Contrat de sous-traitance de traitement des données

Contrat de sous-traitance

entre

_____

_____

_____

_____

_____

_____

Jimdo Website(s):

Responsable du traitement / l'utilisateur Jimdo/ Client(s)

-

et

Jimdo GmbH
Stresemannstr. 375
22761 Hamburg
Germany

-

Sous-traitant ou "Jimdo"

-

Préambule

Le Responsable de traitement est informé du fait que Jimdo propose ses services à un grand nombre de clients (utilisateurs Jimdo). La possibilité pour le Responsable de traitement d'émettre des instructions complémentaires, en particulier celles qui empêcheraient à d'autres clients ou utilisateurs d'utiliser les prestations de service offertes par Jimdo, est limitée par le présent contrat. Il serait impossible pour Jimdo d'opérer normalement tout en prenant en compte une série d'instructions individuelles émises par les responsables de traitement.

1. Généralités

1.1. La prestation de services au Responsable de traitement implique le traitement de données à caractère personnel par Jimdo pour le compte du Responsable de traitement. Selon la volonté de chacune des parties, le présent contrat intègre le consentement écrit concernant le traitement des données en accord avec l'article 11 de la BDSG (loi allemande sur la protection des données) et en accord avec l'article 28 de la réglementation européenne 2016/679 – Règlement général sur la protection des données (RGPD), et définit les droits et obligations des parties dans le cadre du traitement des données.

1.2. Dans la mesure où le présent contrat mentionne les termes « traitement de données » ou « traitement »(de données), la définition du terme « traitement » s'appuie sur le sens donné à l'article 4 N° 2 du RGPD.

1.3. Si la BDSG est mentionnée dans ce contrat, cette mention ne devra être prise en compte que jusqu'au 24.05.2018 inclus. À compter du 25.05.2018, ce sont alors les mentions du RGPD considérées à cet égard qui s'appliqueront au présent contrat.

2. Objet du contrat

2.1. Jimdo fournit un service en ligne grâce auquel les utilisateurs Jimdo, comme l'est le Responsable du traitement, peuvent créer et exploiter leur propre site Internet Jimdo. Le service proposé permet aux utilisateurs d'adapter de façon autonome le design de leur propre site Internet Jimdo et de mettre en place une e-boutique. En outre, l'objet du contrat découle du contrat principal conclu entre les parties. Ce dernier repose sur les CGU de Jimdo qui font partie intégrante de la relation contractuelle liant les parties.

2.2. Ce contrat de sous-traitance du traitement des données vient compléter les CGU de Jimdo.

2.3. Les types de données suivantes font régulièrement l'objet d'un traitement:

- Les données d'Inventaire provenant des clients du Responsable de traitement
  - Nom, adresse
  - Détails de commande
  - Données de paiement pour les e-boutiques Jimdo (cependant, celles-ci seront enregistrées par le fournisseur de la solution de paiement uniquement)

- Les données d'utilisation provenant des visiteurs du site Jimdo du Responsable de traitement
  - Jimdo utilise divers services d'analyse du comportement utilisateur (par ex. Google Analytics), afin de fournir des statistiques aux utilisateurs Jimdo, par ex. le Responsable de traitement, mais aussi dans le but d'évaluer et d'optimiser de façon continue les offres Jimdo.

- Les données de contenu que les visiteurs fournissent sur le site Internet du Responsable de traitement (par ex. les commentaires laissés dans les livres d'or et via les formulaires de contact).

- Les données de communication ou e-mails envoyés via le fournisseur de services e-mails Rackspace Limited. Si un compte e-mail ou une redirection d'e-mails est créé à partir d'un site Internet Jimdo, Jimdo crée un compte auprès de Rackspace Limited pour l'utilisateur Jimdo. Rackspace Limited est alors chargé de fournir la prestation technique et de s'occuper de la gestion des e-mails.

Les types de données susmentionnées concernent des données régulièrement traitées dans le cadre de l'utilisation des services Jimdo. Selon les services Jimdo utilisés par le Responsable de traitement, les types de données peuvent différer ou être étendues à la discrétion de Jimdo. Si les types de données devaient différer de celles mentionnées dans la liste ci-dessus, alors les types spécifiques de données seront définies en annexe du contrat. Dans ce cas, le Responsable de traitement peut contacter Jimdo (datenschutz@jimdo.com) et dresser la liste correspondant aux types de données qui diffèrent et/ou soumettre l'annexe en question. Jimdo garantie le respect des différents principes juridiques s'appliquant à la collecte, au traitement et à l'utilisation des données à caractère personnel, dans la mesure où cela relève de sa responsabilité. La vérification de la légalité du traitement des données de contenu (par ex. celles provenant des formulaires de contact utilisés par le responsable de traitement) ou d'autres données traitées par le Responsable de traitement dans le cadre de l'utilisation de son site Internet, incombe au seul Responsable du traitement qui en assume donc l'entière responsabilité.

2.4. Personnes concernées par le traitement des données:

- Les clients du Responsable du traitement
- Les personnes concernées par le site Internet du Responsable de traitement ou ses visiteurs
- Les employés du Responsable de traitement

3. Droits et devoirs du responsable de traitement

3.1. En vertu de l'article 4 N° 7 du RGPD, le Responsable de traitement ou utilisateur Jimdo représente l'autorité responsable du traitement des données qu'il a confié au Sous-traitant. Conformément au point 4 alinéa 5, le Sous-traitant a le droit d'avertir le Responsable de traitement s'il juge qu'un traitement de données dont il a la charge, ou qui fait l'objet d'une instruction de sa part, n'est pas autorisé par la loi. Dans la mesure où le Sous-traitant peut démontrer que le traitement demandé par le Responsable de traitement peut engager sa propre responsabilité en vertu de l'article 82 du RGPD, le Sous-traitant est libre d'exercer son droit de suspendre la suite du traitement jusqu'à ce que la responsabilité en découlant pour chaque partie soit clairement établie.

3.2. Le Responsable de traitement a l'obligation de se limiter à transmettre ou collecter des données en conformité avec l'Article 6 alinéa 1 du RGPD et de les traiter dans un but préalablement établi par la collecte. Le Responsable de traitement se doit de faire respecter les droits des personnes concernées et plus particulièrement d'honorer son engagement d'informer les personnes concernées de leurs droits en matière de protection des données. Le Sous-traitant informera sans délai le Responsable de traitement si des personnes font valoir leurs droits à l'égard du Sous-traitant et si cela concerne directement le Responsable de traitement.

3.3. Le Responsable de traitement peut adresser des instructions complémentaires à Jimdo concernant le traitement des données à caractère personnel. Ces instructions peuvent être opérées par l'utilisateur Jimdo principalement depuis la zone d'administration de son site en effectuant la configuration correspondante de ces services. Il peut s'agir de modifier le paramétrage des statistiques par exemple. Les instructions sortant de ce cadre doivent être adressées par écrit (par ex. par e-mail) à Jimdo. Jimdo vérifiera ensuite la faisabilité de ces instructions, en tenant compte de l'impact que ces instructions auraient sur le fonctionnement des services de Jimdo pour tous les utilisateurs Jimdo, et il

communiquera au Responsable de traitement le coût qu'implique la mise en œuvre de chaque instruction. La mise en application de l'instruction interviendra après délivrance d'une attestation de prise en charge des coûts y afférents. Les dispositions relatives à la rémunération des travaux additionnels réalisés par le Sous-traitant suite à des instructions complémentaires du Responsable de traitement n'en sont pas affectées.

