Agreement
on
Data Processing pursuant to Article 28 of the GDPR

Goethe-Institut e.V., Oskar-von-Miller-Ring 8, 80333 München

- hereinafter referred to as “Client” or “AG” -

and

Add contractor

- hereinafter referred to as the “Contractor” or “CC” –

1. Subject Matter of This Agreement and Term

1.1 The Client (hereinafter "Client") has commissioned the Contractor (hereinafter "Contractor") under a contract to provide various services (hereinafter "Services"). This agreement ("Data Processing Agreement") supplements the contract with provisions regarding data processing in accordance with Article 28 of the GDPR. The exact title of the contract can be found in Annex 1 to this DPPA.

1.2 To the extent that, in the course of providing services, the Contractor (1) processes personal data that it receives from the Client (hereinafter "Data") and/or (2) is commissioned to perform inspections or maintenance of the Client's automated processes or data processing systems, where the Contractor has the possibility of accessing personal data, this is done exclusively on behalf of the Client and in the sense of commissioned processing pursuant to Art. 28 GDPR (hereinafter: "CP").

1.3 The AG remains the data controller under data protection law, i.e., the "data controller," and is responsible, in relation to the data subjects, for assessing the lawfulness of data processing and for safeguarding the rights of the data subjects.

1.4 This Data Processing Agreement governs the details of data processing in accordance with Articles 28 and 29 of the GDPR and takes precedence over all other agreements between the parties regarding the processing of data by the Contractor. It also supersedes any prior data processing agreements that may exist regarding the processing of data on behalf of the Client.

1.5 The commencement, duration, termination, and notice provisions of this AV Agreement correspond to those of the Contract. To the extent that the Contract does not contain any provisions on these matters, the following applies: This AV Agreement takes effect upon the signing of this AV Agreement and remains in effect indefinitely; it may be terminated in writing by either party with six weeks' notice to the end of a month. The right to terminate the agreement for cause remains unaffected. If there is cause for extraordinary termination of this AV Agreement, this simultaneously constitutes cause for extraordinary termination of the contract

2. Details regarding data processing by the Contractor on behalf of the Client

2.1 The data protection details regarding the services to be provided by the Contractor are set forth in Exhibit 1, which describes the following for each service:

(1) The subject matter, nature, and purpose of the processing of personal data carried out in connection with the provision of services,

(2) the nature of the personal data processed in this context and

(3) the respective categories of data subjects affected by this data processing.

2.2 The Contractor shall process the data exclusively within the scope of this Data Processing Agreement, in particular to the extent specified in the relevant provisions of Annex 1, as well as any documented individual instructions from the Client pursuant to Section 2.3; deviations are not permitted.

The Contractor is only authorized to process the data in other ways to the extent that it is legally required to do so under the law of the EU or the EU Member State to which it is subject; in such a case, the Contractor shall notify the Client in writing of these legal requirements prior to processing, provided that the relevant law does not prohibit such notification on grounds of an important public interest. the exception of the aforementioned legal obligations, the Contractor may not use the data for

use them for any other purpose, in particular not for your own purposes, and not to make any copies or duplicates thereof.

2.3 Individual instructions from the Client must remain within the scope of the contractually agreed scope of services. The Client must issue individual instructions in writing. In cases of imminent delay, the Client may also issue an individual instruction verbally; the Client must then confirm this in writing without delay. The Contractor shall immediately inform the Client if, in its opinion, an individual instruction violates statutory provisions. The Contractor is then entitled to suspend the execution of the corresponding instruction until it is confirmed or amended by the Client following review.

2.4 The Contractor may correct, delete, or restrict the processing of the data only upon specific instruction from the Client or to the extent that this is part of the services specified in Appendix 1. When deleting data, the Contractor must use secure, state-of-the-art methods, which the Contractor must demonstrate to the Client upon request.

2.5. If a data subject contacts the Contractor directly regarding a request for information under data protection law or other rights to which the data subject is entitled, the Contractor must immediately inform the Client and await the Client's specific instructions before taking any further action or engaging in any further communication. Taking into account the nature of the processing, the Contractor shall assist the Client in responding to the data subject's inquiries.

