Where TrustYou within provision of the services subject to the subscription agreement about the use of TrustYou services processes personal data on behalf of a Client the following Data Processing Agreement (DPA) is concluded on the day of signing of agreement between the Client and TrustYou in accordance with section 10.3 of the TrustYou's General Terms and Conditions that are substantial part of the subscription agreement.

DATA PROCESSING AGREEMENT

between

Client *(as determined in subscription agreement about use of TrustYou services)*
(hereinafter referred to as the "Principal")

and

TrustYou GmbH, Schmellerstraße 9, 80337 Germany
(hereinafter referred to as the "Agent")

The Principal and the Agent shall be hereinafter individually referred to as the "Party" and jointly as the "Parties".

1. Subject Matter and Duration

1.1. On the basis of a separate agreement ("Main Agreement") the Agent shall provide the Principal with services (hereinafter collectively referred to as the "Services"). Within the provision of the Services under the Main Agreement, the Agent shall process personal data for the Principal within the meaning of Articles 4(2) and 28 of the General Data Protection Regulation ("GDPR") ("Principal‘s data"). The Principal is the data controller within the meaning of the GDPR with regard to any processing of the Principal‘s data.

1.2. The subject matter and the duration of the data processing activity by the Agent are laid down in the Main Agreement, unless further obligations result from the provisions herein.

1.3. This Agreement sets forth the terms and conditions of the data processing of the Principals' data to be carried out by the Agent for the Principal within the performance of the Main Agreement.

1.4. The duration of this Agreement corresponds to the duration of the Main Agreement.

2. Specification of the Order Content

2.1. The purpose of the data processing, the nature of the personal data and the categories of data subjects, the persons authorised to give instructions on the part of the Principal and the persons authorised to receive instructions on the part of the Agent, as well as the contact persons on both sides for data protection issues are listed in **Appendix 1** to this Agreement.

2.2. The agreed services shall be provided exclusively in a Member State of the European Union or in a signatory state of the Agreement on the European Economic Area. Each and any relocation of the services or of parts thereof to a third country requires the Principal's prior approval and may only take piace if the special prerequisites laid down in Article 44 et sq. in the GDPR are met (e.g. the European Commission adequacy decision, standard contractual clauses, binding corporate rules).

3. Principal's Rights and Obligations, as well as Authority to Issue Instructions

3.1. The Principal shall be solely responsible for the appraisal of the lawfulness of the processing pursuant to Article 6(1) in the GDPR, as well as for the safeguarding of the data subjects' rights pursuant to Articles 12 to 22 in the GDPR. The Agent shall immediately transfer such inquiries to thePrincipal, provided they are obviousiy addressed to the Principal alone.

3.2. The Agent shall immediately forward enquiries from data subjects, insofar as they relate to the processing of Principal‘s data or are caused by the processing of Principal's data, by e-mail to the persons of the Principal specified in **Appendix 1.**

3.3. Changes to the subject matter of the processing and any procedural changes shall be jointly coordinated between the Principal and the Agent, and must be established in writing or in a documented electronic format.

3.4. The Principal's instructions shall be primarily established through the herein arrangement and the Main Agreement. Subsequently, the Principal can amend, supplement or replace individual instructions in writing or in a documented electronic format. in individual cases, instructions can also be communicated orally. Such instructions must be immediately confirmed by the Principal in writingor in a documented electronic format. If the content of the Principal's instructions exceeds the Agent's obligations towards the Principal as per the Main Agreement, the Principal must separately remunerate such services. If an instruction can only be implemented with disproportionately high efforts, the Agent has the right of extraordinary cancellation of the Main Agreement and of this Agreement.

3.5. The Principal is entitled to verify the compliance of the technical and organizational measures taken by the Agent and the observance of the herein obligations, before the beginning of the processing and at regular intervals and in an appropriate manner.

3.6. The Principal shall immediately inform the Agent an any errors or irregularities noticed upon the review of the order results.

3.7. The Principal must treat all the Agent's business secrets and data security measures that the Principal becomes aware of during the contractual relationship, as confidential information. This obligation shall survive the termination of this Agreement.

4. Agent's Obligations

4.1. The Agent processes Principal's data exclusively within the framework of the agreed arrangements and in accordance with the Principal's instructions, provided the Agent is not obliged to another processing by the laws of the Union or of other Member States to which the Agent is subject (e.g. investigations of law enforcement agencies or state protection authorities); in such a case, the Agent shall inform the Principal of that legal requirement before the processing, unless that law prohibits such information on important grounds of public interest (Article 28(3)(2)(a) GDPR).