3.4. Le Responsable de traitement peut désigner des personnes habilitées à donner des instructions dans la zone d'administration de son site Jimdo et d'y enregistrer leur adresse e-mail. En cas de changement des personnes habilitées à donner des instructions pour le compte du Responsable de traitement, ce dernier l'indiquera au Sous-traitant par écrit ou changera les adresses e-mail enregistrées dans la zone d'administration de Jimdo.

3.5. Le Responsable de traitement informera sans délai le Sous-traitant s'il devait constater des erreurs commises par le Sous-traitant ou des anomalies portant sur le traitement des données à caractère personnel.

3.6. S'il existe une obligation d'information à l'égard de tiers en vertu des articles 33 et 34 du RGPD, ou une autre obligation légale de notification incombant au Responsable de traitement, ce dernier est tenu de les respecter.

4. Obligations générales du Sous-traitant

4.1. Le Sous-traitant traite les données à caractère personnel exclusivement dans le cadre des accords contractuels et/ou du respect d'éventuelles instructions complémentaires émanant du Responsable de traitement. Cette règle exclut les dispositions légales imposant au Sous-traitant de procéder au traitement différemment. Dans ce cas, le Sous-traitant informe le Responsable de traitement des exigences légales avant le traitement, dans la mesure où le droit concerné n'interdit pas une telle communication en raison d'un intérêt public important. Sinon, la finalité, la nature et l'étendue du traitement des données sont déterminées exclusivement par le présent contrat et/ou les instructions émanant du Responsable de traitement. Un traitement différent des données par le Sous-traitant est interdit, à moins que le Responsable de traitement ne l'ait approuvé par écrit.

4.2. La prestation des services déterminés par le contrat principal relève du domaine de responsabilité de Jimdo et intègre des sous-traitants au point 6 de ce contrat. Jimdo s'assure donc que le traitement des données est effectué de manière conforme aux dispositions prises par le présent contrat.

4.3. Jimdo s'engage à effectuer le traitement des données, dans la mesure où, en dépit du point 4.1, celui-ci intervient directement pour le compte du Responsable de traitement, uniquement dans des États de l'Union européenne (UE) ou de l'Espace économique européen (EEE), ou dans le cas d'un traitement des données dans un pays tiers, et s'engage à prendre des dispositions permettant un traitement légal conforme à l'article 46 du RGPD.

4.4. Jimdo est tenu d'organiser son entreprise et ses opérations de telle sorte que les données qu'il traite pour le compte du Responsable de traitement, soient à chaque fois sécurisées dans les conditions requises, et protégées de toute consultation par des tiers non autorisés. Jimdo s'entendra préalablement avec le Responsable de traitement concernant des changements dans l'organisation du traitement de données pour le compte de celui-ci, s'ils ont un impact significatif sur la sécurité des données.

4.5. Jimdo informera immédiatement le Responsable de traitement s'il estime qu'une instruction émise par ce dernier s'oppose aux dispositions légales. Le Sous-traitant a le droit de suspendre l'exécution de l'instruction concernée, tant qu'elle n'aura pas été confirmée ou modifiée par le Responsable de traitement. Dans la mesure où le Sous-traitant peut démontrer que le traitement demandé par le Responsable de traitement peut engager sa propre responsabilité en vertu de l'article 82 du RGPD, le

Sous-traitant est libre d'exercer son droit de suspendre la suite du traitement jusqu'à ce que la responsabilité en découlant pour chaque partie soit clairement établie.

4.6. Tout traitement des données effectué pour le compte du Responsable de traitement s'effectuant en dehors des locaux du Sous-traitant ou de ses sous-traitants n'est autorisé que si le Responsable de traitement l'a approuvé par écrit. Un traitement des données effectué pour le compte du Responsable de traitement s'effectuant dans des locaux privés n'est autorisé que si le Responsable de traitement l'a approuvé par écrit au cas par cas.

4.7. Jimdo traitera les données pour le compte du Responsable de traitement et les autres données de façon distincte. Une séparation physique n'est pas impérative. Jimdo identifiera de façon appropriée les données qu'il traite pour le compte du Responsable de traitement. Si les données doivent être traitées pour différentes finalités, Jimdo identifiera les données en fonction de leur finalité.

4.8. Jimdo peut – mais sans y être obligé – indiquer au Responsable de traitement le nom de la/des personne(s) habilitée(s) à recevoir des instructions du Responsable de traitement. En cas de changement des personnes habilitées à recevoir des instructions du Responsable de traitement chez le sous-traitant, ce dernier en informera le Responsable de traitement par écrit.

5. Entreprise chargée par le Sous-traitant de la protection des données

Jimdo a désigné un délégué à la protection des données externes au sens de l'article 37 du RGPD. Il s'agit ici de :

B³ | Informationstechnologie Andreas Bethke
Papenbergallee 34
25548 Kellinghusen
Allemagne
E-mail: privacy@jimdo.com

6. Obligations de notification de la part du Sous-traitant

6.1. Jimdo est tenue d'informer immédiatement le Responsable de traitement de toute violation des dispositions légales relatives à la protection des données ou des engagements contractuels et/ou des instructions du Responsable de traitement produites dans le cadre du traitement des données effectué par lui-même ou autres personnes chargées de ce traitement. Cela s'applique également en cas de violation de données à caractère personnel que le Sous-traitant est chargé de traiter pour le compte du Responsable de traitement.

6.2. En outre, Jimdo informera immédiatement le Responsable de traitement si une autorité de surveillance intervient auprès de Jimdo en vertu de l'article 58 du RGPD, et si cette action peut impliquer le contrôle du traitement que Jimdo réalise pour le compte du Responsable de traitement.

6.3. Jimbo est informée du fait, qu'en vertu des articles 33 et 34 du RGPD, le Responsable de traitement peut être soumis à une obligation de signaler toute violation de la protection des données, laquelle prévoit également de déclarer cette atteinte à l'autorité de surveillance dans les 72 heures après avoir eu connaissance des faits. Le Sous-traitant fournira son assistance au Responsable de traitement dans le cadre de l'application des obligations déclaratives. Le Sous-traitant signalera notamment au Responsable de traitement tout accès non autorisé à des données à caractère personnel qui font l'objet d'un traitement pour le compte du Responsable de traitement, de manière immédiate et au plus tard dans les 48 heures suivant la connaissance de cet accès, sous forme écrite (fax/e-mail). Le Sous-traitant devra notamment fournir les informations suivantes au Responsable de traitement:

- une description de la nature de la violation des données à caractère personnel, si possible en indiquant les catégories et le nombre approximatif des personnes concernées, les catégories concernées et le nombre approximatif des séries de données à caractère personnel concernées;
- une description des mesures prises ou proposées par le Sous-traitant pour remédier à la violation des données à caractère personnel et, le cas échéant, des mesures destinées à en atténuer les possibles conséquences préjudiciables.

7. Obligations de coopération du Sous-traitant

7.1. Jimdo fournira son appui au Responsable de traitement pour remplir son obligation de répondre aux demandes des personnes faisant valoir leurs droits en vertu des articles 12-23 du RGPD. Les dispositions du point 11 du présent contrat doivent s'appliquer.

7.2. Jimdo doit collaborer à l'élaboration par le Responsable de traitement de registres listant toutes les opérations de traitement effectuées. Il devra fournir au Responsable de traitement les informations nécessaires de manière appropriée.