2.6. The Contractor warrants that it will strictly limit access to the data to those persons who need to access the data in order to provide the services. The Contractor further warrants that it will familiarize the persons employed in the performance of the work with the applicable provisions of the and has appropriately obligated them, both during their employment and thereafter, to maintain confidentiality and not to process the data without authorization. As proof of compliance with this obligation, the Contractor shall, upon request, provide the Client with appropriate evidence, in particular (where applicable, anonymized) copies of the confidentiality agreements.

2.7 The Contractor shall regularly monitor and document, both within its own organization and among the subcontractors it engages, the proper processing of data and compliance with data protection regulations by the respective employees, as well as the fulfillment of the obligations under this Data Processing Agreement. Upon request by the Client, the Contractor shall provide written evidence of such monitoring and submit the documentation thereof. The Contractor further ensures that all processing activities it performs for the Client under this Data Processing Agreement are documented in accordance with Art. 30(2) GDPR. Upon the Client's request, the Contractor shall make this documentation available to the Client.

2.8 The Contractor shall immediately notify the Client in writing, providing details of

(1) Suspected violations of personal data protection,

(2) Violations by him or his employees, subcontractors, or third parties of data protection regulations or of the provisions set forth in the contract,

(3) Deviations in the Contractor's technical and organizational measures from the requirements agreed upon with the Client,

(4) Irregularities in data processing,

(5) any unauthorized access to or processing of data and/or

(6) Inquiries, inspections, investigations, or other actions taken by a data protection supervisory authority or another authority (e.g., the police or a court) regarding the Contractor.

The Contractor must notify the Client of the breach, deviation, or irregularity no later than 24 hours after becoming aware of it.

The above reporting obligations apply in particular with regard to any reporting and notification obligations of the Client under Articles 33 and 34 of the GDPR. The Contractor undertakes to provide the Client with appropriate support in fulfilling its obligations under Articles 33 and 34 of the GDPR, such as providing the Client with knowledgeable contacts, making relevant documents available, and answering the Client's questions.

The Contractor may not submit notifications pursuant to Article 33 or 34 of the GDPR on behalf of the Client, unless the Client has provided express, specific instructions to that effect.

2.9 Reports from the Contractor pursuant to Section 2.8.

(1) a description of the nature of the breach, deviation, or irregularity, including, where possible, the categories and approximate number of individuals affected, the categories of data affected, and the approximate number of data records affected;

(2) a description of the likely consequences of the violation, deviation, or irregularity; and

(3) a description of the measures taken or proposed by the Contractor to remedy the breach, deviation, or irregularity and, where applicable, measures to mitigate any potential adverse effects.

2.10 Information regarding the Contractor's Data Protection Officer ("DPO") and further details provided by the Contractor regarding its data protection organization are set forth in Appendix 2 and have been confirmed by the Contractor. The Contractor must immediately notify the Client in writing of any change in the DPO or any other changes to the information in Appendix 2.

2.11 The Contractor shall assist the Client with appropriate technical and organizational measures to comply with the data subject rights under Articles 12 through 23 of the GDPR, as well as to comply with the Client's obligations under Articles 32 through 36 of the GDPR regarding the security of personal data, as well as any necessary data protection impact assessment and prior consultations with supervisory authorities. The Contractor shall furthermore provide the Client, upon the Client's request, with all information and data necessary for the Client to fulfill other legal obligations applicable to it (such as the preparation of the record of processing activities).

2.12 The Contractor warrants that the data will be strictly separated from other data sets (whether the Contractor's own or those of other clients of the Contractor); further details are described in Appendix 5 under the heading "Confidentiality – Segregation of Data." The Contractor shall clearly label data carriers originating from the Client or used on behalf of the Client, and shall document their receipt and return as well as their ongoing use.

3. Location of data processing by the Contractor

3.1 The Contractor generally processes the data in a member state of the European Union (EU) or another signatory state to the Agreement on the European Economic Area (EEA); the status of the country at the time of the respective processing is decisive. This also applies to mere access to the data from such countries.

3.2 However, if the Contractor (see Section 4 regarding subcontractors) does not process the data within the EU/EEA or accesses the data from outside this area, this is permitted only if

- the specific requirements of Articles 44 et seq. of the GDPR are met and the Contractor provides evidence of this to the Client; and
- the Client has expressly consented to this, either by ensuring that Appendix 3 is completed in full and correctly at the time the Service Agreement is concluded, or, in the event of a subsequent transfer of data processing to a jurisdiction outside the EU/EEA, by executing a separate copy of Appendix 3 and providing the Client's prior written consent to such transfer as stated therein.

