SaaS Terms and Conditions

Version: May 30, 2024

1. Subject matter and structure of the contract

1.1 The subject matter of these SaaS Terms and Conditions is the provision of the software solution (the "**Service**") designated in the order form or document (the "**Order Form"**) for use by the Customer and third parties authorized by the Customer for this purpose ("**End Customers**") via the internet in return for payment. To the extent agreed upon in the Order Form, the subject matter of the Agreement also includes the provision of agreed upon support services by Valuecase in accordance with sec. 10. Any additional services are not included in the subject matter of the Contract.

1.2 The Order Form, these SaaS Terms and Conditions and the Annexes incorporated herein are hereinafter collectively referred to as the "**SaaS Contract**". The order of precedence shall be in descending order (1) the Order Form, (2) these SaaS Contract Terms and Conditions, (3) the Annexes incorporated herein; sec. 16.1 remains unaffected.

1.3 The SaaS Contract also applies to changes to the Service made by Valuecase during the term of the SaaS Contract, such as patches, updates, upgrades or other changes to the Service (collectively, "**Updates**").

1.4 The Customer's general terms and conditions of business will not apply unless Valuecase expressly agrees to their validity in writing or text form.

1.5 The SaaS Contract is not a contract for the benefit of third parties. In particular, End Customers cannot demand any services from Valuecase based on the SaaS Contract.

2. Operation and provision of the service

2.1 Valuecase will make the Service available to the Customer within the scope of the agreed availability (cf. sec. 4.1) for access and use via the internet. The Service will be accessed using a common browser in accordance with the minimum technical requirements communicated by Valuecase.

2.2 Valuecase grants the Customer the ability to use the Service by either providing Valuecase with a user name and password (collectively, "**Access Data**") or by allowing the Customer to set up Access Data itself.

2.3 Customer shall establish Access Data solely for use of the Service by its authorized personnel or End Customers authorized by Customer (collectively, "**Authorized Users**") and shall disclose such Access Data only to such **Authorized Users.**

2.4 If the parties have agreed on a maximum number of Users, the Customer shall authorize a maximum of this number of Authorized Users to use the Service and set up corresponding accounts and Access Data. The account and the associated Access Data are individually bound to the respective Authorized User and are not transferable. The Customer may, however, at any time permanently withdraw the authorization to use the Service from an Authorized User and grant the authorization to another person instead, who shall thereby take the place of this Authorized User. In case the Customer exceeds the agreed number of users, sec. 5.5 applies.

2.5 The Customer agrees to and shall take appropriate measures to ensure that

a) only Authorized Users have accounts, Access Data and access to the Service;

b) accounts and Access Data are not set up or used for groups of people or as role accounts; and

c) accounts and Access Data of an Authorized User are not used by other persons, including other Authorized Users.

2.6 The Customer shall adequately protect Access Data against access by unauthorized persons and shall inform each Authorized User in advance of the confidential treatment of the Access Data and compliance with the usage authorizations and restrictions pursuant to sec. 5 and to monitor them appropriately.

2.7 Any use of the Access Data and the Service, including use in violation of the contract and otherwise unauthorized use, is deemed to be use on behalf of the Customer in relation to Valuecase, unless the Customer is not responsible for the unauthorized use.

2.8 If the Customer becomes aware of unauthorized access to Access Data or the Service, or of a violation of sec. 2.4, the Customer will immediately inform Valuecase in text or written form and change the Access Data concerned or have it changed.

2.9 If Valuecase has reason to suspect that Access Data is being misused or used in violation of the contract, Valuecase may block and replace such Access Data. In doing so, Valuecase will give due consideration to the legitimate interests of the customer. This does not affect Valuecase's rights to refuse performance.

3. Nature of the Service

3.1 The Service contains functions to support the Customer in communicating and exchanging data with its End Customers. Valuecase provides the Service in order to enable the Customer, within the scope of the existing functions of the Service, to create individual web pages ("Spaces") for its End Customers and to personalize these by means of various contents. The description of the Service is described in Annex 1 (Description of the Service).

3.2 The Customer is aware of and agrees that the contractual use of the Service requires compliance with the current minimum technical requirements communicated by Valuecase from time to time and a sufficiently dimensioned Internet connection.

3.3 Valuecase may update the Service at any time, even without the separate consent of the Customer, and otherwise make reasonable changes, in particular to adapt it to a changed legal situation, technical developments or to improve IT security. In doing so, Valuecase will give due consideration to the legitimate interests of the Customer.

4. Service availability

4.1 If the minimum technical requirements communicated by Valuecase in each case are met, Valuecase warrants the availability of the Service at the Internet transfer point of the data center in which the respective server is located as agreed in the Annex 2 (Service Level).

4.2 In the event of a not merely insignificant interruption of the agreed availability, the Customer will immediately inform Valuecase in text or written form.

5. Authorizations and restrictions of use

5.1 Valuecase permits the Customer to access the Service via the internet during the Contract Term within the scope of the agreed number of users and to use the functions of the Service as intended.

5.2 The Customer may, in its own name and for its own account, allow End Customers to access the Service themselves via the Internet free of charge and to use the functions of the Service intended for End Customers.

5.3 The Customer is not permitted by Valuecase to use the Service beyond the scope of sec. 5.1 and 5.2. In particular, neither the Customer nor the End Customers are authorized,

a) to reproduce, distribute or make publicly available the Service or parts thereof, except to the extent necessary for their contractual use;

b) to remove, obscure or alter copyright notices and similar information;

c) to grant unauthorized third parties access to the Service or its functions or to tolerate such access. Unauthorized is any third party who is not an Authorized User;

d) to rent out or otherwise make available the Service in whole or in part (under) for a fee.

e) to copy, load or disclose any software used to operate or provide the Service, or any software underlying the Service, in whole or in part, onto its own systems;

f) to access the Service in any other way than by using the Access Data;

g) to take, encourage or tolerate any action that interferes with or damages the Service, or that temporarily or permanently impairs or prevents its use by other customers.

