Technische und organisatorische Maßnahmen zu Datensicherheit gemäß Art. 32 EU-DSGVO (Stand: Dezember 2021)

Die Firma leadtributor unternimmt zahlreiche Maßnahmen zum Schutz der ihr anvertrauten Daten. Insbesondere bekennen wir uns zu dem Schutz von personenbezogenen Daten sowie den Vorschriften der EU-DSGVO (Datenschutzgrundverordnung) und des BDSG (Bundesdatenschutzgesetz), wie sie seit dem 25. Mai 2018 anwendbar sind.

leadtributor.cloud ist ein Produkt der Firma leadtributor und wird von uns sowohl entwickelt als auch betrieben. Dabei handelt es sich um eine auf Cloud-Diensten basierende Plattform, die es unseren Kunden ermöglicht, miteinander in Kontakt zu treten und gemeinsame Vertriebsaktivitäten auszuführen, Unsere Kunden werden innerhalb der Plattform in Form von Mandanten (sog. „Firmen") geführt. Alle personenbezogenen Daten lassen sich auf einen Mandanten zurückführen, welcher die Verantwortung für die Datenverarbeitung trägt.
Jede Verarbeitung der uns durch unsere Kunden zur Verfügung gestellten Daten erfolgt auftragsbezogen gemäß den individuell geschlossenen Vereinbarungen zur Auftragsdatenverarbeitung.

Eingesetzte Datenverarbeitungsanlagen

Die Daten unserer Kunden werden mithilfe elektronischer Datenverarbeitungsanlagen verarbeitet.

Hierfür nutzen wir eine Vielzahl von Diensten, die von ***Amazon Web Services*** (nachfolgend: „AWS") bereitgestellt werden. Das umfasst neben Netzwerk- und Kommunikationsdiensten insbesondere auch Compute- und Storage-Lösungen. leadtributor.cloud basiert nahezu vollständig auf den AWS-Diensten und ist untrennbar mit diesen verbunden. AWS erbringt diese Dienste uns gegenüber als Auftragsverarbeiter, welchen wir wiederum als Unterauftragsverarbeiter für die Verarbeitung unserer Kundendaten einsetzen. AWS verarbeitet unsere Kundendaten auf unsere Weisung hin ausschließlich innerhalb des Europäischen Wirtschaftsraums (EWR). Eine Verarbeitung von personenbezogenen Daten in Drittstaaten findet nicht statt.

AWS und alle von uns eingesetzten AWS-Dienste sind nach ISO/IEC 27001:2013, 27017:2015, 27018:2019, 27701:2019, 9001:2015 und CSA STAR CCM v3.0.1 zertifiziert. Auf Verlangen unserer Kunden legen wir entsprechende Nachweise vor.

Ferner nutzen wir Datenverarbeitungsanlagen in den **Räumlichkeiten der leadtributor GmbH** („Büroräume"). Diese kommen für die Verarbeitung von personenbezogenen bzw. kunden-eigenen Daten ausschließlich anlassbezogenen zur Anwendung und nur zu Zwecken der Überwachung und Wahrung des ordnungsgemäßen Betriebs, der Überprüfung auf Korrektheit sowie der Korrektur von Daten und stets in Übereinstimmung mit der Vereinbarung zur Datenverarbeitung mit den jeweils Verantwortlichen.
In keinem Fall werden personenbezogene Daten dauerhaft auf diesen Geräten gespeichert.

1. Zutrittskontrolle

Maßnahmen, die verhindern, dass Unbefugte Zutritt zu Gebäuden und Räumen erlangen, in denen sich Datenverarbeitungsanlagen befinden.

In unseren Büroräumen:

- Alle Büroräume befinden sich im 1. OG
- Der Zugang zu den Büroräumen ist grundsätzlich verschlossen
- Zylinder Schließsystem mit unmarkierten Schlüsseln
- Besucher werden stets beaufsichtigt

2. Zugangskontrolle

Maßnahmen, die sicherstellen, dass Unbefugte keinen Zugang zu Datenverarbeitungsanlagen haben.

In unseren Büroräumen:

- Einsatz einer Firewall zum Schutz des Büro-Netzwerks
- Einsatz von Anti-Viren-Software auf allen Arbeitsplatz-Computern
- Personalisierte Zugänge zu Arbeitsplatz-Computern mit Passwortschutz
- Master-Passwörter werden in einer verschlüsselten Datenbank aufbewahrt, auf die ausschließlich 4 Personen Zugriff haben: Ein Geschäftsführer, der IT Leiter und zwei seiner Mitarbeiter, die mit Betriebsaufgaben betraut sind
- Computer sind bei Verlassen des Arbeitsplatzes zu sperren
- Unberechtigten Personen ist die Einsicht auf den Monitor zu verwehren

In der Leadtributor-Software:

- Separate Zugänge für unterschiedliche Benutzer
- Anmeldung mittels persönlicher Benutzerkennung (E-Mail-Adresse/Passwort)
- Überprüfung der E-Mail-Adresse eines Benutzers mittels Bestätigungsmail
- Sichere Passwortrichtlinie technisch umgesetzt
- Token-basierte Authentifizerung mit kurzer Lebensdauer

Zu den AWS-Diensten:

- SSO-Anmeldung mit zentraler Benutzerverwaltung und persönlicher Benutzerkennung (Benutzername/Passwort)
- Sichere Passwortrichtlinie technisch umgesetzt
- Begrenzte Sitzungsdauer

3. Zugriffskontrolle

Maßnahmen, die sicherstellen, dass Unbefugte keinen Zugriff auf personenbezogene oder kunden-eigene Daten haben.

