Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen

……..

……..

……..

vertreten durch

……

im Folgenden: **Auftraggeber**

und

stdout UG (haftungsbeschränkt)

Grimmeisenstrasse 19

81927 München

vertreten durch

Peter Hoffmann

im Folgenden: **Auftragnehmer**

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

- Umwandlung von Adressen im Koordinaten (Geocoding)
- Umwandlung von Koordinaten in Adressen (Reverse-Geocoding)
- Bereitstellung einer interaktiven Karte (Hosted Map Tiles)
- Erstellung von statischen Karten als Bild (Static Maps)

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

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags

Der Vertrag beginnt am …….. und wird auf unbestimmte Zeit geschlossen, mindestens aber für die Dauer des Bestehens des Hauptvertrages. Die Kündigungsfrist beträgt einen Monat. Eine isolierte Kündigung dieses Vertrages ist ausgeschlossen.

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

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Das Maps-Portal bietet verschiedene Geodatendienste an, einschließlich der Umwandlung von Adressen in Koordinaten (Geocoding), der Umwandlung von Koordinaten in Adressen (Reverse-Geocoding), der Bereitstellung interaktiver Karten (Hosted Map Tiles) und der Erstellung statischer Karten als Bild (Static Maps). Diese Dienste ermöglichen es Nutzern, geografische Informationen effizient zu verarbeiten und darzustellen.

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):

- Erhebung
- Erfassung
- Organisation
- Speicherung
- Anpassung oder Veränderung
- Auslesen
- Abfrage
- Verwendung
- Offenlegung durch Übermittlung
- Verbreitung oder eine andere Form der Bereitstellung
- Abgleich oder Verknüpfung
- Einschränkung
- Löschung oder Vernichtung

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

- Adressdaten (z.B. Straßenname, Hausnummer, Postleitzahl, Ort)
- Geokoordinaten (Längen- und Breitengrad)
- Nutzungsdaten (z.B. IP-Adresse, Standortdaten)

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

- Kunden und Nutzer des Maps-Portals, die die Geodatendienste in Anspruch nehmen
- Mitarbeiter und Vertreter von Unternehmen, die das Maps-Portal nutzen
- Dritte, deren personenbezogene Daten im Rahmen der Nutzung der Dienste verarbeitet werden (z.B. Empfänger von Lieferungen, deren Adressen geocodiert werden)

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

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.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:

……..

Weisungsempfänger beim Auftragnehmer ist:

Peter Hoffmann, Grimmeisenstrasse 19, 81927 München, Tel.: +49 89 416 164 63

Für Weisung zu nutzende Kommunikationskanäle:

Grimmeisenstrasse 19, 81927 München; info@gdpr-map.eu; Tel.: +49 89 416 164 63

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); 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 (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

- Pseudonymisierung der IP-Adresse
- Pseudonymisierung der Abfragen (Adressdaten, Koordinaten, Map Tiles)

Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO).

Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:

…….

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. **Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:**

…….

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

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 sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragnehmer ist als Beauftragter für den Datenschutz bestellt:

Herr Marco Gariboldi, Grüntal 34, 81925 München, Tel.: +49 89 416 164 63, mg@gdpr-map.eu

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

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 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

Zurzeit ist für den Auftragnehmer folgender Subunternehmer mit der Verarbeitung von personenbezogenen Daten in folgendem Umfang beschäftigt:

Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen (Server Hoster)

Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Das im Anhang 1 beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Beendigung des Vertrags löscht der Auftragnehmer nach Wahl des Auftraggebers alle im Auftrag des Auftraggebers verarbeiteten personenbezogenen Daten oder er gibt alle personenbezogenen Daten an den Auftraggeber zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Sonstige Vereinbarungen

10.1. Entgelte

Ein Entgelt für diesen Vertrag über die Auftragsverarbeitung personenbezogener Daten wird nicht gefordert.

10.2. Rechtswahl

Es gilt das Recht der Bundesrepublik Deutschland.

10.3. Gerichtsstand

Die Parteien vereinbaren als Gerichtsstand den Sitz des für München zuständigen Gerichts.

