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 schriftlich Form oder in Textform (z.B. E-Mail) an die vom Auftragnehmer bezeichnete Stelle 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 ***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.

Erläuterung zum Sonderkündigungsrecht: Der Auftraggeber kann den zugrundeliegenden Hauptvertrag und diesen AVV jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses AVV vorliegt.

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 des **Anhangs 4** 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 373 226 88
- Die für den Auftrag verantwortliche Mitarbeiter:in des Auftragnehmers, erreichbar über dessen Kontaktdaten oder allgemein: support@divera247.com, 0202 373 226 60

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 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 insbesondere technische und organisatorische Maßnahmen zu treffen, gemessen am Risiko für die Rechte und Freiheiten der betroffenen

Personen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer gewährleisten.

Der Auftragnehmer hat die erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung zu dokumentieren und dem Auftraggeber zur Prüfung bereitzustellen. Die Einzelheiten dieser technischen und organisatorischen Maßnahmen ergeben sich aus ***Anlage 2***.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Diese sind vom Auftragnehmer entsprechend zu dokumentieren. Dabei darf das Sicherheitsniveau der in ***Anlage 2*** genannten Maßnahmen nicht unterschritten werden.

3. Der Auftragnehmer unterstützt den Auftraggeber angemessen bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisungen zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die mit der Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben und diese Vertraulichkeitsverpflichtung auch nach Beendigung des Auftrags fortbesteht

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

Eine Meldung von Datenschutzverletzungen muss mindestens enthalten:

- eine Beschreibung des Vorfalls, soweit möglich mit Angabe der Art der Verletzung des Schutzes personenbezogener Daten, Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- eine Beschreibung der wahrscheinlichen Folgen des gemeldeten Vorfalls, eine Beschreibung der ergriffenen Maßnahmen zur Behebung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

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

Internet: http://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, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen (Art. 32 Abs. 1 lit. D DS-GVO).

8. Während der Vertragslaufzeit berichtigt oder löscht der Auftragnehmer auf Weisung des Auftraggebers die vertragsgegenständlichen Daten. Sofern eine datenschutzkonforme Löschung dieser Daten nicht möglich ist, stellt der Auftragnehmer eine datenschutzkonforme Vernichtung der Datenträger und Unterlagen, die vertragsgegenständliche Daten enthalten, sicher.

Dem Auftragsverarbeiter vom Auftraggeber übergebene Datenträger und verarbeitete Daten einschließlich gefertigter Kopien.

Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist.

Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen (schriftlich oder in Textform) des Auftraggebers entweder herauszugeben, sofern sie im Eigentum des Auftraggebers sind, oder zu löschen.

3. Pflichten des Auftraggebers

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

2. Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt Kapitel 2 Abs. 3 entsprechend.

4. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Anträgen gemäß Art. 15 bis 21 DS-GVO an den Auftragnehmer, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen und leitet den Antrag an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung dieser Anträge der betroffenen Personen im erforderlichen Umfang.

5. Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Bedingung niedergelegten Pflichten mit geeigneten Mitteln nach. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die dokumentierten Kontrollen und erforderlichen Auskünfte zur Verfügung zu stellen. Insbesondere ist die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art 32 DS-GVO nachzuweisen.

2. Der Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten kann erfolgen durch

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- Selbstaudits
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, ISO 27001, ISO 27018, ISO 27701)
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO

3. Kontrollrechte

(a) Der Auftragnehmer verpflichtet sich, den Auftraggeber bei seinen Prüfungen gemäß Art. 28 Abs. 3 Satz 2 lit. h DS-GVO zur Einhaltung der Vorschriften zum Datenschutz sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang zu unterstützen.

(b) Die Prüfungen werden durch den Auftraggeber selbst oder einen von ihm beauftragten Dritten durchgeführt. Sollte der durch den Auftraggeber beauftragte Dritter in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Beauftragte Dritte müssen durch den Auftraggeber zur Verschwiegenheit verpflichtet werden. Dem Auftragnehmer steht das Recht zu, die Abgabe einer separaten Verschwiegenheitserklärung des beauftragten Dritten zu verlangen. Dies gilt insbesondere für die Abgabe von Erklärungen zur berufsrechtlichen oder gesetzlichen Verschwiegenheit.

