

# Datenschutzhandbuch

## Frank Mayer GbR Heizung-Sanitär-Solar

mit Datenschutzrichtlinie, Verzeichnis von Verarbeitungstätigkeiten,  
Verzeichnis Auftragsverarbeiter, Datensicherheitserklärungen u.a.

Frankenstr7  
89564 Nattheim

Ust-IdNr. : DE 337576444  
Gerichtsstand: IHR Gerichtsstand  
IHR Amtsgericht Heidenheim

**Geschäftszweck** Heizung/ Sanitär/ Solar

Handwerksbetrieb Frank Mayer GbR Geschäftsinhaber Frank Mayer und Joachim Mayer wird  
vertreten durch den Geschäftsführer Joachim Mayer hat insgesamt 1 Mitarbeiter.

Die Richtlinie mit Verfahrensverzeichnis wurde  
erarbeitet und realisiert im Dez.2020

Unterschrift Vertreter des Verantwortlichen  
Joachim Mayer

# Inhalt

	<b>Seite</b>
<b>1. Verantwortlicher</b>	1
<b>2. Zuständige Behörde</b>	3
<b>3. Aufbau und Form der Richtlinie</b>	4
<b>4. Grundsätze der Verarbeitung personenbezogener Daten und allgemeine TOM</b>	5
<b>5. Datensicherheit</b>	6
<b>6. Datenschutz-Folgenabschätzung</b>	7
<b>7. Mitarbeiter die personenbezogene Daten verarbeiten</b>	9
<b>8. Verzeichnis von Verarbeitungstätigkeiten</b> gem. Artikel 30 Abs. 1 DSGVO.	10
1. Personalverwaltung	11
2. Kunden/Lieferanten/Auftragsverwaltung	14
3. Werbemaßnahmen und Kundenakquise	19
4. Beauftragung von Lieferanten und Dienstleistern	21
5. Videoüberwachung	24
<b>9. Verzeichnis Auftragsverarbeitung</b> gem. Artikel 30 Abs. 2 DSGVO	27
<b>10. Datenschutzerklärung Internet</b>	33
<b>11. Anlage</b>	36
Verpflichtung auf die Vertraulichkeit gem. DSGVO Art. 32/Abs. 4 im Umgang mit personenbezogenen Daten – Datensicherheitserklärung (Muster)	37
Schriftliche Einwilligung gemäß Datenschutz (Muster)	38
Mitteilung einer unrechtmäßigen Datenübermittlung bzw. unrechtmäßigen Kenntniserlangung von Daten durch Dritte gemäß § 42a BDSG (bzw. § 15a TMG) an die Datenschutzaufsichtsbehörde	39
Auftragsverarbeitungsvertrag (Muster)	41
<b>Schulungsnachweise</b>	
<b>Verpflichtungen auf die Vertraulichkeit</b>	
<b>Auftragsverarbeitungsverträge</b>	
<b>Schriftliche Einwilligungen gemäß Datenschutz</b>	eigener Ordner
<b>EU-DSGVO</b> aus dem Amtsblatt der Europäischen Union	

## **1. Verantwortlicher im Sinne der EU-DSGVO Artikel 4 Absatz 7**

**Frank Mayer GbR Heizung-Sanitär-Solar**

Anschrift: Frankenstr.7 89564 Nattheim

Telefon: Tel.Nr.: 07321/521661, Fax: 07321/53973, Email: [f.mayer@heizung-solar-mayer.de](mailto:f.mayer@heizung-solar-mayer.de)

E-Mail Adresse und Telefon-Nr. sind auf unserer Homepage [www.heizung-solar-mayer.de](http://www.heizung-solar-mayer.de) veröffentlicht.

Der Vertreter des Verantwortlichen: **Joachim Mayer**

Ein **Datenschutzbeauftragter** ist aufgrund der Personenzahl die personenbezogene Daten verarbeiten und der Kategorie der personenbezogenen Daten die verarbeitet werden nicht bestellt.

## **2. Zuständige Behörde für die Meldung meldepflichtiger Ereignisse**

Zuständige Datenschutz-Aufsichtsbehörden:

Der Landesbeauftragte für den Datenschutz Baden-Württemberg

Königstraße 10a

70173 Stuttgart

Telefon: 07 11/61 55 41 - 0

Telefax: 07 11/61 55 41 - 15

E-Mail: [poststelle@lfd.bwl.de](mailto:poststelle@lfd.bwl.de)

Homepage: [www.baden-wuerttemberg.datenschutz.de](http://www.baden-wuerttemberg.datenschutz.de)

### 3. Aufbau und Form der Richtlinie

Die Datenschutzrichtlinie der **Firma Frank Mayer GbR** und das beinhaltete Verzeichnis von Verarbeitungstätigkeiten, das Verzeichnis Auftragsverarbeiter und die Datensicherheitserklärung befolgt Vorgaben der EU-DSGVO und des BDSG (neu). Ältere ISO Normen wie die 9001 oder 27001 kommen hier ausdrücklich nicht zur Geltung. Die **Heizung-Sanitär-Solar Firma Frank Mayer GbR** ist ein Kleinbetrieb ohne internationale Verflechtung oder Filialnetz. Es werden keine Hochrisikodaten verarbeitet, Adresshandel oder Profiling betrieben. Dementsprechend kommt das in der DSGVO benannte Gebot der Verhältnismäßigkeit zur Anwendung.

