

ZREALITY GmbH

General Terms and Conditions ("GTC")

1. Scope

1.1 These T&Cs apply to all contracts (each a "**Contract**") for software solutions to support business processes for use via the Internet as a web application ("**SaaS Solution**") of ZREALITY GmbH, Zollamtstraße 11, 67663 Kaiserslautern ("**ZREALITY**") and any third-party software as listed by ZREALITY in the offer.

1.2 Customers of ZREALITY can only be companies, i.e. natural or legal persons acting in connection with their business or self-employed activity (each, a "**Customer**"; ZREALITY and Customers are each a "**Party**" and collectively the "**Parties**").

1.3 ZREALITY does not recognize deviating terms and conditions or other contractual terms of the customer, unless ZREALITY has expressly agreed to their validity in writing in advance. ZREALITY already expressly contradicts the applicability of the customer's terms and conditions.

2. Contract

2.1 At the customer's request, ZREALITY will prepare a non-binding offer ("**Offer**") for the use of the SaaS solution desired by the customer. An offer shall only be deemed to have been agreed in the sense of a contract if it has been signed by an authorised representative of the respective contracting party.

2.2 The commencement of the Contract shall be determined by the Parties in the Offer ("**Commencement of the Contract**"). If no specific date has been specified as the start date of the contract, the contract begins on the date of the last signature of an authorized representative in the context of the conclusion of the contract.

3. Object of agreement

3.1 The specific scope of functions of the SaaS Solution as well as the requirements for the hardware and software environment that must be fulfilled on the Customer's side

result from the respective offer and documentation that ZREALITY makes available or makes available to Customers together with the SaaS Solution ("**User Documentation**"). It is not possible to make the SaaS solution available for local installation at the customer's site.

3.2 Insofar as the Customer orders a connection of the SaaS Solution to a third-party solution purchased by the Customer ("**Third-Party Interface**"), ZREALITY shall provide the interface on the SaaS Solution side. The customer is responsible for further services, in particular the interface on the third-party side as well as the services and processing provided by the third-party provider.

3.3 To the extent that ZREALITY integrates third-party solutions as part of the SaaS Solution, such third-party providers are approved subcontractors ("**Integrated Third-Party Providers**"). Customer is required to accept and comply with the license terms of these Integrated Third-Party Providers before using their Solution. The customer is obliged to inform its employees and other users of this and also of any data processing for its own purposes of the third-party provider (e.g. product improvements).

3.4 As part of the SaaS Solution, ZREALITY provides storage space on central servers on which the data and information generated and processed for the Customer with the SaaS Solution (z.B. 3D representations) as well as information uploaded by the Customer (e.g. participant lists) ("**Customer Content**") are stored for the duration of the contractual relationship.

3.5 The power transfer point is the ZREALITY router output to the Internet. On the customer side, the customer must himself ensure that the connection to the Internet, the provision or maintenance of the network connection to the power transfer point and the procurement and provision of network access components for the Internet.

3.6 The customer's access to the SaaS solution is secured via the Internet. After the conclusion of the Agreement, ZREALITY will provide the Customer with access data for access to its account ("**Customer Account**") in the SaaS Solution and for the use of the SaaS Solution. The customer is obliged to keep his access data including password secret and to protect it from misuse by third parties. In this context, ZREALITY points out that employees of ZREALITY are not authorized to request passwords or access data by telephone or in writing. The Client will change the password provided by ZREALITY for the initial login. When choosing a password, the generally known rules should be observed (length, complexity of the password). The customer must inform ZREALITY immediately in the event of loss of the access data including the password or in case of suspicion of misuse of this data. In all other respects, ZREALITY is entitled to block access to the Customer Account for the SaaS Solution in the event of misuse. The customer is liable for misuse for which he is responsible.