(c) Eine Prüfung kann insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch weitere Maßnahmen erfolgen. Zu den weiteren Maßnahmen zählen die Anforderung von Zertifizierungen, Berichte zu Datenschutzaudits und Inspektionen vor Ort. Inspektionen vor Ort nimmt der Auftraggeber mit angemessener Vorankündigung während der üblichen Geschäftszeiten vor. Die Prüfungen müssen ohne Störung des Betriebsablaufs sowie unter Wahrung der Sicherheits- und Vertraulichkeitsinteressen des Auftragnehmers durchgeführt und ist auf eine Prüfung pro Kalenderjahr beschränkt. Ausgenommen sind anlassbezogene Kontrollen. Jede Partei trägt die ihr entstandenen Kosten der Prüfungen in den vorgenannten Fällen (inkl. Nachprüfungen) selbst.

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 datenschutzrechtlichem Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine

einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

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

Die im Annex zu diesem Vertrag aufgeführten Subunternehmer gelten als genehmigt.

7.Übermittlung in Drittstaaten

1. Eine Übermittlung findet nur auf dokumentierte Weisung des Verantwortlichen in Drittstaaten außerhalb der EU und des EWR statt, sofern die Voraussetzungen nach Art. 44ff DS-GVO eingehalten werden.

2. Die Vertragsparteien halten in diesem Vertrag fest, auf welche Art und Weise das angemessene Schutzniveau für die Verarbeitung im Drittstaat sichergestellt ist.

Das angemessene Schutzniveau in den USA wird hergestellt durch entsprechend modulierte Standarddatenschutzklauseln ggf. inklusive zusätzlicher Schutzmaßnahmen (Art. 46 Abs. 2 lit. c und d DS-GVO).

3. Ist hierzu nichts im Vertrag vereinbart, ist die Verarbeitung in einem Drittstaat nur mit vorheriger Zustimmung des Auftraggebers zulässig. Der Auftragnehmer teilt dem Auftraggeber vorab mit, um welche(n) Drittstaat(en) es sich handelt und auf welche Weise das angemessene Schutzniveau im Sinne von Art. 44 ff DS-GVO für die Verarbeitung dort sichergestellt ist.

4. Der Auftragnehmer stellt einen Kontakt zur Verfügung, den der Auftraggeber Betroffenen als Stelle mitteilen kann, bei dem die Garantien verfügbar sind bzw. eine Kopie der Garantie angefordert werden kann.

8.Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

9.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.

3. 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.

4. 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 Mitarbeiter:innen/Einsatzkräften mit Qualifikationen und zeitlicher Verfügbarkeit.
- Analyse und Darstellung der Verfügbarkeit in verschiedenen Ansichten.
- Versenden von Mitteilungen, Terminen und dringenden Benachrichtigungen an die Benutzer:innen 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:innen/Einsatzkräfte
Kommunikationsdaten (z.B. Telefon, E-Mail)	Mitarbeiter:innen/Einsatzkräfte
Vertragsstammdaten	Administrator:in der Einheit, Rechnungsempfänger:in
Planungs- und Steuerungsdaten	Mitarbeiter:innen/Einsatzkräfte
Nutzungsdaten aus Telemediendiensten (z.B. von Webseiten, Apps für mobile Geräte)	Mitarbeiter:innen/Einsatzkräfte
Protokolldaten von IT-Systemen (z.B. Zugriffsprotokolle)	Mitarbeiter:innen/Einsatzkräfte
Daten zur Verfügbarkeit und Alarmauslösung im Einsatzfall	Mitarbeiter:innen/Einsatzkräfte
Technischer Kundendienst / Support / Softwarepflege	Administrator:in der Einheit, Mitarbeiter:innen/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 DS-GVO)

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.
- Das etablierte Verfahren Anlegen und Ändern von Zugängen und Zutrittsrechten stellt sicher, dass nur die Rechte vergeben werden, die zur Aufgabenerfüllung notwendig sind.

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
- Das etablierte Verfahren Anlegen und Ändern von Zugängen und Zutrittsrechten stellt sicher, dass nur die Rechte vergeben werden, die zur Aufgabenerfüllung notwendig sind.

Zugriffskontrolle:

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

- alle Zugriffe können Personen eindeutig zugeordnet werden (keine Nutzung von Mehrbenutzerkonten)
- Das etablierte Verfahren Anlegen und Ändern von Zugängen und Zutrittsrechten stellt sicher, dass nur die Rechte vergeben werden, die zur Aufgabenerfüllung notwendig sind.
- Das etablierte Verfahren für die Einarbeitung und Weggang von Mitarbeiter:innen, stellt sicher, dass alle Rechte nach Beendigung des Arbeitsverhältnisses entzogen werden.