Die hier verwendeten Vorlagen und Formblätter für die Erstellung des Verzeichnis von Verarbeitungstätigkeiten, des Verzeichnis Auftragsverarbeiter, der Datensicherheitserklärung, des Auftragsverarbeitungsvertrag usw. wurden weitgehend von den veröffentlichten und allgemein zugänglichen Mustervorlagen der Landesämter für Datenschutz von Bayern, Baden Württemberg und Nordrhein-Westfalen übernommen. Auf deren sachliche Richtigkeit haben wir uns verlassen und befolgen im Weiteren die Vorgaben der DSGVO.

Da der Betrieb klein und die Zahl der Beschäftigten, die mit personenbezogenen Daten arbeiten ebenso klein ist, sich Tätigkeitsbereiche überschneiden und eine stringente Gliederung in Fachabteilungen nur rudimentär gegeben ist, werden die wichtigsten und in fast allen Abläufen wiederkehrenden Technisch Organisatorische Maßnahmen TOM zur praktischen Umsetzung der Erfordernisse der EU-DSGVO in den Absätzen 4. Grundsätze der Verarbeitung personenbezogener Daten und allgemeine TOM (Technisch organisatorische Maßnahmen), 5. Datensicherheit, 6. Datenschutz-Folgeabschätzungen und 7. Mitarbeiter die personenbezogene Daten verarbeiten zusammengefasst aufgeführt und erläutert. Auf diese TOM wird später in der Beschreibung der einzelnen Verarbeitungstätigkeiten Bezug genommen.

#### 4. Grundsätze der Verarbeitung personenbezogener Daten der **Heizung-Sanitär-Solar Firma Frank Mayer GbR** und allgemeine TOM (Technisch organisatorische Maßnahmen)

In allen Verfahren der Verarbeitung personenbezogener Daten werden die Bestimmungen der DSGVO und des BDSG (neu) befolgt und angewandt.

Sämtliche Mitarbeiter, die Zugang und Umgang mit personenbezogenen Daten haben werden regelmäßig sensibilisiert und fachlich geschult, sowie auf die Vertraulichkeit im Umgang mit den ihnen zugänglichen personenbezogenen Daten verpflichtet.

Sämtliche Verfahren der Verarbeitung personenbezogener Daten wurden und werden auf Ihre **Rechtmäßigkeit** überprüft, und die **Rechtsgrundlage** definiert, die Zweckbindung wird eingehalten, das Gebot der Datenminimierung berücksichtigt, regelmäßig deren Richtigkeit überprüft, die Grundsätze von Integrität und Vertraulichkeit berücksichtigt. Die Notwendigkeit der Datensicherung werden durch geeignete Maßnahmen gewährleistet.

Im Sinne der Wahrnehmung von **Betroffenenrechten** werden die Transparenz und die **Auskunfts- sowie Löschpflicht** unter Berücksichtigung der vorgegebenen Fristen eingehalten. Eine pflichtige Auskunft wird innerhalb von 30 Tagen geleistet. Die besonderen **Rechte Minderjähriger** berücksichtigt und wenn im Verarbeitungsprozess notwendig, die rechtsgültigen **Einwilligungen Betroffener** eingeholt, oder im Falle der Ablehnung der Verarbeitungsprozess nicht durchgeführt.

**Auftragsdatenverarbeiter** sind in einem eigenen Verzeichnis aufgeführt, die entsprechenden vertraglichen Vereinbarungen sind getroffen und werden regelmäßig auf ihre Aktualität und Vollständigkeit geprüft und im Bedarfsfall angepasst.

Die besonderen Verpflichtungen, die beim Transfer von personenbezogenen Daten ins **Ausland** zu berücksichtigen sind, sind bekannt und werden im Bedarfsfall eingehalten. Datenübermittlungen in Nicht-EU/Nicht-EWR-Staaten werden derzeit nicht durchgeführt. Sollte der Fall eintreten werden die notwendigen Vertragsdokumente entsprechend den Regelungen der DSGVO geprüft und angepasst.

Die Notwendigkeit zur **Meldung** meldepflichtiger Vorkommnisse ist bekannt und wird im Eintrittsfall vom Vertreter des Verantwortlichen oder dem von ihm bei Abwesenheit benannten Stellvertreter bei der zuständigen Meldebehörde innerhalb 72 Stunden durchgeführt.

## 5. Datensicherheit

Die Sicherheit der personenbezogenen Daten die in der **Heizung-Sanitär-Solar Firma Frank Mayer GbR** verarbeitet werden wird wie folgt gewährleistet:

### Digitale Daten

durch einen generellen **Passwortschutz** der hier eingesetzten PCs. An sämtlichen Arbeitsstationen werden sichere Zugangspassworte verwendet.

Auf jedem PC ist eine eigene **Firewall** aktiv (**Microsoft Defender**), zudem ein sich ständig selbst aktualisierendes **Antiviren Programm**, derzeit **Microsoft Defender**. Es stehen für jeden PC ausreichend Lizenzen zur Verfügung. Funktionalität und Aktualität werden laufend überprüft.

Der Internetzugang wird eigens durch eine **Firewall** im Router (**FritzBox 7490**) gesichert. Die hier integrierte Software wird laufend aktualisiert. Funktion und Aktualität werden in einem permanenten Prozess geprüft.