7.3. Le Sous-traitant est tenu d'aider le Responsable de traitement à respecter les obligations mentionnées aux articles 32-36 du RGPD, en fonction de la nature du traitement et des informations dont il dispose.

8. Pouvoirs de contrôle

8.1. Afin que le Responsable de traitement soit en mesure d'assumer ses droits et obligations de contrôle, avant l'établissement et pendant la durée du contrat, Jimdo fournira à sa demande un rapport émanant de l'entreprise externe à laquelle il a confié la protection des données. Ce rapport présentera les mesures techniques et organisationnelles prises par Jimdo et mises en place dans les centres de données Jimdo. Le rapport devra être actualisé au minimum tous les 24 mois.

8.2. Pour d'autres questions, le Responsable de traitement peut s'adresser à l'entreprise externe chargée par Jimdo de la protection des données.

8.3. Le Responsable de traitement a le droit de vérifier que Jimdo respecte toutes les dispositions légales mise en places en matière de protection des données et/ou respecte ses engagements contractuels établis entre les parties et/ou les instructions qui lui ont été données par le Responsable de traitement lui-même.

8.4. Jimdo est tenu de fournir au Responsable de traitement les renseignements requis pour l'exercice du contrôle mentionné au paragraphe 8.3.

8.5. Le Responsable de traitement peut exiger l'inspection des données traitées par Jimdo pour son compte, ainsi que des systèmes et programmes de traitement des données utilisés.

8.6. Sur demande et en respectant un préavis approprié (au moins dix jours ouvrés), le Responsable de traitement peut procéder au contrôle mentionné au paragraphe 8.5 dans les locaux de Jimdo GmbH pendant les horaires habituels d'ouverture de l'entreprise. À cet égard, le Responsable de traitement s'assurera que les contrôles soient effectués uniquement si nécessaire, et qu'ils ne perturbent pas le déroulement des activités du Sous-traitant de façon excessive. En principe, le temps d'une inspection chez le Sous-traitant est limité à une journée par année civile. Le Responsable de traitement a l'obligation de respecter la confidentialité des informations internes dont il aura eu connaissance à l'occasion du dit contrôle, notamment les détails relatifs aux mesures techniques et organisationnelles, de ne pas les divulguer à des tiers ou de les rendre accessibles, dans la mesure où cela ne concerne pas l'accomplissement des prestations contractuellement convenues entre le Responsable de traitement et le Sous-traitant.

8.7. En cas de mesures prises par l'autorité de surveillance à l'égard du Responsable de traitement en vertu de l'article 58 du RGPD, notamment portant sur les obligations d'information et de contrôle, Jimdo est tenu de fournir au Responsable de traitement les renseignements requis, et de permettre à chaque autorité de surveillance compétente d'effectuer un contrôle sur place. Le Responsable de traitement doit être informé par le Sous-traitant des mesures prévues dans ce cadre.

8.8. Au cas par cas, le Responsable de traitement est autorisé à faire réaliser le contrôle par un auditeur dont il aura annoncé par écrit l'intervention au moins dix jours avant la date du contrôle, en indiquant clairement son identité, dans la mesure où le Sous-traitant accepte cet audit externe. Le Sous-traitant ne pourra s'y opposer sans motif valable. Le Sous-traitant peut notamment refuser l'intervention de l'auditeur, si celui-ci se trouve en concurrence avec le preneur d'ordre. Les auditeurs externes ont l'obligation de signer un accord de confidentialité avec le Sous-traitant avant de pouvoir procéder à leur audit. Le droit de regard du Responsable du Traitement n'en est pas affecté.

9. Accords de sous-traitance

9.1. Pour fournir ses services aux utilisateurs Jimdo, Jimdo peut confier à des sous-traitants la réalisation de travaux comprenant également le traitement de données à caractère personnel. Jimdo indiquera en « annexe 1 » de ce contrat tous les accords de sous-traitance existants au moment de la conclusion du présent contrat. Il est autorisé à remplacer certains sous-traitants ou à en mandater d'autres à condition de respecter les dispositions prévues au paragraphe 9.4.

9.2. Jimdo doit sélectionner avec soin le sous-traitant, et avant tout engagement, vérifier qu'il est en mesure de respecter les accords contractuels passés entre Jimdo et le Responsable de traitement. Jimdo doit notamment contrôler préalablement, et régulièrement pendant la durée contractuelle, le respect par le sous-traitant des mesures techniques et organisationnelles requises par l'article 32 du RGPD concernant la protection des données à caractère personnel. Les résultats du contrôle seront documentés par Jimdo et communiqués sur demande au Responsable de traitement.

9.3. Jimdo a l'obligation d'imposer au sous-traitant de choisir un responsable opérationnel de la protection des données comme décrit à l'article 37 du RGPD. Dans le cas où aucun responsable de la protection des données n'aurait été désigné par le sous-traitant, Jimdo devra en informer le Responsable de traitement et lui fournir alors les informations justifiant que le sous-traitant n'est pas légalement tenu de désigner un responsable de la protection des données. Jimdo devra s'assurer que les dispositions prévues par le présent contrat s'appliquent aussi à l'égard du sous-traitant. Jimdo doit contrôler régulièrement le respect de ces obligations.

9.4. En cas de prévision d'un changement de sous-traitant ou de la conclusion d'un contrat avec un nouveau sous-traitant, Jimdo en informera par écrit le Responsable de traitement en temps voulu, mais au plus tard 4 semaines avant le changement ou la conclusion du nouveau contrat de sous-traitance (« Information »). Le Responsable de traitement a le droit de s'opposer au changement du sous-traitant ou à la conclusion d'un nouveau contrat de sous-traitance en motivant par écrit son intention dans les trois semaines à compter de la prise de connaissance de l'« information ». Le Responsable de traitement peut revenir sur son refus à tout moment par écrit. En cas de refus, le Sous-traitant peut résilier le contrat conclu avec le Responsable de traitement, en observant un préavis d'au moins 14 jours avant la fin d'un mois civil. Un tel délai de résiliation devrait permettre au Sous-traitant d'évaluer correctement les intérêts du Responsable de traitement. Si aucun refus n'est notifié par le Responsable de traitement dans les trois semaines suivant la réception de l'« information », cela aura valeur d'approbation par le Responsable de traitement du changement de sous-traitant ou de la conclusion d'un nouveau contrat avec le sous-traitant en question.

9.5. Jimdo doit s'assurer que les dispositions prévues par le présent contrat et, le cas échéant, que les instructions complémentaires émanant du Responsable de traitement s'appliquent aussi à l'égard du sous-traitant. Jimdo doit contrôler régulièrement le respect desdites obligations.

9.6. Jimdo doit conclure un contrat de sous-traitance de traitement des données avec les sous-traitants conformément aux dispositions de l'article 28 du RGPD. En outre, Jimdo doit imposer aux sous-traitants les mêmes obligations en matière de protection des données que celles qui ont été définies entre le Responsable de traitement et Jimdo. Le contrat de sous-traitance de traitement des données devra être communiqué au Responsable de traitement à sa demande.

9.7. Jimdo est notamment tenue de s'assurer par des dispositions contractuelles que les pouvoirs de contrôle (point 8 du présent contrat) du Responsable de traitement et des autorités de surveillance s'appliquent aussi au sous-traitant, et que des droits de contrôle correspondants du Responsable de traitement et des autorités de surveillance ont été convenus. Il faut également prévoir contractuellement l'obligation par le sous-traitant de se soumettre à ces mesures de contrôle et à d'éventuels contrôles sur site.

