Standard Client Terms & Conditions

valid from: 01.08.2024, Version 1.0

SCOPE

1.1. These Standard Terms and Conditions (“**General Terms**”) apply to and govern all services that TrustYou GmbH, Schmellerstr. 9, 81369 Munich, Germany (“**Provider**” or “**TrustYou**”) agrees to provide to Client (the“**Services**”). The Services are provided in the form of “Software as a Service” (“SaaS”) to be used via the internet. The hardware and software used by TrustYou to provide its Services are centrally hosted by TrustYouand/or TrustYou’s service providers in one or more data centers, and will not be handed over to the Client. In addition, TrustYou also provides training on the use of the products by agreement.

1.2. Any specific Services to which Client has subscribed are set forth in an online or offline order form which contains any specific terms and conditions agreed by Provider and Client in writing or by completion of an online form (the “**Order Form**”). The Order Form and these General Terms, together, constitute the entire agreement between Client and Provider (the “**Agreement**”). Client’s use of the Services, and Provider’sprovision of the Services, will signify the Parties’ assent to and acceptance of the Agreement.

1.3. Provider shall provide access to the Services to the agreed number of persons designated by Client who are employees of or consultants to Client or employees or consultants of third-parties that shall be entitled (each a**“Subscriber”** or “**User**”), as more fully described in the Order Form. Client is responsible for ensuring that any User uses the Services only in accordance with this Agreement and applicable laws. Client shall be full liable to Provider for any conduct of any User under this Agreement.

1.4. Provider addresses its Services to business customers and/or entrepreneurs, not to consumers.

1.5. The Client and Users must be of legal age in the territory of use in accordance with local laws in order to access and use the Services.

1.6. Provider’s Services are exclusively governed by the Agreement. General terms and conditions of the Clientshall not apply unless Provider has expressly agreed to them in writing (email not sufficient). General termsand conditions of the Client shall particularly not apply if the Client has referred to such general terms and conditions (or provided a copy of them) and Provider has merely not explicitly objected to them.

1.7. The Client hereby acknowledges and agrees to – if applicable – undergo the standard business Know-Your-Customer (KYC) checks prior to or immediately after contract closure, as required by applicable laws, regulations, and industry practices. Failure of the Client to complete the KYC process in time may result in barred or restricted access to certain services or termination of the Client's account at the sole discretion of the provider. The Client further agrees to provide detailed, accurate and up-to-date information and documentation to the provider and/or third party as requested for the purpose of conducting the KYC checks.

2. TERM AND TERMINATION

2.1 Term. The delivery of the Services to Client by Provider will commence on the date set forth in the Specific Terms as “subscription start date” or “license start date” or “effective date” (hereinafter the “**Subscription StartDate**”) and continue for the period stated therein (“**Subscription Period**”). If no specific Subscription Start Dateis set forth in the Order Form, then the Subscription Start Date shall be the date on which Client is first granted access to the Services by receiving account credentials.

Unless otherwise agreed the Subscription Period will continue for twelve (12) months from Subscription Start Date (the “**Initial Term**”), and effective as of each anniversary of the Subscription Start Date, the Agreement shall automatically renew for an additional twelve (12) months period (each such 12 months period a “**RenewalTerm**”) unless Written Notice of termination is provided by either party no later than three (3) months prior to the end of the then-current Initial Term or Renewal Term. For the purposes of this and all other provisions of the Agreement, "written notice" means a document signed by an authorised representative of the party in person or by advanced electronic signature (in accordance with the European eIDAS Regulation No. 910/2014) and provided to the other party as an original form, whereby it shall be sufficient for the Provider to send it by e-mail together with a PDF copy as an attachment.