3. 3 In general, the Contractor may process the data only at its principal place of business and its business locations. Access to the data from outside these locations (e.g., during telework, work from home, mobile work, or similar) is permitted only in exceptional cases due to force majeure (e.g., due to a pandemic), provided, however, that (1) the technical and organizational measures agreed upon in Annex 5 to this AVV also apply at the location of data processing, and (2) the Contractor has access to perform inspections as provided for in this Agreement, and ensures compliance with the provisions of this Agreement, including its Annexes. The Contractor must contractually ensure this with its employees by stipulating at least the following:

- Working from home is permitted only with the equipment provided by the employer for this purpose (including hardware, software, and connectivity options).
- Only applications preinstalled by the IT department or approved by it on a case-by-case basis may be used. This explicitly applies to portable software or operating systems on removable storage media as well.
- A computer's local drives are intended for launching applications and for use during the workday. Data processed locally must also be backed up in the home office by the end of the workday at the latest, e.g., on storage server-based drives. An exception applies only if the connection to the server-based drives or similar is temporarily unavailable. In this case, the backup must be performed at the earliest opportunity

  .

- Printouts containing personal data may only be made while working from home if it is ensured that they can be securely destroyed.
- Working from home may only take place within one's own living quarters at locations and under circumstances that ensure confidentiality, integrity, and availability. In particular, third parties must not have

It should be possible to review the processed data. Third parties also include persons living in the same household as the employee.

- Equipment and information used must also be transported securely and supervised at all times within the living quarters. Laptops, USB drives, etc. must be provided to employees by the contractor in encrypted form.

- If you are away for a short period, lock any devices you are using (e.g., screen lock) and effectively secure information against unauthorized access (e.g., password). If you are away for a longer period, all information and work equipment must be stored securely and, if possible, locked away

4 . Use of subcontractors

4.1 The Contractor may only engage subcontractors to perform the services with the prior and express written consent of the Client.

4.2 The Client has approved the subcontractors listed in Appendix 4.

The Contractor must include any additional subcontractors whose engagement the Client has approved in accordance with the provisions of this AV Agreement in Appendix 4 and send an updated version to the Client.

4.3 To the extent that, with the Client's prior consent, the Contractor is permitted, on an exceptional basis, to engage subcontractors based outside the EU or the EEA, the Contractor must strictly comply with the requirements of Articles 44 through 49 of the GDPR and provide evidence of such compliance to the Client. To the extent that the Client, due to current data protection requirements, may be required to enter into standard data protection clauses directly with the subcontractor, the Contractor shall assist the Client in this regard and, if necessary, become a party to these clauses itself.

4.4 In any case, the Contractor must structure its contracts with subcontractors in such a way that they comply, at a minimum, with the data rotection provisions of this AV Agreement and Articles 28 and 29 of the GDPR, that the responsibilities between the Contractor and the respective subcontractor are clearly delineated, and that the Client has the same rights directly against the respective subcontractor as it has vis-à-vis the Contractor under this Data Processing Agreement. This includes, in particular, the Client's direct control rights over the respective subcontractor. The contract between the Contractor and a subprocessor must also provide sufficient guarantees that the respective subprocessor implements the appropriate technical and organizational measures in such a way that processing is carried out in accordance with the requirements of this Data Processing Agreement and the relevant data protection laws.

4.5 The Contractor is responsible to the Client for selecting the best possible and data protection-compliant subcontractors, as well as for ensuring that the data is processed in a manner compliant with data protection regulations by such subcontractors. The Contractor must select its subcontractors with particular regard to the adequacy of the technical and organizational measures implemented by them within the meaning of Article 32

carefully select in accordance with the GDPR. The Contractor is further obligated to regularly verify and document compliance with these obligations by all subcontractors. Upon request by the Client, the Contractor must provide the Client with the relevant documentation pertaining to the selection process and the regular verification.

4.6 If a subcontractor fails to fulfill its data protection obligations, the Contractor shall be liable to the Client for the subcontractor's compliance with such obligations as if the Contractor had breached its own obligations. The Contractor's liability for its own obligations in connection with the subcontractor remains unaffected

4.7 The transfer of data to subcontractors or their access to such data is permitted only if the Contractor has met the requirements set forth in this Agreement and in Art. 28 of the GDPR, and if the respective subcontractor has fulfilled its obligations under Art. 29 and Art. 32(4) of the GDPR with respect to its employees.

