Data Processing Agreement

DPA

between

_____

_____

_____

_____

_____

_____

Jimdo Website(s):

Controller / Customer / Jimdo User

-

and

Jimdo GmbH
Stresemannstr. 375
22761 Hamburg
Germany

-

Processor or "***Jimdo***"

-

Preamble

The Controller acknowledges that Jimdo renders services for a variety of customers. The Controller's option to issue additional instructions, especially those that may impede the services rendered by Jimdo for other customers or users is therefore limited by this contract. Jimdo would be unable to operate with a variety of individual instructions from the individual Controllers.

1. General

1.1. In connection with rendering its services to the Controller, Jimdo also processes personal data on behalf of the Controller. According to the parties' wishes, this Agreement includes the written data processing agreement pursuant to § 11 German Federal Data Protection Act and, as of the 25.05.2018 the agreement pursuant to Art. 28 EU Regulation 2016/679 – General Data Protection Regulation (GDPR) and shall govern the rights and obligations of the parties in connection with data processing.

1.2. Insofar as the term "data processing" or "processing" (of data) is used in this contract, the definition of "processing" pursuant to Art. 4 No. 2 GDPR shall apply.

1.3. Insofar as the German Federal Data Protection Act(BDSG) is referenced in this contract, these references shall only be valid until the end of 24.05.2018. Any references in this Agreement to GDPR shall apply from 25.05.2018.

2. Subject Matter of the Agreement

2.1. Jimdo provides an online service whereby Jimdo users such as the Controller can create and operate their own Jimdo website. The provided service allows users to customise the design of their own Jimdo website and to operate a shop. Otherwise the subject matter of the Agreement is governed by the primary contractual relationship concluded between the parties. This is based on the terms and conditions of Jimdo, which were effectively included in the contractual relationship between the parties.

2.2. This data processing agreement applies in addition to the Jimdo terms and conditions of service.

2.3. The following types of data are regularly processed:

- Inventory data of customers of the Controller
  - Name, address
  - Order data
  - for Jimdo shops: Payment data (however this is only stored by the payment provider)
- Usage data of visitors to the Jimdo website of the Controller
  - Jimdo uses various user analysis services (e.g. Google Analytics) to generate statistics for Jimdo users e.g. the Controller; but also to regularly evaluate and optimise the Jimdo service.
- Content entered by visitors to Controller websites (e.g. in comments, guest books and forms).
- Communication data and/or email messages sent via the email provider Rackspace Limited. If an email account or email forwarding is established through a Jimdo website, Jimdo shall create an account with Rackspace Limited for Jimdo users. Rackspace Limited shall then assume the technical delivery and management of the emails on behalf of Jimdo.

2.4. The aforementioned data types are normally processed when using Jimdo services. Data types can vary or be expanded at the discretion of Jimdo, depending on the Jimdo services utilised by the respective Controller. Should the data types deviate from the aforementioned list, the specific data

types shall be specified in a separate annex to this contract. In such case the Controller can contact Jimdo (privacy@jimdo.com) and list the deviating data types accordingly and/or request the separate annex. Jimdo shall ensure that the legal grounds applicable to the collection, processing and use of personal data are observed insofar as this falls within the remit of responsibility of Jimdo. The Controller shall be solely responsible for checking that the processing of data content (e.g. from forms used by the Controller) or other data processed by the Controller itself in connection with the use of its website is legally permitted.

2.5. Sphere of data subjects:

- Customers of the Controller
- Interested parties and/or visitors to the Controller website
- Employees of the Controller

3. Rights and Duties of the Controller

3.1. The Controller or Customer is the controller pursuant to Art. 4 No. 7 GDPR for the commissioned data processing performed by the Processor, Jimdo. In accordance with Fig. 4 para. 5 the Processor shall have the right to inform the Controller if it believes the commission and/or instruction constitutes unlawful data processing. Insofar as the Processor can demonstrate that data processing as per the Controller's instruction may expose the Processor to liability pursuant to Art. 82 GDPR, the Processor shall have the right to suspend further processing until the parties have clarified liability.

3.2. The Controller is obligated to only forward to Jimdo or collect via Jimdo, data that is lawfully collected in accordance with Art. 6 para. 1 EU-DSGVO and processed in accordance with the purpose for which it has been collected. The Controller is responsible for upholding the rights of the data subject and in particular to comply with the duty to inform and to enable the persons concerned to exercise their right of objection. The rights of the data subject must be upheld and maintained vis-à-vis the Controller. The Processor shall inform the Controller immediately if data subjects assert their rights vis-à-vis the Processor and this directly affects the Controller.

3.3. The Controller may issue Jimdo additional instructions as regards the processing of personal data. The customer can issue these instructions primarily in the administration area of their Jimdo website and account, through a corresponding service configuration. Thus e.g. web analysis settings can be configured here. Further instructions must be sent to Jimdo in writing (e.g. email). Jimdo shall then check the feasibility of the instructions, taking into account the functionality of Jimdo services in the interest of all customers, and shall inform the Controller of the costs of implementing the individual instruction. The instruction can be implemented after conclusion of a cost assumption declaration. Arrangements concerning any compensation of additional costs incurred by the Processor due to additional instructions of the Controller shall remain unaffected.