2.2 Termination and Suspension.

a. If a party is in material breach of its obligations under the Agreement which is incapable of remedy, or if capable of remedy fails to remedy the same within thirty (30) days (unless another period is agreed between the parties, acting reasonably) of Written Notice to do so by the other party, the other party may, without prejudice to its other rights and remedies and at its option, terminate the Agreement as a whole, orany affected element of the Services provided under it.

b. Provider may suspend access to the Services with immediate effect if Client does not pay the agreed feesby the Due Date. Client’s failure to pay the agreed fees by the due date shall be considered a material breach pursuant to subsection b. above.

c. Provider may terminate the Agreement at any time upon ninety (90) days’ written notice to Client.

d. The Parties´ statutory right to terminate the Agreement for due cause remains unaffected hereby.

2.3 Effects of Termination.

Upon termination of the Agreement:

i. all of the provisions of this Agreement shall cease to have effect, save that the provisions which are expressed, or by its nature, implied to continue, survive or come into force in the event of such termination.

ii. the parties shall (without prejudice to any other rights and remedies) promptly pay to each other all sumswhich are due or outstanding; and

iii. Client´s right to use the Services shall terminate, and Client shall cease all use of the Services upon termination of the Agreement; and

iv. unless necessary in order that Provider may continue to perform its obligations, Provider shall cease allaccess to the systems, if any.

Except to the extent that this Agreement expressly provides otherwise, the termination of this Agreement shall not affect the accrued rights of either party.

3. FEES AND BILLING

3.1 In consideration of Provider providing or granting access to the Services the Client shall pay to Provider thefees set forth in the Order Form in accordance with the payment terms and schedule specified therein.

3.2 If the Order Form do not set forth payment terms or a payment schedule, Client shall prepay Provider, either by valid credit card or through electronic funds transfer (“**EFT**”), the agreed annual subscription charges for the Services within 14 (fourteen) days from the receipt date of the respective invoice (“**Due Date**”). Invoicescan be issued upon signing of the contract for the provision of the Services within the Initial Term and - in the event of renewal - before start of the respective Renewal Term.

3.3 Client shall pay the agreed fees on or before the due date without any deduction. Set off against Provider's claims for the agreed fees shall only be permitted with Client counterclaims that (i) are undisputed, (ii) have been confirmed in binding court decision which cannot be appealed, or (iii) are based on defects of the specificServices for which the respective fee has been agreed.

3.4 If the Client purchases additional services or features ("**Additional Services**") during a subscription period of an already existing Agreement ("**Existing Agreement**"), i) the Subscription Period of the Existing Agreement shall apply to the provision of the Additional Services, ii) the agreed fees for the Additional Services shall be paid upon signing of the agreement about the Additional Services and receipt of the respective invoice, iii) the fees for the Additional Services for the remaining period of the term of the Existing Agreement shall be invoiced and paid *pro rata temporis*, iv) the invoice for the Additional Services' in Renewal Terms shall be issued upfront together with the invoice about the Services purchased by Existing Agreement, i.e. before start of Renewal Terms, and v) all invoices shall be paid within 14 (fourteen) days after invoicing. Upon reaching the start of the next contract period, the parties agree to synchronise the additional services with the already existing ones.

3.5 3.5 The Provider may change the agreed remuneration for the Services with the consent of the Client. The Client's consent to such change shall be deemed to have been given if (i) the Provider notifies the Client of the proposed change in writing or electronically at least thirty (30) days prior to the proposed effective date and (ii) the Client has not exercised its special contractual right of termination within this period, whereby Clause 2.1, sentence 4 shall apply accordingly.

3.6 In the event Provider is unable to successfully charge Client's credit card via EFT, or an invoice is not paid on or before the Due Date of such invoice, Provider reserves the right to suspend Client's access to the Services.Such suspension of access to the Services according to this clause does not terminate the Agreement, does not release the Client from the obligation to pay the fees and shall not entitle the Client to derive any rights or claims against the Provider.

3.7 Any fees more than fourteen (14) days past due are subject to an interest surcharge, calculated at the statutoryrate for late payments.

3.8 Leave or exchange of Users of the Client during the term of the Agreement shall not result in any reduction ofthe Agreed Fees nor shall result in an obligation of Provider to refund paid license fees or any portion thereof unless otherwise expressly agreed between the parties.