4. Servicelevel

4.1 The SaaS solution is subject to the following service levels:

- Operating hours: 24 hours per day on all seven (7) days of the week ("**Operating Hours**");
- Maintenance Hours: Maintenance work that is carried out in advance and that requires an interruption of the availability of the SaaS Solution will be carried out by ZREALITY on working days between 20:00 and 08:30 ("Scheduled Maintenance"), as far as technically feasible;
- Availability during operating hours: 99% on average for a calendar month ("**Availability**"), with planned maintenance and downtime beyond ZREALITY's control excluded from the calculation of availability.

4.2 If, for urgent, unpostponable technical reasons, maintenance work is exceptionally necessary during operating hours that do not constitute planned maintenance work, with the consequence that the SaaS solution is not available during this time, ZREALITY shall, if possible, inform the Customer in good time by e-mail to the address provided by the Customer.

4.3 ZREALITY performs the analysis and correction of documented, reproducible errors of the SaaS solution (hereinafter referred to as "**Support Services**") in accordance with recognized industry standards. ZREALITY does not guarantee success in eliminating errors. "**Error**" within the meaning of these GTC is any fault reported by the Customer that results in the nature and functionality of the SaaS Solution deviating from the offer and user documentation, and

- this has a more than negligible effect on their usability, or
- corruption of data or loss of data processed with or generated by the SaaS solution occurs.

If a malfunction that has occurred cannot be reproduced, it is not considered an error. In this case, the parties will jointly coordinate the further course of action.

4.4 The customer must report any errors that occur immediately with a detailed description of the problem. The notification can initially be made orally, but must be repeated in text form (e-mail) no later than the next working day. ZREALITY can be reached to receive error reports by e-mail Monday – Friday from 09:00 a.m. to 05:00 p.m. at the following e-mail address: support@zreality.com

4.5 The type and duration of testing and processing of defects depends on the defect class and the corresponding response times:

4.5.1 Defect classes

- Error class 1: Productive use of the SaaS solution is not possible or only to a

considerable extent or essential performance characteristics are missed.

- Error class 2: The core functionality is guaranteed, but there is a significant error in a submodule that prevents or significantly restricts working with this module.
- Error class 3: All other errors

4.5.2 Response times depend on the support services agreed between ZREALITY and the customer:

Standard Support

- Error class 1: Until the next working day
- Error class 2: At the discretion of ZREALITY
- Error class 3: At the discretion of ZREALITY

Enterprise Support

- Error class 1: One (1) hour
- Error class 2: Two (2) business days
- Error class 3: Five (5) business days

Within the response times, ZREALITY submits a proposal for fixing the error. The proposal includes the following:

- Conducting an error analysis and presenting the results of the analysis performed;
- Presentation of the impact of the bug on other functionalities (criticality);
- Suggest a course of action to fix the error.

4.6 ZREALITY is not obligated to provide support services (neither standard nor enterprise support):

- in the event of errors resulting from

Availability	Service Credit (% of the monthly fee for the service)
<99.0%	5,0%
<98.0%	7,5%
<97.0%	10%
<96.0%	15%
<95.0%	20%

improper modifications or adjustments to the SaaS Solution by or on behalf of Customer;

- for software other than the SaaS solution (in particular third-party software used on customer systems);
- in the event of errors resulting from improper or unauthorized use of the SaaS Solution or from operating errors of the Customer, provided that the operation is not carried out in accordance with the User Documentation;
- in the event of any hardware defects;
- when using the SaaS Solution by Customer on permitted hardware and operating system environments other than those specified in the User Documentation; or
- in the form of on-site assignments by ZREALITY employees.

4.7 If ZREALITY and the Customer are required to provide support services in accordance with this Section 4.6 outside of ZREALITY's general obligations, ZREALITY shall be entitled to treat such services as a separate assignment and to invoice the Client for the usage fees for the SaaS solution in accordance with the applicable service rates. In the event of unplanned downtime, ZREALITY will make commercially reasonable efforts to remedy the unplanned downtime within a reasonable period of time.

If ZREALITY does not comply with the 4.1 If the Service Level set forth in these Terms and Conditions is not met ("Unavailability"), the Customer shall be entitled to the Service Credits set forth below ("Service Credits"), whereby the Service Credits shall not exceed 10% of the total fees paid by the Customer to ZREALITY for all Services provided in the respective Service Month.

