



CAD-Nördlingen

Datenschutzkonzept

25.04.2018

Datenschutzbeauftragter der CAD-Nördlingen

Anselm Binninger, B.Sc

Landsberger Str. 148, 80339 München

015152507864

anselm.binninger@bwk-technik.de

Inhalt

- 1 Vorbemerkung³
- 2 Verantwortlichkeiten und Datenschutzorganisation³
 - 2.1 Geschäftsführung und sonstige Personen, insbesondere berufene Leiter, die mit Datenverarbeitung vertraut sind³
 - 2.1.1 Vertretungsberechtigte Geschäftsführer³
 - 2.1.2 Leiter die mit der Datenverarbeitung im Bereich der Servicedienstleistungen beauftragt sind³
 - 2.2 Datenschutzbeauftragter³
 - 2.2.1 Zur Beantwortung datenschutzrechtlicher Begehren kann sich der Kunde an den bestellten externen Datenschutzbeauftragten wenden:³
- 3 Rechtliche Rahmenbedingungen⁴
- 4 Kontinuierliche Verbesserung des Datenschutzmanagementsystems⁴
 - 4.1 Datenschutzunterweisungen⁴
 - 4.2 Datenschutz-Audits⁴
 - 4.3 Schutzbedarf⁴
 - 4.4 Maßnahmen für die Sicherheit der Verarbeitung⁴
 - 4.4.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)⁴
 - 4.4.2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)⁵
 - 4.4.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)⁵
 - 4.5 Organisatorische Richtlinien⁵
 - 4.6 Richtlinien zur Auftragsdatenverarbeitung⁶
 - 4.7 Verzeichnis der Verarbeitungstätigkeiten⁶
 - Anlage 1 - Nachweis der Fachkunde des Datenschutzbeauftragten⁷

1 Vorbemerkung

Der Schutz der personenbezogenen Daten der Kunden von CAD Nördlingen unterliegt der höchste Priorität. Das vorliegende Konzept beschreibt, wie Datenschutz bei CAD Nördlingen berücksichtigt und umgesetzt, gelebt wird.

2 Verantwortlichkeiten und Datenschutzorganisation

Der Datenschutz als auch die Sicherheit informationstechnischer Systeme stellen elementare und unternehmensbezogen umzusetzende Erfordernisse an den täglichen Geschäftsbetrieb. Hierfür sind die Geschäftsleitung sowie deren maßgebenden handelnden Leitungspersonen unmittelbar verantwortlich.

2.1 Geschäftsführung und sonstige Personen, insbesondere berufene Leiter, die mit Datenverarbeitung vertraut sind

2.1.1 Vertretungsberechtigte Geschäftsführer

Angelika Binninger

2.1.2 Leiter die mit der Datenverarbeitung im Bereich der Servicedienstleistungen beauftragt sind

Angelika Binninger

2.2 Datenschutzbeauftragter

Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.

Grundlage und Maßstab der Aufgabenerfüllung Datenschutzbeauftragten sind die für die CAD Nördlingen einschlägigen Rechtsvorschriften zum Datenschutz. Im Rahmen seiner Aufgabenerfüllung sowie der Anwendung seiner Fachkunde ist der Datenschutzbeauftragte weisungsfrei. Gegenüber der Geschäftsführung der CAD Nördlingen hat er ein direktes Vortragsrecht und ist dieser unmittelbar unterstellt.

2.2.1 Zur Beantwortung datenschutzrechtlicher Begehren kann sich der Kunde an den bestellten externen Datenschutzbeauftragten wenden:

Anselm Binninger, B.Sc
BWK Technik GbR
Tetschen-Bodenbacher-Str. 3
86720 Nördlingen

Tel: 089/51997264
E-Mail: anselm.binninger@bwk-technik.de

Nachweise zur erforderlichen Fachkunde des Datenschutzbeauftragten sind in Anlage 1 angeführt (Zertifikate)

3 Rechtliche Rahmenbedingungen

Personenbezogene Daten werden im Allgemeinen lediglich zur Erfüllung von Verträgen gespeichert, für diese Daten gilt eine Aufbewahrungspflicht von 10 Jahren nach § 147 Abs. 4 AO. Weiterhin werden Nutzungsdaten und Inhaltsdaten bei der Nutzung der Website/Webshops erhoben. Diese Daten werden zur Auswertung und zum zuverlässigen Betrieb der DVAs (auch in Bezug auf eventuellen Anfragen von Strafverfolgungsbehörden) erhoben, diese Daten werden jedoch automatisiert nach einer Woche gelöscht. Weiterhin werden bei der Nutzung des Kontaktformulars auf der Website personenbezogene Daten erfasst, um CAD Nördlingen eine Rückantwort zu erlauben. Die genaue Auflistung kann dem Verzeichnisse entnommen werden.