9.8. Ne doivent pas être considérées comme relevant d'un contrat de sous-traitance de traitement des données au sens des paragraphes 9.1 à 9.7 les prestations de services que le Sous-traitant sollicite auprès de tiers au titre de prestations annexes pour exercer son activité commerciale. Cela concerne par exemple les opérations de nettoyage, les simples services de télécommunications sans rapport direct avec les prestations que le Sous-traitant fournit au Responsable de traitement, les services postaux et de messagerie, les services de transport, les services de sécurité. Cependant, le Sous-traitant est aussi tenu, concernant les prestations accessoires fournies par des tiers, de s'assurer que des dispositions appropriées et des mesures techniques et organisationnelles ont été prises, de manière propre à garantir la protection des données à caractère personnel. La maintenance et l'entretien du système informatique ou des applications font l'objet d'un contrat de sous-traitance et d'un traitement en sous-traitance, au sens de l'article 28 du RGPD. Ce contrat est soumis à autorisation si la maintenance et la vérification portent sur des systèmes informatiques également utilisés dans le cadre des prestations fournies au Responsable de traitement, et dont l'entretien peut donner accès à des données à caractère personnel faisant l'objet d'un traitement pour le compte du Responsable de traitement.

10. Devoir de confidentialité

10.1. Dans le cadre du traitement des données pour le compte du Responsable de traitement, Jimdo a l'obligation de protéger la confidentialité des données qu'il reçoit ou qui sont portées à sa connaissance dans le cadre des opérations qui lui sont confiées.

10.2. Jimdo assure qu'il a connaissance des différentes dispositions légales en matière de protection des données et qu'il sait comment les appliquer. Jimdo assure en outre qu'il a bien informé les collaborateurs chargés d'exécuter les opérations des dispositions importantes à leur niveau concernant la protection des données, et qu'ils sont soumis au devoir de confidentialité, conformément au RGPD, ainsi qu'au respect de la protection des données en vertu de l'article 53 de la nouvelle BDSG.

10.3. Les obligations des personnes concernées, conformément au paragraphe 2, devront être prouvées au Responsable de traitement sur simple demande.

11. Protection des droits des personnes concernées

11.1. Le Responsable du Traitement assume seul la responsabilité de la protection des droits des personnes concernées. Les droits des personnes concernées doivent être exercés auprès du Responsable de traitement. Jimdo a l'obligation d'aider le Responsable de traitement à respecter son obligation de traiter les demandes des personnes concernées en application des articles 12-23 du RGPD, dans la mesure où le Responsable de traitement ne peut satisfaire à ces exigences sans l'intervention de JImdo.[1] À cet effet, Jimdo doit s'assurer de fournir au Responsable de traitement

les informations requises dans ce cadre et de manière immédiate, afin que ce dernier puisse notamment s'acquitter de ses obligations découlant de l'article 12 alinéa 3 du RGPD.

11.2. Dans la mesure où l'intervention du Sous-traitant est nécessaire pour que le Responsable de traitement puisse faire appliquer les droits des personnes concernées – notamment le droit d'information, de rectification, de blocage ou de suppression – le Sous-traitant prendra les mesures qui s'imposent, conformément aux instructions laissées par le Responsable de traitement. Dans la mesure du possible, le Sous-traitant aidera le Responsable de traitement à prendre les mesures techniques et organisationnelles appropriées, afin qu'il puisse s'acquitter de son obligation de répondre aux demandes dans le cadre de l'exercice des droits des personnes concernées.

11.3. Les dispositions relatives à une éventuelle rémunération des travaux supplémentaires fournis par le Sous-traitant afin d'apporter l'aide nécessaire requise par le Responsable de traitement dans le cadre de l'exercice des droits des personnes concernées par le traitement restent inchangées.

12. Obligation de confidentialité

12.1. Les deux parties contractantes s'engagent à traiter de manière confidentielle toutes les informations échangées dans le cadre de l'exécution de ce contrat, sans limite de temps, et à ne les utiliser que pour exécuter le présent contrat. Aucune partie n'est autorisée à utiliser ces informations, entièrement ou partiellement, à d'autres fins que celles susvisées, ou à les rendre accessibles à des tiers.

12.2. L'obligation précitée ne s'applique pas aux informations pour lesquelles l'une des parties peut attester qu'elles lui ont été communiquées par des tiers, sans être tenue de respecter une obligation de confidentialité, ou s'il s'agit d'informations accessibles au public.

13. Rémunération

13.1. La rémunération du Sous-traitant fait l'objet d'une convention séparée.

14. Mesures techniques et organisationnelles pour la protection des données

14.1. Jimdo s'engage à l'égard du Responsable de traitement à respecter les mesures techniques et organisationnelles nécessaires pour garantir l'application des dispositions s'imposant en matière de protection des données. Cela inclut notamment les dispositions de l'article 32 du RGPD.

14.2. Les mesures techniques et organisationnelles existantes comme décrites au moment de la conclusion du contrat sont jointes en annexe 2 du présent contrat. Les parties sont d'accord sur le fait que des modifications des mesures techniques et organisationnelles peuvent s'imposer pour s'adapter à la situation technique et juridique. Des modifications importantes susceptibles d'affecter l'intégrité, la confidentialité ou l'accessibilité des données à caractère personnel seront préalablement soumises à l'approbation du Responsable de traitement par Jimdo. Les mesures n'impliquant que des ajustements techniques et organisationnels mineurs qui ne peuvent nuire à l'intégrité, la confidentialité ou l'accessibilité des données à caractère personnel, peuvent être mises en place par Jimdo sans être soumises préalablement à l'approbation du Responsable de traitement. Une fois par an, ou lorsque des circonstances le justifient, le Responsable de traitement peut demander à Jimdo un état actualisé des mesures techniques et organisationnelles qu'il a prises.

14.3. De façon régulière, mais également si les circonstances l'exigent, Jimdo contrôlera l'efficacité des mesures techniques et organisationnelles. Jimdo s'engage à avertir le Responsable de traitement en cas d'optimisations ou modifications nécessaires.

15. Durée du présent contrat

15.1. Le contrat est en vigueur à compter de la date de sa signature et s'applique sur la période du contrat principal existant entre les parties concernant l'utilisation des prestations de services du Sous-traitant. Il est résiliable en respectant un préavis d'un mois avant la date de fin de période contractuelle en cours. La résiliation doit être effectuée par écrit (par exemple par mail).

15.2. Le Responsable de traitement peut résilier le contrat sans préavis en cas de violation grave par Jimdo GmbH des dispositions s'imposant en matière de protection des données ou de ses obligations contractuelles; si Jimdo ne peut pas, ou ne veut pas exécuter une instruction émanant du Responsable de traitement; ou s'il refuse l'accès du Responsable de traitement à une autorité compétente allant à l'encontre des dispositions prises par le contrat.

16. Fin du présent contrat

16.1. Lorsque le contrat arrive à échéance, Jimdo devra, selon l'option choisie par le Responsable de traitement, lui restituer ou supprimer : l'intégralité des documents, données et résultats établis sur le traitement ou l'utilisation des données dans le cadre établie par le contrat. La suppression devra être documentée de façon appropriée. Les éventuelles obligations de conservation ou autres obligations relatives à l'enregistrement des données n'en sont pas affectées. Pour les supports de données, si le Responsable de traitement a souhaité une suppression des données, ils devront être détruits, et à cet effet, un niveau 3 de sécurité conforme à la norme DIN 66399 devra être respecté ; la destruction devra être prouvée au Responsable de traitement en référence au niveau de sécurité conforme à la norme DIN 66399.

