Zusatzvereinbarung

zum Rahmenvertrag zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO vom

## 1. März 2020

zwischen

**MAHLE International GmbH**

**Pragstraße 26-46**

**70376 Stuttgart**

– Verantwortlicher - nachfolgend "Auftraggeber" genannt –

und

**DRIMCO GmbH**

**Am Moosfeld 13**

**81829 München**

– Auftragsverarbeiter - nachfolgend „Auftragnehmer“ genannt –

– gemeinsam die „Parteien“ genannt –

**Inhaltsverzeichnis**

[Präambel 3](#_Toc38620320)

[1. Allgemeine Bestimmungen 3](#_Toc38620321)

[2. Gegenstand der Datenverarbeitung 3](#_Toc38620322)

[3. Dauer der Datenverarbeitung 3](#_Toc38620323)

[4. Art, Zweck und Rechtsgrundlage der Datenverarbeitung 4](#_Toc38620324)

[5. Arten der personenbezogenen Daten 5](#_Toc38620325)

[6. Kategorien betroffener Personen 5](#_Toc38620326)

[7. Technische und organisatorische Maßnahmen 6](#_Toc38620327)

[8. Weisungsberechtigte Personen und Weisungsempfänger des Auftragnehmers 8](#_Toc38620328)

[9. Genehmigte Unterauftragnehmer 9](#_Toc38620329)

# 

# Präambel

Diese Zusatzvereinbarung ergänzt den „Rahmenvertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO“ vom 1. März 2020 zwischen den Parteien und beschreibt die Datenverarbeitung auf Basis der eigenständigen Beauftragung, des Vertrags oder der Bestellung Bitte, geben Sie den Namen und/oder die Bestellnummer der Leistungsvereinbarung vom Klicken Sie hier, um das Vertragsdatum der Leistungsvereinbarung einzugeben (nachfolgend „Leistungsvereinbarung“).

# Allgemeine Bestimmungen

Mit Unterzeichnung ergänzt diese Zusatzvereinbarung die Bestimmungen des Rahmenvertrages.

Die Parteien sind sich einig, dass die im Rahmenvertrag enthaltenen Bestimmungen hinsichtlich der Verarbeitung personenbezogener Daten durch den Auftragnehmer vollumfänglich Anwendung auf die in der Leistungsvereinbarung beschriebene Dienstleistung finden.

Im Folgenden werden Gegenstand, Zweck, Art und Umfang der mit der Leistungsbeschreibung beauftragten Datenverarbeitung festgelegt (Art. 28 Absatz 3 DS-GVO).

# Gegenstand der Datenverarbeitung

Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung.

und/oder

Gegenstand des Auftrags, bei dem der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet, beinhaltet die Durchführung folgender Aufgaben:

Bitte beschreiben Sie die Aufgaben des Auftragnehmers

# Dauer der Datenverarbeitung

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder

Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum **Bitte wählen Sie das Datum der Befristung (soweit zutreffend)**

oder

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von **Anzahl** **an** **Tagen/Wochen/Monaten/Jahren** zum **Monats-/Jahresende** gekündigt werden.

Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt. Eine fristlose Kündigung ist möglich, wenn ein schwerwiegender Verstoß des Auftragsnehmers gegen Datenschutzvorschriften oder Bestimmungen dieser Vereinbarungen vorliegt, der Auftragnehmer eine ordnungsgemäße Weisung nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Endet der Rahmenvertrag, enden auch diese Zusatzvereinbarung sowie der Auftrag zur Datenverarbeitung durch den Auftragnehmer.

# Art, Zweck und Rechtsgrundlage der Datenverarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung

und/oder

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer:

**Bitte beschreiben Sie hier die Art und Zweck der Datenverarbeitung detaillierter als in der Leistungsvereinbarung angegeben.**

Die personenbezogenen Daten des Auftraggebers werden auf Basis folgender Rechtsgrundlage verarbeitet:

|  |  |  |
| --- | --- | --- |
| Einwilligung der betroffenen Personen (Art. 6 I lit. a) DS-GVO) | Vertragsdurchführung/Durchführung vorvertraglicher Maßnahmen mit der betroffenen Person (Art. 6 I lit. b) DS-GVO) | Erfüllung rechtlicher Verpflichtung (Art. 6 I lit. c) DS-GVO) |
| Schutz lebenswichtiger Interessen der betroffenen Personen (Art. 6 I lit. d) DS-GVO) | Wahrnehmung einer öffentlichen Aufgabe (Art. 6 I lit. e) DS-GVO) | Wahrung berechtigter Interessen des Verantwortlichen/eines Dritten (Art. 6 I lit. f) DS-GVO) |