4.8 The provisions of this Section 4 also apply to all subcontractors engaged by subcontractors, as well as to any further subcontractors engaged by them (and so on) throughout the entire chain.

5. Technical and organizational security measures implemented by the Service Provider

5.1 The Contractor shall ensure the security of processing in accordance with Article 32 of the GDPR, in particular in conjunction with Article 5(1) and (2) of the GDPR. In this regard, the Contractor shall ensure a level of protection appropriate to the risk to the rights and freedoms of the natural persons affected by the processing when providing the services. To this end, the Contractor shall take into account the protection objectives of Article 32 of the GDPR, such as confidentiality, integrity, and availability of the systems and services, as well as their resilience with respect to the nature, scope, context, and purposes of the processing, in such a way that, through appropriate technical and organizational measures, the risk is permanently eliminated to the greatest extent possible.

5.2 The data protection concept described in Appendix 5 specifies the selection of technical and organizational measures (hereinafter "TOMs") appropriate to the identified risk, taking into account the protection objectives in accordance with the state of the art, and
specifically addressing the IT systems and processing procedures used by the Contractor. The Contractor is obligated to maintain the TOMs during the term of this Data Processing Agreement. The Contractor shall also observe the principles of proper data processing

5.3 In the context of technical progress and further development, the Contractor is permitted and, where technically necessary, obligated to adapt individual TOMs, provided that such measures are appropriate and the security level of the TOMs specified in Annex 5 is not compromised. Upon request by the Client, the Contractor shall inform the Client of such changes; however, significant changes must be agreed upon by both parties prior to their implementation.

6. Inspections by the AG

6.1 The Contractor agrees that the Client is entitled, at any time and, where applicable, with reasonable notice, to verify compliance with data protection regulations, this Data Processing Agreement and its annexes, in particular the agreed TOMs set forth in Annex 5, either directly or through third parties, in particular by obtaining information and inspecting stored data and the

Data processing programs and on site inspections at the Contractor's premises. The Client is therefore obligated to treat all information obtained regarding the Contractor's trade secrets and data security measures as confidential. This obligation shall remain in effect even after the termination of this contract.

6.2 The Contractor warrants that, to the extent necessary, it will cooperate with the Client during inspections and assist the Client, in particular by granting access and providing documents (minutes, reports from the data protection officer, certifications, etc.).

7. Termination of the employment contract

7.1 Upon request by the Client at any time, but no later than upon termination of the Contract, the Contractor must immediately provide the Client with the Client's data in a standard electronic format readable by the Client, or, upon separate instruction, physically delete such data on its premises in compliance with data protection regulations. The Contractor must request that the Client exercise the above right of choice no later than two weeks after the termination of the Contract. The foregoing provisions apply mutatis mutandis to personal test and scrap material.

7.2 The Contractor must document the deletions referred to in the preceding paragraph and immediately send the deletion log to the Client, confirming in writing the completeness of the data deletion and the accuracy of the information contained therein.

7.3 Documents of the Contractor that serve to demonstrate that the Contractor is processing data in accordance with the contract and applicable laws, as well as documents subject to the Contractor's statutory retention obligations, are exempt from the foregoing provisions to the extent necessary. To the extent that such documents contain data, the Contractor must inform the Client no later than upon termination of the AV Agreement

8. Liability and Mutual Information

8.1 The Contractor shall be liable in accordance with the statutory liability provisions for damages incurred by the Client as a result of the Contractor's breach of this Agreement and/or of the applicable statutory data protection provisions. Fines shall also be considered such damages.

Any limitations of liability set forth in the relevant commercial agreement governing the provision of the services in question shall not apply.

8.2 If, in connection with the data processing carried out pursuant to this Data Processing Agreement, claims for damages (Art. 82 GDPR), fines (Art. 83 GDPR), or other sanctions (Art. 84 GDPR) are threatened or asserted against the Contractor or the Client, the Contractor and the Client shall immediately inform each other thereof. Without prior consultation with the other party, the affected party may not issue any statements, nor may it make any admission or comparable declaration; if the Contractor and the Client cannot agree on the manner of defense, the final decision-making authority lies with the Client as the "data controller." Furthermore, both parties shall support each other in defending against such claims.