3.9 The obligation to pay the agreed fees is independent of the actual use of the Services by Client. The obligationto pay arises and exists with availability of the Services as agreed in the Agreement, regardless of whether andto what extent Client makes use of the available Services. This also applies if the Client is unable to use the available Services because Client ceases to operate the hotel or other facility for which Client originally purchased the Services, or because of a force majeure event such as flood, fire, natural disaster, political unrest, legal or administrative restrictions in the performance territory or in the effect territory, or a pandemic situation.

4. PROVISION OF SERVICES

Provider shall provide the Services to Client with the following specifications

4.1 Provider will provide Client and its Users access to the Services, which shall be password protected for the exclusive use of Users through the Internet. Client may revise its designation of Users upon prior written notice to Provider. Provider reserves the right to automatically update and upgrade the platform in full or partially to which the customer agrees. Provider will advise, inform and instruct the customer comprehensively on any changes which will affect the handling. The 2024 upgrade (CXP) will add to the existing functionality with a new interface being easier to use and will focus on self-service and self-handling, so users can accomplish tasks faster. Improvements will be added in a new organisation onboarding and management (i) providing overviews of all the entities grouped with the customers subscription (ii) introducing segmentation capabilities and (iii) user management for a better data access control used in the other modules is part of the upgrade.

4.2 Where reviews and other information submitted by users on third-party sites ("**External Content**") are subjectof the Services, Provider cannot assure that all relevant reviews, videos, images, blog entries, article postings,references and other information will be found or delivered, or that irrelevant reviews, videos, images, blog entries, article postings, references and other information will not be delivered.

4.3 Provider shall make no effort, and shall not be required hereunder, to substantiate the truthfulness of External Content provided in connection with the Services, or of any other information submitted by users in the contextof Services, and Provider does not endorse, warrant, attest to, or make any judgement about any such information.

4.4 Provider does not guarantee or warrant the uninterrupted availability, functionality and compatibility of Provider's website or Services. From time to time delivery of the Services may be delayed due to scheduled orunscheduled maintenance or factors beyond Provider's control, and Provider's failure to deliver the Services insuch event or events shall not constitute a breach of the Agreement. Provider will try to reduce the resulting down time or unavailability of Services to a minimum and to limit it to times of day with as little use as possible.

4.5 Provider shall not be responsible for disruptions that occur in connection with programs, systems, websites, etc., as well as resulting usage restrictions and other consequences for the Client (including data loss) that arenot part of the Services or which are outside of Provider's reasonable control, e.g. hardware failures or software problems on the part of the Client or disruptions of the data transmission networks, server failures asa result of power failures, or illegal interference by third parties, e.g. hackers, etc. Provider is not responsible for any damages, losses, or damages caused by such disruptions.

4.6 Provider is not responsible for the content, the lawfulness, and the functionality of websites of third parties towhich Provider provides links in connection with the Services. The exclusive liability lies with the providers ofsuch websites.

4.7 In case a force majeure event prevents Provider to provide the Services, Provider is not obligated to performthe Services for the duration of the force majeure event. If such force majeure event continues for more thanthree months, Client is entitled to terminate the Agreement according to clause 2 with Provider.

5. CLIENT OBLIGATIONS

5.1 Client shall provide Provider with the following information prior to start of the Subscription Period: (i) applicablelocation name(s), (ii) location website(s), (iii) the names of three of Client's competitors, and (iv) e-mail addresses of all Users (together the "**Setup Information**"). If Client does not provide the Setup Information in due time this does neither affect the start of the Subscription Period nor the obligation of Client to pay the agreed fees.

5.2 Client acknowledges that with regard to reviews and other content submitted by users on third party sites ("**External Content**"), Provider only aggregates, analyzes and provides, but does not create or generate suchExternal Content underlying the Services, and that information furnished by Provider based on External Content represents the opinions of others and may contain inaccuracies, libelous material, profanity, and pornography and / or may contain other defamatory and illegal content. Provider may block certain comments using specific keywords, and Client will have the ability tocontrol the blocking of key words.