4 Kontinuierliche Verbesserung des Datenschutzmanagementsystems

Das Datenschutzkonzept von CAD Nördlingen wird kontinuierlich weiterentwickelt, um personenbezogene Daten stets bestmöglich zu schützen.

4.1 Datenschutzunterweisungen

Hierzu werden alle Mitarbeiter der CAD Nördlingen regelmäßig (jährlich im Dezember) durch den Datenschutzbeauftragten geschult. Weiterhin sind die Mitarbeiter dazu aufgerufen, bei Fragen den Datenschutzbeauftragten zu kontaktieren. Unterweisungen werden im jeweiligen Bericht des Datenschutzbeauftragten dokumentiert.

4.2 Datenschutz-Audits

Außerdem wird CAD Nördlingen (jährlich im Dezember) durch den Datenschutzbeauftragten auditiert. Hierbei wird eine jeweils ein Bericht mit allen durchgeführten Maßnahmen erstellt und alle Datenschutzdokumente gegebenenfalls aktualisiert. Im Rahmen des Audits findet auch die Schulung der Mitarbeiter statt.

4.3 Schutzbedarf

Bei den personenbezogenen Daten, die durch die CAD Nördlingen erfasst werden handelt es sich um Daten, bei welchen ein geringes Risiko für Betroffene zu erwarten ist, weshalb alle Daten mit normalem Schutzbedarf klassifiziert werden.

4.4 Maßnahmen für die Sicherheit der Verarbeitung

Die folgenden Maßnahmen beschreiben den Schutz der Datenverarbeitungsanlagen der CAD Nördlingen, dies beinhaltet die im Zusatzdokument 01 „IT Infrastrukturerfassung“ gelisteten Geräte (exkl. Der DVAs der Kategorie „Externe Geräte/Services“, diese Anlagen werden vom Dienstleister BWK Technik GbR bereitgestellt, siehe Zusatzdokument 07 „BWK Dienstleistungsvertrag“. Technische und organisatorische Maßnahmen dieser Anlagen sind in Zusatzdokument 09 „BWK Auftragsdatenverarbeitung“ geregelt).

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

4.4.1.1 Zutrittskontrolle

Die IT-Systeme, sowie Dokumente befinden sich in den Räumen der CAD Nördlingen, diese Räume werden nach Arbeitsschluss abgeschlossen um den Zugriff durch Unbefugte zu verhindern. Schlüssel zu diesen Räumen haben folgende Personen:

- Angelika Binninger

Reinigungsdienste werden bei der Ausführung Ihrer Arbeit durch einen Mitarbeiter überwacht und PC-Systeme beim Verlassen des Arbeitsplatzes gesperrt.

Weiterhin sind die Räume mit einer Einbruchmeldeanlage ausgestattet, diese alarmiert bei Erkennung von Bewegung die Geschäftsführung.

Besucher werden stets durch einen Mitarbeiter empfangen und durch das Gebäude geführt.

4.4.1.2 Zugriffskontrolle

Auf die DVAs der CAD Nördlingen haben lediglich autorisierte Personen Zugriff (dies schließt den beauftragten IT Dienstleister BWK Technik GbR ein. Zugriff von außen auf die DVAs ist grundsätzlich nicht möglich, in bestimmten Fällen kann durch den IT Dienstleister eine Fernwartung vorgenommen werden, welche jedoch nur für den Zeitraum der Wartung freigeschaltet wird.

Bei der Übertragung personenbezogener Daten von und zu Geräten aus Anhang 01, welche der Kategorie „Externe Geräte“ zu geordnet sind, kommt aktuelle TLS Verschlüsselung mit regelmäßig neu erstellten Keys zum Einsatz.

4.4.1.3 Trennungskontrolle

Unterschiedliche Daten werden in unterschiedlichen Dateien und Verzeichnissen abgelegt, um eine zweckgebundene, getrennte Verarbeitung realisieren zu können.

