Vertrag über die Verarbeitung von Daten im Auftrag

AV-Vertrag

zwischen

_____

_____

_____

_____

_____

_____

Jimdo Website(s):

Auftraggeber
-

und

Jimdo GmbH
Stresemannstr. 375
22761 Hamburg
Germany
-
Auftragnehmer oder „***Jimdo***"
-

Präambel

Dem Auftraggeber ist bekannt, dass Jimdo seine Dienstleistungen für eine Vielzahl von Kunden anbietet. Die Möglichkeit des Auftraggebers, ergänzende Weisungen zu erteilen, die die Dienstleistungen von Jimdo für andere Kunden oder Nutzer beeinträchtigt, ist daher durch diesen Vertrag beschränkt. Ein Betrieb von Jimdo unter Berücksichtigung einer Vielzahl von Einzelweisungen des Auftraggebers wäre nicht möglich.

1. Allgemeines

1.1. Im Zusammenhang mit der Erbringung seiner Leistungen gegenüber dem Auftraggeber verarbeitet Jimdo auch personenbezogene Daten für den Auftraggeber im Auftrag. Dieser Vertrag enthält nach dem Willen der Parteien 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 (DSGVO) und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

1.2. 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 DSGVO zugrunde gelegt.

1.3. 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 DSGVO in diesem Vertrag.

2. Gegenstand des Auftrags

2.1. Jimdo stellt einen Online-Service zur Verfügung, mit dem sich die Jimdo-Nutzer wie der Auftraggeber eine eigene Jimdo-Webseite selbst erstellen und betreiben können. Der bereitgestellte Service erlaubt es den Nutzern, selbstständig das Design der eigenen Jimdo-Webseite anzupassen, eigene Inhalte einzustellen und einen Shop zu betreiben. Der Gegenstand des Auftrags ergibt sich im Übrigen aus dem zwischen den Parteien geschlossenen Hauptvertragsverhältnis. Dieses beruht auf den AGB von Jimdo, die wirksam in das Vertragsverhältnis zwischen den Parteien einbezogen wurden.

2.2. Dieser Auftragsdatenverarbeitungsvertrag gilt ergänzend zu den AGB von Jimdo.

2.3. Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Bestandsdaten von Kunden des Auftraggebers
  - Name, Anschrift
  - Bestelldaten
  - im Falle von Jimdo-Shops: Zahlungsdaten
    (diese werden jedoch nur vom Payment-Anbieter gespeichert)

- Nutzungsdaten von Besuchern der Jimdo-Website des Auftraggebers
  - Jimdo nutzt diverse Services zur Nutzungsanalyse (z.B. Google Analytics), um Statistiken für Jimdo-Nutzer wie z.B. den Auftraggeber zu ermöglichen; aber auch um die Jimdo-Angebote regelmäßig zu evaluieren und zu optimieren.

- Inhaltsdaten, die Besucher von Internetseiten des Auftraggebers auf diesen eingeben (z.B. in Kommentaren, Gästebüchern und Formularen).

- Kommunikationsdaten bzw. E-Mail Nachrichten die über den Email Anbieter Rackspace Limited gesendet werden. Wenn über eine Jimdo-Webseite ein E-Mail-Konto oder eine E-Mail-Weiterleitung eingerichtet ist, werden Jimdo ein Konto bei Rackspace Limited für Jimdo-Nutzer anlegen. Rackspace Limited übernimmt dann für Jimdo die technische Auslieferung und Verwaltung der E-Mails.

Bei den genannten Datenarten handelt es sich um Daten, die regelmäßig bei der Inanspruchnahme von Leistungen von Jimdo verarbeitet werden. Die Datenarten können abhängig von den jeweiligen vom Auftraggeber in Anspruch genommenen Dienstleistungen von Jimdo abweichen bzw. im Ermessen von Jimdo erweitert werden. Sollte die Datenarten von der oben genannten Liste abweichen, so werden die spezifischen Datenarten in einer gesonderten Anlage zu diesem Vertrag festgelegt. In dem Fall kann sich der Auftraggeber mit Jimdo in Verbindung (datenschutz@jimdo.com) setzen und entsprechend die abweichenden Datenarten auflisten bzw. die gesonderte Anlage anfragen. Jimdo trägt Sorge dafür, dass die jeweils anzuwendenden Rechtsgrundlagen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten beachtet werden, soweit dies im Verantwortungsbereich von Jimdo liegt. Für die Prüfung der Zulässigkeit der Verarbeitung von Inhaltsdaten (z.B.aus vom Auftraggeber genutzten Formularen) oder sonstigen Daten,deren Verarbeitung der Auftraggeber im Zusammenhang mit der Nutzung seiner Internetseiten selbst initiiert hat, ist der Auftraggeber allein verantwortlich.