10.4. Sonderregelungen

Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrages. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

Unterschriften

……...……..…….	……..……..…….
Auftraggeber	Auftragnehmer

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

Anlage 1 zum Auftrag gemäß Art. 28 DS-GVO: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage

1. Vertraulichkeit

Zutrittskontrolle

- Server und Backup System der Logdateien
  - **Zutrittskontrollsystem:** Einsatz eines elektronischen Zutrittskontrollsystems.
  - **Ausweisleser und Magnetkarte:** Zutritt zu den Räumen erfolgt nur mit personalisierten Ausweiskarten.
  - **Schlüsselvergabe:** Ausgabe von Schlüsseln nur an autorisierte Personen, Dokumentation der Schlüsselvergabe.
  - **Werkschutz und Pförtner:** Sicherheitsdienst vor Ort sowie Pförtner zur Kontrolle des Zutritts.
  - **Überwachungseinrichtung:** Videoüberwachung in sensiblen Bereichen.
  - **Alarmanlage und Türsicherung:** Installation von Alarmanlagen und zusätzlichen Türsicherungen in Sicherheitszonen.

Zugangskontrolle

- Online-Benutzeroberfläche
  - Bei der erstmaligen Registrierung vergibt der Auftraggeber ein Login-Passwort, welches nur dem Auftraggeber bekannt ist.
  - Zusätzliche Maßnahmen:
    - **Kennwortverfahren:** Verwendung sicherer Kennwortverfahren, regelmäßige Änderung der Passwörter.
    - **Automatisches Sperren:** Automatisches Sperren der Zugänge nach mehreren fehlgeschlagenen Anmeldeversuchen.
    - **Einrichtung eines Benutzerstammsatzes:** Pro User wird ein individueller Benutzerstammsatz angelegt.
    - **Verschlüsselung von Datenträgern:** Alle relevanten Daten werden auf verschlüsselten Datenträgern gespeichert.
    - **Passwortrichtlinie:** Implementierung einer Passwortrichtlinie, die Anforderungen an Komplexität und regelmäßige Aktualisierung der Passwörter stellt.

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

- API-Schnittstelle
  - Der Auftraggeber generiert auf der Online-Benutzeroberfläche API-Schlüssel, über die er auf die API-Schnittstelle zugreifen kann.
  - Zusätzliche Maßnahmen:
    - **Individuelle API-Schlüssel:** Jeder API-Schlüssel ist eindeutig und individuell an einen Nutzer gebunden.
    - **Regelmäßige Überprüfung und Sperrung:** Regelmäßige Überprüfung und Sperrung nicht mehr benötigter API-Schlüssel.
- Administrationsoberfläche
  - Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer.
  - Zusätzliche Maßnahmen:
    - **Individuelle Zugriffsrechte:** Dokumentation und zentrale Verwaltung der Zugriffsrechte nach dem Need-to-know-Prinzip.
    - **Regelmäßige Überprüfung:** Regelmäßige Überprüfung und Aktualisierung der Zugriffsberechtigungen.
    - **Aufzeichnung von Zugriffen:** Protokollierung und Überwachung aller Zugriffe auf die Administrationsoberfläche.

Zugriffskontrolle

- Interne Verwaltungssysteme des Auftragnehmers
  - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
  - Zusätzliche Maßnahmen:
    - **Individuelle Zugriffsrechte:** Vergabe individueller Zugriffsrechte für jeden Benutzer, dokumentiert in einem schriftlichen Berechtigungskonzept.
    - **Zentrale Verwaltung:** Zentrale Verwaltung und Steuerung der Zugriffsberechtigungen nach dem Need-to-know-Prinzip.
    - **Regelmäßige Überprüfung:** Regelmäßige Überprüfung und Aktualisierung der Zugriffsberechtigungen.
    - **Aufzeichnung von Zugriffen:** Protokollierung und Überwachung aller Zugriffe auf die internen Systeme.
- Benutzeroberfläche und API-Schnittstelle
  - Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
  - Zusätzliche Maßnahmen:

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

- **Regelmäßige Schulungen:** Schulungen für die Mitarbeiter des Auftraggebers zur sicheren Handhabung der Zugänge.
- **Dokumentation der Zugriffe:** Protokollierung und regelmäßige Überprüfung der Zugriffe auf die Benutzeroberfläche und die API-Schnittstelle.