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

4.4.2.1 Weitergabekontrolle

Das Ziel der Weitergabekontrolle ist es zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, vervielfältigt, verändert oder entfernt werden können und dass überprüft sowie festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zu Datenübertragung vorgesehen ist. Folgende Maßnahmen haben wir in Bezug auf die Weitergabe von personenbezogenen Daten getroffen:

- Weitergabe an Dritte nur nach Prüfung der Rechtsgrundlage
- Sichere Übertragung von Datenlieferungen (SFTP, VPN)
- Beschränkung des zur Übermittlung befugten Personenkreises
- Verschlüsselte Übertragung bei HTTP (Verwendung aktueller Cypher Suites und Protokolle)

4.4.2.2 Eingabekontrolle

Das Ziel einer Eingabekontrolle ist es, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten in die Systeme und Anlagen zur Datenverarbeitung eingegeben, verändert oder entfernt worden sind. Die Nachvollziehbarkeit innerhalb der Datenverwaltung stellen wir wie folgt sicher:

Änderungen an personenbezogenen Daten im Shopsystem, werden im selbigen protokolliert. Die Protokollierung enthält Informationen zum Zeitpunkt und Mitarbeiter.

Daten, welche auf den Client PCs von CAD Nördlingen gespeichert werden, werden auf das Cloud System „Seafire“ des IT Dienstleisters BWK Technik GbR gesichert. Dieses System stellt die Erfassung, Protokollierung und Wiederherstellung der Daten sicher.

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

Da die personenbezogenen Daten auf den Systemen des IT Dienstleisters BWK Technik GbR gespeichert werden, sind diese beim Ausfall lokaler Geräte auch auf anderem Geräte verfügbar.

Daten auf den lokalen Systemen werden ebenfalls bei jeder Änderung auf das Cloud System des IT Dienstleisters gesichert und sind damit sofort auf anderen Systemen, bei Ausfall, verfügbar.

4.5 Organisatorische Richtlinien

Daten auf den lokalen Client PCs werden auf das Cloud System des IT Dienstleisters gesichert und dort protokolliert.

4.6 Richtlinien zur Auftragsdatenverarbeitung

Werden personenbezogene Daten im Auftrag verarbeitet so ist ein spezieller Auftragsdatenverarbeitungsvertrag abzuschließen. Bestehende Verträge sind folgende:

- Für den Betrieb des Webshops, Email und die IT Betreuung ist ein Auftragsdatenverarbeitungsvertrag mit BWK Technik GbR abgeschlossen, dieser ist im Zusatzdokument 09 „BWK Auftragsdatenverarbeitung“ zu finden.
- Für die Analyse der Nutzungsdaten des Webshops mit eingeschalteter Anonymisierungsfunktion ist ein Auftragsdatenverarbeitungsvertrag mit Google abgeschlossen, dieser ist im Zusatzdokument 06 zu finden.

4.7 Verzeichnis der Verarbeitungstätigkeiten

Das Verzeichnis der Verarbeitungstätigkeiten kann dem Zusatzdokument 02 „VVT“ entnommen werden.

Anlage 1 – Zertifikate

1 Anlage 1 - Nachweis der Fachkunde des Datenschutzbeauftragten



HOCHSCHULE
FÜR ANGEWANDTE
WISSENSCHAFTEN
MÜNCHEN

ZERTIFIKAT

Herr Anselm BINNINGER
geboren am
hat im Rahmen des Bachelorstudiengangs Informatik
die

Zusatzqualifikation "Betrieblicher Datenschutz"

erworben und verfügt damit über die zur Erfüllung der Aufgaben eines Beauftragten für
Datenschutz gemäß § 4f Absatz 2 Bundesdatenschutzgesetz erforderliche Fachkunde.

Die Zusatzqualifikation beruht auf dem erfolgreichen Abschluss der Fächer:

	Endnoten
Datenschutz *	gut
Wirtschaftsprivatrecht *	gut
IT-Sicherheit *	gut
Aktuelle Probleme des Datenschutzes	gut
Datenschutz-Praktikum	gut

* Die Endnoten dieser Fächer wurden im Rahmen der Bachelorprüfung im Bachelorstudiengang Informatik an der
Hochschule für angewandte Wissenschaften München erzielt.