3.4. The Controller can designate persons authorised to issue instructions in the administration area of its Jimdo page via adding and saving their email address there. Should the persons authorised to issue instructions on behalf of the Controller change, the Controller shall inform the Processor of this in writing in and/or by amending the email address on file in the Jimdo administration area.

3.5. The Controller shall inform the Processor immediately if it ascertains an error or irregularity in connection with the processing of personal data by the Processor.

3.6. Should there be an obligation to inform third parties pursuant to Art. 33, 34 GDPR or another statutory reporting obligation applicable to the Controller, the Controller shall be responsible for observing such an obligation.

4. General obligations of the Processor

4.1. The Processor shall process personal data solely within the context of concluded agreements and/or in accordance with additional instructions issued by the Controller, where applicable. This shall exclude statutory provisions, whereby the Processor is duty-bound to alternative processing. In such case the Processor shall notify the Controller of these legal requirements before processing, insofar as the provision in question does not prohibit such notification for reasons of public interest. Otherwise the purpose, type and scope of data processing shall be governed solely by this Agreement and/or the instructions of the Controller. Any alternative data processing by the Processor shall be prohibited, unless the Controller has approved this in writing.

4.2. Jimdo shall ensure that the data processing rendered as part of its service under the primary contract, which involves subprocessors pursuant to Point 6 of this contract, is performed in accordance with the provisions of this contract.

4.3. Insofar as the data processing is commissioned directly by the Controller notwithstanding Fig. 4.1, Jimdo shall process the data only in member states of the European Union (EU) or the European Economic Area (EEA) or in the event of data processing in an external state, shall set regulations that enable permissible processing pursuant to Art. 46 GDPR.

4.4. Jimdo shall design its company and its operational processes in such a way that ensures the data processed on behalf of the Controller is appropriately secured and protected against unauthorised third-party access. Any changes to the organisation of the commissioned data processing relevant to data security shall be agreed with the Controller in advance.

4.5. Jimdo shall inform the Controller immediately if an instruction issued by the Controller is deemed to be in breach of statutory regulations. The Processor shall be entitled to suspend execution of the instruction in question until this is confirmed or amended by the Controller. Insofar as the Processor can demonstrate that data processing as per the Controller's instruction may expose the Processor to liability pursuant to Art. 82 GDPR, the Processor shall have the right to suspend further processing until the parties have clarified liability.

4.6. The data processing on behalf of the Controller outside the business premises of the Processor or subprocessors shall only be permitted with the written consent of the Controller, unless the parties have otherwise, reached an agreement that in particular ensures the data security and the audit rights under section 4 (General obligations of the contractor) of this Agreement. A processing of data for the Controller in private homes is only permitted with the consent of the Controller in text form, unless the parties concerned (the processor and employee) have entered into a written agreement, in particular the data security and the audit rights in accordance with § 4 below (General obligations of the contractor) ensures this agreement.

4.7. Jimdo shall handle the data processed on behalf of the Controller separately from other data. Physical separation is not strictly necessary. Jimdo shall appropriately label the data processed on behalf of the Controller. Insofar as the data is processed for different purposes, Jimdo shall label the data as per the respective purpose.

4.8. Jimdo can – but is not obligated – to announce to the Controller the authorised recipients for the receipt of the instructions from the Controller. Should the authorised recipients change, the Processor shall inform the Controller of this in text form.

5. Data protection officer of the Processor

Jimdo has appointed an external data protection officer pursuant to Art 37 GDPR. This is:

B³ | Informationstechnologie Andreas Bethke
Papenbergallee 34
25548 Kellinghusen
Germany
Email: privacy@jimdo.com

6. Notification obligations of the Processor

6.1. Jimdo shall immediately inform the Controller of any breach of data protection regulations or any breach of contractual agreements and/or instructions issued by the Controller that occur during data processing by it or by other persons involved in the processing. The same shall apply to any breach of personal data privacy as regards the data processed on behalf of the Controller.

6.2. Furthermore Jimdo shall inform the Controller immediately if a supervisory authority pursuant to Art. 58 GDPR takes action against Jimdo, where this may also involve the monitoring of data processing that Jimdo renders on behalf of the Controller.

6.3. Jimdo acknowledges that the Controller may be subject to a data breach notification obligation pursuant to Art. 33, 34 GDPR that stipulates notification to the supervisory authorities within 72 hours of having become aware of the breach. The Processor shall support the Controller in fulfilling its reporting obligations. In particular, the Processor shall inform the Controller in text form (fax/email) of any unauthorised access to personal data that is processed on behalf of the Controller, immediately but no later than within 48 hours of becoming aware of such an incident. The Processor's report to the Controller must include the following information in particular:

- a description of the type of breach of personal data privacy, where possible with indication of the categories and the approximate number of data subjects affected, categories affected and the approximate number of personal data records affected;
- a description of the measures taken or proposed by the Processor to remedy the breach in protecting the personal data and where necessary, measures to mitigate the potentially negative effects of this.

7. Processor's obligation to cooperate

7.1. Jimdo shall support the Controller in its duty to respond to requests from data subjects to assert their rights pursuant to Art. 12-23 GDPR. The regulations of Point 11 of this Agreement shall apply.

7.2. Jimdo must cooperate in the creation of Records of processing activities by the Controller. It shall share necessary information with the Controller in an appropriate manner.

7.3. Taking into account the type of processing and the information available to him, the Processor shall assist the Controller in complying with the obligations set out in Articles 32-36 GDPR.