In order to receive a Service Credit, Customer must claim such credit from ZREALITY within five (5) business days of receipt of the Service Level Report for the period for which Customer is claiming the Service Credit. This claim by the customer must contain precise information on the days, times and duration of any unavailability claimed by the customer. If, following an audit, ZREALITY accepts Customer's written claim for a Service Credit, ZREALITY will notify Customer that the relevant Service Credit will be offset against the fee paid by Customer for Services in the next monthly invoice for the Services. Service credits cannot be credited retroactively. If Customer fails to claim a Service Credit in a timely manner, Customer will forfeit their entitlement to a Service Credit for that month. Service credits payable by the customer will be offset against any claims for damages by the contracting party due to non-compliance with the service level.

4.8 ZREALITY ensures continuous monitoring of service levels. All service level measurements are made on a monthly basis for each calendar month during the term of the contract.

At the customer's request, ZREALITY provides monthly reports on the measurements of unplanned downtime and the calculation of system availability for the relevant previous month. If Customer has any complaints regarding a measurement or other information specified in this report, Customer must notify such objections to ZREALITY in writing within five (5) calendar days of receipt of the report, and the accuracy of the report will be deemed sufficient in the absence of such notification by Customer. Any such communication must indicate the measurements complained of and describe in detail the nature of the complaint. ZREALITY and Customer agree to resolve any such disagreement regarding Service

Levels and/or related measurements by mutual agreement as far as possible and in a timely manner.

4.9 The rights of the customer in the event of unavailability are exclusively in this section 4 regulated. Further rights are excluded. This does not affect the customer's right to termination and compensation for damages in accordance with these GTC.

5. Backups and data storage

The Customer is obliged to adequately secure Customer Content. ZREALITY also performs daily backups of the customer's service and data. Backups are stored for up to twelve (12) months. Upon termination (ordinary or extraordinary) of the Agreement by either party, the Customer's data processed through the SaaS Solution will be stored for a further three (3) months before it is finally deleted by ZREALITY, subject to any statutory retention periods by ZREALITY.

6. SaaS solution and customer content usage rights

6.1 Subject to the provisions of this Agreement, ZREALITY grants the Client the non-exclusive, worldwide, fee-based right to use the SaaS Solution for internal purposes in accordance with the Agreement during the term of the Agreement, which can only be sublicensable to the number of users of the Client's account agreed in accordance with the Offer. The Customer may only use the SaaS Solution within the capacity agreed in the Offer.

6.2 Subject to the rights granted under these T&Cs, ZREALITY reserves all rights and interest in and to the SaaS Solution, developments or programming based on it, as well as the associated intellectual property and know-how. The Client acknowledges that he/she does not obtain and acquire any rights other than those expressly granted under these T&Cs.

6.3 Customer hereby grants ZREALITY a non-exclusive right to (a) copy, use, modify, distribute, display and disclose Customer Content and Usage Data to the extent necessary to

provide the Services to Customer in accordance with this Agreement, (b) copy, modify and use Customer Content and Usage Data in connection with SaaS Solution features; including, but not limited to, for the purposes of operational analysis and reporting, internal financial reporting and analysis, audit functions and archiving, and (c) use aggregated and anonymized Customer Content and Usage Data for marketing or product optimization purposes, provided that the Aggregated Data does not include any information that identifies or makes identifiable the Customer or User, Brands or User as the source of such data. Usage data within the meaning of this subsection is data and information that arises when using the SaaS solution, e.g. log data, connection data or user input.

7. Trial

If ZREALITY and Customer have agreed to make a version of the SaaS Solution available for testing purposes ("Trial Version"), these Terms shall apply accordingly to the extent applicable to the Trial Version. The specific scope of services for the trial version results from the corresponding offer.