5.3 Client is obliged to keep the access data and passwords secret and not to make them accessible to unauthorized third parties or persons that are not defined as Users. In addition, the Client shall ensure that theUsers entitled under the Agreement also comply with this obligation. If the Client becomes aware of the misuseof access data or a password, the Client will immediately stop the misuse and inform Provider. In case of misuse, Provider is entitled to block access to the Services, if necessary, after prior warning. Client is liable to Provider for any misuse for which Client is responsible.

5.4 Client understands and acknowledges that the Services and the information provided in connection therewith are for Client´s internal review, analysis, and research only, and Client agrees, represents, and warrants to notredistribute such information, in whole or in part, to others, and agrees not to publish or make publicly available(except for publishing or making available on Client´s own website through the Provider´s Marketing Widget), broadcast, or sell any materials received hereunder.

5.5 If the client uses the response AI product, it should be noted that there is no direct response or communication from the Artificial Intelligence to natural persons, as the product only ever suggests an appropriate response or reaction to the client, but the client ultimately decides how to respond to its customer. The Client undertakes to disclose the aforementioned context to its customers and users within the framework of the applicable legal provisions.

5.6 If Client makes use of Provider´s Services to collect reviews from Client´s customers, the Parties agree that such reviews shall be provided independently and uninfluenced. Client shall not solicit reviews from customersby use of means which might reasonably be expected to impair or unduly influence the judgment of the reviewer and therefore the accuracy or veracity of the review. Practices that are deemed likely to so impair or influence a review include, without limitation:

- Compensation payable to the reviewer which is dependent on the content of the review or whichconstitutes an immoderate incentive;
- Exerting pressure on guests to alter or withdraw a review, including through unjustified threat of legalaction;
- Offering incentives for positive reviews, or for changing negative reviews;
- Soliciting or knowingly publishing reviews created by people other than guests, or by insiders or otherparties affiliated with Client; and
- Soliciting reviews only from guests already identified as satisfied or otherwise likely to post a positivereview.

5.7 Client undertakes that its and any User´s access to and use of the Services in accordance with the Specific and these General Terms will comply with all applicable laws, rules and regulations, including but not limited tothose that relate to data protection and electronic communications. Client further warrants that it or any User has all necessary permissions and consents – if necessary – to allow Provider to receive and process Client Content (in particular guest data provided by Client to Provider) and to send communications (e.g. via email orSMS) to individuals on Client's and any User´s behalf. Client is responsible for ensuring that Client and any User meet all information, notice and consent obligations for processing personal information and sending communications to individuals in the jurisdictions where they reside. Client is solely responsible for determining whether the Services are suitable for Client or any User to use in light of any laws and regulations that govern Client or any User, its industry, or its relationship with its customers, including but not limited to consumer protection, privacy, advertising, intellectual property or other laws. Client may not use the Services for any unlawful or discriminatory activities. The Client commissions the provider to process this data and the parties shall conclude a data processing agreement within the meaning of the Data Protection Act prior to the commencement of this Agreement. The client assures that he has received all individual consents for the contractual transfer of this data according to all products of the provider and their individual uses and has complied with all the statutory provisions. Furthermore, the Client confirms that he has obtained the consent of the data processing of the data left by the persons on public or partially public data.

5.8 The Client undertakes, upon request, to provide Provider with copies of documents or acknowledged digital information evidencing compliance with applicable legal requirements, e.g. – where required – consent of the guest i) to be contacted through the used channel, in particular email or direct messaging, for the purpose of Survey Mails or Live Messaging, and ii) to processing of its personal information by the Client and Provider for the purpose of Survey or Messaging. Provider may suspend Survey and Messaging applications temporarily or permanently at any time without prior notice if i) it considers that the Client's undertakings regarding – where required by law – consent collection from or information of the consumer by the Client or any User are not sufficient to guarantee compliance with applicable laws; or ii) if there occur complaints from guests or other third parties questioning the lawfulness of the emails or messages received through Survey or Messaging application or the underlying data processing processes.

