

AUFTRAGSDATENVERARBEITUNGSVERTRAG

lab73 GmbH

Stand: März 2024

1 Auftragsdatenverarbeitung

Dieser Auftragsdatenverarbeitungsvertrag regelt die datenschutzrechtlichen Verpflichtungen der lab73 GmbH als Auftragnehmer bzw Auftragsverarbeiter (nachfolgend auch „AN“) und ihrem Auftraggeber als Verantwortlicher iSd DSGVO (nachfolgend auch „AG“). Die Vereinbarungen dieses Vertrages gelten als Zusatzvereinbarung zum Vertrag. Die Dauer dieser Vereinbarung ist auf den Hauptvertrag beschränkt, wogegen die Pflichten darüber hinaus gelten.

Der AN verarbeitet im Rahmen der Leistungserbringung unter Umständen auch Daten von Kunden des AG (im Folgenden „Endkunden“), sowie allenfalls personenbezogene Daten von Mitarbeitern des AG.

2 Kategorien von Daten

Kategorien derart verarbeiteter Daten von Endnutzern sind sämtliche folgenden Daten:

- Personendaten: Name, Anschrift, Geburtsdatum

3 Kategorien betroffener Personen

Betroffene Personen sind:

- Endkunden im Vorvertrags- und Vertragsstadium
- Mitarbeiter des AG

4 Rechte und Pflichten der Vertragsparteien

Der AN darf personenbezogene Daten ausschließlich auf dokumentierte Weisung des AG verarbeiten, es sei denn, dass er nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet ist.

Der AN informiert den Verantwortlichen unverzüglich, falls Grund zur Annahme besteht, dass eine Weisung des AG gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt. Er informiert den AG unverzüglich über allfällige Hausdurchsuchungen beim AN oder am Ort der Server des AN.

Nach Möglichkeit unterstützt AN den AG mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen (Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit,

Widerspruch und Schutz vor automatisierter Entscheidung). Wenn eine betroffene Person einen Antrag an den AG stellen sollte, so wird dieser Antrag an den AN weitergeleitet.

Unter Berücksichtigung der Art der Verarbeitung und der zur Verfügung stehenden Informationen unterstützt der AN den AG bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen).

Auf Ansuchen des AG stellt der AN alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 DSGVO („Auftragsverarbeitung“) niedergelegten Pflichten zur Verfügung. Auf Wunsch ermöglicht der AN auch Überprüfungen – einschließlich Inspektionen –, die vom AG durchgeführt werden. Den AG trifft die Pflicht, in regelmäßigen Abständen zu prüfen, ob durch geeignete technische und organisatorische Maßnahmen des AN ein angemessenes Datenschutzniveau gewährleistet ist.

Der AN verpflichtet sich dazu, bei Vorliegen der Bedingungen gemäß Artikel 37 DSGVO einen Datenschutzbeauftragten zu bestellen.

Der AN ist zur vertraulichen Behandlung der offengelegten bzw. übermittelten oder sonst zur Verfügung gestellten personenbezogenen Daten und Informationen verpflichtet. Ebenso sind die erlangten Kenntnisse der Verarbeitungsergebnisse von dieser Pflicht zur Vertraulichkeit umfasst.

5 Verschwiegenheit

Die in den AGB des AN vereinbarte Geheimhaltungspflicht erstreckt sich auch auf die gegenständliche Datenverarbeitung und sämtliche datenverarbeitende Personen.

6 Technische und organisatorische Maßnahmen

Der AN sichert das Vorliegen folgender technischer und organisatorischer Maßnahmen im eigenen Betrieb zu:

- Zutrittskontrolle: Kontrolle des Zutritts zu Räumlichkeiten des Betriebs unter anderem durch geregelte Schlüsselverwaltung, Sicherheitstüren bzw. Alarmanlagen,
- Zugangskontrolle: Kontrolle des Zugangs zu Datenverarbeitungssystemen (zB: Kennwörter, Fingerabdruckscan und Virtual Private Network (VPN));
- Zugriffskontrolle: Kontrolle des Zugriffs auf Daten innerhalb des Systems durch ein Berechtigungssystem samt Protokollierung der Zugriffe;
- Schutz der Daten: Schutzvorkehrungen zur Verhinderung der Zerstörung oder des Verlusts von personenbezogenen Daten durch moderne Backup- und Aktualisierungskonzepte, Firewalls und Virensoftware;
- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung

- Eingabekontrolle: Sämtliche Eingaben werden auf Basis einer Dokumentations-Policy nachvollziehbar protokolliert
- Verfügbarkeit/Wiederherstellbarkeit: Die Wiederherstellung z.B. aufgrund technischer Gebrechen verlorener oder zerstörter Daten ist aufgrund entsprechender Recovery-Konzepte innerhalb kürzester Zeit möglich.
- Löschrufen: Bei jeder Datenübertragung sind Löschrufen verpflichtend zu hinterlegen. Die Löschung wird nach Ablauf der Frist automatisch vollzogen.
- Datenschutz-Managementsystem (DSMS): Das bestehende Datenschutzsystem wird laufend evaluiert und angepasst.

7 Sub-Auftragsverarbeitung

Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter oder Sub-Auftragsverarbeiter (im Folgenden zusammen „Sub-Auftragsverarbeiter“), wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben und die Hinzuziehung oder die Ersetzung zu untersagen. Erhebt der Verantwortliche innerhalb von zwei Wochen keinen Einspruch, so gilt die Hinzuziehung oder Ersetzung als genehmigt.

Nimmt der Auftragsverarbeiter einen anderen Sub-Auftragsverarbeiter in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem Sub-Auftragsverarbeiter im Wege eines Vertrages dieselben Datenschutzpflichten auferlegt, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des anwendbaren Datenschutzrechts erfolgt.

Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

8 Erfüllung DSGVO

Der AN hat gemäß Artikel 32 DSGVO alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung umgesetzt und passt diese an den technologischen Wandel bzw. an neue Erkenntnisse im Sinne eines selbstlernenden Datenschutzmanagementsystems an.

Der AN hat ein Verarbeitungsverzeichnis gemäß Artikel 30 DSGVO sowie eine Datenschutzfolgenabschätzung erstellt und hält dieses stets aktuell. Dieses Verarbeitungsverzeichnis umfasst auch alle Verarbeitungstätigkeiten der gegenständlichen Vereinbarung.

9 Überprüfung

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen, einschließlich Inspektionen, die von dem Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden. Hierfür gebührt dem Auftragsverarbeiter kein zusätzliches Entgelt.

Wird im Rahmen einer Überprüfung eine Verletzung dieses Vertrages durch den Auftragsverarbeiter festgestellt, so hat der Auftragsverarbeiter die Kosten des Verantwortlichen für die Durchführung der Überprüfung zu tragen.

10 Löschung

Sofern personenbezogene Daten nach Vertragsbeendigung noch beim AN gespeichert sind und falls keine rechtliche Verpflichtung zur weiteren Aufbewahrung oder Verarbeitung besteht, werden diese sofort gelöscht.