

Data Processing Agreement

Between

Emvi Software GmbH
Nickelstraße 1b
33378 Rheda-Wiedenbrück
Germany
contact@emvi.com

- hereinafter: Processor -

und

.....
.....
.....

- hereinafter: Controller -

the following agreement is concluded:

Clause 1 Purpose and scope

- a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.
- c) These Clauses apply to the processing of personal data as specified in Annex II.
- d) Annexes I to IV are an integral part of the Clauses.
- e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 Invariability of the Clauses

- a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 Interpretation

- a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.
- b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.
- c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 Tying clause

This clause was intentionally left blank.

Clause 6 Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 Obligations of the Parties

1. Instructions

- a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
- b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

4. Security of processing

- a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

- b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

6. Documentation and compliance

- a) The Parties shall be able to demonstrate compliance with these Clauses.
- b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
- d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
- e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7. Use of sub-processors

- a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.
- b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
- d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
- e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

8. International transfers

- a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the

controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

- b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 Assistance to the controller

- a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.
- b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.
- c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
 - 1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
 - 2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

- 3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
 - 4) the obligations in Article 32 Regulation (EU) 2016/679/.
- d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

1. Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

- a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679 shall be stated in the controller's notification, and must at least include:
 - 1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - 2) the likely consequences of the personal data breach;

- 3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- c) in complying, pursuant to Article 34 Regulation (EU) 2016/679 with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

2. Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

- a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- b) the details of a contact point where more information concerning the personal data breach can be obtained;
- c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

Clause 10 Non-compliance with the Clauses and termination

- a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
- b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
 - 1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
 - 2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
 - 3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
- d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Emvi Software GmbH

Company

Rheda-Wiedenbrück, 01.02.2024

Place and Date

Daniel Schramm

Name

Managing Director

Position



Signature

Company

Place and Date

Name

Position

Signature

Annex 1

List of Parties

Controller

1.1	Name and address	
1.2	Contact person	
1.3	Data protection officer	

Processor

1.1	Name and address	Emvi Software GmbH Nickelstraße 1b 33378 Rheda-Wiedenbrück Germany Email: contact@emvi.com
1.2	Contact person	Daniel Schramm (Managing Director) Email: daniel.schramm@emvi.com Marvin Blum (Managing Director) Email: marvin.blum@emvi.com
1.3	Data protection officer	Timo Schusser valvisio consulting GmbH Thorackerstraße 5a 96052 Bamberg Germany Phone: +49 (0)951 974333-0 Email: dsb-extern@valvisio.de

Annex 2

Description of Processing

The processor provides services for the controller in the area of statistical evaluation and analysis of the performance and usage behavior of persons on the controller's websites or apps by using the product "Pirsch Analytics (pirsch.io)" on the basis of the main contract.

The controller shall transmit the following categories of data subjects and data categories to the processor::

(a) Categories of data subjects

- Website visitors
- Customers
- Interested parties
- Others

(b) Types of personal data

- IP addresses
- Country, city (these values are imprecise and cannot be used to identify a specific address or household)

Annex 3

Technical and organizational measures

Company / Authority	Emvi Software GmbH Nickelstraße 1b 33378 Rheda-Wiedenbrück Germany Email: contact@emvi.com
External data protection officer	Timo Schusser valvisio consulting GmbH Thorackerstraße 5a 96052 Bamberg Germany Phone: +49 (0)951 974333-0 Email: dsb-extern@valvisio.de
Admission control	Keys
Access control	Keys (Secure) passwords Anti-virus software clients Firewall Rights management Data protection guidelines
Access authorization	Authorization concepts and needs-based access rights
Separation control	Separation of productive and test environments Physical separation (systems/databases/data carriers) Multi-client capability Control of authorization concept Definition of database rights

Transfer control	Traceability of entries: Entries are never made manually
Input control	Authorization concept Password policy Clear responsibilities for deletions
Pseudonymization	<p>Pirsch Analytics generates a unique number for each visitor, which is calculated from the visitor's IP address, the user agent and a random character string defined for each website. The combination of these three data points ensures that visitors can be distinguished from one another without collecting personal data. The random string guarantees that the number varies from website to website so that it cannot be matched. Sessions are recorded for a maximum of 24 hours. After that, the visitor is assigned a new unique number.</p> <p>Visitor data is therefore anonymized, not pseudonymized, as part of the website analysis via the "Pirsch Analytics (pirsch.io)" product. The General Data Protection Regulation does not apply to the processing of anonymized data Recital 26 of the GDPR.</p>
Availability (of the data)	Backup strategy
Resilience (of the systems)	Virus protection Firewall
Recoverability (of the data / the systems)	Backup strategy