The Customer's mandatory statutory rights shall remain unaffected.

5.4 The Customer will inform Valuecase immediately in text or written form if it becomes aware of a violation of this sec. 5 becomes known.

5.5 If the Customer grants the opportunity to use the Service to a number of persons exceeding the agreed number of users during the same period of time, the Customer is obligated to pay Valuecase the agreed usage fee per user for each person with the opportunity to access the Service exceeding the agreed number of users, unless the Customer is not responsible for this. All other claims and rights of Valuecase remain unaffected.

6. Cooperation obligations and responsibilities of the Customer

6.1 The Customer shall designate a contact person and a deputy for the execution of the SaaS Contract. Valuecase must be notified in advance of any change of contact person or deputy at least in text form via the contact address provided.

6.2 Information reasonably requested by Valuecase from the sphere of the Customer for the performance of the SaaS Contract will be provided by the Customer in full and within a reasonable period of time. This also includes information requested by Valuecase for onboarding purposes.

6.3 The Customer is solely responsible for meeting the minimum technical requirements communicated by Valuecase as well as for the functionality and sufficient dimensioning of the Internet connection to access the Service. The Customer is solely responsible for the security of its systems and their protection against malware and attacks.

6.4 The Customer shall use the Service only within the contractually permissible scope and comply with all legal and regulatory requirements applicable to it. The Customer will oblige Authorized Users accordingly and control them appropriately.

6.5 Customer will thoroughly test the Service for freedom from defects and usability as well as suitability for its purposes before using the Service with real data or otherwise putting it into operation for operational purposes. Customer will take reasonable and appropriate precautions on an ongoing basis to prevent and reduce the potential effects of malfunctions or defects in the Service.

7. Customer Content

7.1 In relation to Valuecase, the Customer is solely responsible for the completeness and accuracy of the information, logos and other content provided by the Customer or by End Customers in the course of Onboarding and entered, uploaded or otherwise stored when using the Service (collectively, "**Customer Content**").

7.2 By entering, uploading or otherwise providing Customer Content, the Customer grants Valuecase a non-exclusive, irrevocable, worldwide right to use the Customer Content for the fulfillment and execution of the SaaS Contract, in particular to reproduce and process it and to display it to the Customer and its End Customers as part of the Service, until the SaaS Contract has been fully executed. Valuecase may have this right exercised by third parties on its behalf, for example, by any vicarious agents used (e.g., hosting service providers). To the extent that the Customer cannot grant this right to Customer Content itself (e.g., to data of End Customers), it will provide Valuecase with this right.

7.3 The Customer must ensure and warrants that Customer Content and its input or processing does not violate any third-party rights, does not violate any laws, and does not contain or spread any viruses or other malware such as worms or spyware. The Customer assumes sole and unlimited liability towards those who claim an infringement of rights in connection with Customer Content against Valuecase or its vicarious agents. All other rights and claims of Valuecase remain unaffected.

7.4 The Customer is aware that Valuecase as well as technical service providers used by Valuecase may have the opportunity to gain knowledge of Customer Content, in particular in connection with the maintenance of the systems used to operate the service. The regulations on confidentiality pursuant to sec. 15.

8. Defects of quality and title

8.1 Valuecase warrants that the Service will be provided in accordance with the SaaS Contract and without any defects in material (cf. sec. 3.1 and Annex 1) and without defects of title. The agreed availability is subject to sec. 4.1 and Annex 2.

8.2 Valuecase will remedy any defects of the Service within a reasonable period of time after proper notification of the defect by the Customer. The defect may also be remedied by means of an Update.

8.3 To the extent that the Customer is wholly or partially deprived of the contractual use of the Service due to a defect in title, Valuecase may, at its own discretion, also remedy such defect by

a) providing the Customer with the necessary rights to use the Service in accordance with the SaaS Contract; or

b) modifying the Service in such a way that the right of the third party no longer prevents the Customer from using the Service in accordance with the SaaS Contract.

Valuecase will give due consideration to legitimate interests of the Customer in this regard.

8.4 In all other respects, §§ 535 ff. BGB apply with the proviso that the strict liability for defects existing at the time of conclusion of the contract pursuant to § 536a para. 1, 1st alternative BGB is excluded.

8.5 If the Customer asserts a defect although there is actually no defect, the Customer will reimburse Valuecase for any expenses and costs incurred as a result, unless it was not apparent to the Customer with due diligence that there was no defect.

9. Third party rights

9.1 If a third party asserts an infringement of rights against the Customer through the Service, the Customer will immediately notify Valuecase thereof in text or written form.

9.2 Valuecase will adequately support the Customer in its defense and provide relevant information. Valuecase's obligation to remedy defects in accordance with sec. 8 shall remain unaffected.

10. Implementation and application support

10.1 To the extent agreed in the Order Form, Valuecase will provide services to support the Customer in the onboarding and use of the Service ("**Support Services**"). Support Services are subject to the provisions of this sec. 10.

10.2 Support Services may include, in particular, services for the instruction and training of Authorized Users, application support via e-mail or other communication channels set up for this purpose, and consulting services by Valuecase to support the Customer in setting up Spaces.

If the parties have agreed on support for the use of the Service, the Customer may contact Valuecase with questions regarding the use of the Service to a reasonable extent via the communication channels provided by Valuecase for this purpose. Valuecase will provide for the support request to be addressed during Valuecase's business hours in the ordinary course of business and will use reasonable efforts to respond to the support request within a reasonable period of time.