Die **Firma Frank Mayer GbR Heizung- Sanitär-Solar** verwendet für die Speicherung der von ihr verwendeten personenbezogenen Daten einen **Server**. Dieser Server hat keinen eigenen Internetzugang und ist über die Benutzerverwaltung, die vom Verantwortlichen persönlich organisiert wird vor unerlaubten Zugriffen geschützt. Die Zugänge werden über Konten gesteuert, die mit sicheren Zugangspasswörtern vor unerlaubtem Zugriff geschützt werden. Auf den einzelnen Arbeitsstationen werden nur die Zugänge eingerichtet, die hier benötigt werden; dies wird regelmäßig auf Aktualität und Notwendigkeit geprüft. Dieser Server befindet sich in einem nur von der Geschäftsführung genutzten und mit Sicherheitsschloss gesicherten Büro.

Sämtliche Dateien mit personenbezogenen Daten werden täglich auf einem **Sicherungss - NAS** gesichert, der nur zu diesem Zweck eingesetzt wird und sich in einem nur von der Geschäftsführung genutzten und mit Sicherheitsschloss gesicherten Büro befindet.

### Analoge Daten

Die **Firma Frank Mayer GbR Heizung-Sanitär-Solar** verfügt über ein eigenes Aktenarchiv **im Hauptgebäudes**, in einem sicheren fest verschließbaren Raum. Zu diesem haben nur die Geschäftsführung und ausdrücklich dafür bestimmte, legitimierte und auf die Grundsätze des Datenschutzes verpflichtete Mitarbeiter Zugang. Den Schlüssel zu diesem Aktenraum verwahrt der Geschäftsführer.

Personenbezogenen Daten in Papierform, die für den täglichen Geschäftsbetrieb benötigt werden, sowie die Personalakten, sind alle in einem Büroraum untergebracht, der nur über

das Hauptbüro, in dem, wenn es geöffnet ist, immer einer der Geschäftsführer und/oder ein auf die Grundsätze des Datenschutzes verpflichtete Mitarbeiter anwesend ist. Der Raum verfügt über eine eigene Tür, die über ein Sicherheitsschloss verriegelt ist und nur im Bedarfsfall geöffnet wird. Alle Akten mit personenbezogenen Daten sind hier in einem immer verschlossenen Aktenschrank untergebracht, der nur im Bedarfsfall geöffnet wird. Den Schlüssel verwahrt die Geschäftsführung persönlich.

## 6. Datenschutz-Folgenabschätzung

Die **Firma Frank Mayer GbR Heizung-Sanitär-Solar** speichert und verarbeitet in keinem ihrer Verfahren Daten mit einem besonderen Risikopotential. Die im wesentlichen verwendeten Kategorien sind Name, Adresse, Telefon, e-mail Adresse und Bankdaten.

Die **Personaldaten** werden mit größter Sparsamkeit erhoben und verwaltet. Hier werden weder Daten besonderer persönlicher Neigung noch irgendwelcher persönlicher Information über Details von Erkrankungen, den Gesundheitszustand allgemein oder gesellschaftliche, politische oder private Aktivitäten gespeichert, lediglich Alter, Geschlecht und Religionszugehörigkeit, so wie die Adressen und betrieblich relevante Daten, wie Funktion, Gehalt und Arbeitszeitregelungen.

Bei den **Kunden und Lieferanten** werden als personenbezogene Daten Name, Adresse, Telefon, Fax, E-Mail, und Bankverbindung gespeichert. Dazu kommen gegebenenfalls projektbezogene Gesprächsnotizen und Rechnungs- sowie Gutschriftsbelege, in dem Maße und der Form, die von den Archivierungspflichten der Finanzbehörden vorgegeben werden.

Für **Auftragsverarbeiter** gilt dasselbe wie für Kunden und Lieferanten.

Bei eventuell verwendeten Adressen für Werbezwecke werden gemäß dem Gebot der Datensparsamkeit ausschließlich Name, Adresse, Branche, eigene Notizen und gegebenenfalls die e-mail Adresse und die damit verbundenen Einwilligungserklärungen zur Verwendung für unsere eindeutig definierten Werbezwecke gespeichert.

Ein **Algorithmen gestütztes Ranking** oder **Profiling** findet nicht statt.

Bei allen Änderungen oder Neuerungen der Verarbeitungen unter Bezug der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung die jeweilige Eintrittswahrscheinlichkeit und die Schwere berücksichtigen, um Datenschutz-Risiken für Rechte und Freiheiten natürlicher Personen zu ermitteln.

## **7. Mitarbeiter,**

die im Unternehmen die personenbezogenen Daten verarbeiten:

Frank Mayer

Joachim Mayer

### **Schulungs- und Sensibilisierungs-Maßnahmen**

In einem Mitarbeitergespräch am **19. Dez. 2020** wurde allen oben genannten Personen die Datenschutzrichtlinie der **Firma Frank Mayer GbR Heizung-Sanitär-Solar** übergeben und erklärt. Die Maßnahme wurde von Joachim Mayer den Vertreter des Verantwortlichen für Datenschutzfragen durchgeführt.