4.2. The Agent shall not use the personal data provided for processing for other purposes, particularly not for own purposes. Copies or duplicates of the personal data shall not be made without the Principal's knowledge thereof.

4.3. For the order-compliant processing of personal data, the Agent guarantees the deployment of all the agreed measures, as per the concluded agreement. It guarantees that the data processed for the Principal is stored separately from other databases, at least at a logical level. The Agent must review the observance of its obligations under this Agreement, at least once per calendar year. The results of the review must be documented and provided to the Principal, upon request.

4.4. For the fulfillment by the Principal of the data subjects' rights pursuant to Articles 12 to 22 GDPR, the Agent must assist the Principal in the preparation of the directories of processing activities, as wellas in the Principal's necessary data protection impact assessments, according to the Agent's possibilities (Article 28(3)(2)(e) and (f) GDPR). Previous written approval of the quotation from the Principal, The Agent is entitled to additional remuneration for the additional costs incurred this way.

4.5. The Agent shall immediately inform the Principal when, according to the Agent's opinion, an instruction given by the Principal is in breach of the legal provisions (Article 28(3)(3) GDPR). The Agent has the right to suspend the implementation of an instruction until it is confirmed or changed, after review, by the Principal's persons in charge.

4.6. The Agent shall correct or delete personal data from the contractual relationship, or shall restrict the processing thereof, if the Principal requests so by means of an instruction and if the Agent's legitimate interests are not prejudiced this way. These deletion obligations do not cover data copies created during the regular backup of extensive databases of the Agent, the isolated deletion of which would imply a major effort for the Agent, and which will be automatically deleted or overwritten no later than one year, within the backup cycle used by the Agent. Restoring and otherwise using such copies before they are automatically deleted and/or overwritten is not allowed after the termination of the Agreement. The Principal may also request the Agent to immediately delete such backup copies, if the Principal reimburses the costs incurred this way by the Agent; this also includes a cost allowance charged by the Agent for the working time of its own personnel.

4.7. Information about personal data from the contractual relationship may be disclosed by the Agent to third parties or to the data subjects only after the Principal's prior instruction or consent, unless the Principal is legally bound to place an order.

4.8. The Agent acknowledges the fact that the Principal - except for urgent grounds, to be documented by the Principal - is entitled to audit the observance of the provisions on data protection and data security, as well as the related contractual arrangements, to the appropriate and required extent, either by themselves or by third parties commissioned by the Principal, subject to an appointment during the Agent's usual business hours, without disturbing the Agent's normal activity and not more often than every 12 months, (Article 28(3)(2)(h) GDPR). If the third party commissioned by the Principal is a competitor of the Agent's, the Agent shall have the right to object to the commissioning of such third party. The Agent undertakes to provide support in such inspections, to the required extent. Previous written approval of the quotation from the Principal, the Agent is entitled to additional remuneration for the additional costs incurred this way.

4.9. The Agent is bound to confidentiality in the ordered processing of the Principal's personal data. This shall survive the termination of the agreement, as well.

4.10. The Agent warrants that it shall make sure that the involved employees are familiar with the relevant data protection provisions, before the commencement of their activity, and are properly

committed to confidentiality, both during their employment and after the termination of the employment relationship (Article 28(3)(2)(b) and Article 29 GDPR). The Agent monitors the compliance with the data protection regulations in its company.

4.11. In accordance with Art.82 of the GDPR, the Agent shall be liable for the damage caused by processing where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the Principal.

5. Data Protection Officer

In accordance with Art. 38 of the GDPR the Agent has appointed a data protection officer and ensures that the data protection officer can perform his duties in accordance with the law. Upon request, the Agent shall provide the Principal with the contact details of the data protection officer.

6. Agent's Notification Obligations in case of Processing Malfunctions and Personal Data Breaches

6.1. The Agent shall immediately inform the Principal on any malfunctions, breaches by the Principal or its employees against the data protection regulations or the specifications in the order, as well as on the suspicion of personal data breaches or irregularities in the processing of personal data. This applies in particular to possible information and notification obligations of the Principal's, in accordance with Articles 33 and 34 in the GDPR.