8. Duties

The cooperation of the customer required for the performance of the contractual services by ZREALITY must be provided in full and in a timely manner. Subject to further specifications in this Agreement, in the Offer to Customer and the User Documentation, Customer's obligations to cooperate include, but are not limited to, the following:

- when using the SaaS Solution, all applicable laws and regulations must be observed. The Client may not transfer any data or content to ZREALITY's servers or use software integrated by means of the SaaS Solution in a manner that violates legal provisions or infringes third-party intellectual property rights, copyrights or other rights of third parties;
- in the event of an error message, ZREALITY shall immediately provide ZREALITY with all documentation,

protocols and other information relevant to troubleshooting by the Client;

- the Client is obliged to regularly participate in the product training offered by ZREALITY or to acquire the necessary knowledge to use the SaaS Solution in any other way;
- the Customer may only transmit such data through the SaaS Solution that is free of computer viruses or other harmful code/technologies;
- Customer shall not use any software or other techniques or procedures in connection with the use of the SaaS Solution that are likely to affect the operation, security, and availability of the SaaS Solution.

9. Adjustment of remuneration

ZREALITY is entitled to adjust the remuneration to be paid by the Client for the use of the SaaS Solution during the term of the Agreement. However, such a price change is only allowed once a year. Price increases must be announced no later than six (6) weeks before they take effect by e-mail from ZREALITY to the e-mail address provided by the customer ("**Price Increase Announcement**"). In the event that the price increase amounts to more than 10% of the previous remuneration, the customer has a special right of termination, which he can exercise in writing with a notice period of one (1) month to the end of the calendar month after receipt of the price increase announcement.

10. Locking of data

If a third party asserts an infringement of rights against ZREALITY by means of data or content transmitted by the Customer to the data storage facilities provided by ZREALITY ("**Reported Content**"), ZREALITY is entitled to provisionally block the corresponding Reported Content if the third party has conclusively demonstrated the infringement. In this case, ZREALITY will ask the customer to stop the infringement within a reasonable period of time or to prove the legality of the reported content. If this request is not complied with or not

sufficiently complied with, ZREALITY shall be entitled, without prejudice to further rights and claims, to terminate the contract for good cause without observing a notice period. Insofar as the customer is responsible for the infringement, he is also obliged to compensate for the resulting damage and must indemnify ZREALITY against any claims by third parties on first request. Further rights are reserved.

11. Changes in performance

ZREALITY is entitled at any time to further develop, modify or supplement the SaaS Solution in whole or in part. ZREALITY will announce any significant changes relevant to the contract at least six (6) weeks before they take effect by e-mail to the e-mail address provided by the customer ("Notice of Change of **Performance**"). The customer may object to the changes with a notice period of one (1) month from receipt of the notification of the change of service in writing or by e-mail. The changes shall be an integral part of the contract between ZREALITY and the Client without being contradicted. The notification of a change in benefits refers to the consequences of the objection. In the event of a timely objection, ZREALITY is entitled to terminate the Agreement in writing with a notice period of one (1) month to the end of the calendar month.

12. Intellectual property rights of third parties

12.1 If ZREALITY's use of the SaaS Solution in accordance with the contract infringes industrial property rights and copyrights of third parties asserts claims against the Customer due to such infringement, ZREALITY shall, at its option, at its own expense, either:

- obtain the usage rights required for the SaaS solution; or
- redesign the SaaS solution so that it no longer infringes the rights of third parties and has at least the characteristics contractually agreed with the customer.

12.2 ZREALITY will defend the Client against or at its own discretion within the scope of the limitations of liability set out in Section 12.4 free from damages that result directly from the

assertion of corresponding claims from infringements of rights by third parties and are asserted against the customer in court, insofar as these claims of the third party are not based on the following:

- Changes to the SaaS Solution by Customer that have not been approved by ZREALITY under this Agreement or otherwise; or
- use of the SaaS Solution in any manner other than agreed upon in accordance with the purpose of this Agreement; or
- Use of the SaaS solution on hardware or operating system environments not released by ZREALITY.