2.4. Kreis der von der Datenverarbeitung Betroffenen:

- Kunden des Auftraggebers
- Interessenten bzw. Besucher der Website des Auftraggebers
- Mitarbeiter des Auftraggebers

3. Rechte, Weisungsrechte und Pflichten des Auftraggebers

3.1. Der Auftraggeber ist die verantwortliche Stelle i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch Jimdo, der Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

3.2. Der Auftraggeber ist verpflichtet, nur solche Daten an Jimdo zu übermitteln oder erfassen zu lassen, die gemäß Art. 6 Abs. 1 EU-DSGVO rechtmäßig erhoben und zweckgemäß weiterverarbeitet werden. Der Auftraggeber ist ferner verpflichtet, die Rechte der betroffenen Personen zu wahren und insbesondere der Informationspflicht nachzukommen sowie die Ausübung des Widerspruchsrechts der betroffenen Personen zu ermöglichen. Der Auftraggeber ist als verantwortliche Stelle für die Wahrung der Betroffenenrechte verantwortlich. Betroffenenrechte sind gegenüber dem Auftraggeber wahrzunehmen. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen und dies unmittelbar den Auftraggeber betrifft.

3.3. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber wird das Ergebnis in geeigneter Weise dokumentieren.

3.4. Der Auftraggeber kann Jimdo ergänzende Weisungen bezüglich der Verarbeitung von personenbezogenen Daten erteilen. Diese Weisungen kann der Kunde vorrangig in seinem Administrationsbereich durch eine entsprechende Konfiguration der Dienste vornehmen. So können dort z.B. Einstellungen zur Webanalyse vorgenommen werden. Darüber hinausgehende Weisungen sind in Textform (z.B. E-Mail) an Jimdo zu senden. Jimdo wird dann die Umsetzbarkeit der Weisungen unter Berücksichtigung der Interessen an der Funktionsfähigkeit der Jimdo-Leistungen für alle Kunden prüfen und dem Auftraggeber die Kosten für die Durchführung der Einzelweisung mitteilen. Die Weisung wird dann nach Abschluss einer Kostenübernahmeerklärung umgesetzt. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

3.5. Der Auftraggeber kann weisungsberechtigte Personen in dem Administrationsbereich seiner Jimdo Seite benennen bzw. deren E-Mail Adresse hinterlegen. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform bzw. über eine Änderung der hinterlegten Email Adresse im Jimdo-Administrationsbereich mitteilen.

3.6. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

3.7. Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

4.2. Jimdo trägt Sorge dafür, dass die Datenverarbeitung im Rahmen der Leistungserbringung nach dem Hauptvertrag in seinem Verantwortungsbereich, der Unterauftragnehmer nach Ziffer 6 dieses Vertrags einschließt, in Übereinstimmung mit den Bestimmungen dieses Vertrags erfolgt.

4.3. Jimdo verpflichtet sich, die Datenverarbeitung, soweit diese abweichend von Ziff. 4.1, unmittelbar im Auftrag für den Auftraggeber erfolgt, nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen oder im Falle einer Verarbeitung von Daten in einem Drittstaat Regelungen zu treffen, die eine Verarbeitung nach Art. 6 DSGVO in zulässiger Weise ermöglicht.

4.4. Jimdo ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Jimdo wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind,

vorab mit dem Auftraggeber abstimmen.

4.5. Jimdo wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt.
Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

4.6. Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Textform zulässig, es sei denn, die Parteien haben eine schriftliche Vereinbarung getroffen, die insbesondere die Datensicherheit und die Prüfungsrechte gemäß nachstehendem § 4 (Allgemeine Pflichten des Auftragnehmers) dieser Vereinbarung sicherstellt.
Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Textform im Einzelfall zulässig, es sei denn, die Parteien haben eine schriftliche Vereinbarung getroffen, die insbesondere die Datensicherheit und die Prüfungsrechte gemäß nachstehendem § 4 (Allgemeine Pflichten des Auftragnehmers) dieser Vereinbarung sicherstellt.

4.7. Jimdo wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich. Jimdo wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, auf geeignete Weise kennzeichnen. Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird Jimdo die Daten mit dem jeweiligen Zweck kennzeichnen.

4.8. Jimdo kann - muss aber nicht - dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Für den Fall, dass sich die weisungempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5. Datenschutzbeauftragter des Auftragnehmers

Jimdo hat einen externen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37 DSGVO benannt. Dabei handelt es sich um:

B³ | Informationstechnologie Andreas Bethke
Papenbergallee 34
25548 Kellinghusen
Deutschland
E-Mail: datenschutz@jimdo.com

6. Meldepflichten des Auftragnehmers

6.1. Jimdo ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen desn Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

6.2. Ferner wird Jimdo den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber Jimdo tätig wird und dies auch eine Kontrolle der Verarbeitung, die Jimdo im Auftrag des Auftraggebers erbringt, betreffen kann.

6.3. Es ist Jimdo bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs in Textform (Fax/E-Mail) mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragnehmers

7.1. Jimdo wird den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO unterstützen. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

7.2. An der Erstellung der Verfahrensverzeichnisse bzw. Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber hat Jimdo mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen

7.3. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. Kontrollbefugnisse

8.1. Damit der Auftraggeber seine Kontrollrechte und -pflichten vor Beginn und während des Vertragsverhältnisses ausüben kann, wird Jimdo dem Auftraggeber auf Anfrage einen Bericht des externen Datenschutzbeauftragten von Jimdo zu den getroffenen technischen und organisatorischen Maßnahmen bei Jimdo und in den von Jimdo genutzten Rechenzentren zur Verfügung stellen. Der Bericht wird spätestens alle 24 Monate aktualisiert.