10.3 If training sessions or other training courses by Valuecase are agreed upon, the Customer is solely responsible for ensuring that the participants attend the respective training course on the day agreed upon for this purpose at the time agreed upon. Valuecase is not obligated to offer another training session if participants do not attend a training session.

10.4 To the extent that intellectual property rights arise in the performance of Support Services, Valuecase grants the Customer a non-exclusive, non-transferable and non-sublicensable right to the work product in question to use the work product in connection with the functions of the Service during Contract Term.

10.5 Valuecase provides Support Services with the due diligence of a prudent businessman. Valuecase is not obligated to achieve or provide certain results or a certain success.

11. Remuneration and terms of payment (unless otherwise agreed in the Order Form)

11.1 The Customer is obliged to pay the agreed usage fee (per user) for the number of users agreed in the Order Form. In case the Customer exceeds the agreed number of users at any given time during Contract Term (as defined in the Order Form), the Customer is obliged to pay additional usage fees for the remainder of the Contract Term (as defined in the Order Form) with respect to the exceeding number of users in accordance with sec. 5.5.

11.2 Valuecase's claim to payment of the usage fee for the Service arises in advance at the beginning of each Contract Term. Agreed Support Services are settled with payment of the usage fee. In case the Customer exceeds the agreed number of users, the claim for payment arises with the end of the day (23:59 Central European Time) in which the agreed number of users has been exceeded.

11.3 Payment claims of Valuecase are due for payment on the day of invoicing. Due claims are to be paid by the Customer to Valuecase within fourteen (14) days from the due date in EUR.

11.4 All prices are subject to statutory value added tax.

12. Limitation of liability

12.1 Valuecase is liable without limitation in cases of intent, gross negligence, and culpable injury to life, limb, or health.

12.2 In the event of slight negligence, Valuecase is only liable in the event of a breach of essential contractual obligations, i.e. obligations the fulfillment of which is a prerequisite for the proper execution of the contract or the breach of which jeopardizes the achievement of the purpose of the contract and on the fulfillment of which the Customer may regularly rely. In these cases, Valuecase's liability is limited to damages that are foreseeable at the time of the conclusion of the contract and are typical for the contract. The unlimited liability according to sec. 12.1 remains unaffected by this.

12.3 Beyond sec. 12.1 and sec. 12.2 Valuecase is not liable for slight negligence.

12.4 The above limitations of liability shall not apply to liability under the Product Liability Act or within the scope of guarantees assumed in writing.

12.5 Sec. 12 also applies in favor of Valuecase's employees, representatives, bodies and vicarious agents.

13. Contract Term and termination

13.1 The SaaS Contract shall become effective on the date specified in the Order Form and shall terminate upon notice in accordance with the following provisions (the "**Contract Term**").

13.2 Unless otherwise agreed in the Order Form, either party may terminate the SaaS Contract with one (1) month notice to the end of the minimum contract term of twelve (12) full calendar months and to the end of each subsequent time interval of twelve (12) full calendar months (the **"Renewal"**). Any calculation of fees for Renewals will be based on fees excluding discounts and the larger of the following two numbers:

- the number of users agreed in the Order Form
- the number of users the Customer has registered with the Service at the time of Renewal

13.3 The right to extraordinary termination remains unaffected. For Valuecase, an extraordinary reason for termination also exists if

a) the Customer repeatedly uses the Service in excess of the usage authorization or violates agreed usage restrictions pursuant to sec. 5;

b) the Customer grants End Customers unauthorized third party access to the Service;

c) Valuecase fails to remedy a defect of title within a reasonable period of time despite reasonable efforts.

13.4 Any termination must be in text form to be effective.

14. Feedback and usage data

14.1 The Customer may communicate impressions, errors, discrepancies, suggestions and otherwise proposals for improvement (collectively "**Feedback**") to Valuecase. In doing so, the Customer shall ensure that the Feedback does not contain any personal data and is free of third party rights.

14.2 By submitting the Feedback, the Customer provides Valuecase with the free, irrevocable, permanent right, unrestricted in terms of content and location, to analyze and evaluate the Feedback and to use it for modifications, improvements and further developments of the Service. This includes, in particular, the right to reproduce the feedback without restriction as to content, to edit it, to link it to further information, to pass it on to third parties permanently or temporarily, and to implement it in any form.

14.3 During the use of the Service by the Customer, Valuecase also collects information on the type of use (such as frequency and scope of use as well as user interactions), system data (such as system log data on incompatibilities or malfunctions) as well as system environment data (such as browser used, operating system and screen resolution) (collectively "**Usage Data**").

14.4 The use of the Usage Data is at the sole discretion of Valuecase. In particular, Valuecase may use Usage Data as well as findings obtained from the analysis of Usage Data to identify and eliminate bugs and other errors, to improve usability and user guidance, and otherwise to improve and further develop the Service.

15. Confidentiality

15.1 "**Confidential Information**" means all information disclosed or otherwise coming to the knowledge of one party ("**Information Recipient"),** both before and after the conclusion of the SaaS Contract, by the other party ("Information Provider"), which has been marked as confidential by the Information Provider or is obviously to be considered confidential, in particular any trade and business secrets, know-how, inventions, business relationships, business strategies, business plans, financial accounting data and processes as well as comparable secret information, including copies or excerpts thereof. The Service and its features are considered Confidential Information of Valuecase.

Information shall not be deemed Confidential Information if and to the extent that it (i) is publicly known or accessible and such knowledge or accessibility is not the result of an improper or unlawful act by Information Recipient (or an affiliate, agent, consultant or employee), (ii) was in the possession of the Information Recipient or known to the Information Recipient prior to receipt in connection with the collaboration, unless such information was unlawfully appropriated, (iii) was lawfully provided to the Information Recipient by a third party, (iv) was obtained by the Information Recipient through independent creation or discovery, or (v) in the cases of Section 5 GeschGehG. Furthermore, Feedback and Usage Data do not count as Confidential Information of the Customer; in this respect, sec. 14 applies.

