Technische und organisatorische Maßnahmen

gem. Art. 32 Abs. 1 Datenschutz Grundverordnung (DSGVO)
für Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

Angaben zum Auftragsverarbeiter

Name	WEMA Hard- und Software GmbH
Straße	Irlham 10
Postleitzahl	84371
Ort	Triftern

Handelsregister: Landshut HR B 4726
Sitz der Gesellschaft: Triftern, Deutschland

Telefon	08562 96997-0
E-Mail-Adresse	datenschutz@wema-gmbh.de
Internet-Adresse	www.wema-gmbh.de

Terminologie

Dieses Dokument verwendet die Terminologie und die Definitionen gemäß der Datenschutz-Grundverordnung (im Folgenden „DSGVO“ bezeichnet). Darüber hinaus bezeichnet

- **„Auftragnehmer“** den Auftragsverarbeiter gemäß den Angaben oben in diesem Dokument;
- **„Auftraggeber“** den Verantwortlichen gemäß DSGVO, der mit dem Auftragsverarbeiter einen Vertrag zur Auftragsverarbeitung vereinbart hat.

Zur Absicherung der Daten des Auftraggebers werden folgende technischen und organisatorischen Maßnahmen für die Systeme des Auftragnehmers verbindlich festgelegt:

1. Vertraulichkeit

a) Zutrittskontrolle

Hierunter fallen alle Maßnahmen, damit Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, auf denen personenbezogene Daten des Auftraggebers verarbeitet werden.

Zutrittskontrolle durch den Auftragnehmer:

- Unbefugte erlangen zu den technischen Einrichtungen keinen Zutritt. Nur durch die Geschäftsleitung autorisierte Personen erlangen nach persönlicher Legimitation Zugang und dies natürlich nur in Begleitung eines Mitarbeiters des Auftragnehmers.
- Die personenbezogenen Daten des Auftraggebers werden in den Büroräumen des Auftragnehmers gespeichert und/oder verarbeitet. Der Zugriff auf die personenbezogenen Daten erfolgt über die Arbeitsplatzrechner des Auftragnehmers. Der Zugriff auf die Arbeitsplatzrechner ist mit einem Benutzernamen und Passwort vor unbefugten Zugriffen geschützt. Weiterhin sind die Zugriffe von den Arbeitsplatzrechnern auf das Rechenzentrum ebenfalls mit einem gesonderten Benutzernamen und Passwort vor unbefugten Zugriffen geschützt.
- Der Zugang zu den Büroräumen ist nur für Mitarbeiter des Arbeitnehmers möglich. Alle separaten Büroräume sind mit einem normalen Türschloss verriegelt und können nur von den Mitarbeitern entriegelt werden. Die Außentüren besitzen außerdem ein Sicherheitsschloss. Jeder Mitarbeiter der einen Schlüssel besitzt ist dokumentiert und hat sich auf die Vertraulichkeit der Daten verpflichtet.
- Die Fenster der Büroräume im Erdgeschoß zur Gebäudeaußenseite sind durch Gitter gesichert, die durch Schrauben fest in der Wand verankert sind. Diese Fenster sind außerdem mit einem separaten Schloss verriegelt.
- Der Eingangsbereich zu den Büroräumen wird durch eine Außenkamera überwacht und bei Bewegung aufgezeichnet.
- Gebäudeschächte sind durch ein fest verankertes Gitter geschützt.

b) Zugangskontrolle

Hierunter fallen Maßnahmen, damit Unbefugte an der Benutzung der Datenverarbeitungsanlagen und Datenverarbeitungsverfahren gehindert werden.

Zugangskontrolle durch den Auftragnehmer:

- Auf Seiten des Auftragnehmers findet der Zugriff auf die Daten des Auftraggebers ausschließlich über Arbeitsplatzrechner statt, die nur mit Benutzername und Passwort entsperrt werden können.
- Alle Räume sind mit einem Schloss verriegelt. Die Außentüren sind mit einem Sicherheitsschloss vor unbefugtem Zugang geschützt.
- Der Zugriff von den Arbeitsplatzrechnern auf die Systeme erfolgt über ein geschütztes Netzwerk, welches von außen durch eine Firewall geschützt ist. Die eingesetzten Applikationen entsprechen dem aktuellen technischen Stand und die Übertragung erfolgt i. d. Regel verschlüsselt. Des Weiteren können Mitarbeiter nur auf Daten bzw. Applikationen entsprechend Ihrer Berechtigung zugreifen.