8.2. Bei weiteren Fragen kann sich der Auftraggeber an den externen Datenschutzbeauftragten von Jimdo wenden.

8.3. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch Jimdo jederzeit im erforderlichen Umfang zu kontrollieren.

8.4. Jimdo ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 8.3 erforderlich ist.

8.5. Der Auftraggeber kann eine Einsichtnahme in die von Jimdo für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

8.6. Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist (zumindest zehn Arbeitstagen) die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte der Jimdo GmbH zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt. Der Auftraggeber ist verpflichtet, die ihm im Rahmen oder bei Gelegenheit einer solchen Kontrolle zur Kenntnis gelangten internen geheimhaltungsbedürftigen Informationen des Auftragnehmers, insbesondere Details zu den technischen und organisatorischen Maßnahmen, streng geheim zu halten, nicht Dritten mitzuteilen oder Dritten zugänglich zu machen, sofern dies nicht zum Zweck der vertraglichen Leistungsbeziehung zwischen Auftraggeber und Auftragnehmer erfolgt.

8.7. Jimdo ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

8.8. Der Auftraggeber ist berechtigt, die Kontrolle durch einen von ihm im Einzelfall zumindest zehn Tage vor der Kontrolle schriftlich namentlich zu benennenden Prüfer durchführen zu lassen, sofern der Auftragnehmer einer solchen externen Prüfung zustimmt. Der Auftragnehmer wird seine Zustimmung nicht unbillig verweigern. Der Auftragnehmer ist insbesondere dann zur Ablehnung des Prüfers berechtigt, wenn der Prüfer in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Externe Prüfer sind verpflichtet, eine schriftliche Verschwiegenheitsvereinbarung mit dem Auftragnehmer zu schließen und erst dann zur Durchführung der Prüfung berechtigt. Die Prüfbefugnis des Auftraggebers bleibt hiervon unberührt.

9. Unterauftragsverhältnisse

9.1. Jimdo darf zur Erbringung seiner Leistungen gegenüber Nutzern des Dienstes Subunternehmer mit der Durchführung von Arbeiten beauftragen, die auch die Verarbeitung personenbezogener Daten umfassen. Jimdo wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der „Anlage 1“ zu diesem Vertrag angeben. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 4 genannten Voraussetzungen zulässig.

9.2. Jimdo hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Jimdo getroffenen Vereinbarungen einhalten kann. Jimdo hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle wird von Jimdo dokumentiert und auf Anfrage dem Auftraggeber zu übermitteln.

9.3. Jimdo ist verpflichtet, sich vom Subunternehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37 DSGVO bestellt hat. Für den Fall, dass kein

Datenschutzbeauftragter beim Subunternehmer bestellt ist, hat Jimdo den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragte zu benennen. Jimdo hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Subunternehmern gelten. Jimdo hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

9.4. Jimdo wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information"). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information" zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information" erfolgt gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

9.5. Jimdo hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber den Subunternehmern gelten. Jimdo hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

9.6. Jimdo hat mit dem Subunternehmer einen Auftragsdatenverarbeitungsvertrag zu schließen, der den Voraussetzungen von Art. 28 DSGVO entspricht. Darüber hinaus hat Jimdo den Unterauftragnehmer den Subunternehmer dieselben Datenschutzpflichten aufzuerlegen, die zwischen Auftraggeber und Jimdo festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

9.7. Jimdo ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 5 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

9.8. Nicht als Unterauftragsverhältnisse i.S.d. Absätze 9.1 bis 9.7 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

10. Vertraulichkeitsverpflichtung

10.1. Jimdo ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

10.2. Jimdo sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Jimdo sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese zur Vertraulichkeit i.S.d. DSGVO sowie auf das Datengeheimnis i.S.d. §53 BDSG (neu) verpflichtet werden.

10.3. Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

11. Wahrung von Betroffenenrechten

11.1. Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Betroffenenrechte sind gegenüber dem Auftraggeber wahrzunehmen. Jimdo ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen, sofern der Auftraggeber die Ansprüche nicht ohne Mitwirkung der Jimdo GmbH erfüllen kann. Jimdo hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

11.2. Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung – durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

11.3. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

12. Geheimhaltungspflichten

12.1. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

12.2. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

13. Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

14.1. Jimdo verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

14.2. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 2 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird Jimdo im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können von Jimdo ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der von Jimdo getroffenen technischen und organisatorischen Maßnahmen anfordern.

14.3. Jimdo wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird Jimdo den Auftraggeber informieren.

15. Dauer des Auftrags

15.1. Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über Nutzung der Dienstleistungen des Auftragnehmers. Er ist mit einer Frist von einem Monat zum zum Ende der jeweiligen Laufzeit kündbar. Die Kündigung bedarf der Textform.