The obligation to pay compensation is excluded if ZREALITY proves that the customer is responsible for the infringement of third-party rights.

12.3 The Client is obliged to inform ZREALITY immediately in the event that third parties assert infringements of intellectual property rights against the Client in connection with the SaaS Solution. The Client is only entitled to take measures, in particular to defend itself in court against the claims or to satisfy legal claims of the third party with reservations, provided that ZREALITY has previously notified that ZREALITY will not defend the Client against the claim.

12.4 The Customer shall defend ZREALITY against or indemnify ZREALITY at its own discretion against claims or damages that arise directly from the assertion of such claims and are asserted against ZREALITY if and to the extent that these claims are based on the fact that the Customer has allegedly or actually infringed the rights of third parties in the course of using the SaaS Solution.

13. Liability

ZREALITY shall be liable for all damages arising in connection with this contract, regardless of the factual or legal grounds, only in accordance with the following provisions:

13.1 In the event of intent and gross negligence, claims under the German Product Liability Act as well as in the event of injury to life, limb or health, ZREALITY shall be liable without limitation in accordance with the statutory provisions.

13.2 In all other respects, the liability per calendar year is limited to the damage foreseeable at the time of conclusion of the contract up to a total amount for all claims per calendar year corresponding to 50% of the remuneration paid by the customer in this calendar year. This limitation of liability also applies in the event of data loss and deterioration as well as for data protection violations by ZREALITY within the meaning of the order processing agreement between the parties.

14. Privacy

When the SaaS Solution is made available, ZREALITY may have access to personal data that ZREALITY processes as a processor for the Customer on the basis of the Data Processing Agreement ("DPA") concluded with the Customer under this Agreement.

15. Confidentiality

The provisions of the non-disclosure agreement agreed between the parties shall prevail.

Unless an agreement has been expressly concluded, the following applies:

15.1 The parties are aware that during the term of the Agreement they will have access to certain confidential information of the other party or confidential information of third parties that the disclosing party is obliged to keep confidential. Confidential Information means any written, electronic, or oral information that (i) a party has disclosed to the other party, (ii) is not generally known or publicly available, in whole or in the exact arrangement and composition of its components, (iii) relates to the activities of a party or a third party, (iv) is subject to the disclosing party's appropriate technical and organizational safeguards, and (v) is either as a confidential or should reasonably be treated as confidential due to the nature of the circumstances under which the disclosure is made ("**Confidential Information**"). Each party

acknowledges that the disclosing party or third party retains ownership of all rights in Confidential Information.

15.2 Each party undertakes to (i) keep the Confidential Information disclosed by the other party only to the extent permitted and intent in this Agreement, (ii) treat the Confidential Information obtained from the other party as strictly confidential and protect it from knowledge and use by third parties by implementing appropriate technical and organizational measures, (iii) allow access to the Confidential Information disclosed by the other party at the to restrict those of its employees, agents and/or any consultants who have a need to know such information and who have been required in writing to keep such information confidential in accordance with this Agreement, and (iv) to surrender or destroy any Confidential Information disclosed by the other party that is in its possession upon termination or expiration of this Agreement. Notwithstanding the foregoing, Customer acknowledges that ZREALITY may use anonymized statistical data about Customer's use of ZREALITY and may disclose such statistical data to third parties. The contractual confidentiality obligations shall continue to apply for two (2) years after the termination of the Agreement.

15.3 Notwithstanding the foregoing, the provisions of Sections 15.1 and 15.2 of the Terms and Conditions shall not apply to Confidential Information that (i) is freely accessible or generally known at the time of its disclosure, (ii) becomes freely available or generally known through no fault of the Recipient, (iii) has been lawfully disclosed to the Recipient by persons who have not been bound by confidentiality obligations in this regard, (iv) are already in the possession of the recipient at the time of disclosure without any confidentiality obligations, (v) have been independently developed by the recipient, or (vi) are approved for release or distribution by the disclosing party without restriction. Notwithstanding the foregoing, each party may disclose Confidential Information to the extent necessary (i) to comply with a court or regulatory order or otherwise to comply with mandatory legal requirements, provided that the party disclosing the Confidential Information pursuant to the order shall provide the other party with prior written notice and reasonable efforts to: to obtain a protective order, or (ii) to

have a court determine a party's rights under this Agreement; this includes the applications required for this purpose.