Weiter wurde jeder der benannten Personen die Schrift:  
Erste Hilfe zur Datenschutzgrundverordnung überreicht und aufgetragen, diese zu lesen.  
Die Überprüfung fand am **19.Dez. 2020** statt. Dabei wurde festgestellt, dass alle Beteiligten den Inhalt der Schrift erfasst und verstanden haben.

Da alle der oben genannten Personen in einem engen betrieblichen Kontakt stehen, werden Fragen des Datenschutzes regelmäßig im jeweils relevanten Fall besprochen und abgestimmt.

Die nächste Datenschutz bezogene Besprechung ist für den **11. Oktober 2021** vorgesehen.

Verpflichtung auf die Vertraulichkeit gem. DSGVO Art. 32/Abs. 4 sind die einzelnen rechtskräftig unterschriebenen Datenschutzverpflichtungserklärung und Bestätigungen an der Teilnahme der Schulungs- und Sensibilisierungs--Maßnahmen aufgeführt.

## 8. Verzeichnis von Verarbeitungstätigkeiten

Neue Verfahren werden mit Ihrer Inbetriebnahme in dieses Verzeichnis aufgenommen und bereits enthaltene Verfahren regelmäßig geprüft. Dafür ist der Vertreter des Verantwortlichen persönlich verantwortlich und gewährleistet dies durch seine Funktion als Geschäftsführer/Betriebsleiter. Sämtliche Neuerungen und relevante Veränderungen werden persönlich von ihm initiiert oder unterliegen seiner aktuellen Kenntnisnahme.

### Derzeit betriebene Verfahren:

1. Personalverwaltung	11
2. Kunden/Lieferanten/Auftragsverwaltung	14
3. Werbemaßnahmen und Kundenakquise	19
4. Beauftragung von Lieferanten und Dienstleistern	21

<b>Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher gem. Artikel 30 Abs. 1 DSGVO</b>	Vorblatt
<b>Angaben zum Verantwortlichen</b>	
Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc. Hauptniederlassung: <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein	
Name	Joachim Mayer
Straße	Frankenstr.7
Postleitzahl	89564
Ort	Nattheim
Telefon	07321 51661
E-Mail-Adresse	f.mayer.heizung-sanitaer@gmx.de
Internet-Adresse	www.heizung-solar-mayer.de
<b>Angaben zum Vertreter des Verantwortlichen</b>	
Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.	
Name	Frank Mayer
Straße	Frankenstr.7
Postleitzahl	89564
Ort	Nattheim
Telefon	07321 51661
E-Mail-Adresse	f.mayer.heizung-sanitaer@gmx.de

<b>Personalverwaltung</b>		Anlage
Datum der Anlegung:		Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse	Personalabteilung/Geschäftsführung  Joachim Mayer 07321 51661 j.mayer@heizung-solar-mayer.de	
Bezeichnung der Verarbeitungstätigkeit	Personalverwaltung	
Zwecke der Verarbeitung	Durchführung des Beschäftigtenverhältnisses, Durchführung von Bewerbungen, Erfüllung vertraglich und gesetzlicher Pflichten ggü. Beschäftigten und Bewerbern	
Beschreibung der Kategorien betroffener Personen	<input checked="" type="checkbox"/>	Beschäftigte
	<input checked="" type="checkbox"/>	Interessenten
	<input type="checkbox"/>	Lieferanten
	<input type="checkbox"/>	Kunden
	<input type="checkbox"/>	Patienten
	<input type="checkbox"/>	Sonstige:
Beschreibung der Datenkategorien	<input checked="" type="checkbox"/>	Adressdaten, Geburtsdatum, Bankverbindung, Steuermerkmale, Lohngruppe, Arbeitszeit, bisherige Tätigkeitsbereiche, Qualifikation,.
	<input checked="" type="checkbox"/>	Besondere Arten personenbezogener Daten: Religionszugehörigkeit, Krankmeldung, gesundheitliche Beeinträchtigung
	<input type="checkbox"/>	sonstige

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden	<input checked="" type="checkbox"/> intern Personalabteilung
	<input checked="" type="checkbox"/> extern Öffentliche Stellen: Sozialversicherungsträger, Finanzbehörden
Datenübermittlung	<input type="checkbox"/> Datenübermittlung findet nicht statt und ist auch nicht geplant <input checked="" type="checkbox"/> Datenübermittlung findet wie folgt statt: Telefonisch, postalisch <input type="checkbox"/> Drittland, Name: <input type="checkbox"/> internationale Organisation, Bezeichnung:
Nennung der konkreten Datenempfänger	Empfängerkategorie Buchhaltung, Lohn Steuerbüro <b>Russ Haible Kubina GMBH&amp;CO.KG</b>
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien	Bewerberdaten 6 Monate nach Ablehnung Beschäftigtendaten 10 Jahre nach Ausscheiden der/des Beschäftigten
Rechtsgrundlage der Verarbeitung	Art. 88 DSGVO und § 26 BDSG-neu
Dokumentation, dass die Verarbeitung für Betroffene transparent erfolgt.	Den Bewerbern und Beschäftigten wird die Datenschutzerklärung der Firma ausgehändigt, die Ihre persönlichen Rechte und den Umgang mit personenbezogenen Daten im Betrieb beschreibt.