16.2. Le Responsable de traitement a le droit de contrôler auprès du Sous-traitant que ce dernier a effectivement restitué et/ou détruit l'intégralité des données conformément aux dispositions du présent contrat. Ceci peut aussi s'effectuer sous la forme d'une inspection des installations de traitement de données au sein des locaux du sous-traitant. Le Responsable de traitement doit annoncer la réalisation d'un contrôle sur site en respectant un préavis adéquat.

17. Droit de rétention

17.1. Les parties sont d'accord pour exclure l'exercice du droit de rétention par le Sous-traitant au sens de l'article 273 du BGB (code civil allemand) concernant les données traitées et les supports de données qui s'y rapportent.

18. Dispositions finales

18.1. Si les biens appartenant au Responsable de traitement devaient être menacés en raison de mesures prises par des tiers à l'égard du Sous-traitant (telles qu'une saisie ou une confiscation), dans le cadre d'une procédure pour insolvabilité ou autres circonstances, le Sous-traitant devra en informer le Responsable de traitement dans les plus brefs délais. Le Sous-traitant devra immédiatement informer les créanciers qu'il s'agit de données traitées pour le compte d'un tiers de manière contractuelle.

18.2. Les accords annexes doivent être formulés par écrit.

18.3. Si certaines dispositions de ce contrat devaient être invalides, la validité des dispositions restantes du présent contrat ne seront pas affectées.

18.4. En cas de différences résultant de la traduction, c'est la formulation en langue allemande qui s'applique.

19. Signatures

_____	_____
Lieu / Date	- Responsable du traitement -
	
Hamburg, 11.05.2018	- ***Sous-traitant***/Jimdo -
	Matthias Henze
	(CEO)
_____	Dennis Manzke
Lieu/ Date	(Head of Finance and Administration)

Annexe 1 – Sous-traitance

Le Sous-traitant utilise les services de tiers dans le cadre du traitement des données pour le compte du Responsable de traitement, auxquels il confie le traitement de ces données (« sous-traitants »).

Infrastructure / Plateforme technique			
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	Newsletter, Notifications	SendGrid Inc., 1801 California St #500, Denver, CO 80202, USA	https://sendgrid.com/policies/privacy/
Google Tag Manager	L'outil Gestionnaire de balises est un domaine sans cookie et ne collecte pas d'informations personnellement identifiables: l'outil déclenche d'autres balises qui peuvent collecter des données.	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://www.google.com/analytics/tag-manager/use-policy/
Google Analytics	Statistiques utilisateur	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	Édition d'images depuis le CMS	Adobe Systems Incorporated, 345 Park Avenue, San Jose, CA 95110-2704, USA	http://www.adobe.com/privacy.html
Firebase	Firebase est une base de données en temps réel que nous utilisons pour l'échange de données en temps réel et le stockage (par exemple dans nos applications). Toutes les données des utilisateurs sont anonymisées lors de la transmission à Firebase	Firebase is a Google subsidiary and is based in San Francisco (CA), USA.	https://www.firebase.com/terms/privacy-policy.html
Sipgate	Service de fax pour l'envoi et la réception de fax	sipgate GmbH Gladbacher Straße 74 40219 Düsseldorf Deutschland	https://www.sipgate.de/datenschutz.html
Rackspace	Une application web pour la distribution technique et la gestion d'e-mails ou de comptes e-mail du fournisseur 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	Outil de détection de fraude	Sift Science, Inc., 123 Mission Street, 20th Floor, San Francisco, CA 94105	https://siftscience.com/service-privacy
Stripe	Opérateur de paiement	Stripe Inc.,185 Berry Street, Suite 550, San Francisco, CA 94107, USA	https://stripe.com/de/privacy
Global Collect	Opérateur de paiement	Global Collect Service B.V., Planetenweg 43 - 59, 2132 HM Hoofddorp, NL	http://www.globalcollect.com/Privacy

Zuora	Gestion des abonnements	Zuora Inc., 3050 S. Delaware Street, Suite 301, San Mateo, CA 94403, USA	https://www.zuora.com/privacy-statement/
Add This	Une plateforme de bookmarking qui permet d'enregistrer facilement des listes de sites web	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	Rapport des bugs et problèmes	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	Administration des domaines	InterNetX GmbH, Maximilianstr. 6, 93047 Regensburg, Germany	https://www.internetx.com/rechtliches/datenschutz/
RankingCoach	Outil d'optimisation des résultats sur les moteurs de recherche	rankingCoach GmbH, Brügelmannstrasse 3, 50679 Köln, Germany	https://www.rankingcoach.com/en-us/privacy-policy
status.io	Status page avec des informations à jour sur l'accessibilité et la fonctionnalité de notre système	T3CH.com LLC, 19 N. County Line Road, Jackson, NJ 08527, USA	https://status.io/privacy
Paypal	Opérateur de paiement	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	Système de Blog	WP Engine Irongate House, 22-30 Duke's Place London, EC3A 7LP United Kingdom	https://wpengine.com/legal/privacy/
Fastly Inc.	Livraison de contenu	Fastly, Inc., General Counsel, 475 Brannan St, Suite 300, San Francisco, CA 94107, USA	https://www.fastly.com/privacy
Disqus	Systéme de commentaires	DISQUS, Inc., 301 Howard St, Floor 3, San Francisco, California 94105, USA	https://help.disqus.com/terms-and-policies/disqus-privacy-policy
G-Suite	Utilisation des systèmes de productivité Google avec le système de messagerie Jimdo	Un produit de Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://policies.google.com/privacy?hl=de
Twyla	Système de support de chat	Twyla GmbH, Winterfeldtstraße 21, 10781 Berlin, Germany	https://www.twylahelps.com/
Zendesk	Sytème de ticket pour le service client	Zendesk, Inc., 1019 Market Street, San Francisco, CA 94103, USA	https://www.zendesk.de/company/customers-partners/#privacy-policy
Launchdarkly	Rapport des bugs et problèmes	Catamorphic, Co. ("LaunchDarkly"), 405 14th Street, Oakland, CA 94612, USA	https://launchdarkly.com/policies/privacy/
Facebook Login	Technologie Single-Sign-On	Facebook Inc., 1 Hacker Way, Menlo Park, CA 94025, USA	https://www.facebook.com/about/privacy/
Google Plus Login	Technologie Single-Sign-On	Un produit de Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://www.google.de/intl/de/policies/privacy/
Youtube	Fonction d'intégration Youtube pour afficher et lire des vidéos du fournisseur" "Youtube"	Un produit de Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://www.google.de/intl/de/policies/privacy
Prefinery	Outil pour l'acquisition de clients et les publications de produits	Prefinery, 1108 Lavaca Street, Suite 110-318, Austin, TX 78701, USA	https://www.prefinery.com/privacy
Redis	Fournisseur de banque de données	Redislabs, 700 E El Camino Real Suite 250, Mountain View, CA 94040	https://redislabs.com/privacy/