München, den 10. März 2016

Der Präsident



(Siegel geprägt)

Die Vorsitzende
der Prüfungskommission

Prof. Dr. M. Kortstock

Prof. Dr. E. Eich-Soellner

Notenstufen:
sehr gut = 1,0 bis 1,5; gut = 1,6 bis 2,5; befriedigend = 2,6 bis 3,5; ausreichend = 3,6 bis 4,0; nicht ausreichend = über 4,0



CAD-Nördlingen
Verzeichnis von Verarbeitungstätigkeiten
25.04.2018

Datenschutzbeauftragter der CAD-Nördlingen

Anselm Binninger, B.Sc

Landsberger Str. 148, 80339 München

015152507864

anselm.binninger@bwk-technik.de

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Hauptblatt

Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DS-GVO)

1. Verantwortlicher (=Firma/Legaleinheit)

CAD Nördlingen

Tetschen-Bodenbacher-Str. 3

86720 Nördlingen

2. Gesetzlicher Vertreter (= Geschäftsführung)

Angelika Binninger

Tetschen-Bodenbacher-Str. 3

86720 Nördlingen

09081/8098667

3. Vertreter in der EU (gemäß Art. 27 DS-GVO)

Siehe 2)

4. Datenschutzbeauftragter

Anselm Binninger, B.Sc

BWK Technik GbR

Tetschen-Bodenbacher-Str. 3

86720 Nördlingen

015152507864

anselm.binninger@bwk-technik.de

Optionale Inhalte / Übergreifende Regelungen und Sachverhalte

5. Zuständige Aufsichtsbehörde

BayLDA

Meldung des/der Datenschutzbeauftragten erfolgt:

Ja

Nein

6. Regelungen zur Datensicherheit

Siehe Anhang 4 „Datenschutzkonzept“ und 5 „Datensicherungskonzept“ zum Datenschutzbericht vom 25.04.2018

7. Regelungen zur Datenlöschung

Siehe Anhang 4 „Datenschutzkonzept“ zum Datenschutzbericht vom 25.04.2018

8. Sachverhalte zu Drittstaatenübermittlungen

Findet nicht statt

Erläuterungen

Nr. 1	<p>Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DS-GVO)</p> <p>Angaben: Name/Firma, ladungsfähige Anschrift</p>
Nr. 2	<p>Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter</p> <p>Angaben: Namen der geschäftsführenden Personen</p>
Nr. 3	<p>Bei Unternehmen ohne Niederlassung in der Europäischen Union ist hier der benannte Vertreter des Verantwortlichen (Art. 4 Nr. 17 DS-GVO, Art. 27 Abs. 1 DS-GVO) anzugeben.</p>
Nr. 4	<p>Vom Verantwortlichen bestellter Datenschutzbeauftragter* [Name, Kontaktdaten]</p>
Nr. 5	<p>Die Meldung der Kontakt-Informationen des DSB – z.B. (Funktions-)e-mail-Adresse, Telefonnummer – ist verpflichtend.</p>
Nr. 6	<p>Gegebenenfalls Verweise auf übergreifende Regelungen (<i>falls solche existieren, die grds. alle Verarbeitungen betreffen</i>) – Der Verweis an dieser Stelle auf übergreifende Regelungen entbindet nicht von der Dokumentation von ggf. erforderlichen Abweichungen zu den einzelnen Verarbeitungstätigkeiten.</p> <p>Verweis z.B. auf ein IT-Sicherheitskonzept, das alle Verarbeitungstätigkeiten einschließt. Eventuell auch Verweise auf relevante Dokumente eines ISMS nach ISO27001.</p>
Nr. 7	<p>Verweis auf Löschkonzepte, die grds. für alle Verarbeitungen gelten.</p>
Nr. 8	<p>Ein Verweis Regelungen zur Drittstaatenübermittlung sind hier sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen hierdurch geregelt werden, z.B. durch BCR.</p>

Verzeichnis von Verarbeitungstätigkeiten

Anlage Nr. 1

Angaben zur Verarbeitungstätigkeit und zur Verantwortlichkeit (Art. 30 Abs. 1 lit. b DS-GVO)

1. Bezeichnung der Verarbeitungstätigkeit Verkauf und Vertrieb
2. Verantwortlicher Fachbereich/verantwortliche Führungskraft (optionaler Inhalt) Angelika Binninger
3. Bei gemeinsamer Verantwortlichkeit: -