15.2 The Parties undertake to (i) treat all Confidential Information of the Information Provider disclosed during the collaboration as strictly confidential and to protect it by appropriate security measures, (ii) to use it exclusively for production for the purpose of the collaboration and (iii) to disclose it only to such third parties (affiliates, agents, consultants or employees) who need the Confidential Information for the aforementioned purposes and are similarly bound to secrecy, unless there is a mandatory duty of disclosure by law or on the basis of a court or regulatory decision, in which case the Information Recipient shall use its best efforts to limit the disclosure to the extent possible and shall inform the Information Provider of any impending or effected disclosure to the extent permitted by law respectively by authority decision, in which case the Information Recipient shall use its best efforts to limit disclosure to the extent possible and shall notify the Information Provider of any impending or completed disclosure to the extent permitted by law.

15.3 At the end of the Contract Term, the Information Recipient shall release to the Information Provider, destroy or delete the Confidential Information received and confirm this to the Information Provider in writing, unless the Receiving Party is required by law to retain the respective information.

15.4 The obligations arising from this sec. 15 shall continue to apply for a further five (5) years after the end of the Contract Term.

16. Privacy

16.1 Insofar as Valuecase processes personal data on behalf of the Customer within the scope of the provision of services, this shall be done in accordance with the Data Processing Agreement in Annex 3. The Data Processing Agreement shall always have priority in its scope of application.

16.2 In the relationship with Valuecase, the Customer bears sole responsibility for the permissibility of the processing of personal data and the fulfillment of the requirements of applicable data protection law, in particular the proper information of data subjects (Art. 12 et seq. GDPR).

16.3 The Customer shall fully indemnify Valuecase against all claims and official measures and sanctions in connection with the processing of personal data, except to the extent that Valuecase is solely responsible for the unauthorized processing and has carried out such processing contrary to the Customer's instructions. The Customer's liability includes the reimbursement of reasonable legal defense costs. All other claims and rights of Valuecase remain unaffected.

17. Customer name and logo

17.1 Unless expressly agreed otherwise in the Order Form, Valuecase may use the Customer's name and logo on websites, on social media platforms, in press releases and for other marketing materials, including as a customer reference. Design specifications provided by the Customer to Valuecase for this purpose will be given due consideration by Valuecase.

17.2 The Customer may revoke the above permission in text or written form. Marketing activities prior to receipt of the revocation remain unaffected. In particular, Valuecase is not obligated to recall or destroy marketing materials that have already been published.

18. Free Trial Phase

18.1 If the parties have agreed on a free trial phase for the Service ("**Free Trial Phase**"), the provisions of this sec. 18 shall take precedence over the other provisions of these SaaS Terms and Conditions in the event of contradictions during the Free Trial Phase.

18.2 During the Free Trial Phase, Valuecase will provide the Service to the Customer free of charge. The Customer is aware and agrees that during the Free Trial Phase the Service may not be available, may be available only in a limited manner, may be available with significant interruptions and/or may be defective.

18.3 Valuecase does not promise availability of the Service during the Free Trial Period. Sec. 4 and Annex 2 shall not apply.

18.4 During the Free Trial Phase, Valuecase is liable in accordance with the provisions of the law governing loan agreements (§§ 598 et seq. BGB). Sec. 8, 9 and 12 do not apply beyond this.

18.5 The Free Trial Phase shall end automatically upon expiry of the agreed duration of the Free Trial Phase. Unless otherwise agreed by the parties and subject to termination of the SaaS Contract pursuant to sec. 18.6, the SaaS Contract shall remain unaffected thereby. In particular, the Customer shall be obligated to pay the agreed remuneration for the Service from this point in time.

18.6 During the Free Trial Phase, either party may terminate the SaaS Contract without prior notice.

19. Applicable law and place of jurisdiction

19.1 The SaaS Contract and all claims and rights arising therefrom or otherwise in connection therewith shall be governed by the laws of the Federal Republic of Germany. The UN Convention on Contracts for the International Sale of Goods (CISG) is excluded.

19.2 The exclusive place of jurisdiction for all disputes between the parties arising from or in connection with the SaaS Contract shall be Hamburg.

20. Final provisions

20.1 The SaaS Contract contains the final regulation of all rights and obligations of the Parties with respect to its subject matter. It replaces any previous agreements concerning the subject matter. There are no ancillary agreements upon conclusion of the contract.

20.2 Unless otherwise agreed, amendments and supplements to this SaaS Contract must be made in text or written form. This shall also apply to any waiver of this formal requirement. Sec. 3.3 remains unaffected.

20.3 The Customer may only offset claims against Valuecase arising from this SaaS Contract that are undisputed, legally established or ready for decision, and may only exercise a right of retention on the basis of such claims.

20.4 The parties may assign or transfer claims or rights under the SaaS Contract only with the consent of the other party. Section 354a HGB remains unaffected.

20.5 Should individual provisions of the SaaS Contract be invalid or unenforceable, this shall not affect the validity of the remaining provisions. The parties shall replace such provisions by effective and feasible provisions, which correspond as closely as possible to the meaning and economic purpose as well as the intention of the parties. The same shall apply to unintended loopholes.

Attachments

Annex 1 - Description of the Service
Annex 2 - Service Level Agreement (Availability)
Annex 3 - Data Processing Agreement

Annex 1 - Description of the service

The Service operates as set forth below:

Upon entering into a contract for the use of the service offered by Valuecase (the "Service"), incorporating the SaaS Contract Terms, Customer will be granted access to a personal Admin Area for the Service.