sentry.io	Rapport des bugs et problèmes	Un produit de Functional Software, Inc., 132 Hawthorne St, San Francisco, CA 94107	https://sentry.io/privacy
Name.com	Administration des domaines	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
		Outils internes:	
Jira	Résolution de problèmes et documentation	Atlassian, 55 Broadway Floot 17&25 New York, NY 10006 USA	https://www.atlassian.com/legal/privacy-policy
Slack	Solution de communication interne	436 Lafayette Street, 1008 Western Ave #401, Seattle, WA 98104	https://slack.com/intl/de-de/privacy-policy
Trello	Outil de planification interne et de communication	Atlassian, 55 Broadway Floot 17&25 New York, NY 10006 USA	https://trello.com/privacy
Tableau	Outil pour l'analyse des données et des journaux de données	Tableau Germany GmbH, An der Welle 4, 60322 Frankfurt am Main, Germany	https://www.tableau.com/de-de/privacy
Github	Service en ligne pour les projets de développement de logiciels	Github, 88 Colin P Kelly Jr St, San Francisco, CA 94107, USA	https://help.github.com/articles/github-privacy-statement/
Microsoft	Utilisation interne de Microsoft Office et Skype	Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA	https://privacy.microsoft.com/en-us/privacystatement
Hootsuite	Outil de médias sociaux	Hootsuite Media Inc. 5, East 8th Avenue, Vancouver BC, Canada V5T 1R6	https://hootsuite.com/de/legal/privacy
		Performance et Marketing:	
Facebook Pixel & Custom Audiences	Après obtention du consentement explicite et positif, ce dispositif donne l'autorisation de traquer le comportement des utilisateurs après avoir vu ou cliqué sur une publicité Facebook. Ce procédé vise à évaluer l'efficacité des publicités Facebook, à des fins statistiques et marketing, et permet d'optimiser les efforts publicitaires à venir.	Facebook Inc., 1 Hacker Way, Menlo Park, CA 94025, USA	https://www.facebook.com/about/privacy/
Hotjar	Optimisation de la conversion	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	Plateforme de recommandation de contenu	Taboola, Inc., 28 West 23rd Street, 5th Floor, New York, NY 10010, USA	https://www.taboola.com/privacy-policy

Tv-Squared	Ce site utilise TVSquared pour l'analyse statistique du trafic des visiteurs en lien avec la publicité télévisée	TV Squared Limited, Codebase, Argyle House, 3 Lady Lawson St, Edinburgh, EH3 9DR	http://tvsquared.com/privacy-policy/
bunchbox	Outil d'optimisation de site pour l'implémentation de tests A/B et d'analyses multivariées	app.bunchbox.co, Peaks & Pies GmbH, Raboisen 30, 20095 Hamburg, Deutschland	http://peaksandpies.com
smartly.io	Outil pour les campagnes publicitaires pour Facebook et 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 enregistre le comportement des utilisateurs sur notre site web. La collecte des données des visiteurs permet à Jimdo d'analyser et d'améliorer l'expérience des visiteurs sur le site. Fullstory collecte et stocke les données sous forme anonyme par le biais de cookies. Ce Tracking (c'est-à-dire la collecte des données générées par le cookie et liées à l'utilisation du site web) peut être désactivé à tout moment. Il vous suffit de suivre les instructions indiquées à la page suivante : https://www.fullstory.com/optout..	Fullstory Inc., 818 Marietta Street, Atlanta, GA 30318, USA	https://www.fullstory.com/legal/privacy/
Surveymonkey	Pour les enquêtes, nous utilisons les services de SurveyMonkey.	SurveyMonkey Europe UC, 2 Shelbourne Buildings, Second Floor, Shelbourne Rd, Ballsbridge, Dublin 4, Ireland	https://de.surveymonkey.com/mp/policy/privacy-policy/
Trustpilot	Avis des clients	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

Annexe 2 – Mesures techniques et organisationnelles du sous-traitant

Le Sous-traitant s'engage à prendre les mesures techniques et organisationnelles suivantes afin de garantir la sécurité des données, et ce, de manière conforme à l'article 32 du RGPD.

Le responsable de traitement (le Sous-traitant signataire du contrat de sous-traitance de traitement des données) doit, dans le cadre des traitements qui lui sont confiés, avoir pris les mesures techniques et organisationnelles propres à garantir un niveau de protection adéquat des données à caractère personnel, en tenant compte de l'état actuel de la technologie, des coûts de réalisation, de la nature, de l'étendue, du contexte et des finalités de son traitement, ainsi que de la probabilité de survenance et de la gravité des risques inhérents à ce traitement quant aux droits des personnes concernées.

Les mesures décrites, ci-après, en conformité avec la liste issue de l'article 64 de la BDSG (2017), se réfèrent aux mesures prises dans le cadre du traitement des tâches demandées. Pour des raisons de sécurité, seule une description générale est présentée ci-dessous.

1. Confidentialité

1.1 Contrôle d'accès

Les mesures suivantes ont été prises afin d'empêcher un accès non autorisé aux installations de traitement des données, au moyen desquelles des données à caractère personnel sont traitées ou utilisées (contrôle d'accès):

- Le siège de l'entreprise Jimdo GmbH se trouve dans un immeuble constitué de bureaux à Hambourg, et l'accès à ces bureaux est fermé jour et nuit. Seuls le locataire et le propriétaire de l'immeuble disposent d'un accès aux locaux. Les bureaux et locaux commerciaux de Jimdo sont sécurisés par des systèmes de fermeture électronique. Seules les personnes autorisées disposent des clés électroniques leur garantissant l'accès. En principe, aucune donnée à caractère personnel n'est conservée pour le compte du Responsable de traitement sur place. Tous les systèmes informatiques utilisés pour effectuer les opérations de traitement par Jimdo se trouvent dans des centres de données utilisés par Jimdo.
- Jimdo est tenu de s'assurer que seuls des centres de données répondant aux différentes exigences légales de la République fédérale d'Allemagne en matière de protection des données sont utilisés.
- Les centres de données utilisés par Jimdo sont certifiés ISO 27001 et disposent de mécanismes de contrôle d'accès équipés en conséquence. Le centre de calcul utilisé pour le Responsable de traitement répond aux exigences de la norme de sécurité de niveau 3.
- L'octroi et la gestion des clés se font en respectant une procédure précise qui détermine, pour la durée contractuelle de travail, l'attribution ou le retrait des autorisations d'accès aux locaux.
- Les autorisations d'accès sont attribuées à un collaborateur seulement lorsque cela a été demandé par le responsable dont il dépend et/ou le service du personnel. L'octroi d'autorisation se fait en vertu du principe de nécessité.
- Les visiteurs n'ont accès aux locaux que lorsque le personnel de l'accueil leur ouvre la porte. Le personnel de l'accueil peut voir la porte d'entrée et s'assure que chaque visiteur vienne se présenter à l'accueil.
- Chaque visiteur est enregistré dans un registre des entrées avant d'être accompagné jusqu'à son interlocuteur. Les visiteurs sont toujours accompagnés par un collaborateur de Jimdo après leur entrée dans les locaux. Des règles ont été définies en ce qui concerne le personnel extérieur et l'accompagnement des visiteurs.

- Les portes d'entrée et les fenêtres des locaux des bureaux de la Jimdo GmbH sont sécurisées par un système d'alarme. Celui-ci peut être activé et désactivé manuellement. Indépendamment de cela, le système d'alarme est cependant toujours activé quotidiennement à partir de 21 heures.