9. Other Provisions

9.1 The Client may terminate this AV Agreement and the underlying contractual engagement at any time for cause without notice if the Contractor seriously violates data protection regulations or the provisions of this AV Agreement, fails to comply with an instruction from the fails to carry out an instruction to be followed under this AV Agreement despite a reminder, or denies the Client its rights of inspection in breach of the contract.

9.2. The assertion of a right of retention under Section 273 of the German Civil Code (BGB) with respect to the data, parts thereof, and the client's data storage media is excluded.

9.3 If the data held by the Contractor is at risk due to seizure or attachment, insolvency proceedings, or other vents or actions by third parties, the Contractor must immediately notify the Client. The Contractor must inform all parties involved in this matter that the Client alone is the data controller and "owner of the data."

9.4 No separate remuneration for the Contractor's services, in particular support services, is payable under this AV Agreement; rather, such services are covered by the remuneration provided for in the commercial contract.

9.5 Any amendments or additions to the AV Agreement or its components and attachments—including any representations made by the Contractor—require a written agreement and an explicit statement that such changes constitute an amendment or addition to this Agreement. This also applies to any waiver of this formality requirement. "In writing" in the foregoing sense means the form specified in § 126 BGB, which may also be satisfied by signing and sending via fax or scan.

9.6 Legal Provisions EU Regulations. Within the meaning of this AV Agreement also include

9.7 With the exception of Section 9.5, written form (such as email) is also sufficient to satisfy the written form requirement under this General Terms and Conditions agreement

9.8 This AV Agreement is governed by the laws of the Federal Republic of Germany, unless the GDPR contains provisions that take precedence. To the extent that a jurisdiction has been agreed upon in the commercial contract, this agreement shall also apply to all claims or matters arising out of or in connection with this AV Agreement.

9.9 If any provision of this Terms of Service agreement is invalid, this shall not affect the validity of the remainder of the Terms of Service agreement.

10. Appendix

The following appendices are an integral part of this AV Agreement:

Appendix 1: Details on order processing

Appendix 2: Information on the Contractor's data protection organization

Appendix 3: Location of data processing by the Contractor outside the EU/EEA

Appendix 4: List of approved subcontractors

Appendix 5: Description of the technical and organizational measures taken by the Contractor to protect the Client's data

11. Signatures

Client	**Contractor**
Place, Date	Place, Date
Position and Name in block letters	Position and Name in block letters
_____	_____
Client's signature	Signature of the Contractor

APPENDIX 1: Details on Data Processing on Behalf of a Client

1. Table of Services and the Associated Processing of Client Data

Lfd. Nr.	**Brief description of the services that the Contractor provides to the Client** **(In brief)**	**Subject matter, nature, and purpose of the related processing of personal data** (What specific processes involving personal data are to be carried out: Collection? Storage? Transmission? How? Etc.)	**Does the contractor store the client's data on their own premises?**	**When will the data be deleted?**	**Group of data subjects (= the groups of people whose data is processed)** (Examples: Employees of the company, the company's end customers, the company's trainees, etc.)	**Type of personal data that the Contractor receives/processes** "Order data," etc. (= categories of data, such as "address data" or	**Location (city/ country) where the data is processed**
	EXAMPLE: *Printing of business cards for AG employees*	*EXAMPLE:* *The personal data of the employee to be printed must be collected and temporarily stored for technical purposes. This data is then processed and printed for the business cards.*	*EXAMPLE:* *Yes.* *Deletion will take place after the printed business cards have been sent to the client and the client has approved the cards*	*EXAMPLE:* *7 Days* *After the event has ended*	*EXAMPLE:* *Employees of the AG*	*EXAMPLE:* *Name and professional contact information of the employees*	*EXAMPLE:* *Munich*

APPENDIX 2: Information on the Contractor's Data Protection Organization

a. Recipients of instructions on the contractor's side – name, position

List here

b. Data Protection Officer

☐ The employer has appointed a Data Protection Officer (DPO). Name and contact information : _____

☐ No DSB has been ordered. Reason: _____

c. Confidentiality, etc.