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO  
Bemerkungen: *siehe TOM-Beschreibung*

Verantwortlicher \_\_\_\_\_ Datum 19. Dez. 2020 Unterschrift 

## **TOM Personalverwaltung**

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO

Bewerberdaten werden nicht auf elektronischem Wege übermittelt. / Werden direkt an die den/Personalverantwortlichen übermittelt. Die Personalverantwortlichen sind angehalten, die Daten nicht innerhalb des Unternehmens zu verschicken. Bewerberdaten werden nach 6 Monaten gelöscht.

Krankmeldungen werden direkt in einem verschlossenen Umschlag an den/die Personalverantwortliche übermittelt.

Personalakten werden in Papierform geführt und in verschlossenen, nur zuständigen Personen zugänglichen, Schränken aufbewahrt.


Beschäftigte die im Rahmen von Wartungsarbeiten Zugriff auf personenbezogene Daten von Kunden erhalten können dürfen sind gem. Art. 32 Abs. 4 DSGVO zur Verschwiegenheit verpflichtet worden.

Die weiteren hier angewandten Technische und organisatorische Maßnahmen sind in den Absätzen, 4. Grundsätze der Verarbeitung personenbezogener Daten und allgemeine TOM (Technisch organisatorische Maßnahmen), 5. Datensicherheit, 6. Datenschutz-Folgeabschätzung und 7. Mitarbeiter die personenbezogene Daten verarbeiten, beschrieben.

<b>2. Kunden/Lieferanten/Auftragsverwaltung</b>		Anlage
Datum der Anlegung:		Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse	Auftragsverwaltung/Geschäftsführung  Frank Mayer 07321/51661 f.mayer.heizung-sanitaer@gmx.de	
Bezeichnung der Verarbeitungstätigkeit	Auftragsverwaltung	
Zwecke der Verarbeitung	Durchführung von Aufträgen, Anlage von Kunden und Interessenten, Reklamationswesen,	
Beschreibung der Kategorien betroffener Personen	<input type="checkbox"/> Beschäftigte <input checked="" type="checkbox"/> Interessenten <input type="checkbox"/> Lieferanten <input checked="" type="checkbox"/> Kunden <input type="checkbox"/> Patienten <input type="checkbox"/> Sonstige:	
Beschreibung der Datenkategorien	<input checked="" type="checkbox"/> Name, Adressdaten, Bankverbindung, Steuermerkmale.  <input type="checkbox"/> Besondere Arten personenbezogener Daten: Religionszugehörigkeit, Krankmeldung, gesundheitliche Beeinträchtigung  <input type="checkbox"/> sonstige	

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden	<input checked="" type="checkbox"/> intern Auftragsverwaltung
	<input checked="" type="checkbox"/> extern Öffentliche Stellen: Finanzbehörden
Datenübermittlung	<input type="checkbox"/> Datenübermittlung findet nicht statt und ist auch nicht geplant <input checked="" type="checkbox"/> Datenübermittlung findet wie folgt statt: postalisch, email <input type="checkbox"/> Drittland, Name: <input type="checkbox"/> internationale Organisation, Bezeichnung:
Nennung der konkreten Datenempfänger	Empfängerkategorie Kunden, Interessenten
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien	Interessenten ohne Auftragsrealisierung werden nach 6 Monaten gelöscht.
Rechtsgrundlage der Verarbeitung	Art. 6 DSGVO
Dokumentation, dass die Verarbeitung für Betroffene transparent erfolgt.	Den Kunden und Interessenten wird die Datenschutzerklärung der Firma ausgehändigt, bzw. auf die Veröffentlichung auf unserer Homepage verwiesen, die Ihre persönlichen Rechte und den Umgang mit personenbezogenen Daten im Betrieb beschreibt.

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO  
Bemerkungen: *siehe TOM-Beschreibung*

19. Dez. 2020


Verantwortlicher                      Datum                      Unterschrift

## **TOM Kunden/Lieferanten/Auftragsverwaltung**

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO

Sämtliche personenbezogenen Kunden- und Lieferanten-Daten werden ausschließlich in dem Betriebsverwaltungsprogramm **Win CWS (Bizerba)** gespeichert und bearbeitet. Die **Firma Bizerba** verfügt seit dem 1. April 2018 über ein eigenes Datenschutz- und Datensicherungsmodul. **Dieses Modul hat eigens dafür programmierte Lösch-, Auskunfts- und Sicherungsfunktionalitäten.**

Mit der Selektions- und **Löschfunktion** lassen sich Kunden- und Lieferanten ermitteln, mit denen für einen beliebig bestimmten Zeitraum keine Geschäfte mehr getätigt wurden. Die so selektierten Adressen lassen sich dann aus den Adressbeständen löschen. So kann das **Recht auf Vergessenwerden** einfach umgesetzt werden. Einzelne Aufforderungen auf Löschung in den Datenbeständen lassen sich über die Adressverwaltung der Software direkt erfüllen. Für beide Prozesse sind die Geschäftsführer direkt verantwortlich.

