MAH Schliesstechnik Hessen GmbH

Vereinbarung zur Auftragsdatenverarbeitung gemäß Art. 28 DS-GVO (EU Verordnung 2016/679 - Datenschutz-Grundverordnung)

zwischen

_____ (Verantwortlicher, nachfolgend Auftraggeber)

und

MAH Schliesstechnik Hessen GmbH (Auftragsverarbeiter, nachfolgend Auftragnehmer)

§ 1 Vertragsgegenstand

a) Diese Vereinbarung gilt für die Auftragsdatenverarbeitung durch den Auftragnehmer für den Auftraggeber im Hinblick auf alle beim Auftragnehmer zum Einsatz kommenden Systeme und Datenbanken.

b) Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftragnehmers den schriftlichen Auftrag zur Auftragsdatenverarbeitung i.S.d. § 11 BDSG bzw. den Vertrag i.S.d. Art. 28 der Verordnung (EU) 2016/679 - Datenschutz-Grundverordnung (EU DSGVO) und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung. Sofern in diesem Vertrag der Begriff "Datenverarbeitung" oder "Verarbeitung" (von Daten) benutzt wird, wird die Definition der "Verarbeitung" i.S.d. Art. 4 Nr. 2 EU DSGVO zugrunde gelegt. Soweit das BDSG hier im Vertrag erwähnt wird, sind diese Erwähnungen nur noch bis zum Ablauf des 24.05.2018 zu berücksichtigen. Ab dem 25.05.2018 gelten dann die insoweit vorgenommenen Erwähnungen der EU DSGVO in diesem Vertrag.

c) Diese Vereinbarung ersetzt ab dem Datum ihres Wirksamwerdens alle früheren zwischen den Vertragspartnern getroffenen Vereinbarungen zur Auftragsdatenverarbeitung.

d) Der Auftragnehmer verarbeitet personenbezogene und andere Daten im Auftrag des Auftraggebers. Die Auftragsdatenverarbeitung bezieht sich auf die folgenden personenbezogenen Daten (nachfolgend gemeinsam bezeichnet als "ADV-Daten") und gilt für den direkten Zugriff auf die Daten vor Ort sowie den sogenannten Fernzugriff (remote):

Für die ADV-Daten fungiert der Auftraggeber als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften. Hierbei handelt es sich um:

Daten, die der Auftraggeber oder dessen Mitarbeiter selbst in die Systeme eingegeben haben
Daten, die aus dem individuellen Verhalten des Auftraggebers oder von dessen Mitarbeitern resultieren
insbesondere Daten zur individuellen Nutzung von Systemen und Anlagen
Vertragsdaten und Zutritts-Berechtigungsdaten

Daten, die sich allgemein auf das Bestehen, den Vollzug und die Abrechnung von laufenden oder noch nicht vollständig abgewickelten Verträgen des Auftraggebers beziehen, insbesondere Daten zum Vertragsbeginn, zum Vertragsende, etc., sowie die zugehörigen Vertragsdokumente und Abrechnungen, sind keine ADV-Daten. Der Auftragnehmer ist Verantwortlicher für die Verarbeitung dieser Daten in den genannten Systemen.