6.2. The Agent undertakes to properly assist the Principal in its obligations pursuant to Articles 33 and 34 GDPR, as required (Article 28(3)(2)(f) GDPR).

6.3. The Agent shall immediately notify the Principal of an enquiry by the supervisory authority within the meaning of Art. 31 GDPR.

7. Sub-contractual Relationships with Subcontractors (Article 28(3)(2)(d) GDPR)

7.1. The commissioning of subcontractors for the processing of the Principal's data is generally allowed, Article 28(2) GDPR. The Agent must make sure that it attentively selects the subcontractor under special consideration of the suitability of the taken technical and organizational measures, within the meaning of Article 32 GDPR.

7.2. The Agent shall always inform the Principal on every intended modification in relation to the addition or replacement of subcontractors, whereby the Principal shall be given the opportunity to object to such modifications. If the Principal does not object to a change in relation to subcontractors within 4 weeks of receipt of the change information, the change shall be deemed to have been confirmed.

7.3. Any commissioning of subcontractors in third countries may only take place if the special prerequisites laid down in Article 44 et sq. in the GDPR are met (e.g. the European Commission adequacy decision, standard contractual clauses, binding corporate rules).

7.4. The Agent must ensure, by means of contractual clauses, that the agreed rules between the Principal and the Agent are also enforceable in relation to the subcontractors. The contract with the subcontractor must be in writing, which may also be in an electronic format (Art. 28 para. 4 and para. 9 GDPR). The Principal has the right to inspect the relevant contractual conditions upon request.

7.5. The Agent shall be liable towards the Principal for the observance by the subcontractor of the data protection obligations that have been contractually imposed to it by the Agent in accordance with this paragraph.

7.6. Within the meaning of this Agreement, a sub-contractual relationship exists when the services are directly related to the provision of the services in the Main Agreement. This does not include ancillary services used by the Agent e.g. telecommunications services, postal and transportation services, maintenance and user service or the disposal of data carriers, as well as other measures in order to ensure the confidentiality, availability, integrity and capacity of the hardware and software of the data processing systems. However, the Agent must implement proper and lawful contractual arrangements and control measures in order to guarantee the data protection and data security of the Principal's personal data within the outsourced ancillary services, as well.

7.7. The subcontractors currently entrusted by the Agent with the processing of personal data are indicated in the table in **Appendix 2** and are approved by the Principal with signature of this agreement.

8. Technical and Organizational Measures, Article 32 GDPR (Article 28(3)(2)(c) GDPR)

8.1. For the specific order processing, the Agent shall ensure an adequate level of protection of the rights and freedoms of the data subjects affected by the processing, in line with the risks. For this, the protection objectives laid down in Article 32(1) GDPR, such as confidentiality, integrity and availability of the systems and services, as well as their capacity in relation to the nature, scope, context and purposes of processing shall be considered in such a way that the risk is permanently mitigated through adequate technical and organizational remedial actions.

8.2. The Agent's data protection concept attached as **Appendix 3** describes in detail the selection of technical and organisational measures in line with the identified risk, taking into account the protection objectives according to the state of the art and taking particular account of the IT systems and processing methods used by the Agent.

8.3. The Agent acknowledges the fact, that the Principal is entitled to audit the technical and organizational measures taken by the Agent according to Art. 32 GDPR to the appropriate and required extent, either by themselves or by third parties commissioned by the Principal.

8.4. In the course of the contractual relationship, the measures taken by the Agent can be adapted to the further technical and organizational development, but they shall not fall short of the agreed standards.

9. Agent's Obligations after the Termination of the Agreement

Upon the termination of the Agreement, the Agent must delete all the data, documents and prepared processing and usage results related to the contractual relationship, which are in the possession of the Agent, as well as of the subcontractors. Until the termination of the Agreement, the Principal may retrieve the data from the standard interfaces with the Agent, via the Internet, and store such data with them. The Principal may also request the Agent to provide the data in another form, if the Principal reimburses the costs incurred this way by the Agent; this also includes a cost allowance charged by the Agent for the working time of its own personnel.

10. Miscellaneous

10.1. Side agreements or amendment agreements require the written form or a documented electronic format.

10.2. In case of any inconsistencies, the provisions in this Agreement on personal data processing shall take precedence over the ones in the main agreement.

10.3. If the Principal's data to be processed by the Agent are jeopardized by measures of third parties (e.g. by garnishment or seizure), by insolvency proceedings or other events, the Agent must immediately notify the Principal.

