter)

1. Der Auftragnehmer bedient sich zur Erfüllung seiner vertraglichen Verpflichtungen der in ***Anhang 3*** genannten Subunternehmen.

2. Ein solches Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

3. Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber mit einer Frist von drei Wochen. Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben.

4. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

7. Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

2. Änderungen und Ergänzungen dieser Bedingungen und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrags zur Auftragsverarbeitung den Regelungen der AGB und der Nutzungsbedingungen vor. Sollten einzelne Teile dieser Bedingungen unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

3. Es gilt deutsches Recht.

Anhang 1: Umfang, Art und Zweck der Verarbeitung, die Art der zu verarbeitenden Daten und die Kategorien der betroffenen Personen

Umfang, Art und Zweck der Verarbeitung:

- Erfassung der Verfügbarkeit von Einsatzkräften mit Qualifikationen und zeitlicher Verfügbarkeit.
- Analyse und Darstellung der Verfügbarkeit in verschiedenen Ansichten.
- Versenden von Mitteilungen, Terminen und dringenden Benachrichtigungen an die Benutzer mittels Push-Diensten und der DIVERA 24/7 App, sowie mittels Sprachanruf oder SMS (vom Auftraggeber konfigurierbar).
- Statistische Auswertungen
- Technischer Kundendienst und Softwarewartung
- Aufbereitung und Bereitstellung der Daten für Drittsysteme (z. B. Einsatzleit- und Führungssysteme) (vom Auftraggeber konfigurierbar)

Art der zu verarbeitenden Daten und die Kategorien der betroffenen Personen:

Art der zu verarbeitenden Daten	Kategorien der betroffenen Personen
Personenstammdaten	Mitarbeiter/Einsatzkräfte
Kommunikationsdaten (z.B. Telefon, E-Mail)	Mitarbeiter/Einsatzkräfte
Vertragsstammdaten	Administrator der Einheit, Rechnungsempfänger
Planungs- und Steuerungsdaten	Mitarbeiter/Einsatzkräfte
Nutzungsdaten aus Telemediendiensten (z.B. von Webseiten, Apps für mobile Geräte)	Mitarbeiter/Einsatzkräfte
Protokolldaten von IT-Systemen (z.B. Zugriffsprotokolle)	Mitarbeiter/Einsatzkräfte
Daten zur Verfügbarkeit und Alarmauslösung im Einsatzfall	Mitarbeiter/Einsatzkräfte
Technischer Kundendienst / Support / Softwarepflege	Administrator der Einheit, Mitarbeiter/Einsatzkräfte

Anhang 2: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO:

Im Folgenden sind die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die die DIVERA GmbH mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität, Belastbarkeit und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Die DIVERA GmbH hat die Kernfunktionalitäten der SaaS Divera 24/7 und die damit verbundene Datenverarbeitung und -speicherung auf Server der Firma Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, ausgelagert. Die Server der DIVERA GmbH im Unternehmen dienen als reine Entwicklungs- und Testumgebungen.

Mit der Firma Hetzner Online GmbH hat die DIVERA GmbH einen Auftragsverarbeitungsvertrag geschlossen.

Die technischen und organisatorischen Maßnahmen der Firma Hetzner Online GmbH können Sie hier einsehen: https://www.hetzner.com/AV/TOM.pdf

Gleichwohl hat die DIVERA GmbH auch vor Ort technische und organisatorische Maßnahmen eingerichtet, die den Zugang zum Gebäude, die Büroräume und den Zugriff auf die Datenverarbeitungssysteme schützen.

Vertraulichkeit (Art. 32 Abs. 1b DSGVO)

Zutrittskontrolle:

(Kein unbefugter Zutritt zu Räumlichkeiten und Datenverarbeitungsanlagen)

- Die Zugangstüren zu den Büroräumen sind mit Token-Schloss gesichert.
- Die Tokens werden nur an berechtigte Personen ausgegeben.
- Im Falle des Verlustes eines Tokens wird dieser Verlust sofort gemeldet und der Token deaktiviert.

Zugangskontrolle:

(Verhinderung der unbefugten Benutzung der Datenverarbeitungssysteme)

- Zugang zu den Datenverarbeitungssystemen ist passwortgeschützt
- verwendete Passwörter müssen eine vorgegebene Mindestlänge haben
- automatische Sperren von Rechnern oder Benutzerkonten bei wiederholter Eingabe von falschen Zugangsdaten bis zur Freischaltung durch die Geschäftsführung

Zugriffskontrolle:

(Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen innerhalb des Datenverarbeitungssystems)

- alle Zugriffe können Personen eindeutig zugeordnet werden, z.B. keine Mehrbenutzerkonten

Trennungskontrolle:

- Entwicklungs-, Test- und Produktivsysteme sind getrennt. Auf den Entwicklungs- und Testsystemen der DIVERA GmbH werden keine personenbezogenen Daten des Auftraggebers verarbeitet.
- Die Mandantentrennung erfolgt logisch, bei DIVERA 24/7 SERVER zusätzlich physisch oder virtuell. Anhänge werden Mandantenspezifisch verschlüsselt.
- Die Datensicherung erfolgt auf physisch getrennten Systemen

Integrität (Art. 32 Abs. 1 b DSGVO)

Weitergabekontrolle:

(Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)

- Übertragung von personenbezogenen und vertraulichen Daten über sichere Verbindungen: Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung zur Verfügung gestellt
- Verschlüsselung nach Industriestandards bei der Übertragung von vertraulichen Daten über das Internet (z.B. sFTP, https, VPN) ist möglich, soweit dies nach der DS-GVO notwendig ist
- Nachvollziehbarkeit der Übertragung von personenbezogenen und vertraulichen Informationen ist gewährleistet

Eingabekontrolle und Protokollierung:

(Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind)

- Änderungen in den gespeicherten Datensätzen werden protokolliert, d. h. es ist nachvollziehbar, ob und von wem personenbezogenen Informationen hinzugefügt, geändert oder gelöscht wurden
- der Schutz der Log-Dateien vor unerlaubten Zugriff und Änderung ist gewährleistet

Auftragskontrolle:

- Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen
- Mitarbeiter sind vertraut mit den Verfahrensanweisungen Benutzerrichtlinien für die Datenverarbeitung im Auftrag auch im Hinblick auf das Weisungsrecht des Auftraggebers
- die verwendeten AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers
- alle Mitarbeiter sind i.S.d. Art. 32 Abs. 4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen
- Incident Response Management ist vorhanden
- die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers
- der Auftragnehmer hat einen externen Datenschutzbeauftragten bestellt
- der Datenschutzbeauftragte ist durch die betriebliche in die relevanten, betrieblichen Prozesse eingebunden

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 b DSGVO)

Verfügbarkeitskontrolle:

(Schutz der Datenverarbeitungssysteme gegen Zerstörung bzw. Verlust)

- für alle internen Systeme des Auftragnehmers ist eine Eskalationskette definiert, die vorgibt, wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen (rasche Wiederherstellbarkeit gemäß Art. 32 Abs. 1 lit. c DS-GVO)
- Back-up- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten
- eine ausreichend dimensionierte unterbrechungsfreie Stromversorgung ist gewährleistet (Einsatz unterbrechungsfreie Stromversorgung (USV), Netzersatzanlage)
- sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, Spamfilter)
- Monitoring aller relevanten Server
- Einsatz von Festplattenspiegelung bei allen relevanten Servern
- Einsatz von Software Firewall und Port-Reglementierungen

Belastbarkeitskontrolle:

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Belastbarkeit der Datenverarbeitungssysteme werden eingesetzt

- Prüfungen der eigenen IT
- Kontrollen des betrieblichen Datenschutzbeauftragten

- Datenwiederherstellungs-Tests werden durchgeführt

Wiederherstellbarkeit der Daten und des Datenzugangs nach physischem oder technischem Zwischenfall und Kontrollverfahren

Datensicherung (Art. 32 Abs. 1 lit. c DS-GVO)

Für die Datensicherung wird auf die technischen und organisatorischen Maßnahmen der Firma Hetzner Online GmbH verwiesen.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art.32 Abs. 1 lit. d DS-GVO

- Die vorhandenen Dokumentationen der Datensicherheit werden regelmäßig auf Aktualität geprüft
- Es erfolgt mindestens jährlich ein technischer Check der Datenverarbeitungssysteme
- Protokolle über alle Aktivitäten auf dem Datenverarbeitungssystem werden auf etwaige Unregelmäßigkeiten in regelmäßigen zeitlichen Abständen ausgewertet
- Sicherheitsvorfälle werden dokumentiert und ausgewertet
- Es erfolgen interne Audits durch den betrieblichen Datenschutzbeauftragten oder die IT
- Es erfolgen externe Audits durch zertifizierte Prüfer

Organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs-1 d DSGVO)

- Ein betrieblicher Datenschutzbeauftragter wurde bestellt (Extern)
- Der Datenschutzbeauftragte oder von ihm oder der Geschäftsleitung beauftragte Mitarbeiter führen regelmäßig interne Kontrollen der Einhaltung der technischen und organisatorischen Maßnahmen der Datensicherheit durch
- Alle Mitarbeiter, die personenbezogene Daten verarbeiten, sind auf Vertraulichkeit (das Datengeheimnis) verpflichtet
- Fremdpersonal ist ebenfalls auf Vertraulichkeit verpflichtet
- Datenschutzschulungen für die Mitarbeiter werden regelmäßig durchgeführt
- Die private Nutzung betrieblicher Kommunikationstechnik ist geregelt
- Es existiert ein dokumentiertes Datenschutzkonzept

Datenschutzfreundliche Voreinstellungen:

- Privacy by Default und Privacy by Design werden bei Softwareentwicklung berücksichtigt (Art. 25 Abs. 2 DS-GVO)

Anhang 3: Genehmigte Subunternehmer

Im Folgenden die Liste der Subunternehmer, welche Dienstleistungen für den Auftragnehmer erbringen.