Angaben zur Verarbeitungstätigkeit

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit Verkauf und Vertrieb von Waren und Dienstleistungen (wie Zeichnungen digital oder gedruckt)

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit Art. 6 Abs. 1 b DSGVO
--

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)	
6.1 Betroffene Personengruppen	6.2 Kategorien personenbezogener Daten
Kunden	Name
	Vorname
	Titel
	Geschlecht
	E-Mail
	Name des Unternehmens
	Postleitzahl
	Stadt
	Straße
	Hausnummer
	Telefonnummer (Mobil/Festnetz)

	Kundennummer
	Daten zu gekauften Waren oder Dienstleistungen

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden (Art. 30 Abs. 1 lit. d DS-GVO)

Externe Empfänger:

Architekt Erich Lokietsch, Dipl. Ing

8. Datenübermittlungen in Drittländer oder internationale Organisationen (Art. 30 Abs. 1 e DS-GVO)

Übermittlung

Ja

Nein

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 lit. f DS-GVO)

Bei personenbezogenen Daten des Verkaufs / Vertriebs ist davon auszugehen, dass diese buchhaltungsrelevant sind. Eine Speicherung erfolgt daher grundsätzlich für 10 Jahre, wobei der Fristbeginn sich nach § 147 Abs. 4 AO richtet.

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

10.1 Art der eingesetzten DV-Anlagen und Software (optional)

EasyShop Shopsystem

10.2 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

Siehe Anhang 09 „Nachweis Technischer Maßnahmen“ und Anhang 04 „Datenschutzkonzepts“ des Datenschutzberichts vom 25.04.2018

Verzeichnis von Verarbeitungstätigkeiten

Anlage Nr. 2

Angaben zur Verarbeitungstätigkeit und zur Verantwortlichkeit (Art. 30 Abs. 1 lit. b DS-GVO)

1. Bezeichnung der Verarbeitungstätigkeit Internetseite
2. Verantwortlicher Fachbereich/verantwortliche Führungskraft (optionaler Inhalt) Angelika Binninger
3. Bei gemeinsamer Verantwortlichkeit: -

Angaben zur Verarbeitungstätigkeit

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit Betrieb einer Internetseite zur Außendarstellung des Unternehmens und zur Kontaktaufnahme inkl. Kontaktformular

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit Art. 6 Abs. 1 a DSGVO
--

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)	
6.1 Betroffene Personengruppen	6.2 Kategorien personenbezogener Daten
Interessenten	Name
Besucher	Vorname
Kunden	E-Mail
	Nutzungsdaten
	Inhaltsdaten

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden (Art. 30 Abs. 1 lit. d DS-GVO) Externe Empfänger: Hosting-Anbieter (BWK Technik GbR)

8. Datenübermittlungen in Drittländer oder internationale Organisationen (Art. 30 Abs. 1 e DS-GVO)

Übermittlung

Ja

Nein

Übermittlung der Sitzungsdaten und Nutzungsdaten an Google Inc., siehe Anhang 06 „Analytics Auftragsdatenverarbeitungsvertrag“

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 lit. f DS-GVO)

E-Mails werden für mindestens 6 Jahre aufbewahrt, um den handelsrechtlichen Aufbewahrungspflichten für Geschäftsbriefe nachzukommen.

Nach Ablauf von 6 Jahren wird zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.

Ausgenommen hiervon sind Daten, die als buchhaltungsrelevante Daten einzuordnen sind. Hier gelten die jeweiligen steuerrechtlichen Aufbewahrungspflichten.

Sitzungs- und Nutzungsdaten werden auf dem Server automatisch nach einer Woche gelöscht

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

10.1 Art der eingesetzten DV-Anlagen und Software (optional)

EasyShop Shopsystem

10.2 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

Siehe Anhang 09 „Nachweis Technischer Maßnahmen“ und Anhang 04 „Datenschutzkonzepts“ des Datenschutzberichts vom 25.04.2018

Verzeichnis von Verarbeitungstätigkeiten

Anlage Nr. 3

Angaben zur Verarbeitungstätigkeit und zur Verantwortlichkeit (Art. 30 Abs. 1 lit. b DS-GVO)