8. Supervisory powers

8.1. To enable the Controller to exercise its supervisory rights and obligations prior to and during the contractual relationship, upon request Jimdo shall provide the Controller with a report written by its external data protection officer concerning the technical and organisational measures adopted by Jimdo and used in Jimdo data centres. The report shall be updated at least every 24 months.

8.2. For further questions the Controller can contact Jimdo's external data protection officer.

8.3. The Controller shall have the right to monitor Jimdo's compliance with statutory data protection regulations and/or compliance with contractual regulations agreed between the parties and/or compliance with instructions of the Controller, at any time and to the necessary extent.

8.4. Jimdo shall be obligated to share information with the Controller, insofar as this is necessary to conduct the monitoring pursuant to paragraph 8.3.

8.5. The Controller can ask to inspect the data processed by Jimdo for the Controller, as well as the data processing systems and programs used.

8.6. After prior notification with appropriate notice (at least ten business days), the Controller may inspect the business premises of Jimdo GmbH during standard business hours pursuant to paragraph 8.5. In order to avoid disproportionate disruption to the operations of the Processor, the Controller shall ensure that the inspections are limited to the extent required. In principle, the effort involved in an inspection by the Processor shall not exceed one day per calendar year. Where confidential internal information is disclosed by the Processor for or during such an inspection, particularly details on technical and organisational measures, the Controller shall protect this confidentiality and shall not share this information with or disclose it to third parties, unless for the purpose of the contractual relationship between Controller and Processor.

8.7. Should supervisory authorities take action against the Controller pursuant to Art. 58 GDPR, particularly as regards disclosure and inspection obligations, Jimdo shall share the necessary information with the Controller and shall facilitate an on-site inspection by the relevant supervisory authorities. The Controller must be informed of corresponding measures planned by the Processor.

8.8. The Controller shall be entitled to have the inspection performed by an auditor appointed individually in text form at least ten days prior to the inspection, provided the Processor consents to such an external audit. The Processor shall not unreasonably withhold its consent. In particular, the Processor shall be entitled to deny the auditor access if the auditor is in direct competition with the Processor. External auditors shall conclude a written confidentiality agreement with the Processor and only then shall be granted leave to conduct the audit. The auditing powers of the Controller shall remain unaffected.

9. Subcontracting

9.1. Jimdo may engage subprocessors to render its services vis-à-vis service users, which also includes the processing of personal data. Jimdo shall indicate all subprocessor relationships that pre-exist the Agreement in "Annex 1" of this contract. The change of subprocessors or the instruction of additional subprocessors shall be permitted subject to the conditions stipulated in point 9.4.

9.2. Jimdo must select subprocessors carefully and shall check prior to engagement that these subprocessors can comply with the agreements made between the Controller and Jimdo. In particular, prior to and regularly during contractual term, Jimdo must check that the subprocessor has taken the necessary technical and organisational measures pertaining to personal data privacy pursuant to Art. 32 GDPR. Jimdo shall document its findings and convey these to the Controller at their request.

9.3. Jimdo shall have the subprocessor confirm that it has appointed a corporate data protection officer pursuant to Art. 37 GDPR. If the subprocessor has not appointed a data protection officer, Jimdo must inform the Controller accordingly and must demonstrate that the subprocessor is not legally obligated to appoint a data protection officer. Jimdo must ensure that the regulations agreed in this Agreement also apply to the subprocessor. Jimdo must regularly monitor its compliance with these obligations.

9.4. Jimdo shall promptly inform the Controller in writing if it intends to change or engage a new subprocessor, however no later than 4 weeks before the change and/or the new engagement ("information"). The Controller shall have the right to object to the change/new engagement of subprocessor in writing, citing reasons, within three weeks of receiving the "information". The

Controller can withdraw its objection in writing at any time. In the event of an objection, the Processor can terminate the contractual relationship with the Controller with a notice period of at least 14 days to the end of a calendar month. With such notice period the Processor shall give appropriate consideration to the interests of the Controller. If no objection of the Controller is received within three weeks of receiving the “information”, the change and/or new engagement of the relevant subprocessor shall be deemed approved by the Controller.

9.5. Jimdo must ensure that the regulations agreed to in this Agreement and any supplementary instructions of the Controller also apply to the subprocessor. Jimdo shall regularly monitor its compliance with these obligations.

9.6. Jimdo must conclude a data processing Agreement with the subprocessors, which meets the requirements of Art. 28 GDPR. Furthermore, Jimdo must impose the same data protection obligations on the subprocessor as those established between the Controller and Jimdo. The Controller can request a copy of the relevant data processing Agreement upon request.

9.7. In particular Jimdo shall ensure through contractual provisions that the supervisory powers (Point 5 of this contract) of the Controller and of supervisory authorities also apply to the subprocessor and that corresponding supervisory rights are agreed by Controller and supervisory authorities. It shall also be contractually agreed that the subprocessor must accept these supervisory measures and any on-site inspections.