15.2. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß der Jimdo GmbH gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, Jimdo eine Weisung des Auftraggebers nicht ausführen kann oder will oder Jimdo den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

16. Beendigung

16.1. Nach Beendigung des Vertrages hat Jimdo sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

16.2. Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen.
Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

17. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

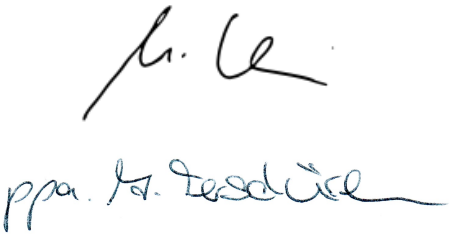
18. Schlussbestimmungen

18.1. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

18.2. Für Nebenabreden ist die Schriftform erforderlich.

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

18.4. Bei Abweichungen, die aus der Übersetzung entstehen, gilt die Formulierung in deutscher Sprache.

_____	_____
Ort, Datum	- Auftraggeber -
Hamburg, 11.05.2018	
_____	
Ort, Datum	- Auftragnehmer/Jimdo - Matthias Henze (CEO) Anna Terschüren (VP Finance)

Anlage 1 - Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Infrastruktur/Technische Plattform:

Mandrill	Newsletter, Benachrichtigungen	Mailchimp by The Rocket Science Group, LLC, 675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308, USA	Opt-Out im Newsletter, https://mailchimp.com/legal/privacy/
SendGrid	Benachrichtigungen via E-Mail	SendGrid Inc., 1801 California St #500, Denver, CO 80202, USA	https://sendgrid.com/policies/privacy/
Google Tag Manager	Das Tool Tag Manager ist eine cookie-lose Domain und erfasst keine personenbezogenen Daten. Das Tool sorgt für die Auslösung anderer Tags, die ihrerseits unter Umständen Daten erfassen.	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://www.google.com/intl/de/tagmanager/faq.html
Google Analytics	Nutzerstatistiken	Google LLC, 1600, Amphitheatre Parkway, Mountain View, CA 94043, USA	Browser Plugin, Opt-Out Link
Adobe Image Editor	Bildbearbeitung im CMS	Adobe Systems Incorporated, 345 Park Avenue, San Jose, CA 95110-2704, USA	http://www.adobe.com/privacy.html
Firebase	Firebase ist eine Echtzeit-Datenbank, welche wir für Echtzeit-Datenaustausch und -Speicherung (Beispielsweise bei unseren Apps) nutzen. Hierbei werden die Nutzerdaten anonymisiert an Firebase übermittelt	Ein Produkt von Google LLC., 1600 Amphitheatre Parkway, Mountain View, CA 94043, SA	https://www.firebase.com/terms/privacy-policy.html
Sipgate	Faxdienst für den zuverlässigen Versand und Empfang von Faxnachrichten	sipgate GmbH Gladbacher Straße 74 40219 Düsseldorf Deutschland	https://www.sipgate.de/datenschutz.html
Rackspace	Eine webbasierten Anwendung, für die technische Auslieferung und Verwaltung von E-Mails beziehungsweise E-Mail-Konten des Anbieters Rackspace	Rackspace US Inc., Rackspace, 1 Fanatical Place, City of Windcrest, San Antonio, TX 78218, USA	https://www.rackspace.com/de-de/information/legal/privacystatement
SiftScience	Tool zur Betrugsbekämpfung	Sift Science, Inc., 123 Mission Street, 20th Floor, San Francisco, CA 94105	https://siftscience.com/service-privacy
Stripe	Zahlungsabwickler	Stripe Inc.,185 Berry Street, Suite 550, San Francisco, CA 94107, USA	https://stripe.com/de/privacy
Global Collect	Zahlungsabwickler	Global Collect Service B.V., Planetenweg 43 - 59, 2132 HM Hoofddorp, NL	http://www.globalcollect.com/Privacy
Zuora	Abonnement-Verwaltung	Zuora Inc., 3050 S. Delaware Street, Suite 301, San Mateo, CA 94403, USA	https://www.zuora.com/privacy-statement/
Add This	Ein Bookmarking-Dienst, der das vereinfachte Bookmarken von Webseiten ermöglicht.	AddThis Inc., Oracle America Inc.,1595 Spring Hill Rd, Suite 300, Vienna, VA 22182, USA	http://www.addthis.com/privacy https://www.oracle.com/legal/privacy/index.html