Wenn nicht anders angeben haben die Unternehmen ihren Sitz in Deutschland. Mit * markierte Dienstleister sind durch den Auftraggeber zu- bzw. abschaltbar.

Über diese werden teils Kernfunktionalitäten bereitgestellt.

Subunternehmen	Zweck der Datenverarbeitung	Sitz	*
Apple Inc, Deutschland, Kurfürstendamm 26 · 10719 Berlin bzw. One Apple Park Way, Cupertino, CA 95014	Apple Push Notification Service (APNS): Alarmierungen/Mitteilungen/Termine per Push-Nachricht	DE, USA	
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland	Firebase Cloud Messaging (FCM): Alarmierungen/Mitteilungen/Termine per Push-Nachricht	IRL, USA	
Placetel von BroadSoft Germany GmbH, Lothringer Straße 56, 50677 Köln	Telefonanbieter für Kundendienst		
Ebuero AG, Hauptstr. 8 im Meisenbachhaus, 10827 Berlin	Dienstleister für „24/7 Störungshotline“		
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland	Google Cloud Platform: Geocoding, Reverse Geocoding, Autovervollständigung von Adressen (Per Default abgeschaltet)	IRL, USA	*
Hetzner Online GmbH, Sigmundstr. 135 · 90431 Nürnberg	Rechenzentrum		
SMSFLATRATE.NET von Kloppe Media GmbH, Ansbacher Str. 85, 91541 Rothenburg	Alarmierungen/Mitteilungen/Termine, Telefonnummern der Kunden über SMS/TTS Telekommunikationsdienste SMS/Fax/Sprachanrufe		*

Subunternehmen	Zweck der Datenverarbeitung	Sitz	*
ScopeVisio AG, Rheinwerkallee 3, 53227 Bonn	Buchhaltung und CRM		
Toplink GmbH, Robert-Bosch-Straße 20, 64293 Darmstadt	Telefonanbieter für „Statussetzen über Telefonanruf“-Funktion		*
MapBox, 740 15th St NW Floor 5, Washington, DC 20005, USA	Routenberechnung im Monitor für Bestimmung des Einsatzort/Koordinaten	USA	*

Anhang 4: Übermittlung von Daten in Drittländer

Auflistung aller Datenübermittlungen in Drittländer außerhalb der EU / des EWR einschließlich der jeweiligen Maßnahme zur Sicherung eines angemessenen Datenschutzniveaus:

Erläuterung zu Push-Diensten:

Je nach Endgerät werden bei der Verwendung von Push-Nachrichten die Dienste von Apple oder Google genutzt. Dabei werden nicht die vollständigen Daten übertragen, sondern nur die Titelbezeichnungen wie z.B. Alarmstichwort und Titel von Mitteilungen und Terminen. Je nach Konfiguration wird das Stichwort durch den Preset „ALARM“ ersetzt.

Eine Übertragung von Detailinformation wie Adresse, Zusatzinformationen etc. findet nicht statt.

Sofern der Kunde Push-Dienste auf Android Endgeräte nutzt, trifft Punkt 1 zu. Sofern der Kunde Push Dienste auf iOS-Endgeräten nutzt, trifft Punkt 2 zu. Wenn der Kunde keinen Push Dienst nutzt, werden diese Dienste nicht genutzt.

	Übermittlungsort der Daten	**Maßnahme zur Sicherung des angemessenen Datenschuzniveaus**
1.	USA (Firebase Cloud Messaging, Google Cloud)	☐ Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO) ☐ Verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO) ☒ Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO) ☐ Genehmigte Verhaltensregeln (Artt. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO) ☐ Genehmigter Zertfizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DSGVO) ☐ Sonstige Maßnahmen nach Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DS-GVO ☐ Erforderlichkeit zur Vertragserfüllung (Art. 49 Abs. 1 lit. c DS-GVO)
2.	USA (Apple Push Notification)	☐ Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO) ☐ Verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO)

		☐ Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO) ☐ Genehmigte Verhaltensregeln (Artt. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO) ☐ Genehmigter Zertfizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DSGVO) ☐ Sonstige Maßnahmen nach Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DS-GVO ☒ Erforderlichkeit zur Vertragserfüllung (Art. 49 Abs. 1 lit. c DS-GVO)
3.	USA (MapBox)	☐ Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO) ☐ Verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO) ☒ Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO) ☐ Genehmigte Verhaltensregeln (Artt. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO) ☐ Genehmigter Zertfizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DSGVO) ☐ Sonstige Maßnahmen nach Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DS-GVO ☐ Erforderlichkeit zur Vertragserfüllung (Art. 49 Abs. 1 lit. c DS-GVO)