Die **Auskunftspflicht** wird auch von diesem Modul unterstützt. So kann die Adresse einer Person, die Auskunft über ihre von der **Firma Frank Mayer GbR Heizung-Sanitär-Solar** gespeicherten Daten haben möchte, selektiert werden. Zu dieser Adresse kann dann ein Auszug der Daten im PDF-Format oder als reiner ASCII Text (um dem **Recht auf Datenübertragbarkeit** Folge leisten zu können), generiert werden. Dieser wird dann nach Überprüfung der Richtigkeit der Angaben, der Person persönlich ausgehändigt, oder per Briefpost oder per E-mail Anhang zugeschickt. Der E-Mail Anhang wird vorher mit der Software WINRAR in eine Archivdatei gepackt, die mit einem nur für diesen einzelnen Zweck generierten sechsstelligen Passwort geschützt, das mindestens eine Zahl, ein Sonderzeichen und einen Buchstaben in Großschreibung beinhaltet. Dieses Passwort wird dem Empfänger per sms, Fax oder telefonisch mitgeteilt.

Die **Aktualität und Richtigkeit** der personenbezogenen Daten wird durch die Aufforderung an alle Mitarbeiter gewährleistet, bei jedem aktiven Geschäftsprozess mit einem Kunden oder Lieferanten diese Daten abzugleichen (siehe Mitarbeiter Datensicherheitserklärung im Anhang).

Die Software **Win CWS (Bizerba)** verfügt über eine eigene Benutzerverwaltung, in der jeder Nutzer mit Zugangsname und sicherem Zugangspasswort legitimiert wird. Die legitimierten Mitarbeiter haben alle die betriebliche Datenschutz- und Datensicherheitserklärung erhalten, gelesen, verstanden und unterschrieben.

Mit dieser Zugangskennung haben die legitimierten Mitarbeiter Zugang zu den Programmfunktionen, die für den täglichen Geschäftsbetrieb in Ihrem Einsatzbereich notwendig sind. **Die Adressverwaltung als solche wird durch ein weiteres Passwort**

geschützt. Diese Passwörter sind nur der Geschäftsführung und den Mitarbeitern bekannt die aufgrund ihrer Tätigkeit Zugang zu diesen Daten benötigen.

In der Software **Win CWS (Bizerba)** werden dem Gebot der **Datensparsamkeit** folgend, nur die Daten erfasst, die für die jeweils notwendigen Geschäftsprozesse notwendig sind.

Für die **Geschäftsprozesse**, dem Formulieren von Angeboten, dem Verfassen von Auftragsbestätigungen, dem Schreiben von Rechnungen und Gutschriften, sowie dem Erstellen von Mahnschreiben wird bei der Bearbeitung eines entsprechenden Vorgangs aus den in der Software **Win CWS (Bizerba)** gespeicherten Adresstammdaten der relevante Adressatz über die Kundennummer oder einen Namensbestandteil gesucht, ausgewählt und dem Vorgang zugeordnet. Dabei werden nur die personenbezogenen Daten angezeigt und zur Verfügung gestellt, die für den jeweiligen Vorgang tatsächlich gebraucht werden.

Die weiteren hier angewandten Technische und organisatorische Maßnahmen sind in den Absätzen, 4. Grundsätze der Verarbeitung personenbezogener Daten und allgemeine TOM (Technisch organisatorische Maßnahmen), 5. Datensicherheit, 6. Datenschutz-Folgeabschätzungen und 7. Mitarbeiter die personenbezogene Daten verarbeiten, beschrieben.

<b>3. Werbemaßnahmen und Kundenakquise</b>		Anlage
Datum der Anlegung:		Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse	<b>Auftragsverwaltung/Geschäftsführung</b>  Frank Mayer Joachim Mayer 07321 51661 j.mayer@heizung-solar-mayer.de	
Bezeichnung der Verarbeitungstätigkeit	Auftragsverwaltung	
Zwecke der Verarbeitung	Durchführung von Aufträgen, Anlage von Kunden und Interessenten, Reklamationswesen,	
Beschreibung der Kategorien betroffener Personen	<input type="checkbox"/> Beschäftigte <input type="checkbox"/> Interessenten <input type="checkbox"/> Lieferanten <input checked="" type="checkbox"/> Kunden <input type="checkbox"/> Patienten <input type="checkbox"/> Sonstige:	
Beschreibung der Datenkategorien	<input checked="" type="checkbox"/> Name, Adressdaten  <input type="checkbox"/> Besondere Arten personenbezogener Daten: Religionszugehörigkeit, Krankmeldung, gesundheitliche Beeinträchtigung  <input type="checkbox"/> sonstige	

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden	<input checked="" type="checkbox"/> intern	Auftragsverwaltung
	<input type="checkbox"/> extern	
Datenübermittlung	<input checked="" type="checkbox"/>	Datenübermittlung findet nicht statt und ist auch nicht geplant Datenübermittlung findet wie folgt statt: postalisch, email Drittland, Name: internationale Organisation, Bezeichnung:
Nennung der konkreten Datenempfänger		Empfängerkategorie
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.		Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien		Kunden werden nach einem Jahr ohne Angebotsanfrage, Auftragserteilung oder Rechnungsstellung gelöscht
Rechtsgrundlage der Verarbeitung		Art. 6 DSGVO
Dokumentation, dass die Verarbeitung für Betroffene transparent erfolgt.		Den Kunden und Interessenten wird die Datenschutzerklärung der Firma ausgehändigt, bzw. auf die Veröffentlichung auf unserer Homepage verwiesen, die Ihre persönlichen Rechte und den Umgang mit personenbezogenen Daten im Betrieb beschreibt.