5.9 Client undertakes to indemnify, defend, and hold harmless Provider and its employees and agents from and against any and all claims, suits, actions, costs, damages, expenses (including, but not limited to, reasonable legal costs) and losses incurred by any of such parties arising out of or related to or occurring in connection with (i) Client's or any User´s breach of any of its obligations arising out of or in connection with the Agreement, including Client's publication, making publicly available, transmission, delivery, or other use of any information or material contained in the Services or provided or furnished to Client or any User´s pursuant to the Agreement, (ii) Client's and any User´s access to and use of the Services; (iii) any Client Content (as definedbelow); and (iv) Client's or any User´s violation or infringement of any rights of any third party (including intellectual property rights or privacy rights).

Upon written request from Provider, Client shall promptly defend or settle such claim, suit, or action at Client's sole expense through counsel reasonably acceptable to Provider; provided, however, Client may not settle orcompromise any claim without the prior written consent of Provider, which consent shall not be unreasonablywithheld.

In the event Client elects not to defend any claim hereunder, Provider may settle or defend such claim, and shall be entitled to recover from Client the amount of any final settlement or judgment, as well as all costs andfees incurred by Provider in connection with such settlement or defense, including reasonable attorney's fees and expenses.

5.10 The foregoing notwithstanding, nothing herein shall prevent Provider, in its sole discretion, from defending orsettling any such claim, suit or action at its own expense and through its own counsel.

6. INTELLECTUAL PROPERTY RIGHT

6.1 The Provider is and shall remain the sole owner and/or owner of all rights in its trademarks, patents, utility models, designs, copyrights, trade secrets and other intellectual property rights, including all software code, business processes, sales and other data, including all data collected through the Services (collectively, "IP"), developed by, for or on behalf of the Provider, whether existing or hereafter developed, and whether or not relating to the Client, and all derivative works thereof, excluding Client Content, as defined below ("Provider IP").

6.2 The graphic design of the Services, including all page headers, custom graphics, button icons, scripts as well as business designations represent the corporate identity of the Provider and are also subject to the Provider IP. The Provider grants the Client simple, non-exclusive, non-transferable and non-sublicensable rights of use to the Provider IP within the scope of the respective Services, limited in time to the duration of the contractual cooperation and limited in space to the territory of the Client. For the rest, all rights to the Provider IP are and remain with the Provider and may not be copied, imitated or used by the Client, in whole or in part, without the Provider's prior written consent.

6.3 The Client retains all rights to the content that the Client provides to the Provider as part of the Services, including all logos, designs, texts, data, graphics, images, customer lists, message content and other campaign materials of the Client (together " Client Content"). The Client grants the Provider simple but transferable and sub-licensable as well as spatially unrestricted rights of use thereto for the purposes and duration of the contractual cooperation. The granting of rights includes the rights to use, store, reproduce, modify, publish, make publicly available, distribute, translate and display Client Content for the purpose of providing and further developing the Services.

6.4 If the Client acquires its own IP within the scope of the provision of the Services by the Provider, it shall grant the Provider simple, but transferable and sub-licensable as well as spatially unrestricted rights of use for the purposes and duration of the contractual cooperation within the scope of section 6.3.

6.5 The Provider shall only be liable to the Client in respect of the Provider IP for infringement of any third party rights if (i) the Client notifies the Provider promptly of the alleged infringement of which the Client becomes aware; (ii) the Client does not acknowledge any infringement or agree to settle any such claim without the Provider's prior written consent; (iii) the Client permits the Provider (or any relevant third party provider) to conduct and/or settle, at the Provider's expense, any negotiations and litigation arising in connection with the alleged infringement; and (iv) the Client provides the Provider (or any relevant third party provider), at the Provider's expense, with such reasonable assistance as may be required for this purpose.

6.6 The Provider shall not be liable for any claim for infringement of any third-party rights to the extent that such claim arises (i) from the Client's use of the Services in breach of the Agreement; (ii) if the Client fails to take any action directed by the Provider; or (iii) if the claim arises from any interference with or modification of the Services made at the Client's request.