- Der Zugriff von außerhalb erfolgt durch eine gesicherte VPN-Verbindung. Für befugte Mitarbeiter wird ein separater Zugang bereitgestellt und Berechtigungen wurden entsprechend der benötigen Supporttätigkeiten eingerichtet.
- Zum Schutz vor Angriffen ist eine Anti-Virus Software von AVG auf allen PCs und Servern installiert und wird regelmäßig gewartet bzw. angepasst.
- Jegliche Datenträger werden, je nach Art, in einem separaten Raum verwahrt, der ebenfalls durch ein Türschloss abgesperrt ist. Mindestens ein separater Sicherungsdatenträger befindet sich in einem Bankschließfach, zu dem nur Mitarbeiter mit einer entsprechenden Berechtigung Zugriff haben.
- Die Datenträger werden nach neuer Verwendung vollständig von bereits bestehenden Daten gereinigt. Bei einer Weitergabe werden sämtliche Daten sicher und nicht wiederherstellbar gelöscht.
- Alle Mitarbeiter des Auftragnehmers haben sich auf die Vertraulichkeit der Daten verpflichtet.

c) Zugriffskontrolle

Hierunter fallen Maßnahmen, mit denen gewährleistet wird, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können.

- Die Mitarbeiter des Auftragnehmers haben Zugriff auf die Systeme, um Aufgaben der Wartung der Server, der Software, der Datenbestände und auch der Weiterentwicklung, Systemadministration und entsprechende Aufgaben erfüllen zu können. Dies aber nur, wenn es der Auftraggeber ausdrücklich wünscht. Die Freigabe erfolgt meist per Telefon oder E-Mail-Verkehr. Alle Mitarbeiter des Auftragnehmers haben sich auf die Vertraulichkeit der Daten verpflichtet.
- Die Zahl der Administratoren ist auf das Notwendigste reduziert und wird regelmäßig intern überprüft. Ebenso wird das Berechtigungskonzept nur durch Administratoren geprüft und ggf. überarbeitet.
- Die Datenträger werden nach neuer Verwendung vollständig von bereits bestehenden Daten gereinigt. Bei einer Weitergabe werden sämtliche Daten sicher und nicht wiederherstellbar gelöscht.
- Die vom Auftragnehmer genutzte WEMA-Warenwirtschaft protokolliert teilweise Änderungen und vollständig die Löschung von Datensätzen.
- Passwörter werden vom jeweiligen Mitarbeiter selbst vergeben. Es wurde daraufhin gewiesen, dass alle Passwörter komplex vergeben und regelmäßig geändert werden müssen.
- Dokumente, die personenbezogene Daten beinhalten, werden ausschließlich mit einem sicheren Aktenvernichter geschreddert, genauso wie CDs und DVDs.

d) Auftragskontrolle

Hierunter fallen Maßnahmen, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Auftragskontrolle durch den Auftragnehmer:

- Der Auftragnehmer führt in der Regel keine Änderungen an den personenbezogenen Daten des Auftraggebers durch. Änderungen erfolgen nur nach einer schriftlichen, mündlichen oder elektronischen Anweisung.
- Alle Mitarbeiter des Auftragnehmers haben sich auf die Vertraulichkeit der Daten verpflichtet.
- Die Kontrollrechte des Auftragnehmers und des Auftraggebers sind im Vertrag zur Auftragsverarbeitung klar geregelt.

e) Trennungskontrolle

Hierunter fallen alle Maßnahmen, die gewährleisten, dass die personenbezogenen Daten des Auftraggebers getrennt von anderen Kundendaten verarbeitet werden.