The Customer may invite additional Authorized Users to this admin area within the agreed number of users. Each of these users can create a personal profile (in particular, profile picture and contact data). Furthermore, users have the option to permanently connect their Valuecase account with their CRM to enable automatic data exchange (currently HubSpot is supported).

Templates can be created in the account in advance of the end customer contact. A template is a reusable template of a Space that can be freely designed by customers within the scope of the existing functions of the service. Each Space consists of one or more pages, which in turn consist of several blocks. The blocks can be filled with different content (e.g., text, images, videos, and documents).

In addition, the service offers the possibility of using interactive blocks, where the end customers can also enter or change information. This includes the ability to include their own business case. Furthermore, customers can add a task management module with which the customer and end customer can plan and track their sales process. Finally, external content can be displayed in a block via HTML embed.

From a template, customers can create individualized spaces for end customers. These can be customized by the customer at any time. Basically, the created Spaces are personalized with the profile and contact data of the creating user as well as the data of the end customer. The creation can be done from the Service as well as from a connected CRM (after prior authentication; currently HubSpot is supported).

A created Space is made available to the end customer by the customer via Internet link; a general password is not required, but individual pages can be protected with a password chosen by the customer. The customer has access to an anonymized overview of the actions performed on a Space (e.g., creation of a new task in the task management module).

The described functions of the Service are available to the Customer as Software-as-a-Service within the scope of the agreed availability for access and use via the Customer's Internet connection by means of a common browser. The Service does not include the provision of software code to the Customer or the installation of software on the Customer's premises.

Annex 2 - Service Level Agreement

1. Service availability

Valuecase warrants an average monthly availability of the service of at least **99,0 %** during the contract year. If the Contract Term ends prematurely during a contract year, the averaged availability will be calculated pro rata.

2. Routine maintenance

Routine maintenance will be performed on Saturdays between 09:00 and 24:00 (CET). Scheduled maintenance work outside this time window affecting the availability of the Service will generally be notified to Customer by Valuecase five (5) business days in advance.

3. Availability calculation

Interruptions in the time window for routine maintenance work, interruptions outside of the Service's operating hours (Monday through Sunday with the exception of public holidays in Hamburg as well as December 24th and 31st), and interruptions due to circumstances beyond Valuecase's direct control will not be taken into account when calculating (non-) availability.

Annex 3 – Data Processing Agreement

Data Processing Agreement

according to Art. 28 GDPR ("DPA")

as an annex to the contract

Preamble
This DPA specifies the obligations of the contracting parties regarding data protection arising from the contract ("**SaaS Contract**").
It applies to all activities related to the SaaS Contract in which employees of the Contractor or persons authorized by the Contractor may come into contact with personal data ("**pD**") of the customer.
In the following, Valuecase is referred to as the "Contractor" and the customer as the "Client".

1. Subject, duration and specification of the DPA

1.1 The subject matter of the DPA is essentially that the Contractor provides the sales software "**Valuecase"** to the Client as a SaaS solution (the "Service"). Details are set forth in the SaaS Contract. In order for the Client to be able to use this SaaS solution, it is necessary for the Contractor to process pD of the Client (or its customers) within the meaning of Art. 28 GDPR. The subject of this DPA is the associated data processing.

1.2 Contractor shall enable Client through the Service to process pD for the following purposes:

Support the Client's sales and other processes by providing a web-based application that the Client's sales and other staff use to provide information to employees and other authorized parties of potential business Clients (B2B) during the sales, onboarding, customer success and potentially other processes.

1.3 The processing includes the types of data mentioned below:

- E-mail address
- First and last name
- Job Title
- Work phone number
- Any type of (personal) data that the Client or persons authorized by the Client, at their own discretion, upload to Valuecase or store via text entry.

1.4 The following categories of persons are concerned by the processing:

- Employees and other authorized persons of companies who interact with sales employees of the Client as part of a sales process,
- Employees of customers of the Client,
- Employees of the Client.

1.5 The term of this DPA shall be in accordance with the term of the SaaS Contract, unless the provisions of this Agreement impose obligations beyond the term of the SaaS Contract.

2. Scope and responsibility

2.1 The Contractor shall process pD on behalf of the Client (cf. Section 1). With regard to the processing of the pD, the Client is responsible for compliance with the statutory provisions on data protection, in particular for the lawfulness of the data processing.

2.2 The instructions shall initially be determined by the present DPA and may thereafter be amended, supplemented or replaced by individual instructions ("**Individual Instructions**") by the Client in writing or in text form to the office designated by the Contractor. Instructions that go beyond the contractually agreed performance shall be treated as a request for a change in performance.

3. Duties of the Contractor

3.1 The Contractor may only process pD of data subjects within the scope of the DPA and the documented instructions of the Client. If the Contractor is obligated by national or European law to process data in a manner that deviates from this, it shall - insofar as this is legally permissible - inform the Client of this circumstance prior to the start of the processing.

3.2 The Contractor shall organize the internal organization within its area of responsibility in such a way that it meets the special requirements of data protection. It shall take the technical and/or organizational measures described in the **Annex 1** to adequately protect the Client's pD. The measures shall ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing on a permanent basis.

3.3 The Contractor reserves the right to change the technical and/or organizational measures taken, but it must be ensured that the contractually agreed level of protection is not undercut. The Contractor informs the Client of such a change by email.

3.4 The Contractor shall support the Client within the scope of its possibilities and the contractually owed performance in fulfilling the requests and claims of data subjects pursuant to Chapter III of the GDPR as well as in complying with the obligations set forth in Art. 33 to 36 of the GDPR.

3.5 The Contractor warrants that the employees involved in the processing of the Client's pD and other persons working for the Contractor are prohibited from processing the respective pD outside the Client's instructions. Furthermore, the Contractor warrants that the persons authorized to process the pD have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality. The confidentiality and non-disclosure obligation shall continue to exist after termination of the order processing agreement.