§ 2 Art, Umfang, Zweck und Laufzeit der Auftragsdatenverarbeitung

a) Der Auftragnehmer erhebt, verarbeitet und nutzt die ADV-Daten im Auftrag und nach dokumentierter Weisung des Auftraggebers i.S.v. § 11 BDSG, mit Wirkung ab 25.05.2018 i.S.v. Art. 28 DSGVO (im Folgenden: "Auftragsverarbeitung").
b) Die Erhebung, Verarbeitung und Nutzung der ADV-Daten im Rahmen der Auftragsverarbeitung erfolgt entsprechend der in dieser Ergänzungsvereinbarung enthaltenen Festlegungen und bezieht sich auf die hier festgelegte Art der ADV-Daten und den mit dieser Vereinbarung bestimmten Kreis der Betroffenen.
c) Der Zweck der Datenerhebung und -verarbeitung liegt allein in der durch den Auftraggeber fallspezifisch explizit beauftragten Wartung oder Reparatur von Datenbanken oder Systemen. Der Auftragnehmer hat im Normalbetrieb keinerlei Zugriff auf Daten des Auftraggebers.
d) Die Erhebung, Verarbeitung und Nutzung der ADV-Daten findet ausschließlich auf deutschem Staatsgebiet, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU DSGVO erfüllt sind.
e) Die Laufzeit dieser Ergänzungsvereinbarung entspricht der Laufzeit der Vereinbarung bezüglich der zur Anwendung kommenden oben genannten Systeme und Datenbanken. Eine Beendigung der Vereinbarung zur Nutzung der oben genannten Systeme bewirkt automatisch auch eine Beendigung dieser Ergänzungsvereinbarung zum selben Zeitpunkt. Wird der Vertrag zur Nutzung der genannten Datenbanken und Systeme durch einen Nachfolgevertrag ersetzt, gilt diese Ergänzungsvereinbarung auch als Teil des Nachfolgevertrags, ohne dass sie neu vereinbart werden muss. Eine isolierte Kündigung dieser Ergänzungsvereinbarung ist ausgeschlossen.

Das angemessene Schutzniveau des Auftragnehmers:

=> wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 EU DSGVO)
=> wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d EU DSGV/0)
=> wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 EU DSGVO)

Arten der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien

=> Personenstammdaten
=> Kommunikationsdaten (z.B. Telefon, E-Mail)
=> Vertragsstammdaten {Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
=> Kundenhistorie
=> Vertragsabrechnungs- und Zahlungsdaten
=> Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
=> Alle Daten die im Rahmen der Nutzung der LSM Software von SimonsVoss benötigt werden

Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

=> Kunden
=> Interessenten
=> Beschäftigte
=> Lieferanten
=> Ansprechpartner

§ 3 Weisungsbefugnisse des Auftraggebers

a) Der Auftragnehmer verwendet die ADV-Daten ausschließlich in Übereinstimmung mit den dokumentierten Weisungen des Auftraggebers, auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. Die Weisungen ergeben sich im Übrigen aus der Nutzungsvereinbarung zu den genannten Systemen und der durch den Auftraggeber vorgenommenen Einstellung und Konfiguration des Dienstes. Einzelweisungen nach Abschluss des Vertrages bedürfen der Textform und der Auftraggeber hat sie, falls der Auftragnehmer dies anfordert, schriftlich zu bestätigen.
b) Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, bedarf dies der Zustimmung durch den Auftragnehmer. Etwaige durch die Befolgung einer solchen Weisung entstehende Aufwände vergütet der Auftraggeber gern. § 14.
c) Der Auftragnehmer wird den Auftraggeber darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

§ 4 Pflichten des Auftraggebers

a) Der Auftraggeber ist für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der ADV-Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Erhebung, Verarbeitung oder Nutzung von ADV-Daten Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.
b) Der Auftraggeber ist Inhaber aller etwaigen erforderlichen Rechte, die die ADV-Daten betreffen.
c) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer oder seiner Weisungen feststellt.

§ 5 Pflichten des Auftragnehmers

a) Der Auftragnehmer stellt sicher, dass die Datenverarbeitung und -nutzung in seinem Verantwortungsbereich, der Unterauftragnehmer nach § 11 dieser Ergänzungsvereinbarung einschließt, in Übereinstimmung mit den Bestimmungen dieser Ergänzungsvereinbarung erfolgt.
b) Der Auftragnehmer unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde im Rahmen des Zumutbaren und Erforderlichen, soweit diese Kontrollen die Datenverarbeitung durch den Auftragnehmer betreffen. Er wird dem Auftraggeber die Informationen zur Verfügung stellen, die dieser benötigt, um nachzuweisen, dass er hinsichtlich dieser Auftragsverarbeitung die Anforderungen des anwendbaren Datenschutzrechts erfüllt hat.
c) Sofern der Auftragnehmer seine Datenverarbeitung zertifizieren lässt, stellt er dem Auftraggeber auf Anforderung eine Kopie des jeweils aktuellen Zertifikats zur Verfügung. Darüber hinaus wird der Auftragnehmer Überprüfungen - einschließlich Inspektionen - die vom Auftraggeber oder einem von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und dazu beitragen. Der Auftraggeber wird höchstens einmal im Jahr eine Überprüfung oder Inspektion durchführen, es sei denn, der Auftraggeber hat konkrete Anhaltspunkte dafür, dass die Datenverarbeitung nicht im Einklang mit den gesetzlichen Vorschriften oder dieser Ergänzungsvereinbarung erfolgt.
d) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen auf Anforderung bei der Einhaltung der folgenden Pflichten:

(i) Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten,
(ii) Meldung der Verletzung des Schutzes personenbezogener Daten an Aufsichtsbehörden und betroffene Personen und, sofern die Auftragsverarbeitung durch den Auftragnehmer davon betroffen ist,
(iii) Durchführung einer Datenschutzfolgenabschätzung sowie
(iv) Durchführung einer erforderlichen vorherigen Konsultation der Datenschutzbehörde

e) Der Auftragnehmer hat die bei der Verarbeitung von ADV-Daten beschäftigten Personen auf den vertraulichen Umgang mit den verarbeiteten personenbezogenen Daten zu verpflichten (Datengeheimnis). Der Auftragnehmer wird gewährleisten, dass diese Pflicht auch durch etwaige Unterauftragnehmer eingehalten wird. Die Vertraulichkeit bezüglich der auf Basis dieser Vereinbarung verarbeiteten Daten gilt über die Kündigung oder anderweitig initiierte Beendigung dieser Vereinbarung hinaus auf unbestimmte Zeit.

f) Der Auftragnehmer wird einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten bestellen, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind.

g) Der Auftraggeber vergütet die Unterstützung oder Mitwirkung des Auftragnehmers nach nach Aufwand gemäß § 14.

§ 6 Technische und organisatorische Maßnahmen §64 BDSG {neu) und Art 28 und 32 DSGVO

a) Der Auftragnehmer hat vor Beginn der Verarbeitung der ADV-Daten die in Anlage 1 dieser Ergänzungsvereinbarung aufgelisteten technischen und organisatorischen Maßnahmen zu implementieren und während der Laufzeit aufrechtzuerhalten.

b) Es ist dem Auftragnehmer gestattet, alternative und adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in Anlage 1 festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer wird solche Änderungen dokumentieren. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers und sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

c) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

d) Der Auftragnehmer hat die Sicherheit gern. Art. 28 Abs. 3 lit. c, 32 EU DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 EU DSGVO zu berücksichtigen. 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.

e) Spätestens ab dem 25.05.2018 wird der Auftragnehmer dem Auftraggeber die von ihm nach Art. 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen zur

Gewährleistung des nach Art. 32 EU DSGVO und des in diesem Vertrag geregelten Schutzniveaus in dokumentierter Form und in geeigneter Weise zur Verfügung stellen.

§ 7 Berichtigung, Einschränkung und Löschung von Daten

a) Der Auftragnehmer wird die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

b) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 8 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 EU DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten nach § 38 BDSG (neu), der seine Tätigkeit gemäß Art. 38 und 39 EU DSGVO ausübt. Als Datenschutzbeauftragte ist beim Auftragnehmer Rechtsanwältin Friederike Scholz bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b, 29, 32 Abs. 4 EU DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftraggeber unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 lit. c, 32 EU DSGVO.

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der

Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse.

§ 9 Mitzuteilende Verstöße des Auftragnehmers

a) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der EU DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.

   Hierzu gehören u.a.

   die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

   die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

   die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihr in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

   die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

   die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

b) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber ab dem 25.05.2018 eine Meldepflicht nach Art. 33 EU DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei entsprechenden Meldepflichten unterstützen.

c) Der Auftragnehmer informiert den Auftraggeber, wenn ihm eine Verletzung des Schutzes personenbezogener Daten im Rahmen der Auftragsverarbeitung bekannt wird.

d) Soweit den Auftraggeber aufgrund eines Vorkommnisses gesetzliche Informationspflichten wegen einer unrechtmäßigen Kenntniserlangung von ADV-Daten treffen, hat der Auftragnehmer den Auftraggeber bei der Erfüllung der Informationspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen zu unterstützen. Die Mitwirkung ist

vergütungspflichtig, es sei denn die Verletzung beruht auf einem Verschulden des Auftragnehmers.