fabric.io	Mobil App-Absturz-Berichterstattung	Fabric ist eine Google-Tochter und hat seinen Sitz in San Francisco (CA), USA.	https://fabric.io/terms?locale=en-us&utm_campaign=fabric-marketing&utm_medium=natural
InternetX	Verwaltung von Domains	InterNetX GmbH, Maximilianstr. 6, 93047 Regensburg, Germany	https://www.internetx.com/rechtliches/datenschutz/
RankingCoach	Add-on für die Suchmaschinenoptimierung	rankingCoach GmbH, Brügelmannstrasse 3, 50679 Köln, Germany	https://www.rankingcoach.com/de-de/datenschutz
New Relic	Bereitstellung von Analysen auf https://www.jimdo-status.com, die es uns ermöglichen, Service-Fehler zu beheben.	New Relic Inc, 188 Spear Street, Suite 1200, San Francisco, CA 94105, USA	https://newrelic.com/termsandconditions/privacy
status.io	Status-Seite mit aktueller Informationen zur Erreichbarkeit und Funktionalität unseres Systems.	T3CH.com LLC, 19 N. County Line Road, Jackson, NJ 08527, USA	https://status.io/privacy
Paypal	Zahlungsanbieter bzw. -abwickler	PayPal (Europe) S.à r.l. et Cie, S.C.A., 22-24 Boulevard Royal, 2449 Luxembourg	https://www.paypal.com/de/webapps/mpp/ua/privacy-full?locale.x=de_DE
Wordpress	Webseite des Jimdo Bloges https://de.jimdo.com/magazin/	Wordpress is a product of Automattic Inc., 60 29th Street #343, San Francisco, CA 94110, USA	https://de.wordpress.org/about/privacy/
Fastly Inc.	Auslieferung von Inhalten inkl. Google Fonts	Fastly, Inc., General Counsel, 475 Brannan St, Suite 300, San Francisco, CA 94107, USA	https://www.fastly.com/privacy
Disqus	Kommentarfunktion	DISQUS, Inc., 301 Howard St, Floor 3, San Francisco, California 94105, USA	https://help.disqus.com/terms-and-policies/disqus-privacy-policy
G-Suite	Nutzung von Google Produktivitätssystemen mit dem Jimdo E-Mail-System	Ein Produkt der Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://policies.google.com/privacy?hl=de
Twyla	Chat-Support-System	Twyla GmbH, Winterfeldtstraße 21, 10781 Berlin, Germany	https://www.twylahelps.com/
Zendesk	Ticketsystem für Supportanfragen	Zendesk, Inc., 1019 Market Street, San Francisco, CA 94103, USA	https://www.zendesk.de/company/customers-partners/#privacy-policy
Launchdarkly	Wir nutzen die Feature Flags von LaunchDarkly für unsere internen Flighting-Systeme	Catamorphic, Co. ("LaunchDarkly"), 405 14th Street, Oakland, CA 94612, USA	https://launchdarkly.com/policies/privacy/
Facebook Login	Single-Sign-On Technik	Facebook Inc., 1 Hacker Way, Menlo Park, CA 94025, USA	https://www.facebook.com/about/privacy/
Google Plus Login	Single-Sign-On Technik	Ein Produkt der Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://www.google.de/intl/de/policies/privacy/
Youtube	Youtube-Einbettungsfunktion zur Anzeige und Wiedergabe von Videos des Anbieters „Youtube“	Ein Produkt der Google LLC., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://www.google.de/intl/de/policies/privacy
Prefinery	Werkzeug für Kundengewinnung und Produktveröffentlichungen	Prefinery, 1108 Lavaca Street, Suite 110-318, Austin, TX 78701, USA	https://www.prefinery.com/privacy
Redis	Datenbankanbieter	Redislabs, 700 E El Camino Real Suite 250, Mountain View, CA 94040	https://redislabs.com/privacy/
sentry.io	Absturz Berichterstattung für mobile Apps	Ein Produkt der Functional Software, Inc., 132 Hawthorne St, San Francisco, CA 94107	https://sentry.io/privacy
Name.com	Verwaltung von Domains	Name.com Inc., 414 14th Street #200, Denver, Colorado 80202, USA	http://www.name.com/media/policies/privacy-policy.pdf
Amazon Web Services	DNS, Javascript Code, Stylesheet Dateien	Amazon Web Services, Germany GmbH, Krausenstr. 38, 10117 Berlin, Germany	https://aws.amazon.com/de/privacy/?nc1=f_pr

Interne Werkzeuge:

Jira	Fehlerbehebung und Dokumentation	Atlassian, 55 Broadway Floot 17&25 New York, NY 10006 USA	https://www.atlassian.com/legal/privacy-policy
Slack	Interne Kommunikations-Lösung	436 Lafayette Street, 1008 Western Ave #401, Seattle, WA 98104	https://slack.com/intl/de-de/privacy-policy
Trello	Internes Planungs- und Kommunikations-Tool	Atlassian, 55 Broadway Floot 17&25 New York, NY 10006 USA	https://trello.com/privacy
Tableau	Werkzeug zur Analyse von Daten	Tableau Germany GmbH, An der Welle 4, 60322 Frankfurt am Main, Germany	https://www.tableau.com/de-de/privacy
Github	Online-Dienst für Software-Entwicklungsprojekte	Github, 88 Colin P Kelly Jr St, San Francisco, CA 94107, USA	https://help.github.com/articles/github-privacy-statement/
Microsoft	Interne Nutzung von Microsoft Office und Skype	Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA	https://privacy.microsoft.com/en-us/privacystatement
Hootsuite	Social Media Tool	Hootsuite Media Inc. 5, East 8th Avenue, Vancouver BC, Canada V5T 1R6	https://hootsuite.com/de/legal/privacy

Performance und Marketing:

Facebook Pixel und Custom Audiences	Im Falle der Erteilung einer ausdrücklichen Einwilligung kann hierdurch das Verhalten von Nutzern nachverfolgt werden, nachdem diese eine Facebook-Werbeanzeige gesehen oder angeklickt haben. Dieses Verfahren dient dazu, die Wirksamkeit der Facebook-Werbeanzeigen für statistische und Marktforschungszwecke auszuwerten und kann dazu beitragen, zukünftige Werbemaßnahmen zu optimieren.	Facebook Inc., 1 Hacker Way, Menlo Park, CA 94025, USA	https://www.facebook.com/about/privacy/
Hotjar	Optimierung der Conversion Rate	Hotjar Ltd., Level 2, St Julian's Business Centre, 3, Elia Zammit Street, St Julian's STJ 1000, Malta	https://www.hotjar.com/legal/compliance/opt-out
Taboola	Content-Empfehlungs-Plattform	Taboola, Inc., 28 West 23rd Street, 5th Floor, New York, NY 10010, USA	https://www.taboola.com/privacy-policy
Tv-Squared	Diese Website nutzt TVSquared zur statistischen Auswertung der Zugriffe von Besuchern im Zusammenhang mit TV-Werbung	TV Squared Limited, Codebase, Argyle House, 3 Lady Lawson St, Edinburgh, EH3 9DR	http://tvsquared.com/privacy-policy/
bunchbox	Site-Optimization-Tool für die Umsetzung von A/B-Tests und multivariaten Analysen	app.bunchbox.co, Peaks & Pies GmbH, Raboisen 30, 20095 Hamburg, Deutschland	http://peaksandpies.com
smartly.io	Werkzeug für Werbekampagnen für Facebook und Instagram	SMARTLY.IO SOLUTIONS OY, Elielinaukio 2 G, 00100 Helsinki, Finland	https://cdn2.hubspot.net/hubfs/1570479/Privacy%20Policy/Smartly.io%20Privacy%20Policy.pdf

Zoho	Jimdo Pages Promotions Database	Zoho Corp B.V., Hoogoorddreef 15, 1101BA, Amsterdam, NL	https://www.zoho.eu/privacy.html
Fullstory	Fullstory zeichnet das Nutzerverhalten auf unserer Webseite auf. Die Aufzeichnungen von Besuchersitzungen ermöglichen es Jimdo, diese zu analysieren und anschließend die Webseitenerfahrung für Besucher zu verbessern. Fullstory speichert und sammelt Daten in anonymisierter Form mithilfe von Cookies.Das Tracking (d.h. die Erfassung der durch das Cookie erzeugten und auf die Nutzung der Website bezogenen Daten) kann jederzeit deaktiviert werden. Bitte folgen Sie hierzu der Anleitung auf https://www.fullstory.com/optout.	Fullstory Inc., 818 Marietta Street, Atlanta, GA 30318, USA	https://www.fullstory.com/legal/privacy/
Surveymonkey	Für Umfragen nutzen wir das Angebot von SurveyMonkey.	SurveyMonkey Europe UC, 2 Shelbourne Buildings, Second Floor, Shelbourne Rd, Ballsbridge, Dublin 4, Ireland	https://de.surveymonkey.com/mp/policy/privacy-policy/

Anlage 2 - Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

Der Auftragsverarbeiter (Auftragnehmer des Auftragsverarbeitungsvertrags) hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die für eine Auftragsverarbeitung erforderlichen technischen und organisatorischen Maßnahmen getroffen, um bei der (Auftrags-)Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die nachstehenden entsprechend dem Katalog aus § 64 BDSG (2017) beschriebenen Maßnahmen beziehen sich auf ergriffene Maßnahmen, die im Rahmen der Auftragsverarbeitung erforderlich sind. Aus Sicherheitsgründen erfolgt nachstehend nur eine allgemeine Beschreibung.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle):

- Die Büroräume der Jimdo GmbH befinden sich in einem Bürohaus in Hamburg und die Zugänge zu den Büroräumen der Jimdo GmbH sind Tag und Nacht verschlossen. Zugang zu den Bürohaus haben nur der Vermieter und die Mieter der Büroräume. Die Büro- und Geschäftsräume von Jimdo sind durch elektronische Schließsysteme gesichert. Nur berechtigte Personen haben entsprechende elektronische Schlüssel. In den Büroräumen von Jimdo werden grundsätzlich keine personenbezogenen Daten für den Auftraggeber gespeichert. Alle auftragsbezogen genutzten IT-Systeme befinden sich in Rechenzentren, die Jimdo nutzt.
- Jimdo trägt Sorge dafür, dass nur Rechenzentren zum Einsatz kommen, die den jeweils geltenden Datensicherheitsanforderungen der Bundesrepublik Deutschland genügen.
- Die von Jimdo verwendeten Rechenzentren sind nach ISO 27001 zertifiziert und verfügen über entsprechend gut ausgestattete Zutrittskontrollmechanismen und –vorkehrungen. Das für den Auftraggeber verwendete Rechenzentrum erfüllt die Anforderungen des Tier 3 -Standards.
- Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.
- Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

- Besucher erhalten erst nach Türöffnung durch den Empfang Zutritt zu den Büroräumen. Der Empfang kann die Eingangstür einsehen und trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet.
- Jeder Besucher wird in einem Besucherbuch protokolliert und dann von der Empfangsperson zu seinem jeweiligen Ansprechpartner begleitet. Zutritte von Besuchern werden stets durch Jimdo-Beschäftigte begleitet. Regelungen für Fremdpersonal und zur Begleitung von Gästen sind vorhanden.
- Die Eingänge und Fenster der Büroräume der Jimdo GmbH sind mit einer Alarmanlage gesichert. Diese kann manuell aktiviert und deaktiviert werden. Unabhängig davon wird die Alarmanlage täglich jedoch stets um 21 Uhr automatisch aktiviert.