1. Bezeichnung der Verarbeitungstätigkeit Email
2. Verantwortlicher Fachbereich/verantwortliche Führungskraft (optionaler Inhalt) Angelika Binninger
3. Bei gemeinsamer Verantwortlichkeit: -

Angaben zur Verarbeitungstätigkeit

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit Elektronische Kommunikation

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit Art. 6 Abs. 1 a DSGVO
--

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)	
6.1 Betroffene Personengruppen	6.2 Kategorien personenbezogener Daten
Interessenten	Name
Besucher	Vorname
Kunden	E-Mail
	Nutzungsdaten
	Inhaltsdaten

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden (Art. 30 Abs. 1 lit. d DS-GVO) Externe Empfänger: Hosting-Anbieter Ggf. Dritte

8. Datenübermittlungen in Drittländer oder internationale Organisationen (Art. 30 Abs. 1 e DS-GVO)

Übermittlung

Ja

Nein

Übermittlung der Sitzungsdaten und Nutzungsdaten an Google Inc., siehe Anhang 06 „Analytics Auftragsdatenverarbeitungsvertrag“

Gleichwohl ist beim Versand von E-Mails über das Internet nie ausgeschlossen, dass eine Weiterleitung über einen Drittstaat erfolgt.

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 lit. f DS-GVO)

E-Mails werden für mindestens 6 Jahre aufbewahrt, um den handelsrechtlichen Aufbewahrungspflichten für Geschäftsbriefe nachzukommen.

Nach Ablauf von 6 Jahren wird zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.

Ausgenommen hiervon sind Daten, die als buchhaltungsrelevante Daten einzuordnen sind. Hier gelten die jeweiligen steuerrechtlichen Aufbewahrungspflichten.

Sitzungs- und Nutzungsdaten werden auf dem Server automatisch nach einer Woche gelöscht

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

- 10.1 Art der eingesetzten DV-Anlagen und Software (optional)

E-Mail Portal des Hosting Anbieters (OpenXChange)

Microsoft Outlook

Mozilla Thunderbird

- 10.2 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

Siehe Anhang 09 „Nachweis Technischer Maßnahmen“ und Anhang 04 „Datenschutzkonzepts“ des Datenschutzberichts vom 25.04.2018

Verzeichnis von Verarbeitungstätigkeiten

Anlage Nr. 4

Angaben zur Verarbeitungstätigkeit und zur Verantwortlichkeit (Art. 30 Abs. 1 lit. b DS-GVO)

1. Bezeichnung der Verarbeitungstätigkeit Finanzbuchhaltung
2. Verantwortlicher Fachbereich/verantwortliche Führungskraft (optionaler Inhalt) Angelika Binninger
3. Bei gemeinsamer Verantwortlichkeit: -

Angaben zur Verarbeitungstätigkeit

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit Ermittlung und Verwaltung aller Einnahmen und Ausgaben, insbesondere für Zwecke der Ermittlung und Abfuhr von Steuern und Abgaben

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit Art. 6 Abs. 1 c DSGVO
--

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)	
6.1 Betroffene Personengruppen	6.2 Kategorien personenbezogener Daten
Kunden	Name
	Vorname
	Titel
	Geschlecht
	E-Mail
	Name des Unternehmens
	Postleitzahl
	Stadt
	Straße
	Hausnummer

	Telefonnummer (Mobil/Festnetz)
	Kundennummer
	Daten zu gekauften Waren oder Dienstleistungen
	Bankdaten

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden (Art. 30 Abs. 1 lit. d DS-GVO)

Externe Empfänger:
Steuerbüro Künzler, Reimlingen

8. Datenübermittlungen in Drittländer oder internationale Organisationen (Art. 30 Abs. 1 e DS-GVO)

Übermittlung

Ja

Nein

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 lit. f DS-GVO)

Personenbezogene Daten der Finanzbuchhaltung sind buchhaltungsrelevant. Eine Speicherung erfolgt daher grundsätzlich für 10 Jahre, wobei der Fristbeginn sich nach § 147 Abs. 4 AO richtet.

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

10.1 Art der eingesetzten DV-Anlagen und Software (optional)

EasyShop Shopsystem
Microsoft Excel

10.2 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

Siehe Anhang 09 „Nachweis Technischer Maßnahmen“ und Anhang 04 „Datenschutzkonzepts“ des Datenschutzberichts vom 25.04.2018