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO  
Bemerkungen: *siehe TOM-Beschreibung*

Verantwortlicher

Datum

Unterschrift

## **TOM Werbemaßnahmen und Kundenakquise**

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO

Wir verzichten völlig auf **Direktwerbung** uns nicht bekannter Firmen und Personen.

**Direktwerbung** findet ausschließlich bei Bestandskunden für Produkte und Dienstleistungen statt, die sie in gleicher, ähnlicher oder artverwandter Form in der Vergangenheit bereits bei uns bestellt haben. Wir informieren über die Weiterentwicklung und Neuerungen in diesen Produkten und Dienstleistungen. Wir weisen sie in der E-mail oder Briefpost auf ihr Widerspruchsrecht auch zu dieser Werbemaßnahme hin. Auf Telefonakquise verzichten wir vollständig.

Die weiteren hier angewandten Technische und organisatorische Maßnahmen sind in den Absätzen, 4. Grundsätze der Verarbeitung personenbezogener Daten und allgemeine TOM (Technisch organisatorische Maßnahmen), 5. Datensicherheit, 6. Datenschutz-Folgeabschätzungen und 7. Mitarbeiter die personenbezogene Daten verarbeiten, beschrieben.

4. Beauftragung von Lieferanten und Dienstleistern		Anlage
Datum der Anlegung:		Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse	<b>Auftragsverwaltung/Geschäftsführung</b>  Frank Mayer 07321 51661 f.mayer.heizung-sanitär@gmx.de	
Bezeichnung der Verarbeitungstätigkeit	Beauftragung von Lieferanten und Dienstleistern	
Zwecke der Verarbeitung	Auftragsvergabe an Lieferanten und Dienstleister	
Beschreibung der Kategorien betroffener Personen	<input type="checkbox"/> Beschäftigte <input type="checkbox"/> Interessenten <input checked="" type="checkbox"/> Lieferanten <input type="checkbox"/> Kunden <input type="checkbox"/> Patienten <input type="checkbox"/> Sonstige:	
Beschreibung der Datenkategorien	<input checked="" type="checkbox"/> Name, Adressdaten  <input type="checkbox"/> Besondere Arten personenbezogener Daten: Religionszugehörigkeit, Krankmeldung, gesundheitliche Beeinträchtigung  <input type="checkbox"/> sonstige	

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden	<input checked="" type="checkbox"/> intern Auftragsverwaltung
	<input checked="" type="checkbox"/> extern Öffentliche Stellen: Finanzbehörden
Datenübermittlung	<input type="checkbox"/> Datenübermittlung findet nicht statt und ist auch nicht geplant <input checked="" type="checkbox"/> Datenübermittlung findet wie folgt statt: postalisch, email <input type="checkbox"/> Drittland, Name: <input type="checkbox"/> internationale Organisation, Bezeichnung:
Nennung der konkreten Datenempfänger	Empfängerkategorie Öffentliche Stellen: Finanzbehörden
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien	Kunden werden nach einem Jahr ohne Angebotsanfrage, Auftragserteilung oder Rechnungsstellung gelöscht
Rechtsgrundlage der Verarbeitung	Art. 6 DSGVO
Dokumentation, dass die Verarbeitung für Betroffene transparent erfolgt.	Den Lieferanten wird die Datenschutzerklärung der Firma ausgehändigt, bzw. auf die Veröffentlichung auf unserer Homepage verwiesen, die Ihre persönlichen Rechte und den Umgang mit personenbezogenen Daten im Betrieb beschreibt.

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO  
Bemerkungen: *siehe TOM-Beschreibung*

19. Dez. 2010


---

Verantwortlicher
Datum
Unterschrift

## **TOM Beauftragung von Lieferanten und Dienstleistern**

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO

Dienstleister und Lieferanten, wie Elektriker, Maler, Putzdienst oder Paketboten haben durch unser Sicherungssystem keinerlei Zugriff auf personenbezogene Daten. Diese betreten unsere Räumlichkeiten ausschließlich in ständiger Anwesenheit der Geschäftsführer oder eines Mitarbeiters.

Personenbezogene Daten eines Dienstleisters werden ausschließlich in dem Maße erhoben, die für die Durchführung des jeweiligen Auftrags erforderlich sind, also Name, Adresse, Telefon, Fax, E-Mail. Endet die Geschäftsbeziehung, werden die Daten unter Berücksichtigung der vom Finanzamt vorgeschriebenen Aufbewahrungsfristen für Rechnungs- und Zahlbelege, nach 6 Monaten gelöscht.

Im Weiteren gelten die Regelungen, wie sie unter 2. Kunden/Lieferanten/Auftragsverwaltung beschrieben sind.

<b>5. Videoüberwachung</b>		Anlage
Datum der Anlegung:		Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse	Geschäftsführung  Joachim Mayer 07321 51661 j.mayer@heizung-solar-mayer.de	
Bezeichnung der Verarbeitungstätigkeit		
Zwecke der Verarbeitung		
Beschreibung der Kategorien betroffener Personen	<input type="checkbox"/> Beschäftigte <input type="checkbox"/> Interessenten <input type="checkbox"/> Lieferanten <input type="checkbox"/> Kunden <input type="checkbox"/> Patienten <input type="checkbox"/> Sonstige: Besucher	
Beschreibung der Datenkategorien	<input type="checkbox"/> <b>Videomaterial</b>  <input type="checkbox"/> Besondere Arten personenbezogener Daten: Religionszugehörigkeit, Krankmeldung, gesundheitliche Beeinträchtigung  <input type="checkbox"/> sonstige	



## **TOM Beauftragung Videoüberwachung**

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO

Eine Videoüberwachung findet zur Zeit nicht statt und befindet sich im Planungsstadium. Es sind auch keine entsprechenden Geräte oder Verbindungseinrichtungen installiert. Es werden daher noch keine personenbezogenen Daten verarbeitet.