1.2 Zugangskontrolle

Es wurden folgenden Maßnahmen getroffen, die die Nutzung der Datenverarbeitungssysteme (Computer) durch unbefugte Dritte verhindern:

- Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von dem jeweiligen Vorgesetzten beantragt wurde. Der Antrag kann auch über die Personalabteilung gestellt werden.
- Der Benutzer erhält dann einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.
- Passwörter werden alle 90 Tage gewechselt. Ausgenommen hiervon sind Passwörter, die über eine Mindestlänge von 32 Zeichen verfügen. Hier ist ein automatischer Passwortwechsel nicht indiziert.
- Eine Passworthistorie ist hinterlegt. So wird sichergestellt, dass die vergangenen 10 Passwörter nicht noch einmal verwendet werden können.
- Fehlerhafte Anmeldeversuche werden protokolliert. Bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.
- Remote-Zugriffe auf IT-Systeme der Jimdo GmbH erfolgen stets über verschlüsselte Verbindungen.
- Auf den Servern der Jimdo GmbH ist ein Intrusion-Prevention-System im Einsatz. Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist.
- Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.
- Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.
- Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.
- Passwörter werden grundsätzlich verschlüsselt gespeichert.

1.3 Zugriffskontrolle

Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Es ist Sache des Auftraggebers, die Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz/Webspace für die Dauer des Vertrages einer geeigneten Zugriffskontrolle zu unterziehen, insbesondere nur geeigneten Dritten (z.B. Webagenturen, Administratoren) Zugang und Zugriff zu gewähren.
- Berechtigungen für IT-Systeme und Applikationen der Jimdo GmbH werden ausschließlich von Administratoren eingerichtet.
- Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind.
- Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten. Der Antrag kann auch bei dem Office Team gestellt werden.
- Es erfolgen Protokollierung von Zugriffen auf die IT-Systeme, um eine unberechtigte Nutzung zu erkennen und auszuschließen.
- Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.
- Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet.
- Alle Mitarbeiter bei Jimdo GmbH sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen.
- Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.
- Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

1.4 Trennung

Die folgenden Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Alle IT-Systeme, die Jimdo für Auftraggeber nutzt, verfügen über eine logische Mandantentrennung, so dass eine Trennung der Daten von Daten, die für andere Zwecke verarbeitet werden, gewährleistet ist.
- Es erfolgt eine getrennte Verarbeitung und/oder Lagerung von Daten mit unterschiedlichen Verarbeitungszwecken.
- Es ist ein System von Befugnissen abgestufter Zugriffsberechtigungen durch die Beschäftigten in den Abteilungen Technik (Administration), Support, Domainverwaltung und Kundenbuchhaltung errichtet.
- Es ist Sache des Auftraggebers, für die Trennung von personenbezogenen Daten auf dem ihm überlassenen Speicherplatz und Baukasten-System, selbst Sorge zu tragen.

1.5 Pseudonymisierung & Verschlüsselung

Die folgenden Maßnahmen gewährleisten, dass die Verarbeitung personenbezogene Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- Es ist Sache des Auftraggebers, personenbezogenen Daten auf dem ihm überlassenen Baukastensystem bzw. Webspace selbst zu pseudonymisieren, soweit dies gesetzlich erforderlich ist.

- Es ist Sache des Auftraggebers, die Daten auf dem ihm vertragsgemäß überlassenen Baukastensystem bzw. Speicherplatz für die Dauer des Vertrages durch geeignete Techniken (Software) zu verschlüsseln.
- Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.
- Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme im Einsatz.

2. Integrität

2.1 Eingabekontrolle

Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Die Eingabe, Änderung und Löschung von Daten wird auf Datenbankebene protokolliert.
- Es ist Sache des Auftraggebers, ggf. personenbezogene Daten dem ihm vertragsgemäß überlassenen Baukastensystem für die Dauer des Vertrages einzugeben und dazu, insbesondere nur geeigneten Dritte einzusetzen (z.B. Webagenturen, Administratoren). Die Beschäftigten des Auftragsverarbeiters dürfen grundsätzlich nicht auf diese Daten zugreifen bzw. Daten eingeben, verändern oder löschen.
- Das Verarbeiten von personenbezogenen Daten erfolgt somit grundsätzlich durch den Auftraggeber, so dass durch den Auftragsverantwortlichen nicht nachträglich überprüft werden und festgestellt werden kann, welche personenbezogenen Daten der Kunde zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert hat.
- Nur im Rahmen seiner Tätigkeiten nach zusätzlicher Weisung, die in schriftform und außerhalb des Webseite-Administrationsbereichs stattfindet, protokolliert der Auftragsverarbeiter diese Eingaben und Veränderungen in angemessener Weise und dokumentiert die Uhrzeit und den Eingebenden.
- Muss der Auftragsverarbeiter(Jimdo) aus gesetzlichen Gründen Informationen entfernen oder den Zugang zu ihnen sperren (etwa im Falle der Nutzung vom Kunden auf den IT-Systemen für Dritte bereit gehaltenen Telemediendiensten bzw. elektronischen Kommunikationsdiensten), wird die Sperrungen bzw. die Entfernung von Inhalten protokolliert. Die Protokolldaten werden aufbewahrt und enthalten die Mitarbeiterkennung. Die Löschung erfolgt nach dem Vertragsende automatisiert und wird protokolliert.