3.6 The Contractor shall inform the Client without delay if it becomes aware of any violations of the Client's pD protection. The Contractor shall take the necessary measures to secure the pD and to mitigate any possible adverse consequences of the persons concerned and shall consult with the Client on this without delay.

3.7 The Contractor shall inform the Client of the contact person for data protection issues arising within the scope of the DPA.

3.8 The Contractor warrants to comply with its obligations under Article 32(1)(d) of the GDPR and to implement a procedure for the regular review of the effectiveness of the technical and organizational measures to ensure the security of the Processing.

3.9 The Contractor shall correct or delete the pD that are the subject of the contract if the Client instructs it to do so and this is covered by the scope of instructions. If a deletion in compliance with data protection or a corresponding restriction of data processing is not possible, the Contractor shall undertake the destruction of data carriers and other materials in compliance with data protection on the basis of an individual order by the Client, unless already agreed in the contract.

3.10 The Contractor confirms that it is aware of the data protection regulations of the GDPR relevant to the commissioned processing.

3.11 Data, data carriers as well as all other materials shall be either surrendered or deleted upon the Client's request after the end of the DPA.

4. Obligations of the Client

4.1 The Client shall inform the Contractor immediately and in full if it discovers errors or irregularities in the results of the order with regard to data protection regulations.

4.2 In the event of a claim by a data subject with regard to any claims pursuant to Art. 82 GDPR, the Client and the Contractor undertake to support each other with regard to the verification of the active legitimacy in the defense against the claim.

4.3 The Client shall name the Contractor the contact person for data protection issues arising within the scope of the agreement.

5. Requests from affected parties

If a data subject approaches the Contractor with requests for correction, deletion or information, the Contractor will refer the data subject to the Client, provided that an assignment to the Client is possible according to the data subject's information.

6. Detection options

6.1 The Contractor shall provide the Client with evidence of compliance with the obligations set forth in Art. 28 GDPR and this DPA by appropriate means. To prove compliance with the agreed obligations, the Contractor may in particular provide the Client with certificates and test results of third parties (e.g. in accordance with Art. 42 GDPR or ISO 27001) or test reports of the company data protection officer.

6.2 If, in individual cases, inspections by the Client or an auditor commissioned by the Client are necessary, these shall be carried out during normal business hours without disrupting operations after notification, taking into account a reasonable lead time. The Contractor may make such inspections conditional upon the signing of an appropriate confidentiality agreement. Should the auditor commissioned by the Client be in a competitive relationship with the Contractor, the Contractor shall have a right of objection against him.

6.3 Should a data protection supervisory authority or any other sovereign supervisory authority of the Client carry out an inspection, Section 6.2 shall apply accordingly in principle. It shall not be necessary to sign a confidentiality agreement if this supervisory authority is subject to professional or statutory confidentiality where a violation is punishable under the German Criminal Code (StGB).

6.4 The Contractor may demand reasonable remuneration for support in the performance of an inspection pursuant to Sections 6.2 or 6.3, unless the inspection was prompted by the urgent suspicion of a data protection incident in the Contractor's area of responsibility. In this case, the suspicious facts shall be presented by the Client with the announcement of the inspection.

7. Subcontractors (other processors)

7.1 The Client agrees that the Contractor may use subcontractors. These may also process personal data in a third country. Prior to the involvement or replacement of subcontractors, the Contractor shall inform the Client in text form with a notice period of four weeks. The Client may object to the change only for good cause. The objection must be made within 14 days and all important reasons must be expressly stated. If no objection is made within this period, the change shall be deemed to have been approved. If there is an important reason which cannot be eliminated by the Contractor by adjusting the order, the Contractor shall have a special right of termination. This special right of termination shall apply both to this DPA and to the SaaS Contract. No separate information shall be provided about the subcontractors listed in the **Annex 2,** which already existed at the time of conclusion of the contract. The Client shall not have a right of objection for these subcontractors.

7.2 If personal data is transferred to recipients in third countries outside the EU and the EEA, such data transfer will generally be based on the EU standard data protection clauses, and/or – in case of transfers into the US – based on the EU Commission’s Adequacy Decision for the EU-US Data Privacy Framework dated July 10, 2023.

You can access further information on the EU standard data protection clauses and the corresponding template via the following website: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-prote

ction/standard-contractual-clauses-scc_en. You can access the EU Commission's Adequacy Decision for the EU-US via the following website: https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

7.3 If the Contractor places orders with subcontractors, it shall be incumbent upon the Contractor to transfer its data protection obligations under this DPA to the subcontractor.

7.4 Upon written request of the Client, the Contractor shall at any time provide information on the data protection-related obligations of its subcontractors.

8. Liability

Reference is made to Art. 82 GDPR. In all other respects, liability under this DPA shall be governed by the SaaS Contract.

9. Information obligations, written form clause, choice of law

9.1 If the Client's data at the Contractor is endangered by seizure or attachment, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Client thereof without undue delay. The Contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Client as the "responsible person" within the meaning of the GDPR.

9.2 The following annexes are an integral part of this agreement. In the event of contradictions, the provisions of the text of this agreement shall take precedence over the annexes:
Annex 1: Description of technical-organizational measures (TOMs)
Annex 2: List of approved subcontractors

9.3 Amendments and supplements to this DPA and all of its components - including any warranties of the Contractor - require a written agreement, which may also be in text form, and the express indication that it is an amendment or supplement to this agreement. This shall also apply to the waiver of this formal requirement. If an individual agreement to this DPA exists, it shall take precedence.

9.4 In the event of any contradictions, the provisions of this Data Processing Agreement shall take precedence over the provisions of the SaaS Contract. Should individual parts of this DPA be invalid, this shall not affect the validity of the rest of the DPA.