9.8. Third-party services engaged by the Processor as purely supplementary services to facilitate its business activities shall not be considered a subcontractual relationship pursuant to paragraphs 9.1 to 9.7. For example this includes cleaning services, purely telecommunication services without specific reference to services rendered by the Processor on behalf of the Controller, postal and courier services, transport services as well as security services. For supplementary services rendered by third parties, the Processor shall nevertheless ensure that appropriate precautions and technical and organisation measures are taken to guarantee personal data privacy. The service and maintenance of IT systems or applications shall constitute a subcontractual relationship and commissioned processing pursuant to Art. 28 GDPR if the service and maintenance concerns IT systems that are also used in connection with the provision of services for the Controller and if access to personal data processed on behalf of the Controller may be obtained during maintenance.

10. Obligation of Confidentiality

10.1. When processing data on behalf of the Controller, Jimdo shall protect the confidentiality of data that it receives and/or ascertains in connection with the contract.

10.2. Jimdo shall ensure that it is familiar with the respective, applicable data protection regulations and their application. Jimdo shall also ensure that employees entrusted with carrying out data processing tasks are familiar with relevant data protection provisions and that such employees are bound by confidentiality pursuant to GDPR and by data secrecy pursuant to §53 German Federal Data Protection Act (new).

10.3. The personnel obligation pursuant to paragraph 2 must be demonstrated to the Controller upon request.

11. Protection of data subjects’ rights

11.1. The Controller is solely responsible for protecting the rights of the data subject. The Processor is obliged to support the Controller in his duty to process requests from data subjects in accordance with Articles 12-23 GDPR insofar as the Controller is unable to satisfy the demands without the cooperation of Jimdo GmbH. The Processor shall in particular ensure that the information required in this respect is

provided to the Controller without delay so that the Controller is able to fulfil his obligations under section 12 (3) GDPR in particular.

11.2. Insofar as cooperation of the Processor is required to enable the Controller to protect data subjects' rights – particularly rights to information, correction, blocking or erasure – the Processor will undertake the necessary measures on instruction by the Controller. Where possible, the Processor shall assist the Controller with appropriate technical and organisational measures to fulfil his obligation to respond to requests for the exercise of the data subjects' rights.

11.3. Provisions concerning remuneration of additional expenses incurred through participation of the Processor in connection with assertion of data subjects' rights against the Controller remain unaffected.

12. Confidentiality obligations

12.1. Both Parties hereby undertake to treat all information received in connection with the processing of this Agreement indefinitely confidential and to use the information only for carrying out the Agreement. No Party has the right to use the information in part or as a whole for other than those mentioned purposes or to make this information available to Third Parties.

12.2. The foregoing obligation shall not apply for information that one Party received demonstrably from Third Parties, without being bound by secrecy or which are publicly known.

13. Remuneration

13.1. The Processor's remuneration is provided for by way of a separate agreement

14. Technical and organisational data security measures

14.1. Jimdo has a duty towards the Controller to comply with the technical and organisational measures required to ensure compliance with the applicable data protection regulations. In particular this shall include the provisions of Art. 32 GDPR.

14.2. The technical and organisational measures in their current version at the time of concluding the Agreement are attached to this Agreement as Annex 2. The parties shall also agree that amendments to the technical and organisational measures may be required in order to adapt to technical and legal circumstances. Significant amendments that may impair the integrity, confidentiality or availability of the personal data shall be agreed by Jimdo and the Controller in advance. Measures that involve only minor technical or organisational changes and that do not negatively affect the integrity, confidentiality and availability of personal data can be implemented by Jimdo without the consent of the Controller. Once per year or where reasonable grounds exist, the Controller can request a current version of the technical and organisational measures taken by Jimdo.

14.3. Jimdo will regularly, and as the occasion may warrant, monitor the effectiveness of the technical and organisational measures it takes. Jimdo shall inform the Controller should the need for optimisation and/or amendment arise.

15. Duration of the Agreement

15.1. The Agreement shall commence upon signature and shall be valid for the duration of the primary Contract concluded between the parties concerning utilisation of the services of the Processor. The Agreement may be terminated one month to the end of the respective term. The termination must be rendered in text form.

15.2. The Controller can terminate the Agreement without notice at any time should Jimdo GmbH commit a serious breach of the applicable data protection regulations or obligations under this contract; if Jimdo cannot or will not perform an instruction of the Controller; or if Jimdo denies the Controller or relevant supervisory authorities access contrary to the contract.

16. Termination

16.1. After termination of the contract, at the discretion of the Controller Jimdo shall return or delete all documents and data in its possession, as well as all processing or usage results generated in connection with the contractual relationship. The deletion must be documented in an appropriate manner. Any statutory retention requirements or other obligations to store the data shall remain unaffected. Should the Controller request deletion, data carriers must be destroyed in accordance with at least DIN 66399 Security Level 3 of the national standard DIN 66399 (Office machines - Destruction of data carriers - Part 1: Principles and definitions) must be observed. The destruction must be verified to the Controller with reference to the security level in accordance with DIN 66399.

16.2. The Controller shall have the right to verify the complete and contractual return and deletion of the data by the Processor. This can also be performed by inspecting the data processing systems at the business premises of the Processor. The Controller should provide appropriate notice(at least 10 working days) for the on-site inspection.

17. Right of retention

17.1. The Parties agree that the plea of retention by the Processor in the meaning of section 273 German Civil Code (Bürgerliches Gesetzbuch, BGB) concerning the processed data and associated data storage devices is excluded.