- Der Auftragnehmer trennt die personenbezogenen Daten des Auftraggebers mithilfe der eigenprogrammierten WEMA-Warenwirtschaft. Firmeninterne Daten des Auftraggebers werden in einer separaten Dokumentation geführt.
- Der Auftragnehmer stellt durch geeignete Maßnahmen (wie z.B. passwortgeschützte Zugänge, SSL-Verschlüsselung beim E-Mailverkehr, etc.) sicher, dass die Daten des Auftraggebers auf den Datenverarbeitungsanlagen nicht anderweitig durch nicht autorisierte Dritte verarbeitet werden können.
- Dokumente und Datenträger sind je nach ihrem Zweck in getrennten Räumen und zusätzlich in abschließbaren Schränken untergebracht. Es haben nur Mitarbeiter mit entsprechender Befugnis darauf Zugriff.
- Ein Berechtigungskonzept, sowie die Festlegung von Datenbankrechten wurden durch die Administratoren entsprechend erstellt und werden regelmäßig überprüft.

f) Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. A DS-GVO, Art. 25 Abs. 1 DS-GVO)

Damit die Zwecke der Auftragsverarbeitung erreicht werden können, ist eine Pseudonymisierung der personenbezogenen Daten nicht möglich.

Verschlüsselung auf den Systemen des Auftragnehmers

- Die persönlichen Daten des Auftraggebers werden in der Datenbank der genutzten Software vom Auftragnehmer größtenteils in Klartext gespeichert, mit Ausnahme des Passwortes. Das Passwort wird nur verschlüsselt gespeichert.
- Neben der Datenbank werden die Daten in einem Backup gespeichert. Auch dort bleibt die Verschlüsselung des Passwortes erhalten. Das Backup wird auf einem gesicherten NAS gespeichert, auf das ohne Kenntnis des Benutzers und Passworts kein Zugriff möglich ist.
- Der für den Zugriff erforderliche Benutzername und das Passwort sind lediglich den befugten Mitarbeitern des Auftragnehmers bekannt. Die Mitarbeiter wurden zur Vertraulichkeit verpflichtet.
- Die genutzte WEMA-Warenwirtschaft versendet Emails an die Nutzer der Software, sowie ggf. an den Auftraggeber. Der Auftragnehmer stellt sicher, dass der Email-Verkehr verschlüsselt über SSL/TLS (Secure Socket Layer / Transport Layer Security) stattfinden kann, sowohl beim Versand von Emails als auch beim Empfang von Emails. Damit werden Emails außerhalb der beteiligten Email-Verarbeitungssysteme des Auftraggebers und des Auftragnehmers abhör- und fälschungssicher. Damit der verschlüsselte Transport möglich ist, muss der Auftraggeber bei seinen Email-Systemen ebenfalls die verschlüsselte Kommunikation einstellen und ermöglichen. Der Auftraggeber ist somit dafür verantwortlich, die Transport-Verschlüsselung für den Email-Versand und –Empfang an seinen Email-Systemen bereitzustellen und aktuell zu halten.

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

a) Weitergabekontrolle

Hierunter fallen Maßnahmen, die sicherstellen, 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:

- Eine Weitergabe und Übermittlung personenbezogener Daten ist grundsätzlich nur im Rahmen vorliegender Weisung des Auftraggebers möglich. Eine Weitergabe zu Zwecken der Strafverfolgung ist nur bei Vorliegen eines richterlichen Beschlusses möglich. Der Auftraggeber wird darüber zeitnah informiert.
- Der E-Mail-Verkehr zwischen dem Auftragnehmer und den Auftraggeber ist über SSL/TLS (Secure Socket Layer / Transport Layer Security) verschlüsselt.
- Der Zugriff von außerhalb auf die Systeme des Auftraggebers erfolgt durch eine professionelle Fernwartungssoftware (TeamViewer). Die Verbindungen laufen über komplett gesicherte Datenkanäle, die mit einem 2048 Bit RSA Public-/Private Key Exchange aufgebaut und mit 256 Bit AES verschlüsselt sind.

b. Eingabekontrolle

Hierunter fallen Maßnahmen die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Der Auftragnehmer führt in der Regel keine Änderungen an den personenbezogenen Daten des Auftraggebers durch. Änderungen erfolgen nur nach einer schriftlichen, mündlichen oder elektronischen Anweisung.
- Die genutzte Software (WEMA-Warenwirtschaft) des Auftragnehmers protokolliert in verschiedenen Bereichen, wer/wann Änderungen vorgenommen hat.
- Bei dem Erstellen eines neuen Benutzerkontos protokolliert die vom Arbeitnehmer genutzte Software den Ersteller des Benutzerkontos, so dass nachträglich nachvollziehbar ist, wer das neue Benutzerkonto angelegt hat.
- Jeder Mitarbeiter hat nur je nach Benutzerrechte Zugriff auf Daten.
- Die eingesetzten Applikationen entsprechen dem aktuellen technischen Stand und die Übertragung erfolgt i. d. Regel verschlüsselt. Des Weiteren können Mitarbeiter nur auf Daten bzw. Applikationen entsprechend Ihrer Berechtigung zugreifen.