2.2 Weitergabekontrolle

Die folgenden Maßnahmen gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht von Unbefugten 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.

- Für die Administration von Servern kommen nur verschlüsselte Verbindungen zum Einsatz. Eine Weitergabe von Daten des Auftraggebers findet grundsätzlich nicht statt. Ausgenommen hiervon sind Fälle, in denen Jimdo aufgrund gesetzlicher Regelungen oder richterlichen Anordnungen zur Herausgabe von Daten verpflichtet ist.
- Eine Weitergabe von Daten, die auf IT-Systemen von Jimdo im Auftrag des Auftraggebers gespeichert werden, erfolgt ansonsten nur im Zusammenhang mit dem vom Auftraggeber vorgesehenen Betrieb seiner Internetpräsenz (Aufruf der Internetseiten durch Besucher der Internetseite) im jeweils technisch erforderlichen Umfang.

- Die Gewährleistung der Vertraulichkeit der Übermittlung von personenbezogenen Daten wird durch SSL/TSL-Verschlüsselungen über die Webseiten des Auftragsverarbeiters gewährleistet.
- Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.
- Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.
- Die Nutzung von privaten Datenträgern ist den Beschäftigten bei Jimdo GmbH im Zusammenhang mit Kundenprojekten untersagt.
- Mitarbeiter bei der Jimdo GmbH werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.
- Im Übrigen ist es Sache des Kunden, die Daten auf dem ihm vertragsgemäß überlassenen Baukastensystem bzw. Speicherplatz für die Dauer des Vertrages einer geeigneten Transportkontrolle zu unterziehen und geeignete Verschlüsselungstechniken einzusetzen.

3. Verfügbarkeit und Belastbarkeit

Die folgenden Maßnahmen gewährleisten, dass die eingesetzte Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Die von Jimdo genutzten Rechenzentren verfügen über nachfolgende unterbrechungsfreie Stromversorgung (USV), Klimaanlagen in Serverräumen, Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen, Feuer-und Rauchmeldeanlagen, Alarm- und Sicherungssysteme.
- Es ist ein flächendeckendes Brand- und Frühwarnsystem im Einsatz.Daten auf Serversystemen von der Jimdo GmbH werden mindestens täglich inkrementell und wöchentlich „voll“ gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort verbracht.
- Das Einspielen von Backups wird regelmäßig getestet.
- Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich eine Brandmeldeanlage sowie eine CO2-Löschanlage. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.
- Es gibt bei der Jimdo GmbH einen Notfallplan, der auch einen Wiederanlaufplan beinhaltet.
- Daten auf Serversystemen von der Jimdo GmbH werden mindestens täglich inkrementell und wöchentlich „voll“ gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort verbracht.
- Das Einspielen von Backups wird regelmäßig getestet.
- Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich eine Brandmeldeanlage sowie eine CO2-Löschanlage. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Gewährleistungsziel: Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung.

4.1 Datenschutz-Management

- Jimdo setzt einen Kernbestand an langjährig und dauerhaft beschäftigten Technikerpersonal mit DV-technischer Erfahrung und Expertise ein.
- Es erfolgt eine regelmäßige Schulung der Beschäftigten.

- Bei der Jimdo GmbH ist ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.
- Es ist Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.
- Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.
- Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.
- Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnis von dem Vorfall erfolgen.

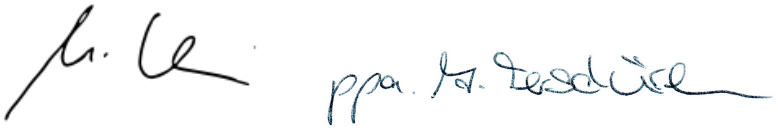
4.2 Auftragskontrolle (Outsourcing an Dritte)

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

- Bei der Jimdo GmbH ist ein betrieblicher Datenschutzbeauftragter benannt.
- Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag nach zuvor durchgeführten Audit durch den Datenschutzbeauftragten von der Jimdo GmbH abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

4.3 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

- Bei der Jimdo GmbH wird schon bei der Entwicklung der Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit schon im Zusammenhang mit Benutzer-Interfaces Rechnung getragen wird. So sind z.B. Formularfelder, Bildschirmmasken flexibel gestaltbar. So können Pflichtfelder vorgesehen oder Felder deaktiviert werden.
- Die Software der Jimdo GmbH unterstützt sowohl die Eingabekontrolle durch einen flexiblen und anpassbaren Audit-Trail, der eine unveränderliche Speicherung von Änderungen an Daten und Nutzerberechtigungen ermöglicht.
- Berechtigungen auf Daten oder Applikationen können flexibel und granular gesetzt werden.



- Auftragnehmer/Jimdo -