6.7 In addition, the look and feel of the Services, including without limitation, all page headers, custom graphics, button icons and scripts, constitute the trademark or corporate identity of Provider and may not be copied, imitated or used, in whole or in part, without Provider's prior written permission. Nothing contained in the Agreement is intended to convey, or shall be construed to convey, to Client any right, title or interest in or to theServices or the Provider IP, the information gathered or provided in connection therewith, or any of the software underlying the gathering of information in connection with the Services. All right, title and interest in and to the Services and the Provider IP and any information gathered or provided in connection therewith (except for personal data under Client's control) is owned exclusively by Provider.

7. LIMITATIONS OF LIABILITY

7.1 With regard to defects that already exist at the time the Agreement is concluded Provider shall only be liable to the extent that Provider is responsible for such defects (i.e. no strict liability).

7.2 Provider shall only be liable for damage caused by ordinary negligence if such damage is due to a material breach of duty, endangers the achievement of the object of the Agreement, or is due to a failure to comply withduties the very discharge of which is an essential prerequisite for the proper performance of the Agreement.

7.3 In the cases of clause 7.2 above and in the event of damage attributable to gross negligence of an ordinary employee (i.e. not an executive employee or officer) of Provider, Provider's liability shall be limited to damages that are typical and foreseeable for the type of the Agreement.

7.4 In the cases of clause 7.3 above, the liability of Provider shall be limited to a maximum amount of EUR 25,000for each damaging event with a maximum total liability per calendar year of EUR 50,000. Liability for indirect damages, consequential damages and loss of profit shall be fully excluded in the cases of clause 7.3.

7.5 Provider shall be liable for loss of data or programs only to the extent that such loss could not have been prevented by reasonable precautions taken by Client against data loss (including, without limitation, creating at least daily backup copies of all programs and data). Apart from that, any liability of Provider for loss of data shall be subject to the other limitations of this clause 7.

7.6 Except for breaches of contractual guarantees, intentionally caused damages or fraudulently concealed defects or in case of damage to life, body, or health, the limitations of liability stated above shall apply for all claims for damages on whatever legal grounds (including claims in tort).

7.7 The above limitations of liability shall also apply for any claims for damages which Client may assert directlyagainst employees or agents of Provider.

7.8 In the event of liability claims within the meaning of statutory provisions on the use of AI tools or AI-driven technologies (artificial intelligence) used in connection with a Service, the parties agree that the Client shall bear the burden of proof that the relevant Service has a defect with regard to the AI tools or AI-driven technologies contained therein and that this defect has causally led to damage suffered by the Client, even if local statutory provisions provide for a reversal of the burden of proof of the manufacturer, provider or distributor.

8. DATA PROTECTION

8.1 The provision of the Services may require processing of personal data. The Parties will ensure compliance withall applicable data protection laws.

8.2 In particular, if and where Provider, within provision of the Services, processes personal data as processor forClient as controller, the Parties acknowledge that it is the sole responsibility of Client as controller to fulfil Controller´s obligations, in particular to collect – where required by law - necessary consents from data subjects, inform the data subjects about data processing activities, and ensure the data subjects´ rights according to the applicable laws. Provider will assist Client with complying to these obligations as far as required by law. The data processing agreement available at www.trustyou.com/dpa shall apply in this regard, and shall be considered an integral part of the Agreement.

9. CONFIDENTIALITY INFORMATION

9.1 "**Confidential Information**" for purposes of the Agreement is information that (i) has been or is developed or isotherwise owned by either party hereto or any of their respective affiliates, whether developed by such party oran affiliate of such party or by any other person for or on behalf of such party or affiliate of such party, (ii) is notreadily available to the public and not generally ascertainable by proper means by the public, (iii) if disclosed tothe public, would be harmful to the interests of a party or an affiliate of a party, and (iv) is treated or designatedby a party hereto or an affiliate of a party hereto as being confidential.