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

a. Verfügbarkeitskontrolle

Hierunter fallen Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Verfügbarkeitskontrolle durch den Auftragnehmer:

- Der Auftragnehmer führt nächtlich automatisiert ein Backup aller Daten durch, die er vom Auftraggeber dokumentiert hat. Das Backup wird automatisiert auf einem speziell für Datensicherungen vorgesehenen NAS kopiert. Auf das NAS hat nur der Auftragnehmer bzw. die Administratoren Zugriff.
- Durch die physische Trennung des Servers ist bei einem mit Datenverlust verbundenen Hardware- oder Softwareausfall die Verfügbarkeit der Daten durch das getrennt gespeicherte Daten-Backup gewährleistet.
- Es besteht in allen Büroräumen ein ausdrückliches Rauchverbot. Der Serverraum ist durch eine Feuerschutztür zusätzlich gesichert und in den Büroräumen ist ein Feuerlöschgerät bereitgestellt.
- Jeder Mitarbeiter hat nur je nach seiner Berechtigung Zutritt zu den jeweiligen Räumen. Die Schlüsselübergabe wurde protokolliert und alle Mitarbeiter haben sich auf die Vertraulichkeit der Daten verpflichtet.
- An allen Arbeitsplätzen ist eine unterbrechungsfreie Stromversorgung (USV) installiert, die regelmäßig überprüft wird.

b. Wiederherstellbarkeit

Hierunter fallen Maßnahmen, die sicherstellen, dass personenbezogene Daten bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

- Der Auftragnehmer setzt ein technisches Verfahren ein, mit dem der Datenbestand automatisiert und regelmäßig (alle 24 Stunden) auf einem von der Laufzeitumgebung physisch und logisch getrennten System gesichert wird. Im Falle eines physischen oder technischen Zwischenfalls auf dem System der Laufzeitumgebung können die Daten aus dem Backup-Server wiederhergestellt werden und dem Auftraggeber wieder zur Verfügung gestellt werden.

c) Löschkonzept

Hierunter fallen Maßnahmen, die sicherstellen, dass die richtigen personenbezogenen Daten zum richtigen Zeitpunkt gelöscht werden.

Artikel 17 der Verordnung enthält Vorgaben, wann personenbezogene Informationen zu löschen sind. Das ist laut Artikel 17, Absatz 1 dann der Fall, wenn

- *die Speicherung aus fachlichen Gründen nicht mehr notwendig ist,*
- *ein Betroffener seine Einwilligung zurückzieht, dass die Daten verarbeitet werden dürfen,*
- *ein Unternehmen oder eine öffentliche Einrichtung solche Informationen unrechtmäßig verarbeitet oder*
- *die Löschung "zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich" ist.*

Grundsätzlich werden keine Daten gelöscht, außer dies wird ausdrücklich vom Auftraggeber gewünscht oder einer der oben genannten Punkte tritt in Kraft.

Wenn Daten gelöscht werden, wird dies nach unserem Löschkonzept durchgeführt.

Backup Daten

Die Daten, die in der genutzten Software des Auftragnehmers gehalten werden (genauer: in einer Datenbank der Software) und auch die Daten, die zweckgetrennt auch außerhalb dieser Software gehalten werden, werden zur Sicherstellung der Verfügbarkeit und Wiederherstellbarkeit in einem Sicherungskonzept automatisiert und regelmäßig in einem Datenbackup gesichert.

4. Anpassung an den technischen Fortschritt

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.

Alle Mitarbeiter werden regelmäßig geschult und sind auf die Vertraulichkeit der Daten verpflichtet, auch über das Arbeitsverhältnis hinaus.