16. Contract Term and Termination

16.1 The contract comes into force at the beginning of the contract and, unless otherwise agreed on the basis of the offer, runs for twelve (12) months ("**Minimum**"), unless it is subject to the provisions of this paragraph 16 is terminated. The Agreement will automatically renew for one year at a time, unless terminated in writing by either party with three (3) months' notice prior to the end of the current renewal period (the Minimum Term and any Renewal Periods shall be collectively referred to as "**Runtime**").

16.2 In the event of termination of a contract with a notice period or minimum term agreed in accordance with the offer, the customer shall continue to be entitled to the contractually agreed services until the end of the contractual term.

16.3 If the 4 of the GTC for a period of three (3) consecutive calendar months or of three (3) calendar months within a period of six (6) calendar months (availability during operating hours below 95%) and ZREALITY is responsible for the shortfall, the Customer is entitled to terminate the contract without notice and to claim damages in lieu of performance.

16.4 Any notice of termination must be made in text form (letter, fax, e-mail). Non-use of the SaaS solution is not considered termination. Without notice of termination received in due time and form, the term of the contract is automatically extended.

17. Termination, consequences of termination

17.1 The right of both parties to terminate for good cause remains unaffected. In particular, ZREALITY is entitled to terminate this contract extraordinarily without observing a notice period if:

- the Customer is in default of payment for a period of more than two (2) months

equal to at least the agreed fee for use for the period of two (2) months;

- insolvency proceedings or other judicial or extrajudicial proceedings for the purpose of settling debts have been or will be initiated in respect of the Client's assets;
- the third party's user account has been transferred or the access data to the SaaS solution has been made available to third parties in each case without the prior consent of ZREALITY;
- the customer has otherwise violated its obligations under this contract and, despite the setting of a deadline, does not cease the breach of contract or provides evidence of measures that are suitable to exclude the repetition of the breach of contract in the future.

17.2 In the event of termination of the contractual relationship, regardless of the legal grounds, the parties are obliged to properly process the contractual relationship. To this end, ZREALITY will be used in accordance with the GCU

- transfer the data stored under the Agreement to ZREALITY to the Client or a third party designated by the Client no later than four (4) weeks after the termination of the Agreement, at the Client's option, either by means of remote data transmission or on data carriers;
- delete the data immediately after confirmation of the successful transfer of data by the customer or a designated third party and destroy all copies made.

17.3 About the number 17.2 ZREALITY can provide additional support services for the migration of the data on the basis of a separate commission. Such further support services will be remunerated in accordance with the applicable price list of ZREALITY.

18. Terms of payment

18.1 The Client is obliged to pay ZREALITY the fees agreed in the Offer in Euros or, if applicable, a different currency specified in the Offer in advance at the intervals agreed in the Offer (if nothing has been agreed: annually) in accordance with Section 18.2 .

18.2 The fees due under this Agreement shall be invoiced during the term of the contract at the intervals agreed in the order (unless agreed: annually), in each case in advance for the following year, for the first time with the invoice date of the first day of the contract term. The customer accepts an electronic invoice.

18.3 Each invoice amount is due fifteen (15) days after receipt of the invoice by the customer.

18.4 All fees are exclusive of VAT and any other applicable tax, the payment of which is the sole responsibility of the customer.

18.5 Customer will default on payment if it fails to pay the invoice amount within thirty (30) days of the invoice being issued. The default interest amounts to 9 percentage points above the base interest rate per year from the due date.