Pseudonymisierung

- der Zugriffs-Logdateien der API-Schnittstelle
  - Logdateien werden 14 Tage lang gespeichert und beinhalten IP-Adresse, Datum, URL mit Parametern, Response Code, Referer, Browser User-Agent und API-Schlüssel
  - Nach Ablauf von 14 Tagen werden die Log-Dateien auf das Log-Backup System übertragen und es werden folgende Daten gespeichert: die ersten 6 Stellen der IP-Adresse, Datum, Endpunkt-URL ohne Parameter, API Schlüssel und Response Code

2. Integrität

Weitergabekontrolle

- Schulung und Verpflichtung der Mitarbeiter
  - Alle Mitarbeiter sind gemäß Art. 32 Abs. 4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
  - Regelmäßige Schulungen und Sensibilisierungen zum Thema Datenschutz und Datensicherheit.
- Datenschutzgerechte Löschung
  - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung gemäß den geltenden gesetzlichen Vorschriften und internen Richtlinien.
  - Implementierung eines dokumentierten Löschkonzepts, welches die sichere und unwiderrufliche Löschung der Daten sicherstellt.
- Verschlüsselte Datenübertragung
  - Möglichkeit zur verschlüsselten Datenübertragung über TLS-gesicherte Verbindungen.
  - Sicherstellung, dass alle Datenübertragungen zwischen dem Auftraggeber und dem Auftragnehmer sowie zwischen internen Systemen des Auftragnehmers verschlüsselt erfolgen.

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

Eingabekontrolle

- Automatisierte Protokollierung
  - Implementierung eines Systems zur automatisierten Protokollierung aller Dateneingaben, Änderungen und Löschungen.
  - Jede Dateneingabe, -änderung oder -löschung wird protokolliert und kann nachträglich überprüft werden.
- Protokollierungs- und Überwachungssystem
  - Einführung eines zentralen Protokollierungs- und Überwachungssystems, das die Integrität der Daten überwacht und sicherstellt.
  - Regelmäßige Überprüfung und Analyse der Protokolle durch Sicherheitsbeauftragte zur Erkennung und Vermeidung von Unregelmäßigkeiten.
- Zugriff auf Protokolle
  - Zugriff auf die Protokolle ist nur autorisierten Mitarbeitern gestattet und erfolgt nach dem Need-to-know-Prinzip.
  - Sicherstellung der Vertraulichkeit und Integrität der Protokolle durch geeignete Schutzmaßnahmen.

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

Verfügbarkeitskontrolle der Server

- Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
  - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
  - Monitoring aller relevanten Server.
  - Einsatz unterbrechungsfreier Stromversorgung.
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);
  - Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Auftragskontrolle

- Regelmäßige Datenschutzunterweisungen

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu

- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sind mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag vertraut. Dies schließt auch das Weisungsrecht des Auftraggebers ein.

- Detaillierte Angaben in den AGB
  - Die Allgemeinen Geschäftsbedingungen (AGB) enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
- Betrieblicher Datenschutzbeauftragter
  - Die stdout UG (haftungsbeschränkt) hat einen betrieblichen Datenschutzbeauftragten bestellt. Er ist in die relevanten betrieblichen Prozesse eingebunden und überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.
  - Der Datenschutzbeauftragte steht den Mitarbeitern und dem Auftraggeber als Ansprechpartner für Fragen zum Datenschutz zur Verfügung.
- Hinzuziehung von Unterauftragsverarbeitern
  - **Vertragliche Regelungen:** Vor der Hinzuziehung von Unterauftragsverarbeitern erfolgt eine vertragliche Regelung, die sicherstellt, dass die Unterauftragsverarbeiter denselben Datenschutzstandards unterliegen wie die stdout UG (haftungsbeschränkt).
  - **Prüfung und Auswahl:** Unterauftragsverarbeiter werden sorgfältig ausgewählt und regelmäßig überprüft, um sicherzustellen, dass sie die datenschutzrechtlichen Anforderungen erfüllen.
  - **Informationspflicht:** Der Auftraggeber wird vor der Beauftragung von Unterauftragsverarbeitern informiert und besitzt ein Einspruchsrecht.
  - **Vereinbarung zur Datenverarbeitung:** Mit jedem Unterauftragsverarbeiter wird eine Vereinbarung zur Auftragsdatenverarbeitung abgeschlossen, die den Anforderungen der DSGVO entspricht.
  - **Kontinuierliche Überwachung:** Die Einhaltung der Datenschutzvorgaben durch die Unterauftragsverarbeiter wird kontinuierlich überwacht und dokumentiert.

stdout UG (haftungsbeschränkt)
Geschäftsführer: Peter Hoffmann
Registergericht: München, HRB 272216
USt.Id: DE 352 336 777

Grimmeisenstrasse 19
81927 München
Tel.: +49 (0) 89 – 41 61 64 63
E-Mail: info@gdpr-map.eu