18. Final provisions

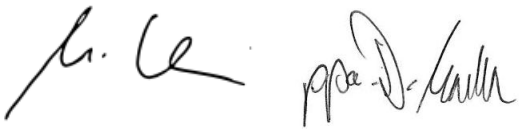
18.1. The Processor must inform the Controller immediately should property of the Controller in the possession of the Processor be compromised by third-party measures (e.g. by attachment or seizure), by insolvency proceedings or by other circumstances. The Processor shall immediately inform the creditors of the fact that the data is processed as part of a commissioned data processing contract.

18.2. Written form is compulsory for ancillary agreements.

18.3. Should individual parts of this Agreement be invalid, this shall not affect the validity of the other provisions of the contract.

18.4. In the event of translation discrepancies, the German formulation shall apply.

19. Signatures

_____	_____
Place, date	- Controller -
Hamburg, 11.05.2018	
_____	- Processor/Jimdo -
Place, date	Matthias Henze (CEO) Dennis Manzke (Head of Finance and Administration)

Annex 1 - Subprocessors

For the purpose of processing data on behalf of the Controller, the Processor shall engage services of third parties to process data on its behalf ("Subprocessors").

Infrastucture / Technical platform:			
Mandrill	Newsletter, Notifications	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	Notifications, Newsletter	SendGrid Inc., 1801 California St #500, Denver, CO 80202, USA	https://sendgrid.com/policies/privacy/
Google Tag Manager	The Tag Manager tool is a cookie-less domain and does not collect personally identifiable information. The tool triggers other tags, which may collect data.	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://www.google.com/analytics/tag-manager/use-policy/
Google Analytics	User Statistics	Google LLC, 1600, Amphitheatre Parkway, Mountain View, CA 94043, USA	Browser Plugin, Opt-Out https://tools.google.com/dlpage/gaoptout?hl=en/
Adobe Image Editor	Image editing via the user menu	Adobe Systems Incorporated, 345 Park Avenue, San Jose, CA 95110-2704, USA	http://www.adobe.com/privacy.html
Firebase	Firebase is a real time database, which we use for real time data-exchange and storage(For example in our apps). All user data are anonymized for transmission to Firebase	Firebase is a Google subsidiary and is based in San Francisco (CA), USA.	https://www.firebase.com/terms/privacy-policy.html
Sipgate	Fax service for the sending and receipt of faxes.	sipgate GmbH Gladbacher Straße 74 40219 Düsseldorf Deutschland	https://www.sipgate.de/datenschutz.html
Rackspace	A web based application for the technical delivery and management of emails or email accounts	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	Fraud detection tool	Sift Science, Inc., 123 Mission Street, 20th Floor, San Francisco, CA 94105	https://siftscience.com/service-privacy
Stripe	Payment processor	Stripe Inc.,185 Berry Street, Suite 550, San Francisco, CA 94107, USA	https://stripe.com/de/privacy
Global Collect	Payment processor	Global Collect Service B.V., Planetenweg 43 - 59, 2132 HM Hoofddorp, NL	http://www.globalcollect.com/Privacy
Zuora	Subscription Management	Zuora Inc., 3050 S. Delaware Street, Suite 301, San Mateo, CA 94403, USA	https://www.zuora.com/privacy-statement/