10.4. If individual parts of this Agreement become ineffective, the effectiveness of the remaining provisions shall be preserved.

10.5. The German law shall apply, excluding any possible references to other legal systems and excluding the UN sales law.

10.6. Unless the Main Agreement stipulates another jurisdiction, the exclusive place of jurisdiction for disputes resulting from or in connection to this Agreement shall be the Agent's registered office.

For the Principal	For the Agent
(Signature of Agreement shall apply)	Nikolai Visnjic, Chief Financial Officer

Appendix 1 — Purpose of the processing, nature of the data, categories of data subjects, authorised officers and recipients, contact persons

1. Purpose of the processing

Providing and delivering online reputation management services, specifically, Hotel Analytics, Hotel Survey and Hotel Marketing Services in particular through the website www.trustyou.com.

2. Type of data

The subject of the processing of personal data regularly is:

- E-mail address
- First name and surname
- Language

3. Categories of data subjects

The categories of data subjects to be processed shall include

- Employees of the Principal
- Hotel guests of the Principal

4. Persons entitled to issue instructions to the Agent

Principal shall inform Agent immediately after the entry into force of this Agreement of those persons who are to be entitled to issue instructions to the Agent. Should there be a change in the persons entitled to issue instructions, the Principal shall inform the Agent thereof in text form (sufficient email).

5. Persons entitled to receive instructions from the Principal

For its part, the Agent shall inform the Principal immediately after the entry into force of the contract of those persons who are to be entitled to receive instructions. Should there be a change in the persons entitled to receive instructions, the Agent shall inform the Principal thereof in text form (sufficient email).

6. Contact person for data protection questions / enquiries about data subjects

The Principal shall inform the Agent immediately after this Agreement has come into force of those persons who are to be informed in the event of enquiries relating to data protection law or enquiries concerning data subjects or to whom these enquiries concerning data subjects are to be forwarded. Agent will inform Principal immediately after this contract has come into force of those persons who are to be contacted in the case of data protection issues. If Agent receives enquiries from hotel guests of Principal concerning the persons concerned, it shall forward them immediately to dataprotection@trustyou.com. Upon receipt, the Principal shall inform the Agent whether and how he can or should support the Customerin fulfilling the rights of the persons concerned.

Appendix 2: Agent's subcontractors

Name	Country	Address	Activity	Basis
Hetzner OnlineGmbH	Germany	Industriestr. 25, 91710 Gunzenhausen, Germany	Webhosting and mailings	Data Processing Agreement (DPA)
TrustYou, Inc.	USA	8343 Douglas Ave Suite 400 Dallas, TX, 75225 USA	Customer Service	Data Processing Agreement (DPA) & Standard Contractual Clauses
TrustYou Pte Ltd	Singapore	6 Raffles Boulevard Marina Square #03-308 Singapore 039594	Customer Service	Data Processing Agreement (DPA) & Standard Contractual Clauses
TrustYou K.K.	Japan	Shinjuku Mitsui Building Floor 11, Workstyling 2-1-1 Nishi-shinjuku, Shinjuku-ku, Tokyo 163-0411 Japan	Customer Service	Data Processing Agreement (DPA) & Standard Contractual Clauses & Adequacy Decisionby European Commission
Trinix Software Srl	Romania	Abatorului 142, 407280,Floresti, Romania	Customer Serviceand Engineering	Data Processing Agreement (DPA)
Salesforce.com Germany GmbH	Germany, USA	Erika-Mann-Str. 31, 80636 München, Germany	Cloud Database, contract management	Data Processing Agreement (DPA) & Standard Contractual Clauses
OpenAI Ireland Limited	Republic of Ireland	1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	AI response processing	Data Processing Agreement (DPA)
Chargebee Inc.	The Netherlands	Piet Heinkade 55 1019 GM Amsterdam Netherlands	Billing, contract processing, Customer management	Data Processing Agreement (DPA)
Candis	Germany	Candis GmbH Schönhauser Allee 180 10119 Berlin	Digital accounting	Data Processing Agreement (DPA)
Datev	Germany	DATEV eG Paumgartnerstr. 6 - 14 90429 Nürnberg	Taxation, accounting	Data Processing Agreement (DPA)
Lucanet	Germany	LucaNet AG Alexanderplatz 1 10178 Berlin Deutschland	Financial reporting, accounting	Data Processing Agreement (DPA)

Appendix 3: Technical and Organizational Measures of TrustYou GmbH pursuant to Article 32 GDPR for the Agreement pursuant to Article 28 GDPR

The technical and organizational measures for the data protection and data security to be taken and permanently maintained by the Agent are established in what follows. The purpose is to ensure, in particular, the confidentiality, integrity and availability of the information commissioned for processing.