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 DS-GVO)

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, SSH) 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 personenbezogene Informationen hinzugefügt, geändert oder gelöscht wurden
- der Schutz der Log-Dateien vor unerlaubten Zugriff und Änderung ist gewährleistet

Auftragskontrolle:

- Mitarbeiter:innen werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen
- Mitarbeiter:innen sind vertraut mit den Verfahrensanweisungen 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
- die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers
- alle Mitarbeiter:innen 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
- der Auftragnehmer hat einen externen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt
- beide sind durch die betriebliche Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 b DS-GVO)

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)
- Das Datensicherungskonzept (inkl. Notfallhandbuch und Wiederanlaufplänen) regelt die Sicherung aller relevanten Daten.
- 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

- Regelmäßige Prüfungen durch die eigene IT
- Kontrollen des betrieblichen Datenschutzbeauftragten
- Regelmäßige Durchführung von Datenwiederherstellungs-Tests
- Ständige Überwachung der Serverkapazitäten und frühzeitige Anpassung der Systemleistung, um auch während einer hoher Belastung den ordnungsgemäßen Betrieb sicherstellen zu können

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

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

- Es wurde eine Schutzbedarfsfestellung durchgeführt, um besonders schützenswerte IT-Systeme zu erkennen und zusätzliche Sicherheitsmaßnahmen ergreifen zu können.
- Besonders schützenswerte IT-Systeme sind (mehrfach) redundant ausgelegt, um auch bei einem Ausfall von einzelnen Servern die Verfügbarkeit zu gewährleisten.
- Im Rahmen des ISMS wird ein Datensicherungskonzept, ein Notfallhandbuch und Wiederanlaufpläne gepflegt, um auf möglichst viele Ausfallszenarien vorbereitet zu sein. Auch bei einem Totalausfall des Systems ist es uns so möglich, dieses schnell wiederherstellen zu können.
- Bei Auftreten eines möglichen Sicherheitsvorfalls ist das Vorgehen in der Richtlinie zur Behandlung von Sicherheitsvorfällen und in dem Verfahren Behandlung Sicherheitsvorfall festgehalten.

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

- Die vorhandenen Richtlinien, Verfahren und sonstige Dokumente werden jährlich auf Aktualität geprüft
- Die Server werden ständig überwacht (Zabbix, Grafana) um bei Auffälligkeiten reagieren zu können.
- 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, ausgewertet und Verbesserungen umgesetzt
- Es erfolgen interne Audits durch den externen Datenschutzbeauftragten
- Es erfolgen externe Audits durch zertifizierte Prüfer

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

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

Datenschutzfreundliche Voreinstellungen:

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

Maßnahmen zur Identifizierung und Autorisierung der Nutzer:innen

- Für Endnutzer:innen: Login durch Eingabe von Benutzername und Passwort. Für den Verwaltungszugriff kann zusätzlich ein 2. Faktor über eine TOTP-App hinterlegt werden.
- Ein Berechtigungskonzept inkl. Berechtigungsgruppen ermöglicht das feingranulare Verwalten von Berechtigungen.
- Der Zugriff auf die Server-Infrastruktur ist nur durch die DIVERA 24/7 IT-Abteilung mit SSH-Zertifikaten möglich.

Maßnahmen zum Schutz der Daten während der Speicherung

- Sicherheitsrelevante Informationen wie API-Keys und Private-Keys werden auf den Endgeräten der Endanwender:innen verschlüsselt gespeichert, sofern eine verschlüsselte Speicherung vom Endgerät unterstützt wird. Alle Daten auf den Endgeräten werden in einer vom Betriebssystem/Browser bereitgestellten Sandbox isoliert gespeichert, um vor Zugriffen durch andere Apps oder Websiten zu schützen.
- Die Backups werden verschlüsselt gespeichert.
- Es greift die Zutrittskontrolle des Rechenzentrums, um einen physischen Zugriff auf die Daten zu verhindern.

Maßnahmen zur Protokollierung von Ereignissen

- Das Logging ist auf ein Mindestmaß reduziert, um die verarbeiteten Daten zu minimieren.

- Der Schutz der Log-Dateien vor unerlaubten Zugriff und Änderung ist gewährleistet.

Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

- Alle Schritte zur Einrichtung eines neuen Servers sind dokumentiert, die Dokumentation wird fortlaufend aktualisiert.
- Die Konfigurationen werden deklarativ in Konfigurationsdateien geschrieben, die über das Quellcodeverwaltungssystem Git versioniert sind, sodass alle Änderungen nachvollziehbar und protokolliert sind
- Der Lese- und Schreib-Zugriff auf die Konfigurationsdateien-Repositories sind auf berechtigte Personen beschränkt.
- Die Konfigurationsdateien werden über Git auf Server synchronisiert, sodass Integrität und Konsistenz gewährleistet sind.
- Die Konfigurationen werden vererbt und so gesetzt, dass sie, wo es möglich ist, in allen Umgebungen identisch sind (Entwicklersystem, Test/Staging- und Produktivumgebung). Abweichungen werden explizit überschrieben.
- Verwendung von Containervirtualisierung über Docker, sodass identische Abbilder der Software veröffentlicht werden, um auch dort Integrität zu gewährleisten.

Maßnahmen für die interne Governance und Verwaltung der IT und der Informationssicherheit

- Die Verantwortlichkeiten sind in der DIVERA GmbH eindeutig und widerspruchsfrei zugewiesen. Insbesondere die Positionen der IT-Leitung und des Informationssicherheitsbeauftragten sind besetzt.
- Eine Leitlinie zur Informationssicherheit ist von der Geschäftsführung verabschiedet worden. Allen Mitarbeitenden wurde das Dokument bekannt gemacht und werden zu Themen der Informationssicherheit geschult.
- Weitere Richtlinien und Verfahren sind von der Geschäftsführung verabschiedet und zielgruppengerecht bekannt gemacht worden.
- Die DIVERA GmbH hat ein ISMS etabliert (erfolgreiches Audit zur Zertifizierung gemäß VdS 10000, mittelfristiges Ziel: Zertifizierung gemäß BSI IT-Grundschutz).

Maßnahmen zur Gewährleistung der Datenminimierung

- Umgesetztes Löschkonzept mit Löschfristen.
- Bei der Einspeisung der Alarmierungsdaten über eine Schnittstelle werden die notwendigen Informationen mit der jeweiligen Leitstelle besprochen und ausgefiltert.
- Verwendung von Pseudonymen in Log-Dateien, sowie Filtern von sensitiven Daten wie Passwörtern vor möglichem Logging.
- Alle Personen können pseudonymisiert angelegt werden.
- Reduziertes Logging auf ein Mindestmaß.

Maßnahmen zur Gewährleistung der Datenqualität

- Die Speicherung der Daten erfolgt in einem relationalen Datenbankmanagementsystem. Mit Hilfe von Transaktionen wird eine atomare Konsistenz und die Aktualität der Daten garantiert.

Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

- Das Datensicherungskonzept sieht für die Kundendaten 24 Sicherungen am Tag vor (jede Stunde eins). Davon wird jeweils eins für 14 Tage gesichert.
- Verwendung eines zentralen Log-Servers, der eingestellte Löschfristen zentral steuert und garantiert.
- Vermeidung von Datei-Logs

Maßnahmen zur Gewährleistung der Rechenschaftspflicht

- Erstellung und Pflege eines Verzeichnis der Verarbeitungstätigkeiten.
- Bestellung eines externen Datenschutzbeauftragten.
- Dokumentation von Datenschutzvorfällen.
- Verpflichtung aller Mitarbeitenden auf Vertraulichkeit.

Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

- Offen dokumentierte Web-Schnittstellen (https://api.divera247.com/).
- Exportmöglichkeit aller Daten einer Einheit.
- Backups reichen maximal 14 Tage in die Vergangenheit zurück.

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	
Plusnet GmbH, Mathias-Brüggen-Str. 55, 50829 Köln	Cloud-Telefonanlage		
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		*
ScopeVisio AG, Rheinwerkallee 3, 53227 Bonn	Buchhaltung und CRM		

Subunternehmen	Zweck der Datenverarbeitung	Sitz	*
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 (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO) ☒ Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DS-GVO) ☐ Genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO) ☐ Genehmigter Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO) ☐ Sonstige Maßnahmen nach Art. 46 Abs. 2 lit. a, Abs. 3 lit. 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 (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO)

		☐ Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DS-GVO) ☐ Genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO) ☐ Genehmigter Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO) ☐ Sonstige Maßnahmen nach Art. 46 Abs. 2 lit. a, Abs. 3 lit. 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 (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO) ☒ Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DS-GVO) ☐ Genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO) ☐ Genehmigter Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO) ☐ Sonstige Maßnahmen nach Art. 46 Abs. 2 lit. a, Abs. 3 lit. a und b DS-GVO ☐ Erforderlichkeit zur Vertragserfüllung (Art. 49 Abs. 1 lit. c DS-GVO)