Add This	A bookmarking service that simplifies the bookmarking of websites	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	Crash/Problem Reporting	Fabric is a Google Inc. subsidiary and is based in San Francisco (CA), USA.	https://fabric.io/terms?locale=en-us&utm_campaign=fabric-marketing&utm_medium=natural
InternetX	Domain administration	InterNetX GmbH, Maximilianstr. 6, 93047 Regensburg, Germany	https://www.internetx.com/rechtliches/datenschutz/
RankingCoach	Search engine result optimization tool	rankingCoach GmbH, Brügelmannstrasse 3, 50679 Köln, Germany	https://www.rankingcoach.com/en-us/privacy-policy
status.io	Status page with up-to-date information on the accessibility and functionality of our system.	T3CH.com LLC, 19 N. County Line Road, Jackson, NJ 08527, USA	https://status.io/privacy
Paypal	Payment Provider	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
wpengine	Webspace for the Jimdo Blog	WP Engine Irongate House, 22-30 Duke's Place London, EC3A 7LP United Kingdom	https://wpengine.com/legal/privacy/
Fastly Inc.	Content Delivery	Fastly, Inc., General Counsel, 475 Brannan St, Suite 300, San Francisco, CA 94107, USA	https://www.fastly.com/privacy
Disqus	Comments system	DISQUS, Inc., 301 Howard St, Floor 3, San Francisco, California 94105, USA	https://help.disqus.com/terms-and-policies/disqus-privacy-policy
G-Suite	Use of Google productivity systems with the Jimdo email system	A product of 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	Ticket system for support requests	Zendesk, Inc., 1019 Market Street, San Francisco, CA 94103, USA	https://www.zendesk.de/company/customers-partners/#privacy-policy
Launchdarkly	We use the Feature Flags of LaunchDarkly for our intrernal Flighting-Systeme	Catamorphic, Co. ("LaunchDarkly"), 405 14th Street, Oakland, CA 94612, USA	https://launchdarkly.com/policies/privacy/
Facebook Login	Single-Sign-On technology	Facebook Inc., 1 Hacker Way, Menlo Park, CA 94025, USA	https://www.facebook.com/about/privacy/
Google Plus Login	Single-Sign-On technology	A product of Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://www.google.de/intl/de/policies/privacy/
Youtube	Youtube embedding function for displaying and playing videos of the provider "Youtube"	A product of Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://www.google.de/intl/de/policies/privacy
Prefinery	Tool for customer acquisition and product publications	Prefinery, 1108 Lavaca Street, Suite 110-318, Austin, TX 78701, USA	https://www.prefinery.com/privacy
Redis	Data bank provider	Redislabs, 700 E El Camino Real Suite 250, Mountain View, CA 94040	https://redislabs.com/privacy/
sentry.io	Crash/Problem Reporting for the mobile app	A product of Functional Software, Inc., 132 Hawthorne St, San Francisco, CA 94107	https://sentry.io/privacy
Name.com	Domain administration	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 Files	Amazon Web Services, Germany GmbH, Krausenstr. 38, 10117 Berlin, Germany	https://aws.amazon.com/de/privacy/?nc1=f_pr
Internal Tools:			
Jira	Problem solving and documentation	Atlassian, 55 Broadway Floot 17&25 New York, NY 10006 USA	https://www.atlassian.com/legal/privacy-policy
Slack	Internal communications solution	436 Lafayette Street, 1008 Western Ave #401, Seattle, WA 98104	https://slack.com/intl/de-de/privacy-policy
Trello	Internal planning and communications tool	Atlassian, 55 Broadway Floot 17&25 New York, NY 10006 USA	https://trello.com/privacy
Tableau	Tool for the analysis of data and data logs	Tableau Germany GmbH, An der Welle 4, 60322 Frankfurt am Main, Germany	https://www.tableau.com/de-de/privacy
Github	Online service for software development projects	Github, 88 Colin P Kelly Jr St, San Francisco, CA 94107, USA	https://help.github.com/articles/github-privacy-statement/
Microsoft	Internal use of 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 & Custom Audiences	In the case of explicit consent, this may track the behavior of users after they have seen or clicked on a Facebook ad. This process is designed to evaluate the effectiveness of Facebook advertisements for statistical and market research purposes and may help to ptimize future advertising efforts.	Facebook Inc., 1 Hacker Way, Menlo Park, CA 94025, USA	https://www.facebook.com/about/privacy/
Hotjar	Conversion optimisation	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 recommendation platform	Taboola, Inc., 28 West 23rd Street, 5th Floor, New York, NY 10010, USA	https://www.taboola.com/privacy-policy
Tv-Squared	This website uses TVSquared for statistical analysis of visitors' traffic in connection with TV advertising	TV Squared Limited, Codebase, Argyle House, 3 Lady Lawson St, Edinburgh, EH3 9DR	http://tvsquared.com/privacy-policy/
bunchbox	Site Optimization tool for the implementation of A / B tests and multivariate analyzes	app.bunchbox.co, Peaks & Pies GmbH, Raboisen 30, 20095 Hamburg, Deutschland	http://peaksandpies.com
smartly.io	Tool for advertising campaigns for Facebook and 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 records user behavior on our website. Visitor recordings allow Jimdo to analyze them and then improve the visitors' website experience. Fullstory stores and collects data in an anonymous form using cookies.Tracking (that is, the collection of data generated by the cookie and related to the use of the website) can be deactivated at any time. Please follow the instructions on https://www.fullstory.com/optout.	Fullstory Inc., 818 Marietta Street, Atlanta, GA 30318, USA	https://www.fullstory.com/legal/privacy/
Surveymonkey	For surveys we use the services of SurveyMonkey.	SurveyMonkey Europe UC, 2 Shelbourne Buildings, Second Floor, Shelbourne Rd, Ballsbridge, Dublin 4, Ireland	https://de.surveymonkey.com/mp/policy/privacy-policy/
Trustpilot	Customer Reviews	Trustpilot A/S, Pilestræde 58, 5, 1112 Kopenhagen, Dänemark – de.trustpilot.com	http://legal.trustpilot.de/end-user-privacy-terms
Bing	Online Marketing	Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA	http://choice.microsoft.com/de-de/opt-out

Annex 2 - Technical and organisational measures of the Processor

The Processor shall take the following technical and organisational data security measures pursuant to Art. 32 GDPR.

The processor (Processor of the commissioned data processing contract) has taken the necessary technical and organisational measures for commissioned data processing in order to guarantee a level of security appropriate to the risks involved in the (commissioned) processing of personal data, taking into account the state-of-the-art, implementation costs, type, scope, circumstances and the purpose of processing, as well as the probability of occurrence and the gravity of the risks associated with data processing as regards the legal interests of the data subjects.

The measures described below as per the catalogue from § 64 GDPR (2017) refer to measures taken that are necessary in the context of the commissioned processing. For security reasons only a general description is shown below.