<p>Order control</p>	<p>No order processing within the meaning of Art. 28 GDPR without corresponding instructions from the client</p> <p>Clear contract design</p> <p>Strict selection of service providers</p> <p>Obligation to convince in advance</p> <p>Follow-up checks</p>
<p>Data protection management</p>	<p>Data protection impact assessment carried out for the Pirsch Analytics service</p> <p>Data protection obligations of employees</p> <p>Data protection guidelines</p> <p>Process for data protection breaches</p> <p>Process for data subject requests</p> <p>List of processing activities within the meaning of Art. 30 (1) and (2) GDPR</p>

Annex 4

Sub-processors

For the processing of data on behalf of the controller, the processor uses the services of third parties who process data on its behalf ("subcontractors").

The company in question is as follows:n:

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
Germany
Phone: +49 (0)9831 505-0
Email: info@hetzner.com

The company provides the required storage space for our "Pirsch Analytics (pirsch.io)" service via cloud storage. The place of processing is Nuremberg and Falkenstein in Germany.

Anlage 5: Technical and organizational measures of the subcontractor Hetzner Online GmbH (as of 01.02.2023)

Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage

I. Vertraulichkeit

- Zutrittskontrolle
 - Datacenter-Parks in Nürnberg, Falkenstein und Helsinki
 - elektronisches Zutrittskontrollsystem mit Protokollierung
 - Hochsicherheitszaun um den gesamten Datacenter-Park
 - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation- Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
 - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
 - 24/7 personelle Besetzung der Rechenzentren
 - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
 - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
 - Verwaltung
 - elektronisches Zutrittskontrollsystem mit Protokollierung
 - Videoüberwachung an den Ein- und Ausgängen
- Zugangskontrolle
 - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
 - Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
 - Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.
 - für Managed Server, Webhosting und Storage Share
 - Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert
- Zugriffskontrolle
 - bei internen Verwaltungssystemen des Auftragnehmers
 - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.

- Revisionsssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
- für Dedicated Server, Colocation Server, Cloud Server und Storage Box
 - Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
- für Managed Server, Webhosting und Storage Share
 - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
 - Revisionsssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
 - Für übertragene Daten/Software ist einzig der Auftraggeber in Bezug auf Sicherheit und Updates zuständig.
- Datenträgerkontrolle
 - Datacenter-Parks in Nürnberg, Falkenstein und Helsinki
 - Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
 - Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).
- Trennungskontrolle
 - bei internen Verwaltungssystemen des Auftragnehmers
 - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
 - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
 - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
 - Die Trennungskontrolle obliegt dem Auftraggeber.
 - für Managed Server, Webhosting und Storage Share
 - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
 - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
- Pseudonymisierung
 - Für die Pseudonymisierung ist der Auftraggeber verantwortlich

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

- Weitergabekontrolle
 - Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
 - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.
- Eingabekontrolle
 - bei internen Verwaltungssystemen des Auftragnehmers
 - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
 - Änderungen der Daten werden protokolliert.
 - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
 - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
 - für Managed Server, Webhosting und Storage Share
 - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
 - Änderungen der Daten werden protokolliert.

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

- Verfügbarkeitskontrolle
 - bei internen Verwaltungssystemen des Auftragnehmers
 - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
 - Sachkundiger Einsatz von Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
 - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
 - Monitoring aller relevanten Server.
 - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
 - Dauerhaft aktiver DDoS-Schutz.
 - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
 - Datensicherung obliegt dem Auftraggeber.
 - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
 - Dauerhaft aktiver DDoS-Schutz.
 - für Managed Server, Webhosting und Storage Share
 - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
 - Einsatz von Festplattenspiegelung.
 - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
 - Einsatz von Softwarefirewall und Portreglementierungen.
 - Dauerhaft aktiver DDoS-Schutz.
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);
 - Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).
- Auftragskontrolle
 - Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
 - Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
 - Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.