<b>Übersicht von Verarbeitungstätigkeiten</b> <b>Auftragsverarbeiter</b> <b>gem. Artikel 30 Abs. 2 DSGVO</b>	Vorblatt
<b>Angaben zum Auftragsverarbeiter</b> Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc. Hauptniederlassung: <input type="checkbox"/> ja <input type="checkbox"/> nein  Name Straße Postleitzahl Ort Telefon E-Mail-Adresse Internet-Adresse	
<b>Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)</b> * sofern gem. Artikel 37 DS-GVO benannt Anrede, Titel  Name Straße Postleitzahl Ort Telefon E-Mail-Adresse	

<b>Angaben zum jeweiligen Auftraggeber</b>		Anlage
Unternehmen (Auftraggeber)	Name Straße Postleitzahl Ort Telefon E-Mail-Adresse Internet-Adresse	
Kategorien von Verarbeitungen (mit Erläuterung der jeweiligen Verarbeitung)	<input type="checkbox"/> Aktenvernichtung <input type="checkbox"/> Archivierung <input type="checkbox"/> Bürokommunikation <input type="checkbox"/> Cloud-Services <input type="checkbox"/> Finanzbuchhaltung <input type="checkbox"/> Hosting E-Mail-System <input type="checkbox"/> Hosting Internetsystem <input type="checkbox"/> Hosting von Verarbeitungen <input type="checkbox"/> Aktenvernichtung	
	<input type="checkbox"/> Lohn- und Gehaltsabrechnung <input type="checkbox"/> Personalverwaltung <input type="checkbox"/> Werbung / Letter Shop <input type="checkbox"/> Zeiterfassung <input type="checkbox"/> Reisekosten <input type="checkbox"/> Sonstige	

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden	<input type="checkbox"/>	intern Abteilung/ Funktion
	<input type="checkbox"/>	extern Empfängerkategorie
Datenübermittlung	<input type="checkbox"/>	Datenübermittlung findet nicht statt und ist auch nicht geplant
	<input type="checkbox"/>	Datenübermittlung findet wie folgt statt:
	<input type="checkbox"/>	Drittland, Name:
	<input type="checkbox"/>	internationale Organisation, Bezeichnung:
Nennung der konkreten Datenempfänger		Empfängerkategorie
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.		Dokumentation geeigneter Garantien
Subunternehmer	<input type="checkbox"/>	

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO  
 Bemerkungen: *siehe TOM-Beschreibung*

Verantwortlicher

Datum

Unterschrift

**Übersicht von Verarbeitungstätigkeiten**  
**Auftragsverarbeiter**  
**gem. Artikel 30 Abs. 2 DSGVO**

Vorblatt

**Angaben zum Auftragsverarbeiter**

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Hauptniederlassung:  ja  nein

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Internet-Adresse

**Angaben zur Person des Datenschutzbeauftragten \* (extern mit Anschrift)**

\* sofern gem. Artikel 37 DS-GVO benannt

Anrede, Titel

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

<b>Angaben zum jeweiligen Auftraggeber</b>		Anlage
Unternehmen (Auftraggeber)	Name Straße Postleitzahl Ort Telefon E-Mail-Adresse Internet-Adresse	
Kategorien von Verarbeitungen (mit Erläuterung der jeweiligen Verarbeitung)	<input type="checkbox"/>	Aktenvernichtung
	<input type="checkbox"/>	Archivierung
	<input type="checkbox"/>	Bürokommunikation
	<input type="checkbox"/>	Cloud-Services
	<input type="checkbox"/>	Finanzbuchhaltung
	<input type="checkbox"/>	Hosting E-Mail-System
	<input type="checkbox"/>	Hosting Internetsystem
	<input type="checkbox"/>	Hosting von Verarbeitungen
	<input type="checkbox"/>	Aktenvernichtung
	<input type="checkbox"/>	Lohn- und Gehaltsabrechnung
	<input type="checkbox"/>	Personalverwaltung
	<input type="checkbox"/>	Werbung / Letter Shop
	<input type="checkbox"/>	Zeiterfassung
	<input type="checkbox"/>	Reisekosten
	<input type="checkbox"/>	Sonstige
	<input type="checkbox"/>	

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden	<input type="checkbox"/> intern Abteilung/ Funktion  <input type="checkbox"/> extern Empfängerkategorie
Datenübermittlung          Nennung der konkreten Datenempfänger          Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	<input type="checkbox"/> Datenübermittlung findet nicht statt und ist auch nicht geplant <input type="checkbox"/> Datenübermittlung findet wie folgt statt: Drittland, Name: <input type="checkbox"/> internationale Organisation, Bezeichnung:  Empfängerkategorie     Dokumentation geeigneter Garantien
Subunternehmer	<input type="checkbox"/>

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO  
 Bemerkungen: *siehe TOM-Beschreibung*

---

Verantwortlicher                      Datum                      Unterschrift