1. Confidentiality

1.1 Access Control

The following measures have been taken to prevent unauthorised entry to the data processing facilities in which personal data is processed or used (entry control):

- The offices of Jimdo GmbH are located in an office building in Hamburg and access points to the offices of Jimdo GmbH are locked day and night. Only the lessor and lessees of offices have access to the office building. The offices and business premises of Jimdo are secured by electronic locking systems. Only authorised persons have corresponding electronic keys. Under normal circumstances, no personal data shall be stored for the controller on the office premises. All IT systems used in relation to the Agreement are located in data centres used by Jimdo.
- Jimdo shall ensure that only data centres that satisfy the applicable data security standards of the Federal Republic of Germany are used.
- The data centres used by Jimdo are certified in accordance with ISO 27001 and are equipped with suitable access control mechanisms and precautions. The data centre used for the Controller satisfies the requirements of the Tier 3 Standard.
- Keys are distributed and managed in accordance with a defined process that governs the issue and/or withdrawal of entry permissions to premises both at the start and end of an employment relationship.
- Entry permissions shall only be issued to an employee where requested by relevant senior personnel and/or the human resources department. The principle of necessity shall be considered in the allocation of permissions.
- Visitors shall only be permitted to enter the office premises once the main doors are opened by the reception. The reception can see the entry door and shall ensure that each visitor reports to the reception.
- Each visitor shall be recorded in a visitors' book and then be accompanied to his/her respective contact by reception personnel. Visitors shall be accompanied by Jimdo employees at all times. Rules for external personnel and for accompanying guests are available.
- The doors and windows of the Jimdo GmbH office premises are fitted with an alarm system. This can be manually activated and deactivated. However, the alarm system always activates automatically at 21:00 regardless.

1.2 System Access Control

The following measures have been taken to prevent use of the data processing systems (computers) by unauthorised third parties:

- Users must have a corresponding access authorisation to gain access to IT systems. Corresponding user authorisations are issued by administrators. However, these are only issued by corresponding request of relevant senior personnel. The request can also be made through the human resources department.
- The user then receives a user name and a temporary password, which must be changed upon initial login. The password requirements include a minimum password length of 8 characters, whereby the password must include capital/lower case letters, numbers and special characters.
- Passwords shall be changed every 90 days. This shall exclude passwords that have a minimum length of 32 characters. Here an automatic password change is not indicated.
- A password history is stored. This ensures that the previous 10 passwords cannot be re-used.
- Unsuccessful login attempts shall be logged. In the event of 3 incorrect entries, the respective user account shall be locked.
- Remote access to the IT system of Jimdo GmbH is always through encrypted connections.
- An intrusion prevention system is employed on the Jimdo GmbH servers. All server and Controller systems have virus protection software, which guarantees a daily provision of signature updates.
- All servers are firewall-protected, which are constantly serviced and maintained with updates and patches.
- Server and Controller access to the internet and access to these systems via the internet is also secured by firewalls. This also guarantees that only the ports required for the respective communication are usable. All other ports are blocked accordingly.
- All employees are instructed to lock their IT systems when leaving these unattended.
- As a matter of principle, passwords are stored in encrypted form.

1.3 Data Access Control

The following measures have been taken to guarantee that persons authorised to utilise a data processing system solely have access to the data within their authorisation remit, and that personal data cannot be read, copied, amended or removed by unauthorised persons during processing, utilisation and after storage.

- It is the Controller's responsibility to establish suitable access control for the data on the memory/webspace supplied for the duration of the contract; in particular physical access and access may only be granted to suitable third parties (e.g. web agencies, administrators).
- Authorisations for IT systems and applications of Jimdo GmbH shall be established solely by administrators.
- As a matter of principle, authorisations shall be granted on a need-to-know basis. Accordingly only persons who update and maintain and/or are involved in the development of data, applications or databases shall obtain access rights to said data, databases or applications.
- This is subject to a corresponding authorisation request lodged by senior personnel for an employee. The request can also be made to the office team.
- An access log for the IT system is created to identify and eliminate unauthorised use.
- There is a role-based authorisation concept with the option of differentiated assignment of access authorisations, which ensures that personnel obtain access rights to applications and data depending on their respective remit and project, where applicable.
- Data carriers and paper shall be destroyed by a service provider that guarantees destruction in accordance with DIN 66399.
- All employees of Jimdo GmbH are instructed to dispose of information containing personal data and/or information about projects in the designated destruction receptacles.
- In principle employees are prohibited from installing non-approved software on the IT systems.
- All server and Controller systems are regularly updated with security updates.

1.4 Separation

The following measures guarantee that the data collected for different purposes can be processed separately:

- All IT systems that Jimdo uses for Controllers are equipped with a logical Controller separation, which guarantees the separation of the data from data processed for other purposes.

- Data with various processing purposes is processed and/or stored separately.
- A framework of graduated access authorisations is established by personnel in the technical (administration), support, domain management and customer accounting departments.
- It is the Controller's responsibility to ensure the separation of personal data on the memory and modular system supplied.

1.5 Pseudonymisation & Encryption

The following measures guarantee that personal data is processed in such a way that the data can no longer be attributed to a specific data subject without additional information, insofar as this additional information is stored separately and is subject to corresponding technical and organisational measures.

- It is the Controller's responsibility to pseudonymise the personal data processed/saved on and via the Jimdo website system, where required by law.
- It is the Controller's responsibility to encrypt the data processed/saved on and via their Jimdo website system supplied for the duration of the Agreement using suitable technology (software).
- Administrative access to server systems is provided via encrypted connections.
- Furthermore, data on server and Controller systems shall be stored on encrypted data carriers. Corresponding hard drive encryption systems are employed.