§ 10 Kontrollrechte des Auftraggebers

a) Der Auftraggeber überzeugt sich auf eigene Kosten vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß Anlage 1 und dokumentiert das Ergebnis. Dies geschieht durch Einholung einer Selbstauskunft des Auftragnehmers, die dieser auch durch Vorlage eines geeigneten Zertifikats eines Sachverständigen erfüllen kann.
b) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.
c) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.
d) Aufwände des Auftragnehmers bei der Durchführung der Kontrollen vergütet der Auftraggeber gern. § 14.

§ 11 Unterauftragsverhältnisse

a) Der Auftragnehmer darf Unterauftragsverhältnisse hinsichtlich der Verarbeitung oder Nutzung von ADV-Daten begründen. Dies gilt insbesondere für die Einschaltung der nach §§ lSff. AktG mit dem Auftragnehmer verbundenen Unternehmen
b) Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern informieren. Der Auftraggeber kann die Zusatzvereinbarung zum Zeitpunkt des Wirksamwerdens der Änderung kündigen.
c) Der Auftragnehmer wird die Pflichten nach dieser Ergänzungsvereinbarung an seine Unterauftragnehmer weitergeben, einschließlich der Gewährleistung angemessener technisch-organisatorischer Maßnahmen. Diese müssen den Anforderungen des anwendbaren Datenschutzrechts entsprechen.
d) Der Auftragnehmer wird mit allen Unterauftragnehmern Geheimhaltungsvereinbarungen treffen, soweit diese nicht bereits einer entsprechenden gesetzlichen Geheimhaltungspflicht unterliegen.

§ 12 Rechte der Betroffenen

a) Die Rechte der durch die Verarbeitung von ADV-Daten betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen.
b) Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Auskunft, Berichtigung, Löschung oder Sperrung der ihn betreffenden Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.
c) Für den Fall, dass eine betroffene Person ihre datenschutzrechtlichen Rechte geltend macht, wird der Auftragnehmer den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung dieser Ansprüche in angemessenem und für den Auftraggeber erforderlichen Umfang unterstützen, sofern der Auftraggeber die Ansprüche nicht ohne Mitwirkung des Auftragnehmers erfüllen kann.
d) Der Auftragnehmer wird es dem Auftraggeber ermöglichen, ADV-Daten zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Löschung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.
e) Aufwände des Auftragnehmers bei der Erfüllung der Pflichten nach diesem Abschnitt, die über den üblichen Leistungsumfang hinausgehen, vergütet der Auftraggeber gern. § 14.

§ 13 Rückgabe und Löschung überlassener Daten und Datenträger und personenbezogener Daten

a) Der Auftragnehmer hat sämtliche ADV-Daten nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung der Vereinbarung) zu löschen und von dem Auftraggeber erhaltene Datenträger, die zu diesem Zeitpunkt noch ADV-Daten enthalten, an den Auftraggeber zurückzugeben, soweit dem nicht vertragliche oder gesetzliche Aufbewahrungspflichten entgegenstehen
b) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.
c) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
d) Die Vertraulichkeit bezüglich der auf Basis dieser Vereinbarung verarbeiteten Daten gilt über die Kündigung oder anderweitig initiierte Beendigung dieser Vereinbarung hinaus auf unbestimmte Zeit.

§ 14 Vergütungspflicht

a) Sofern der Auftraggeber die Leistungen des Auftragnehmers nach dieser Vereinbarung zu vergüten hat, vergütet er die Aufwände des Auftragnehmers nach Zeit- und Materialaufwand.
b) Vorbehaltlich anderer Vereinbarungen gilt für die Vergütung von Arbeitskräften des Auftragnehmers ein pauschaler Stundensatz i.H.v. 110 EUR pro Stunde zuzüglich gesetzlicher Umsatzsteuer. Materialaufwand und Reisekosten rechnet der Auftragnehmer gegenüber dem Auftraggeber in der tatsachlich entstandenen Höhe zzgl. Umsatzsteuer ab. Sollte der Auftragnehmer einen höheren Kostenaufwand nachweisen können, kann er den höheren Betrag abrechnen.