9.2 Confidential Information shall not include any information that (i) is or becomes publicly available, other than through the fault or negligence of the receiving party; (ii) was known to the receiving party, without restriction, at the time of receipt; (iii) is rightfully and lawfully obtained by the receiving party from a third party rightfully and lawfully possessing the same without restriction; (iv) is independently developed by the receiving party without having had access to the information disclosed hereunder; or (v) is obligated to be produced under an order ofa court of competent jurisdiction, provided that the disclosing party is immediately notified by the recipient.

9.3 Each party hereto agrees that such party will not, directly or indirectly, at any time disclose to any person, or take or use for any purpose, other than for purposes in accordance with the intent of the Agreement, any Confidential Information. The obligations of the parties in this Section apply to, and are intended to prevent, the direct or indirect disclosure of any Confidential Information to any person where such disclosure of the Confidential Information would reasonably be considered to be useful to the competitors of a party or a party'saffiliates or to any other person to become a competitor based, in whole or in part, on such Confidential Information.

9.4 Despite the clause on confidentiality of this contract and the non-disclosure agreement, the Parties hereby agree to define rules for internal and external communication about their products and how to proceed if one or both Parties wish to issue a publication.

9.5 Internal communication means all kind of written or oral communication inside the company structure of each Party, including (but not limited to) the Parties' internal networks, internal e-mail (distribution), in-house reports and presentations as well as internal briefings or meetings.

9.6 Each Party shall be allowed to announce or report about the Agreement internally, accompanied the announcement with the other Party's logo and to report about the technical solutions and economic key points by internal communication in the sense of this Section.

9.7 External communication means all kind of written or oral communication that does not fall under the definition of 9.5. Except to the extent required to comply with applicable law, regulation, rule or legal process or as otherwise permitted in accordance with this Section, neither Party nor such Party's Affiliates or Parent Companies shall make any public announcements, press releases or other public statements without prior consent of the other Party. The consent of the Parties for external communication is granted for:

a.) the use of the other Party's logo (as per the sample sent),

b.) naming the other Party by publishing it on its website on a list naming its partners, suppliers and / or customers,

c.) listing of each Party on the other Party's announcements and website next to logos and names of other partners, suppliers and / or customers, including a link to the other Party's website [as well as Twitter, facebook, LinkedIn and other social media or on an exhibition stands, etc.].

9.8 Despite the other Party's approval to the exact wording, general prior consent is granted for

a) articles, public statements, press releases or case studies, containing a description of

(1) how the customer experience has improved through the TrustYou product,

(2) how the TrustYou products helped to optimize cost,

(3) how the TrustYou products enabled hotel/branch transformation and

(4) how the TrustYou products enhanced security.

b) Articles must not contain any information that the counterparty has expressly identified as strategic or sensitive.

c.) For all other situations where Parties have not granted consent, Parties agree on the following approval process: The Party wishing to publish sends a draft by email to the other Party as soon as possible. The other Party is obliged to confirm or reply with comments and /or change requests highlighted in the text, within 10 calendar days. Failure to reply on time, its silence signifies approval. Based on the amendments of the other Party, the Party wishing to publish can propose a second version which the other Party can comment and improve. If the other Party refuses a third version, the draft shall not be published.

d.) The Parties agree under the same conditions as per c.) on the insertion of the logo of the other Party, a link to the other Party's website as well as on the media and journals in which the article shall be published.

9.9 Each Party is obliged and confirms that it has implemented effective internal measures that guarantee the compliance of its employees with the agreed limitation of communication. Any infringement to the above rules results in the right for one Party to claim a fine of EUR 15,000 per violation if the approval was expressly denied.

10. MISCELLANEOUS

10.1 Provider can assign the Agreement (including all its rights and obligations hereunder) to Provider's affiliated companies according to § 15 German Stock Corporation Act by providing Written Notice of such assignment toClient; assignments to any other third parties require the prior written consent of Client (which shall not be unreasonably withheld or delayed). Client may assign the Agreement only with prior written consent of Provider(which shall not be unreasonably withheld or delayed). If at any time during the contractual period a third party performs the contractual payment obligations of the customer, the customer shall be obliged to notify this in writing prior to receipt of payment and to provide the explanations pursuant to Clause 1.8 without being requested to do so.