2. Integrity

2.1 Data Entry control

The following measures can be used to subsequently review and establish whether and by whom personal data has been entered, amended or removed from data processing systems:

- The input, amendment and deletion of data is logged at database level.
- It is the Controller's responsibility to input personal data into the Jimdo website builder system supplied for the duration of the contract; in particular only suitable third parties (e.g. web agencies, administrators) shall be engaged. In principle, the personnel of the processor may not access this data and/or enter, amend or delete data.
- The Controller shall process the data in such a way that the processor cannot subsequently examine and establish which personal data the customer has entered or amended in automatic processing systems, or at what time and by whom such operations were performed.
- The processor shall log these entries and amendments and document the time and the individual only in the context of its activities as per additional instruction, which must be lodged in writing and outside the website administration area.
- If the processor (Jimdo) must remove information or block access to information on legal grounds (e.g. in cases where the customer uses telemedia services and/or electronic communication services retained for third parties on the IT systems), the blocks and/or the removal of content shall be logged. The logged data is stored and includes the employee identification. Deletion takes place automatically after the end of the Agreement and is logged.

2.2 Data Transmission Control

The following measures guarantee that personal data cannot be read, copied, amended or removed by unauthorised persons during electronic transmission, or during its transport or storage on data carriers, and that it is possible to examine and establish where personal data is to be transmitted by data transmission equipment.

- Only encrypted connections are used for the administration of servers. Controller data is categorically not transmitted. This shall exclude cases in which Jimdo is obligated to surrender data in accordance with statutory regulations or judicial orders.
- Otherwise data stored on IT systems of Jimdo on behalf of the Controller shall only be transmitted in connection with the operation of the Controller's intended online presence (retrieval of web pages by website users) within the necessary technical scope.
- SSL/TSL encryptions via the websites of the processor guarantee the confidential transmission of personal data.
- All employees working on a customer project shall be instructed in the permissible use of data and the methods of transmitting data.
- Wherever possible, data is transmitted to the recipient in encrypted form.

- The use of private data storage media by employees of Jimdo GmbH in connection with customer projects is prohibited.
- Employees of Jimdo GmbH are regularly trained in data protection. All employees have an obligation to treat personal data confidentially.
- Otherwise it is the responsibility of the Controller to establish suitable transport controls for the data on the Jimdo website builder system and/or memory supplied to them for the duration of the Agreement and to use suitable encryption technology.

3. Availability and Resilience

The following measures guarantee that the data processing system used functions perfectly at all times and that personal data is protected against accidental destruction and loss.

- The data centres used by Jimdo are equipped with an uninterruptible power supply (UPS), air-conditioned server rooms, temperature and moisture monitoring equipment in server rooms, fire and smoke alarms, alarm and security systems.
- A comprehensive fire and early warning system is in use. Incremental backups of data on Jimdo GmbH server systems are performed at least daily and a full backup is performed weekly. The backup media are encrypted and taken to a physically separate location.
- The import of backups is regularly tested.
- The IT system has an uninterruptible power supply. The server room is equipped with a fire alarm and a CO2 extinguishing system. All server rooms are monitored, whereby immediate alerts are sent to an administrator in the event of faults.
- Jimdo GmbH has an emergency plan, which also includes a recovery plan.
- Incremental backups of data on Jimdo GmbH server systems are performed at least daily and a full backup is performed weekly. The backup media are encrypted and taken to a physically separate location.
- The import of backups is regularly tested.
- The IT system has an uninterruptible power supply. The server room is equipped with a fire alarm and a CO2 extinguishing system. All server rooms are monitored, whereby immediate alerts are sent to an administrator in the event of faults.

4. Procedure for Regular Review, Assessment and Evaluation

Guarantee objective: Procedure for the regular review, assessment and evaluation of the efficacy of technical and organisational measures to guarantee data protection-compliant processing.

4.1 Data protection management

- Jimdo employs a core team of long-term and permanent technical personnel with experience and expertise in data processing.
- Employees receive regular data protection and security training.
- Jimdo GmbH implements data protection management. There are guidelines on data protection and data security, as well as policies to guarantee the implementation of the guideline objectives.
- A Data Protection and Information Security Team (DST) has been established to plan, implement, evaluate and update measures in data protection and data security.
- The effectiveness of guidelines are regularly evaluated and adapted.
- In particular, it shall also be ensured that data protection incidents are recognised by all employees and reported to the DST immediately. The DST shall investigate the incident immediately. Insofar as data being processed on behalf of customers is affected, these shall be notified immediately of the type and extent of the incident.
- If data is processed for internal purposes, where the conditions of Art. 33 GDPR exist the supervisory authorities must be notified within 72 hours of discovery of the incident.

4.2 Contract control (third-party/Subprocessor outsourcing)

The following measures guarantee that personal data processed as part of commissioned processing can only be processed as per the instructions of the Controller.

- Jimdo GmbH shall appoint a company data protection officer.
- Where external service providers or third parties are involved, a data processing Agreement shall be concluded in accordance with the provisions of applicable data protection legislation following the audit conducted previously by the data protection officer of Jimdo GmbH. Processors shall also be monitored regularly during the contractual relationship.

4.3 Data Protection through Technology Design and Default Privacy Settings

- The software development process of Jimdo GmbH ensures that the principle of necessity is taken into account as regards user interfaces. Form fields and screen masks, for example, are designed to be flexible. Thus mandatory fields can be designated or fields can be deactivated.
- The Jimdo GmbH software also supports input control through a flexible and adjustable audit trail, which enables immutable storage of changes to data and user permissions.
- Data or application permissions can be configured in a flexible and granular way.

- Processor/Jimdo -