§ 15 Kündigung

a) Diese Vereinbarung kann von beiden Parteien mit einer Frist von vier Wochen zum Ende eines Monats gekündigt werden.
b) Beide Vertragspartner können diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, sofern ein schwerwiegender Verstoß des jeweils anderen Vertragspartners gegen die Bestimmungen dieses Vertrages vorliegt.

§ 16 Schlussbestimmungen

Die mit dieser Vereinbarung getroffenen Regelungen zum Themenkreis der Datenschutz Grundverordnung umfassen explizit auch die in Artikel 82 DSGVO gefassten Regelungen zu Haftung und Recht auf Schadenersatz. Für Nebenabreden ist die Schriftform erforderlich.

Verfahrensänderungen bezüglich dieser Vereinbarung sind zwischen beiden Parteien abzustimmen und bedürfen einer von beiden Parteien schriftlich vereinbarten Genehmigung.

Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____

Ort, Datum, Unterschrift - Auftraggeber/ Verantwortlicher

_____

Ort, Datum, Unterschrift -Auftragnehmer/ Verarbeiter (MAH Schliesstechnik Hessen GmbH)

Anlage 1: Technische und organisatorische Maßnahmen

Anlage 1: Technische und organisatorische Maßnahmen

Beim Auftragnehmer wurde ein umfassendes Datensicherungskonzept realisiert, das sowohl in baulicher, personeller und organisatorischer als auch in technischer Hinsicht die erforderlichen Vorkehrungen enthält, um die Sicherheit der Objekte und des Datenbestandes sowie den ungestörten Betriebsablauf in optimaler Weise zu gewährleisten.

folgende technische und organisatorische Maßnahmen sind getroffen:

Vertraulichkeit {Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle: Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden.

=> Regelungen zur Zutrittskontrolle
=> Sicherheitsbereiche sind klar definiert und wenige Zugangswege vorhanden
=> Entsprechende Ausgestaltung der Maßnahmen zur Objektsicherung (z. B. Spezialverglasung, Absicherung von Schächten, Brandschutz, etc.)
=> Türsicherung (elektronische Türschließer, Ausweisleser, Fernsehmonitor, Empfang)
=> Gesicherter Eingang für An- und Ablieferung (Kontrolle vor Eintritt zu den Zugangspunkten; Trennung von informationsverarbeitenden Systemen)
=> Festlegung befugter Personen (Betriebsangehörige und Betriebsfremde)
=> Nutzung von Berechtigungsausweisen
=> Regelung für Firmenfremde
=> Nutzung von Besucherausweisen
=> Schlüsselregelung
=> Aufzeichnung der Zutrittszeiten bei Externen
=> Steuerung des gesamten Systems nur über die verantwortlichen Operator oder Mitarbeiter der Systemsteuerung
=> Gegenseitige Überwachung (4-Augen-Prinzip)

Zugangskontrolle: Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen.

=> Regelung der Benutzerberechtigung (Verwaltung inkl. Vergabe von Rechten, Vergabe von Sonderrechten, Entzug von Berechtigungen, regelmäßige Reviews)
=> Passwortrichtlinie (sichere Passwörter, regelmäßiger Wechsel, regelmäßige Reviews)
=> Differenzierte Zugriffsregelung z. B. durch Segmentzugriffssperren
=> Vergabe und Sicherung von Identifizierungsschlüsseln
=> Zuordnung einzelner Clients und Identifizierungsmerkmale ausschließlich für bestimmte Funktionen
=> Einsatz von Verschlüsselungsroutinen für Dateien
=> Einsatz von Verschlüsselungsroutinen für mobile Datenträger (inkl. Notebooks, USB-Sticks]
=> Authentisierung von Benutzern mit Fernzugriff (kryptografische Techniken, Hardware-identifikation, VPN-Lösungen)
=> Verpflichtung auf das Datengeheimnis nach Art 28 Abs. 3 lit. b DSGVO