1. Confidentiality

a. Access control (Article 32(1)(b) GDPR)

aa. Measures that prevent the unauthorized access to data processing equipment, which process or use personal data:

The Agent's office

- The business premises of the Agent are protected against unauthorized access by means of an electronic access control system.
- Only the employees of the Agent receive a token to open and close the access system. Doors lock automatically. The handing over and return of the token are documented.
- Third parties, i.e. persons who are not employed by the Agent, may only enter the office premises when accompanied by an employee.
- The entrance area is equipped with video surveillance systems.
- The server room for office IT and infrastructure is permanently locked and video-monitored.

Data warehouse

- A provider with a certified information security management system in accordance with ISO/IEC 27001 was selected to operate the computer centre.
- The access controls include, among others
    - Access only for authorized employees and authorized external personnel
    - Use of electronic access control systems
    - Logging of accesses
    - Accompaniment and identification of guests
    - Video surveillance of inputs and outputs
    - Computer center 24/7 staffed

- The technical and organisational measures implemented by the data center operators are regularly audited by an independent third party.

bb. Measures that prevent the use of the data processing systems by unauthorized persons:

- Each employee has a unique and customized user account.
- There is a documented application process for user IDs with authentication instance
- All user accounts are secured by individual passwords, each password is known only by the account holder and may not be communicated to other persons, not even within the organization.
- User passwords must consist of at least 9 characters and contain at least one upper case character and lower case characters, one figure and a symbol. User passwords must be changed at least every 90 days. In doing so, the last 10 used passwords cannot be used again. User accounts are automatically locked alter 5 consecutive unsuccessful authentication attempts.
- After maximum 5 minutes of inactivity, the PC is automatically locked by the system and can be unlocked only after the input of the user password.
- All log-in actions are recorded.
- There is a policy for the safe and proper handling of passwords.
- The admin access to the server systems is reserved to authorized admins. The authentication occurs via encrypted connections with cryptographic keys (SSH with password).
- All the productive server systems are secured via firewalls that allow only for the intended (incoming and outgoing) transfer protocols (default deny).
- All Computers have centrally managed antivirus software installed that automatically updates them.

cc. Measures which ensure that the persons authorized to use a certain data processing system can access exclusively the data assigned to their individual access rights, and that personal data cannot be read, copied, edited or deleted upon the processing, use and subsequent storage thereof:

- The use of Internet and e-mail accounts is allowed exclusively for business purposes. This significantly reduces the risk of malware.
- The use of IT and telecommunications systems is also allowed only for business purposes. External persons may not operate such systems.

- The introduction of personal IT and telecommunication systems, such as laptops, smartphones and USB sticks is not allowed.
- The organization WLAN is encoded and can be used only by the registered devices. A separate, protected WLAN is available for guests and visitors, and such WLAN does not enable the access into the organization's network.
- Mobile computers are provided with privacy screens and PC locking devices.
- The allocation of access rights within the systems occurs on the basis of documented procedures with authorization instance.
- The user management takes place in a rolling manner and follows a standardized rolling and authorization concept.
- The user rights are limited to the minimum level required for the performance of the activities (need-to-know principle).
- The created backups are also protected to the same extent as the productive data.

dd. Measures which ensure that data collected for different purposes are separately processed:

- Data collected for different purposes and data of different clients are kept and processed separately, by means of logic access controls.
- The development, test, integration and production system are reliably separated.
- Only anonymized data are used for testing purposes.