1.2 Contrôle d'accès

Les mesures suivantes ont été prises afin d'empêcher que des tiers non autorisés puissent utiliser les systèmes de traitement des données (ordinateurs) :

- Pour être en mesure d'accéder aux systèmes informatiques, les utilisateurs doivent disposer d'une autorisation d'accès. À cet effet, des autorisations correspondantes pour chaque utilisateur sont octroyées par les administrateurs. Néanmoins, cela n'intervient que si les responsables compétents l'ont demandé. La demande peut aussi être faite par le service des ressources humaines.
- L'utilisateur reçoit ensuite un identifiant et un mot de passe provisoire, qui doit être changé lors de sa première connexion. Les conditions de création d'un mot de passe imposent un minimum de 8 caractères, pour lesquels il faut intégrer des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.
- Les mots de passe sont changés tous les 90 jours. Font exception à cette règle les mots de passe composés d'un minimum de 32 caractères. Pour ceux-là, un changement automatique de mot de passe n'est pas indiqué.
- L'historique des mots de passe est conservé. De cette façon, on s'assure que les 10 derniers mots de passe qui ont déjà été utilisés ne le seront pas à nouveau.
- Les tentatives de connexion erronées sont également enregistrées. Après 3 saisies erronées, le compte de l'utilisateur concerné est bloqué.
- Les accès à distance aux systèmes informatiques de Jimdo se font toujours via des connexions cryptées.
- Les serveurs de Jimdo sont équipés d'un système de prévention des intrusions. Tous les systèmes serveur et client sont dotés d'un logiciel antivirus, pour lequel une actualisation des signatures est assurée quotidiennement.
- Tous les serveurs sont protégés par des pare-feux, constamment entretenus, mis à jour et corrigés.
- L'accès des serveurs et des clients à Internet, de même que l'accès à ces systèmes via Internet sont aussi sécurisés par des pare-feux. De cette façon, on s'assure également que seuls les ports nécessaires à la communication soient utilisables. Tous les autres ports sont alors bloqués.
- Tous les collaborateurs ont reçu l'instruction de verrouiller leurs systèmes informatiques lorsqu'ils cessent de les utiliser.
- Les mots de passe sont systématiquement enregistrés de façon cryptée.

1.3 Contrôle d'accès

Les mesures suivantes ont été prises pour garantir que les personnes autorisées à utiliser un système de traitement de données puissent accéder exclusivement aux données soumises à leur autorisation d'accès, et qu'après leur enregistrement, les données à caractère personnel ne puissent être lues, copiées, modifiées ou supprimées sans autorisation.

- Le Responsable de traitement est tenu de soumettre les données à une autorisation d'accès appropriée sur l'espace de stockage/interface administrateur mis à sa disposition durant la durée du contrat conformément à ce qui a été défini contractuellement. Il s'agit notamment de restreindre le droit d'accès ou d'intervention sur des données qu'à des tiers soigneusement choisis (par ex. agences Web, administrateurs).
- Les autorisations concernant les systèmes informatiques et applications de l'entreprise Jimdo GmbH sont exclusivement créées par les administrateurs.
- Les autorisations sont strictement octroyées suivant le principe du « Need to know » (« besoin de savoir »). Selon ce principe, seules les personnes disposant de droits d'accès à des données, bases de

données ou applications, sont chargées de la maintenance, de l'actualisation ou du développement de ces données, applications ou bases de données.

- La condition à remplir est qu'une demande d'autorisation correspondante soit faite pour un employé par son responsable. La demande peut aussi être faite par l'Office Team.
- Les accès aux systèmes informatiques sont inscrits dans un journal d'accès, afin de détecter d'éventuelles utilisations non autorisées ou exclusions.
- Les autorisations d'accès sont attribuées en fonction des rôles assignés, et donnent donc la possibilité d'octroyer des autorisations d'accès différenciées, garantissant que les employés disposent d'autorisations se rapportant uniquement à leur domaine propre de compétence et, éventuellement, de droits d'accès à des données et des applications qui sont limités au cadre des projets en cours.
- La destruction de supports de données et de documents papier est réalisée par un prestataire qui garantit une destruction répondant à la norme DIN 66399.
- Tous les employés Jimdo ont reçu l'instruction de mettre les informations contenant des données à caractère personnel et/ou les informations relatives à des projets dans des réceptacles de destruction prévus à cet effet.
- Il est strictement interdit aux employés d'installer des logiciels non autorisés sur les systèmes informatiques.
- Tous les systèmes serveur et client sont régulièrement actualisés par mises à jour de sécurité.

1.4 Séparation

Les mesures suivantes garantissent que les données recueillies pour différentes finalités puissent être traitées séparément :

- Tous les systèmes informatiques que Jimdo utilise pour le Responsable de traitement sont catégorisés de manière logique par client, garantissant de pouvoir séparer certaines données d'autres données lorsqu'elles doivent être traitées à des fins différentes.
- Il s'opère donc un traitement et/ou un stockage séparés des données lorsque la finalité du traitement est différente.
- Un système d'habilitation en fonction des différents niveaux d'autorisation d'accès gradués a été mis en place pour les employés du service technique (administration), du support client, de la gestion des domaines et de la comptabilité client.
- Il appartient au Responsable de traitement de s'assurer lui-même de la séparation des données à caractère personnel sur l'espace de stockage et le système de modules (CMS) mis à sa disposition.

1.5 Pseudonymisation et cryptage

Les mesures suivantes garantissent que le traitement des données à caractère personnel s'effectue de telle manière que ces données ne puissent plus être attribuées à une personne en particulier sans indication supplémentaire à ce sujet, dans la mesure où ces indications supplémentaires sont conservées séparément et soumises à des mesures techniques et organisationnelles adéquates.

- Il appartient au Responsable de traitement de procéder lui-même à la pseudonymisation des données à caractère personnel sur le système de modules (CMS) mis à sa disposition, dans la mesure où la loi l'impose.
- Il appartient au Responsable de traitement de procéder au cryptage des données sur le système de modules (CMS) mis à sa disposition pour la durée contractuelle, en utilisant les techniques appropriées (logiciels).
- Un accès administratif aux systèmes de serveur est fourni via une connexion cryptée.
- En outre, les données sont stockées sur les systèmes serveur et client via des supports de données cryptés. Des systèmes appropriés de cryptage pour disques durs sont utilisés.

2. Intégrité

2.1 Contrôle de saisie des données

À l'aide des mesures suivantes, il est possible de vérifier et d'établir ultérieurement si, et par qui des données à caractère personnel ont été saisies, modifiées ou supprimées via des systèmes de traitement de données :

- La saisie, la modification ou la suppression de données sont enregistrées au niveau de la base de données.
- Il incombe au Responsable de traitement, le cas échéant, de saisir les données à caractère personnel sur le système de modules (CMS) mis à sa disposition durant la durée du contrat comme prévu par ce dernier, et notamment de ne recourir qu'à des tiers compétents (par ex. agences Web, administrateurs) pour ce faire. En principe, les employés du responsable des traitements ne peuvent intervenir sur ces données, les saisir, les modifier ou les supprimer.
- Ainsi, le traitement des données à caractère personnel est en principe réalisé par le Responsable de traitement, de sorte que le responsable du traitement ne peut vérifier et constater ultérieurement quelles données à caractère personnel du client ont été saisies ou modifiées dans les systèmes automatisés de traitement, ni à quel moment, ni par qui.
- Ce n'est que lors d'activités réalisées dans le cadre d'une éventuelle instruction supplémentaire, laquelle intervient sous forme écrite et en dehors du domaine de l'administration du site Internet, que le responsable du traitement consigne ces saisies et modifications sous forme appropriée, et enregistre l'heure et l'identité des personnes qui ont effectué les saisies.
- Si, pour des raisons légales, le responsable du traitement (Jimdo) doit supprimer des informations ou en bloquer l'accès (par ex. en cas d'utilisation par les clients de services de télémédia ou de communication électronique proposés sur les systèmes informatiques destinés aux tiers), le blocage ou la suppression de contenu seront consignés. Les données de journal d'activités sont conservées et incluent l'identification des employés. La suppression est réalisée de façon automatisée à la fin du contrat en plus d'être consignée.