=> Einsatz von Benutzercodes für Daten und Programme (PIN)
=> Kontrollierte Vernichtung von Datenträgern
=> Kontrollsysteme
=> Programmprüfungs- und Freigabeverfahren

Zugriffskontrolle: Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

=> Regelung der Zugriffsberechtigung (Differenzierte Berechtigungen über Profile, Rollen, Transaktionen, Objekte, zeitliche Begrenzung)
=> Bereitstellung angemessener Funktionen zur Authentisierung
=> Verschlüsselung
=> Überprüfung der Berechtigung, maschinell z. B. durch Identifizierungsschlüssel
=> Aufzeichnung von Protokollen (erfolglose und erfolgreiche Authentifizierungsversuche).
=> Richtlinien zur Pseudonymisierung von personenbezogenen Daten

Trennungskontrolle: Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

=> Mandantentrennung
=> Funktionstrennungen

Integrität (Art. 32 Abs. 1 lit. b DS-GVO}

Weitergabekontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

=> Leitlinien zum Austausch von Informationen aller Art
=> Verschlüsselung bei Datenübertragung (Netzwerkverschlüsselung, TLS, PGP]
=> Verfahren zur Erkennung und Schutz von Schadsoftware
=> Zugriff für bestimmte autorisierte Benutzer
=> Gesicherter RZ-Eingang für An- und Ablieferung
=> Verschlüsselung der Datenträger vor Transport
=> Ausgabe von Datenträgern nur an autorisierte Personen (z. B. Auftragsquittung, Begleitpapier)
=> Direktabholung, Kurierdienst, Transportbegleitung
=> Datenträger-Verwaltung
=> Bestandskontrolle
=> Festmontierte Plattenspeicher
=> Gesonderter Verschluss vertraulicher Datenträger
=> Gegenseitige Überwachung (4-Augen-Prinzip)

=> Regelung der Anfertigung von Kopien
=> Verbot der Mitnahme von Taschen und sonstigen Gepäckstücken in die Sicherheitsbereiche
=> Kontrollierte Vernichtung von Datenträgern (z. B. Fehldrucke)
=> Löschung von Datenresten vor Datenträgeraustausch

Eingabekontrolle: Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

=> Nachweis der organisatorisch festgelegten Zuständigkeiten für die Eingabe
=> Protokollierung von Eingaben
=> Verfahrens-, Programm- und Arbeitsablauforganisation
=> Verpflichtung auf das Datengeheimnis

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

Verfügbarkeitskontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

=> Geregelter Prozess zur Sicherstellung des Geschäftsbetriebes
=> Notfallpläne
=> Regelmäßige Back-Ups gemäß Back-Up-Plan
=> Absicherung der Systeme gegen Ausfall der Datenbank, Service-Level-Agreements mit den IT-Dienstleistern
=> Spiegeln von Daten
=> Virenschutz/Firewall
=> Redundante Hardware

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

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen

Auftragskontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

=> Schriftlicher Vertrag mit Festlegung der Weisungen
=> formalisierte Auftragserteilung
=> Sorgfältige Auswahl des Auftragnehmers
=> Kontrolle der ordnungsgemäßen Vertragsausführung
=> Funktionstrennung

=> Datenschutz-Management;
=> Incident-Response-Management;
=> Auftragskontrolle (siehe oben)

Weisungsberechtigte Personen im Sinne dieser Vereinbarung auf Seite des Auftragnehmers sind:

Marcel Henninger (Geschäftsführer-Gesellschafter)
Alberto Pereira (Gesellschafter)
Nicole Schettino (Leiterin Projekte)

Weisungsberechtigte Personen im Sinne dieser Vereinbarung auf Seite des Auftraggebers sind:

_____
_____
_____
_____

Bei einem Wechsel oder einer längerfristigen Verhinderung der oben genannten weisungsberechtigten Personen sind dem jeweils anderen Vertragspartner unverzüglich schriftlich die Nachfolger bzw. Vertreter mitzuteilen.