In der Leadtributor-Software:

- Benutzer agieren stets für einen Mandanten und haben nur Zugriff auf die Daten des Mandanten
- Protokollierung aller Zugriffe auf das System; pseudonymisiert
- Mandanten können das Löschen von Leads über die Software selbst anweisen; Löschungen sind unmittelbar, irreversibel und dauerhaft

Organisatorisch:

- Rollen-/Rechte-Konzept für Mitarbeiter
- Zugriff für Mitarbeiter nach dem „Least to know" Prinzip
- Lediglich 2 Administratoren verfügen über Vollzugriff
- Keine dauerhafte Speicherung von kunden-eigenen Daten in den Büroräumen

4. Weitergabekontrolle

Maßnahmen, die sicherstellen, dass personenbezogene bzw. kunden-eigene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben.

- Sichere Transportverschlüsselung für alle Daten, die mit der Leadtributor-Software oder den AWS-Diensten ausgetauscht werden; insbesondere administrative Zugriffe sowie Nutzdaten der Leadtributor-Software
- Sichere Verschlüsselung von Daten „in Ruhe"
- Verschlüsselung nach Stand der Technik
- Kunden-eigene Daten werden nicht dauerhaft auf Datenverarbeitungsanlagen von Mitarbeitern gespeichert

5. Eingabekontrolle

Maßnahmen, die sicherstellen, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat.

In der Leadtributor-Software:

- Jede Datenveränderung wird einzeln erfasst und dauerhaft gespeichert („Event-Sourcing")
- Zu jeder Datenveränderung werden erfasst:
  - Art der Änderung
  - Inhalt der Änderung
  - Zeitpunkt der Änderung
  - Veranlasser der Änderung
- Sollten Mitarbeiter in die Datenverarbeitung eingreifen, dann geschieht dies ausschließlich auf Weisung des Verantwortlichen oder um den ordnungsgemäßen Weiterbetrieb entsprechend den vertraglichen Regelungen bzw. einer vorangegangen Weisung sicher zu stellen; jeder Eingriff wird dokumentiert

6. Auftragskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden.

- Datenschutzbelehrungen und Verschwiegenheitsverpflichtungen aller Mitarbeiter
- Sorgfältige Auswahl von Auftragnehmern und Einsatz beschränkt auf das maximal nötige Maß
- Mit allen Auftragnehmern wird bei Vorliegen der gesetzlichen Voraussetzungen ein Auftragsverarbeitungsvertrag (gemäß Art. 28 EU-DSGVO) vor Aufnahme der Verarbeitungstätigkeit abgeschlossen
- Unser Kunde kann seinen Mandanten über die Leadtributor-Software selbst löschen; in diesem Fall werden alle Daten des Mandanten automatisch, unmittelbar, irreversibel und dauerhaft gelöscht, sofern nicht etwaige gesetzliche oder nachvertragliche Aufbewahrungsfristen dem entgegenstehen

7. Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Verantwortlichen stets verfügbar sind, sowie nach einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

- Backups: 35 Tage Point-In-Time-Recovery für alle Kunden-eigenen Daten
- Hochverfügbarkeit durch mehrfach redundante regionale Speicherung seitens AWS
- Hochverfügbarkeit durch hoch-skalierfähige Netzwerk- und Compute-Infrastruktur seitens AWS
- 24/7 Rufbereitschaft
- Laufende automatische Überwachung der Leadtributor-Dienste und proaktive Benachrichtigung im Fehlerfall

8. Trennungskontrolle

Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

In der Leadtributor-Software:

- Mandantentrennung: Kunden-eigene Daten werden so erfasst, dass zu jeder Zeit der Rückbezug auf genau einen Mandanten als Verantwortlichen der Datenverarbeitung möglich ist
- Jeder Mandant hat nur Zugriff auf seine eigenen Daten
- Mandanten können anderen Mandaten im Rahmen wohldefinierter Programmfunktionen Zugriff auf Teile ihrer Daten gewähren – z.B. Leadverteilung über Marktplätze

9. Wirksamkeitskontrolle

Maßnahmen zur Bewertung und regelmäßigen Überprüfung der Wirksamkeit der hier beschriebenen technisch-organisatorischen Maßnahmen.

- Mindestens einmal jährlich, oder anlassbezogen auch früher, werden die hier aufgeführten Maßnahmen auf ihre Wirksamkeit und Angemessenheit hin durch den Datenschutzverantwortlichen untersucht
- Bei der Überprüfung werden auch die technischen und organisatorischen Maßnahmen unserer Auftragsverarbeiter überprüft