**Bitte beschreiben Sie hier die Ausgestaltung der Rechtsgrundlage (z.B. welcher Vertrag durchgeführt werden soll oder welcher rechtlichen Verpflichtung Sie mit der Verarbeitung nachkommen.**

# Arten der personenbezogenen Daten

Es werden folgende Kategorien personenbezogener Daten verarbeitet:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Personalstammdaten | Kontaktdaten | Vertragsstammdaten | | |
| Bankverbindungsdaten | Abrechnungsdaten | Daten zu Mitarbeiterqualifikationen | |
| Videoaufzeichnungen | Kundenhistorie | Planungs- und Steuerungsdaten | | |
| Tonaufzeichnungen | Kundenstammdaten | Sonstige Arten personenbezogener Daten: \_\_\_\_\_\_\_\_\_\_\_ |

Sonstige Arten personenbezogener Daten: **Bitte geben Sie die weiteren Datenarten an, soweit zutreffend.**

Es werden folgende besondere Kategorien personenbezogener Daten gem. Art. 9 DS-GVO verarbeitet:

|  |  |  |  |
| --- | --- | --- | --- |
| Rassische und ethnische Herkunft | Politische Meinung | Religiöse oder weltanschauliche Überzeugung | |
| Gewerkschaftszugehörigkeit | Genetische Daten | Biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person |
| Gesundheitsdaten | Daten zum Sexualleben oder sexuellen  Orientierung | Strafrechtliche Verurteilung / Straftaten | |

# Kategorien betroffener Personen

Es werden personenbezogene Daten folgender Datensubjekte verarbeitet:

|  |  |  |
| --- | --- | --- |
| Beschäftigte | Pensionäre | Auszubildende, Praktikanten, Werkstudenten |
| Externe Bewerber | Privatkunden | Mitarbeiter von Kunden |
| ehemalige Kunden | Interessenten | Ansprechpartner, Kontaktpersonen von Lieferanten/Dienstleistern |
| Website-Besucher | Handelsvertreter | Leiharbeiter |
| Kinder | Newsletter-Abonnenten |  |

Sonstige Personengruppen: **Bitte geben Sie die weiteren Personengruppen an, soweit zutreffend.**

# Technische und organisatorische Maßnahmen

Der Auftraggeber und der Auftragsnehmer haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten.

Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

* die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
* die **Verfügbarkeit** der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können und
* die regelmäßige **Überprüfbarkeit, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sichergestellt ist.