2.2 Contrôle de la transmission

Les mesures suivantes garantissent que les données à caractère personnel ne puissent être lues, copiées, modifiées ou supprimées par des personnes non autorisées lors de leur transmission électronique, ou de leur transport ou de leur enregistrement sur des supports de données, et la possibilité de vérifier et de constater en quels points une transmission de données à caractère personnel est prévue par les installations de transfert de données.

- Dans le cadre de l'administration de serveurs, seules des connexions cryptées sont utilisées. En principe, aucune transmission des données du Responsable de traitement ne se produit. Font exception à cette règle les cas où Jimdo est dans l'obligation de fournir des données en application de dispositions légales ou sur injonction d'une autorité judiciaire.
- Sinon, une transmission de données stockées sur les systèmes informatiques de Jimdo pour le compte du Responsable de traitement n'intervient que dans le cadre de l'exploitation par le Responsable de traitement de son site Internet (consultation des pages du site Internet par les visiteurs), dans la mesure où cette transmission est requise par les mesures techniques alors sollicitées.
- La garantie de confidentialité de la transmission de données à caractère personnel est assurée par des cryptages SSL/TLS sur les sites Internet du Responsable de traitement.
- Tous les employés intervenant sur le projet d'un client reçoivent des instructions sur l'utilisation autorisée de données et les modalités de la transmission de ces données.
- Dans la mesure du possible, les données sont transmises à leur destinataire de façon cryptée.
- Chez Jimdo, l'utilisation de supports privés de données est interdit aux employés dans le cadre du travail sur le projet d'un client.

- Chez Jimdo, les employés sont régulièrement formés sur les questions se rapportant à la protection des données. Tous les employés ont l'obligation de traiter les données à caractère personnel de façon confidentielle.
- Par ailleurs, il appartient au client d'utiliser sur le système de modules (CMS) ou l'interface d'utilisateur mis à sa disposition conformément au contrat et pour la durée de celui-ci, un contrôle approprié du transport et des techniques de cryptage adaptées.

3. Disponibilité et capacités

Les mesures suivantes garantissent que les systèmes de traitement des données utilisés fonctionnent en permanence de façon irréprochable et que les données à caractère personnel sont protégées contre toute destruction ou perte fortuite.

- Les centres de données utilisés par Jimdo disposent d'un système d'alimentation sans interruption en électricité, d'une climatisation dans les salles de serveurs, d'appareils de contrôle de la température et de l'humidité dans les salles de serveurs, de dispositifs de détection de fumée et d'incendie, de systèmes d'alarme et de sécurité.
- Un système anti-incendie et alarmes couvrant l'intégralité des locaux est utilisé. Les données sont sauvegardées sur les systèmes serveurs de la Jimdo GmbH de façon incrémentielle quotidiennement, et une fois par semaine de façon complète. Les supports de sauvegarde sont cryptés et transférés dans un lieu physiquement séparé.
- L'accomplissement des sauvegardes est régulièrement testé.
- Les systèmes informatiques disposent d'un système d'alimentation sans interruption en électricité. La salle des serveurs dispose d'un système de détection d'incendie ainsi que d'un système d'extinction au CO2. Tous les systèmes serveurs sont soumis à une surveillance qui avertit immédiatement un administrateur en cas de dysfonctionnements.
- La Jimdo GmbH dispose d'un plan d'urgence qui inclut aussi un plan de redémarrage.
- Les données sur les systèmes serveurs de Jimdo GmbH sont sauvegardées au minimum une fois par jour de façon incrémentale et « complètement » chaque semaine. Les supports de sauvegarde sont cryptés et transférés dans un lieu physiquement séparé.
- L'accomplissement des sauvegardes est régulièrement testé.
- Les systèmes informatiques disposent d'un système d'alimentation sans interruption en électricité. La salle des serveurs dispose d'un système de détection d'incendie ainsi que d'un système d'extinction au CO2. Tous les systèmes serveurs sont soumis à une surveillance qui avertit immédiatement un administrateur en cas de dysfonctionnement.

4. Processus de vérification, d'évaluation et d'appréciation périodiques

Finalité de garantie : Processus de vérification, d'évaluation et d'appréciation périodiques de l'efficacité des mesures techniques et organisationnelles, afin de garantir la conformité du traitement des données.

4.1 La gestion de la protection des données

- Jimdo s'appuie sur un socle de collaborateurs permanents qu'il emploie depuis de nombreuses années pour son personnel technique, et disposant d'une expérience technique et d'une grande compétence en traitement de données.
- Les collaborateurs suivent régulièrement des formations.
- La Jimdo GmbH gère la protection des données. Cette gestion suit des instructions particulières mises en place pour garantir la protection et sécurité des données. Ces instructions suivent elles-mêmes des directives pour assurer le bon accomplissement des objectifs fixés par les instructions.

- C’est une équipe dédiée à la protection des données et à la sécurité des informations (DST-Team) qui prévoit, met en œuvre et évalue les mesures dans le domaine de la protection et de la sécurité des données, et qui procède aux adaptations nécessaires.
- Régulièrement, l’efficacité des directives est mesurée et les adaptations nécessaires sont réalisées.
- On s’assure notamment que les incidents concernant la protection des données sont reconnus par tous les employés et immédiatement signalés à l’équipe DST (équipe d’information sur la sécurité). L’incident est tout de suite examiné par celle-ci. Si cela se rapporte à des données traitées pour le compte de clients, on s’assure que ces derniers sont informés immédiatement de la nature et de l’ampleur de l’incident.
- Dans le cadre du traitement de données pour son propre compte, une déclaration est faite auprès de l’autorité de surveillance dans les 72 heures suivant la connaissance de l’incident, si ce dernier est soumis aux dispositions de l’article 33 du RGPD.

4.2 Contrôle des travaux sous-traités (externalisation de tâches)

Les mesures suivantes garantissent que les données à caractère personnel traitées pour le compte d’un tiers, sont traitées suivant les instructions fournies par le Responsable de traitement.

- La Jimdo GmbH a désigné un délégué interne à la protection des données.
- En cas de recours à des prestataires externes ou à des tiers, conformément aux prescriptions légales applicables en matière de protection des données, à l’issue d’un audit, un contrat de sous-traitance est conclu par le délégué à la protection des données de Jimdo GmbH. Les sous-traitants sont régulièrement contrôlés pendant la durée du contrat.

4.3 Protection des données par des aménagements techniques et des préréglages favorisant la protection des données

- Dès le développement d’un logiciel, l’entreprise Jimdo GmbH s’assure de la prise en compte du principe de nécessité dans le cadre des interfaces utilisateur. Ainsi, par ex., les champs des formulaire, les modules, sont configurables de façon flexible. Ainsi, des champs obligatoires peuvent être prévus ou des champs désactivés.
- Les logiciels de la Jimdo GmbH favorisent le contrôle de saisie par un audit-trail flexible et adaptable, qui permet un enregistrement des modifications réalisées sur les données et sur les autorisations des utilisateurs.
- Les autorisations sur les données et les applications peuvent être déterminées de façon flexible et granulaire.

- Processor/Jimdo -