9.5 German law shall apply. As place of jurisdiction, the parties agree on the place of jurisdiction of the SaaS Contract.

Annex 1: General technical and organizational measures according to Art. 32 GDPR

1. Pseudonymization and encryption of personal data

a. Pseudonymization

Personal data ("pD") is processed in such a way that the pD can no longer be attributed to a specific data subject without the addition of further information. Pseudonymization of pD shall be required of the processor if the performance of the transferred data processing tasks is not impaired by the pseudonymization. If necessary, distinctions must be made here between productive, test and training data/systems and differentiated measures must be defined.

b. Encryption

The encryption methods used result from the following technical and organizational measures.

The selection of the data encryption method shall be determined separately in an appropriate form for each form of data access:

- Access to public web pages via http protocol
- Access to external data sources or data sinks via VPN tunnel
- Access to external data sources via remote access connection
- Access to data sources in a trusted WAN environment

Details of encryption and authentication methods are to be agreed in the service level agreements for the individual IT applications.

2. Ability to ensure the confidentiality, integrity, availability and resilience of the systems and services related to the processing on a permanent basis

Data processing is carried out by subcontractors, in particular Amazon Web Services. Amazon Web Services provides the relevant Terms of Service at:
https://aws.amazon.com/de/service-terms/ .

a. Ensuring the resilience of the systems in the long term

This includes appropriate measures to be taken already in the phase before the data processing is carried out by the processor. In addition, continuous monitoring of the systems is also required.

☒ Dynamic processes and memory allocation.

☒ Load balancing.

☒ Set load limit for the respective data processing system in advance above the necessary minimum.

b. Entry control

The aim of access control is to ensure, with the aid of suitable measures, that unauthorized persons are prevented from gaining access to buildings and premises containing data processing systems with which personal data is processed. Data are processed.

The size of the data processing system is irrelevant. The implementation of the following measures supports this requirement.

☒ Determination of the authorized persons.

☒ Access regulations for persons outside the company.

☒ Collection of non-operational persons by employees.

☒ Control of the issued means of access.

c. Access control

The aim of access control is to prevent unauthorized persons from using the data processing systems with which personal data is processed or used. The aim of access control is to use suitable measures to prevent unauthorized persons from using the data processing systems with which personal data is processed or used.

The implementation of the following measures supports this requirement.

☒ Regular checking of the validity of authorizations.

☒ Identification of those authorized to access the system by means of suitable measures.

☒ Securing the monitor workstations in the event of absence and when the system is running.

d. Authorization control

The aim of access control is to ensure that only those authorized to use a data processing system can access exclusively the pD subject to their task-related access authorization and that pD cannot be read, copied, modified or removed without authorization during processing, use and after storage.

The implementation of the following measures supports this requirement.

☒ All employees who handle pD are separately bound to secrecy (e.g. by contract, declaration of commitment) or by law.

☒ Implementing a sufficiently differentiated role and authorization model

☒ Use of user IDs.

☒ Identification and authentication of users.

☒ Automatic verification of authorizations.

☒ Logging of access to specific files.

☒ Use of encryption methods.

☒ Separation of test and production operations.

3. **Ability to ensure the availability of pD and access to them quickly in the event of a physical or technical incident (availability control).**

Availability control is intended to ensure that pD are protected against accidental destruction or loss.

The implementation of the following measures supports this requirement.

☒ Regular data backup.

☒ Presence of sufficient human resources in data processing.

4. **Procedures for periodically reviewing, assessing and evaluating the effectiveness of technical and organizational measures to ensure the security of processing**

a. Regular reviews of the company's own IT systems

Regular reviews and quality assurance are carried out to determine whether the state of the art has changed and whether there is a need to adapt the IT systems accordingly.

The hardware and software used is regularly checked for functionality.

b. Regular inspections of subcontractors (order control)

The aim of the order control is to ensure that pD processed on behalf of the order can only be processed in accordance with the client's instructions. To this end, the Contractor shall also ensure that the Client has the right to carry out the checks agreed here also at subcontractors.

The implementation of the following measures supports this requirement.

☒ Written contract.

☒ Clear demarcation of competencies between client and contractor.

5. **Subcontractor technical and organizational measures: Amazon Web services (AWS), Google, Brevo, Intercom and Auth0 by Okta.**

a. **Amazon Web Services** (https://aws.amazon.com/de/compliance/gdpr-center/ as of 24/7/2023). AWS provides certain features and services to help Clients meet the requirements of the GDPR:

i. **Access control:** Only authorized administrators, users, and applications have access to AWS resources

- Multi-Factor Authentication (MFA)
- Customized access to objects in Amazon S3 buckets, Amazon SQS, Amazon SNS, and more
- Authentication of API requests
- Geographical restrictions
- Tokens for temporary access with AWS Security Token Service

ii. **Tracking and logging:** you see the activity in your AWS resources

- Asset Management and Configuration with AWS Config

- Compliance testing and security analysis with AWS CloudTrail
- Identify configuration challenges with AWS Trusted Advisor.
- Customized logging of access to Amazon S3 objects
- Detailed information about flows in the network with Amazon VPC Flow Logs
- Rule-based configuration checks and actions with AWS Config Rules
- Filtering and monitoring HTTP access to applications with AWS WAF capabilities in AWS CloudFront.

iii. **Encryption:** Data in AWS is encrypted

- Encryption of your data when saving with AES256 (EBS/S3/Glacier/RDS)
- Centrally managed key management (by AWS region)
- IPsec tunnels in AWS with the VPN gateways
- Dedicated HSM modules in the cloud with AWS CloudHSM

iv. Strong compliance framework and security standards: AWS demonstrate compliance with strict international standards, such as:

- ISO 27001 for technical measures
- ISO 27017 for cloud security
- ISO 27018 for cloud data protection
- SOC 1, SOC 2 and SOC 3, PCI DSS Level 1,
- BSI's Cloud Computing Compliance Controls Catalogue (C5)
- ENS High

b. **Google** (https://support.google.com/a/answer/60762?hl=de as of 24/7/2023): Google is a leader in discovering security vulnerabilities in software and comprehensively implementing protections such as data encryption and two-step confirmation.

i. **Access control:** Data is secured according to industry standard SOC 2/3

- Logical security: Control mechanisms provide reasonable assurance that logical access to Google Cloud production systems and data is limited to authorized individuals
- Physical security of data centers: Control mechanisms provide reasonable assurance that data centers with stored Google Cloud data and corporate offices are protected.

ii. **Encryption:** Google encrypts the data during transmission on several levels

- Google enforces HTTPS (HyperText Transfer Protocol Secure) for all transmissions between users and Google Workspace services and use Perfect Forward Secrecy (PFS) for all services.
- Encryption of message transmissions with other mail servers via Transport Layer Security (TLS) with 256 bit
- During validation and crucial exchange phases, Google also uses 2048-bit RSA keys.
- With PFS, the private keys for a connection must not be stored permanently. If a party breaks a single key, it can no longer decrypt connections made over months.
  Not even the server operator can retroactively decrypt the HTTPS sessions.

iii. **Strong compliance framework and security standards:** Google implements tools and safeguards necessary to meet compliance requirements and has compliance audited regularly:

- SOC 1™ (SSAE-18/ISAE-3402): Google Workspace and Google Cloud Platform
- SOC 2™: Google Workspace and Google Cloud Platform
- SOC 3™: Google Workspace and Google Cloud Platform
- ISO 27001: Google Workspace and Google Cloud Platform
- ISO 27017: Google Workspace and Google Cloud Platform
- ISO 27018: Google Workspace and Google Cloud Platform
- ISO 27701: Google Workspace and Google Cloud Platform
- HIPAA: Google Workspace and Google Cloud Platform
- FedRAMP: Google Workspace and Google Cloud Platform

c. **Brevo** (https://www.brevo.com/legal/termsofuse/#annex as of 24/7/2023): Brevo (ex Sendinblue) declares that it offers sufficient guarantees as to the implementation of appropriate technical and organizational measures so that the processing meets the requirements of the GDPR and ensures the protection of the data subject's rights, and undertakes to respect the following obligations.

d. **Intercom:** https://25031393.fs1.hubspotusercontent-eu1.net/hubfs/25031393/Valuecase%20Terms%2BDPA/Subprocessor%20DPA/Data%20Processing%20Agreement%20_%20Intercom-31-5-2024.pdf in connection with EU data hosting addendum https://25031393.fs1.hubspotusercontent-eu1.net/hubfs/25031393/Valuecase%20Terms%2BDPA/Subprocessor%20DPA/Intercom%20Regional%20Data%20Hosting%20Addendum-31-5-2024.pdf as of 31/5/2024.

e. **Auth0 by Okta:** Annex II in https://25031393.fs1.hubspotusercontent-eu1.net/hubfs/25031393/Valuecase%20Terms%2BDPA/Subprocessor%20DPA/Valuecase_OKTA-Data_Processing_Addendu-May2024.pdf as of 31/5/2024

f. **Open AI:** Exhibit B in: https://25031393.fs1.hubspotusercontent-eu1.net/hubfs/25031393/Valuecase%20Terms%2BDPA/Subprocessor%20DPA/Data%20Processing%20Agreement%20(Valuecase%20GmbH%20and%20OpenAI).pdf as of 31/5/2024

Annex 2: List of approved subcontractors

Required

Name	Address	Processing location	Description
AWS	AWS EMEA SARL, Marcel-Breuer-Str. 12, 80807 München, Deutschland	**Frankfurt, Germany** DPA: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf	Central hosting service for all Valuecase spaces, templates and all customer content contained therein as well as end-customer pD.
Google Workspace	ABC-Straße 19 Hamburg, 20354 Germany	**European Union** Further information: https://www.google.com/about/datacenters/locations/?hl=en DPA: https://workspace.google.com/terms/dpa_terms.html	Use of the "Google Sheets" function in context of the block “Interactive Calculator” *(optional)*
Brevo (Sendinblue SAS)	106 boulevard Haussmann 75008 Paris	**European Union (Paris, France)** DPA: https://www.brevo.com/legal/termsofuse/#annex	Used for transactional emails (e.g., Notifications)
Intercom R&D Unlimited Company	2nd Floor, Stephen Court, 18-21 St. Stephen's Green, Dublin 2, Republic of Ireland	**European Union (Dublin, Ireland)** DPA: https://www.intercom.com/legal/data-processing-agreement in connection with https://www.intercom.com/de/legal/european-data-hosting-addendum	Used for in-app customer support.
Auth0 (by Okta GmbH)	Salvatorplatz 3, 80333 München, Germany	**European Union (Frankfurt, Germany; Dublin, Ireland)** Executed DPA: https://www.okta.com/sites/default/files/2023-04/DATA-PROCESSING-ADDENDUM-%28April%203_2023%29.pdf	Identity management provider used for user management.

Optional (can be turned off at any time by an authorized person in the platform)

Name	Address	Processing location	Description
OpenAI Ireland Ltd	1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	**World-wide incl. US** Executed DPA: https://25031393.fs1.hubspotusercontent-eu1.net/hubfs/25031393/Valuecase%20Terms%2BDPA/Subprocessor%20DPA/Data%20Processing%20Agreement%20(Valuecase%20GmbH%20and%20OpenAI).pdf	Used for all AI features within the platform *(optional feature which can at any time be turned off by an authorized admin of the Customer)*

****