Der Auftragnehmer hat folgende Maßnahmen ergriffen:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SZ** | **Datenschutzkontrollen** | **ISO27001** | **Bemerkung** | **Anforderungen erfüllt und ggf. Doku. beigefügt** |
| V | Verfügbarkeitskontrolle | A12.2,3,7, A16.1, A17.2 | Betriebssicherheit, Sicherheitsvorfälle, Notfallkonzept | Ja  : \_\_\_\_\_\_\_\_ |
| V | Wiederherstellbarkeit | A12,1,2,3,  A16.1 | Betriebssicherheit, Sicherheitsvorfälle | Ja  : \_\_\_\_\_\_\_\_ |
| T | Zutrittskontrolle | A11.1. | Sicherheitszonen | Ja  : \_\_\_\_\_\_\_\_ |
| T | Zugangskontrolle | A9.1, A9.2, A9.3 | Zugangskontrolle | Ja  : \_\_\_\_\_\_\_\_ |
| T | Zugriffskontrolle | A7.3, A9.1, A9.2, A9.4 | Beendigung Arbeitsverhältnis, Benutzerzugriff | Ja  : \_\_\_\_\_\_\_\_ |
| T | Benutzerkontrolle | A6.2,A9.2, | Mobile Geräte, Benutzerzugriff | Ja  : \_\_\_\_\_\_\_\_ |
| T | Trennbarkeit | A6.1, A7.2, A8.2, A9.1 | Interne Organisation, Personensicherheit, Klassifizierung, Benutzerzugriff | Ja  : \_\_\_\_\_\_\_\_ |
| Legende: SZ = Schutzziel, V = Verfügbarkeit, T = Vertraulichkeit, I = Integrität, A12.7 … Kontrolle, mehrmals vorhanden | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SZ** | **Datenschutzkontrollen** | **ISO27001** | **Bemerkung** | **Anforderungen erfüllt und ggf. Doku. beigefügt** |
| T, I | Datenträgerkontrolle | A8.3, A10.1 | Media-Handling, Verschlüsselung | Ja  : \_\_\_\_\_\_\_\_ |
| T, I | Speicherkontrolle | A8.2, A9.2 | Information-Klassifizierung, Benutzerzugriff | Ja  : \_\_\_\_\_\_\_\_ |
| I | Eingabekontrolle | A9.2, A12.4 | Benutzerzugriff, Logging und Monitoring | Ja  : \_\_\_\_\_\_\_\_ |
| I | Übertragungskontrolle | A8.2, A13.2, A14.1 | Information-Klassifizierung, Transfer, System Beschaffung, Entwicklung und Wartung | Ja  : \_\_\_\_\_\_\_\_ |
| I | Zuverlässigkeit | A11.2, A12.7, A17.2 | Verlust, Betriebssicherheit, Notfallkonzept | Ja  : \_\_\_\_\_\_\_\_ |
| I | Datenintegrität | A11.2, A12.1 | Verlust, Betriebssicherheit | Ja  : \_\_\_\_\_\_\_\_ |
| I | Auftragskontrolle | A7.1,2, A8.2, A12.1,2, A15.1,2, A18.1 | Personalsicherheit, Klassifizierung, Betriebssicherheit, Lieferantensicherheit, Compliance | Ja  : \_\_\_\_\_\_\_\_ |
|  | Belastbarkeit der Systeme | A11.2, A12.1, A14.2 | Verlust, Betriebssicherheit, Sicherheit im Entwicklungsprozess | Ja  : \_\_\_\_\_\_\_\_ |
|  | Wirksamkeit der TOMs | A5.1, A12.7, A18.2 | Richtlinien, Betriebssicherheit, Überprüfung der Sicherheit | Ja  : \_\_\_\_\_\_\_\_ |
| Legende: SZ = Schutzziel, V = Verfügbarkeit, T = Vertraulichkeit, I = Integrität, A12.7 … Kontrolle, mehrmals vorhanden | | | | |

# Weisungsberechtigte Personen und Weisungsempfänger des Auftragnehmers

**Weisungsberechtigte Personen des Auftraggebers:**

Ansprechpartner auf Seiten des Auftraggebers:

Funktion:

Name:

E-Mail:

Fax:

Telefon:

Weiterer Ansprechpartner:

Name:

E-Mail:

Telefon:

**Weisungsempfänger des Auftragnehmers:**

Ansprechpartner auf Seiten des Auftragnehmers:

Funktion:

Name:

E-Mail:

Fax:

Telefon:

sowie als Vertretung:

Name:

E-Mail:

Telefon:

# Genehmigte Unterauftragnehmer

Der Auftraggeber stimmt der Beauftragung der unten genannten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung zwischen Auftragnehmer und Unterauftragnehmer nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO sowie unter Berücksichtigung der Ziffern 2.7.4. und 2.7.5. des Rahmenvertrags mit Abschluss dieser Vereinbarung zu.

Folgende Unterauftragnehmer dürfen vom Auftragnehmer eingesetzt werden und werden vom Auftraggeber genehmigt:

|  |  |  |
| --- | --- | --- |
| **Unterauftragnehmer**  (Name, Rechtsform, Sitz, Land) | **Ort der**  **Verarbeitungstätigkeit** | **Aufgabenbereich/Beschreibung der ausgelagerten Leistung** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Name in Druckschrift einfügen]

[MAHLE Gesellschaft einfügen]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Name in Druckschrift einfügen]

[MAHLE Gesellschaft einfügen]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Name in Druckschrift einfügen]

[Firma Dienstleister einfügen]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Name in Druckschrift einfügen]

[Firma Dienstleister einfügen]