10.2 In case that any provision in the Agreement is invalid or becomes invalid, the remaining provisions remain unaffected hereby. The parties undertake to replace any invalid provision in the Order Form by a valid provision that comes as close as possible to the invalid provision in legal, economic and factual terms. Thesame applies in case of a lacuna in the Order Form.

10.3 The place of contractual fulfillment is Munich, Germany. The Agreement and any provision of Services underthe Agreement is governed by and is to be construed in accordance with German Law (excluding any references to other jurisdictions and excluding the UN Convention on Contracts for the International Sale of Goods). For any disputes under or in connection with the Agreement the Parties submit to the non-exclusive jurisdiction of the courts in Munich, Germany.

10.4 Provider can modify the terms and conditions of the Agreement with Client's consent. The Client's consent to such change shall be deemed to have been given if (i) the Provider notifies the Client of the proposed change in writing or electronically at least thirty (30) days prior to the proposed effective date and (ii) the Client has not exercised its special contractual right of termination within this period, whereby Clause 2.1, sentence 4 shall apply accordingly.

10.5 Changes and amendments to the Agreement need to be made in writing, i.e. through a document signed personally or through advanced electronic signature (pursuant to the European eIDAS Regulation No 910/2014) by authorized representatives of the parties and provided to the other party as original form, telefax or PDF copy as email attachment. This also applies to a change of this written form requirement.

10.6 The Agreement, consisting of any Order Form and these General Terms, constitute the entire agreement between the Parties with respect to the delivery of Services, and the information provided in connection therewith, and supersedes all prior or contemporaneous agreements, proposals, negotiations, representationsor communications, whether written or oral, relating to such subject matter. The Parties acknowledge and agree that they have not been induced to enter into the Agreement by any representations or promises not specifically stated herein.

10.7 Should a contradiction arise between contractual documents, it is formally agreed that the provisions contained in the document of a higher rank shall supersede. The following document hierarchy shall apply by decreasingorder of priority: 1. Order Form including all appendices and any addendum, 2. General Terms.

Data Processing Agreement

between

Client (as determined in subscription agreement about use of TrustYou services)

(hereinafter referred to as the "Principal")

and

TrustYou
(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".

Whereas 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 TrustYou's General Terms and Conditions that are substantial part of the subscription agreement.

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 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).

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 the Principal, provided they are obviously 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 writing or 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 well as 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, authorized 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: Email address, First name and surname, Language, Address, Nationality, Entry date, date of departure, Revenue, Type of room, Number of people, Purchased products

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 Customer in fulfilling the rights of the persons concerned.

Appendix 2

Agent´s Subcontractors

Name	Country	Address	Activity	Basis
Hetzner Online GmbH	Germany	Industriestr. 25, 91710 Gunzenhausen, Germany	Webhosting and mailings, corporate infrastructure and CXP services	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	KDX Toranomon 1 Chome Building - WeWork 1-10-5 Toranomon Minato-Ku, Tokyo, 105-0001 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)
Microsoft Azure	The Netherlands	Evert van de Beekstraat 354, 1118 CZ Luchthaven Schiphol, Noord-Holland, Netherlands	Webhosting and mailings for CDP services only	Data Processing Agreement (DPA)
Akamai Technologies Inc.	USA	145 Broadway, Cambridge MA,02142, USA	Content Delivery Network, App & API Protector	Via Data Processing Agreement and contract with GlobalDots DE GmbH Akamai being the subcontractor of GlobalDots DE GmbH
GlobalDots DE GmbH	Germany	Urbanstraße 116, 10967 Berlin, Germany	Content Delivery Network, App & API Protector	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 usepersonal data:

<u>The Agent's office</u>

- The business premises of the Agent are protected against unauthorized access by means ofan 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 premiseswhen 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.

<u>Data warehouse</u>

- A provider with a certified information security management system in accordance withISO/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 organizational 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.