All employees of the Contractor who may come into contact with the Client's personal data are familiarized with the applicable data protection regulations and are obligated to maintain confidentiality and handle personal data in a confidential manner.

d. Data Protection Training

The contractor's employees who may come into contact with the client's personal data have received regular training in data protection .

e. Internal Data Protection Controls

The Contractor conducts regular internal data protection audits.

f. Certifications

The Contractor holds the following certificates/certifications (e.g., ISO 27001 certification), which also, or specifically, pertain to the procedures for collecting, processing, or using the Client's data.

☐ None

☐ The following (please attach):

APPENDIX 3: Location of data processing by the Contractor

If the data processing is carried out by the Contractor in or from a Member State of the EU or the EEA:

☐ **Yes** ☐ **NO**

If the Contractor processes data outside an EU or EEA member state, the contracting parties must enter into EU Standard Data Protection Clauses.

Otherwise, the Contractor may provide the following reasons why these clauses are not necessary: An adequate level of data protection

☐ is established by an adequacy decision of the European Commission (Art. 45(3) of the GDPR);

☐ is ensured through binding internal data protection policies at the contractor (Art. 46(2)(b) in conjunction with Art. 47 of the GDPR)

☐ is produced by: _____

APPENDIX 4: List of approved subcontractors

Are subcontractors used? ☐ No

☐ Yes

If subcontractors are used, they must be listed in full in the following table;

Name of the subcontractor	Subcontractor's address	Responsibilities of the subcontractor (= What personal data belonging to the client does the subcontractor process, and for what reasons does the subcontractor have access to it?)

APPENDIX 5: Description of the technical and organizational measures taken by the Contractor to protect the Client's data

Abbreviation	Explanation and examples	*Description of the specific measures taken by the Contractor* *Important note on filling out the form:* *The Contractor must describe, specifically and in detail, (only) the measures it has taken to protect the data it receives from the Client or to which it has access:* - *Simply listing keywords such as "video surveillance" or similar terms is not sufficient* - *It is necessary to provide specific details; for example: "Video surveillance system, consisting of X cameras that monitor, record, and are regularly analyzed in the reception, entrance, and server room areas," or similar.* *If the Client's data is stored on the Contractor's systems in multiple locations—for example, stored on the Contractor's servers and processed on desktop PCs or clients—the Contractor must describe the measures taken for both the servers and the desktops, such as a. measures concerning servers (...), b. measures concerning clients (...)". To the extent that data is processed on laptops or other mobile devices, this constitutes a third category (c. measures for mobile devices) due to the increased security measures required there.*
1 Confidentiality (Art. 32(1)(b) of the GDPR)		
Physical Access Control	No unauthorized access to data processing facilities, e.g.: magnetic or chip cards, keys, electric door openers, security guards or gatekeepers, alarm systems, video surveillance systems;	
Access Control	No unauthorized system access, e.g., (strong) passwords, automatic lockout mechanisms, two-factor authentication, data storage encryption;	
Data Access	No unauthorized reading, copying, modification, or deletion within the system, e.g., authorization models and access rights tailored to specific needs, logging of access events;	
Separation Control	Separate processing of data collected for different purposes, e.g., multi-tenancy, sandboxing;	

Pseudonymization (Art. 32(1) (a) GDPR; Art. 25(1) GDPR)	The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures	
2. Integrity (Art. 32(1)(b) of the GDPR)		
Data sharing control	No unauthorized reading, copying, modification, or removal during electronic transmission or transport, e.g.: encryption, virtual private networks (VPN), electronic signatures	
Input validation	Determining whether and by whom personal data has been entered into, modified, or removed from data processing systems, e.g., logging, document management;	
3. Availability and resilience (Art. 32(1)(b) of the GDPR)		
Availability Check	Protection against accidental or intentional destruction or loss, e.g., backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), antivirus software, firewall, reporting procedures, and emergency plans;	
Rapid recoverability (Art. 3 (2)(1)(c) GDPR);		
4. Procedure for regular review, assessment, and evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)		
Data Protection Management		
Incident-Response-Management;		
Privacy-friendly default settings (Art. 25(2) GDPR);		
Order Tracking	No data processing on behalf of a client within the meaning of Article 28 of the GDPR without appropriate instructions from the client, e.g.: Clear contract terms, formalized contract management, strict selection of the service provider, duty to verify in advance, follow-up checks.	