2. Integrity

a. transfer control (Article 32(1)(b) GDPR)

Measures which ensure that personal data cannot be read, copied, modified or deleted in an unauthorized manner upon electronic transfer, transport or storage on storage media, and that allow for the verification and identification of the locations to which a transmission of personal data is provided through data transfer devices:

- No longer needed hard-copy documents (notes, wrong printouts and copies) and data storage media with personal data or other confidential information are irrecoverably scrapped, unless there are legal or contractual retention periods that prohibit it.
- Hard-copy documents are shredded with shredders of safety level P-3, within a cross process.
- Data storage media are deleted by the IT-department by means of multiple overwriting. No longer usable data storage media are destroyed through a service provider. Mobile data storage devices are protected against unauthorized access by means of encryption.
- Data is transmitted encrypted (HTTPS, SFTP, SMTP-STARTTLS).
- There is a standardized process for the identification and handling of safety incidents.
- Mobile data storage devices are encrypted according to the state of the art, depending on the related need for protection.

b. Input control (Article 32(1)(b) GDPR)

Measures which ensure that it can be subsequently checked and established if and who has entered, changed or deleted personal data in the data processing systems:

- The input control occurs via a comprehensive logging of all the writing, editing and deleting activities within the application.
- The logging comprises the activities of both the Agent's employees and the client's activities.
- Authentication processes are also logged.
- Rights according to the least-privilege principle ensure that unauthorized persons may not enter, edit, delete data.

3. Order control, assessment and evaluation (Article 32(1)(d), 25(1) GDPR

Measures which ensure that the personal data commissioned for processing are processed only in accordance with the Principal's instructions:

- All the employees are obliged to confidentiality. The obligation also covers the employees of subcontractors.
- The employees participate in trainings on data protection and information security at least once a year.
- There are organizational instructions and security policies for the handling of IT systems and data.
- Data protection agreements in accordance with Article 28 GDPR (Agreements for commissioned data processing) with third-parties contain detailed information on the type and scope of the commissioned processing and use of the Principal's personal data.
- Data protection agreements in accordance with Article 28 GDPR (Agreements for commissioned data processing) with third-parties contain detailed information on the limitation of use to specific

purposes with regard to the Principal's personal data, as well as the interdiction for the service provider to use them beyond the written order.
- The rights of control of the Agent in relation to the subcontractors are stipulated in the agreement.
- The technical and organizational measures of the subcontractors are verified. • The Principal's instructions for job processing are rigorously implemented.

4. Availability and capacity (Articie 32(1)(b) GDPR)
Measures which ensure that the personal data are protected against accidental destruction or loss:

General
- Significant changes at the productive systems are approved and documented via a change-management process.
- Software development versions are tested via a multiple-stage system (development environment, testing environment, deployment environment, production environment).
- Software development occurs via source code review management. This way, different versions can be any time restored.
- The availability of the safety patches and known weak points in system and software components are monitored via a patch management process. The Installation of patches occurs via the change management process.

Office Building
- No relevant data storage takes place in the offices of the Agent
- The administrative access to the server system is independent of the availability of the office infrastructure.

5. periodic review, evaluation and evaluation procedures
a. Data Protection Management
TrustYou GmbH takes the following general organisational measures to protect personal data:
- There is a data protection policy and a data protection and information security policy in place
- All employees of TrustYou GmbH are bound in writing to confidentiality with regard to the processing of personal data. This declaration of commitment is part of the employment contract documents.
- All employees of TrustYou GmbH are trained in data protection and information security at least once a year. Participation is obligatory and documented.
- There are guidelines for the handling of personal data, password security and the use of IT and telecommunications systems.
- An external data protection officer has been appointed who, within the scope of his activities, acts without instructions and is appropriately and effectively integrated into the relevant operational processes.
- There is a policy for conducting data protection impact assessments (DPIA) in place
- There is a guideline for dealing with enquiries from data subjects in accordance with Art. 12 - 22 GDPR.
- A recording pursuant to Art. 30 GDPR is maintained.
- An audit concept exists and regular data protection and information security audits take place.
- A data protection and information management system has been implemented.

b. Incident-Response Management
There is a "Data Breach Policy" in place for detecting and dealing with privacy breaches.

c. Privacy Friendly Preferences
Data protection-friendly default settings are taken into account within the framework of software development (Art. 25 para. 2 GDPR)

d. Order control
Measures to ensure that personal data processed on behalf of the Principal are processed only in accordance with the instructions of the Principal:
- Data protection agreements in accordance with Art. 28 GDPR with third parties contain detailed information on the type and scope of the commissioned processing and use of the Principal's data as well as a prohibition on use by the service provider outside the written order.
- The control rights of Agent vis-à-vis the Principal and sub-contractors are contractually agreed.
- The technical and organisational measures of sub-contractors are checked.
- The instructions of the Principal for order processing will be strictly implemented.