18.6 If Customer disputes an invoice or other amount due under this Agreement, Customer shall notify ZREALITY in writing within thirty (30) days of receipt of the invoice or the date of due date, specifying the reasons for the complaint ("**Disputed Invoice**"). With the exception of disputed invoices, all invoices or amounts due are deemed to have been accepted and are payable without deduction. ZREALITY will not assert the rights under Clause 18.4 with regard to fees that are the subject of a substantiated complaint by the Client.

19. Takeover of the contract

ZREALITY is entitled to transfer rights and obligations arising from this contractual relationship to a third party in whole or in part with a notice period of four (4) weeks. In this case, the Client shall be entitled to terminate the Agreement within two

(2) weeks of the announcement of the assumption of the Agreement.

20. Other

20.1 Changes to these T&Cs. ZREALITY reserves the right to amend these T&Cs in accordance with the following provisions, provided that this change is reasonable for the customer, taking into account the interests of ZREALITY; this is in particular the case if the change is without significant legal or economic disadvantages for the customer, e.g. in the case of changes to contact information. In addition, ZREALITY will inform Customers before any change to these Terms and Conditions with reasonable notice, but at least one (1) month before the intended entry into force of the changes, to the e-mail address provided by the Customer ("**GTC Change Notice**").

If the customer does not agree with a change intended by ZREALITY, he has the right to object to the change within one (1) month from receipt of the GTC change notice. In the event of a timely objection, ZREALITY shall be entitled to terminate the Agreement with a notice period of one (1) month to the end of the calendar month.

20.2 Entire contract. This Agreement, including the Offer and Exhibits and Annexes, conclusively governs all agreements between the parties with respect to the subject matter hereof and, except as expressly provided otherwise in this Agreement, supersedes all prior oral and written agreements and understandings between the parties with respect to its subject matter. Neither party shall be bound by any terms or representations other than those expressly provided for in this Agreement, including the Offer and Exhibits and Appendices to this Agreement .

20.3 Changes and Additions. Unless otherwise agreed on the basis of these GTC, amendments and additions to this contract must be made in writing within the meaning of Section 126 (2) of the German Civil Code (BGB) and must be signed by authorized representatives of both parties. This also applies to the waiver of the written form and a change in this written form requirement.

20.4 Cession. The Client shall not be entitled to assign its rights under the Agreement or delegate its obligations under this Agreement without the prior express written consent of ZREALITY; in the absence of such consent, any attempted assignment or delegation shall be void and ineffective.

20.5 Offsetting and retention. The customer is only entitled to offset or withhold against ZREALITY in the case of legally established or undisputed counterclaims.

20.6 No contract for the benefit of third parties. The parties acknowledge that, except as expressly provided otherwise in this Agreement, the provisions of the Agreement are for the sole benefit of the parties. This Agreement does not expressly or imply confer on any third party, whether natural or entity, any provision of this Agreement.

20.7 Severability. To the extent that any provision of this Agreement is for any reason invalid or unenforceable in any jurisdiction, such provision shall be modified to make it valid or enforceable. The invalidity or unenforceability of any provision shall not render that provision invalid or unenforceable in any other case, under any other circumstance or in any other jurisdiction and shall not affect the validity of the remaining provisions of the Agreement.

20.12 Governing Law. The law of the Federal Republic of Germany shall apply exclusively, to the exclusion of its conflict-of-law rules and the United Nations Convention on Contracts for the International Sale of Goods (CISG).

20.8 Disclaimer. No waiver of the Agreement shall be effective and binding unless it is in writing and duly signed by the waiving party. Each waiver constitutes a waiver only with respect to the specific matter governed by it and does not in any way affect the rights of the waiving party in any other respect or at any other time. Any delay or omission by either party in exercising any right under this Agreement shall not be deemed a waiver of such right.

20.9 Venue. The place of performance and jurisdiction for all disputes arising out of or in connection with this contract, including any tortious claims for merchants, legal entities under public law or special funds under public law, is Kaiserslautern, Germany.

20.10 Authoritative language. The English language version of this Agreement shall be authoritative and legally binding in all respects and shall prevail in the event of any conflict.

20.11 Contact details of ZREALITY. Please send complaints and cancellations to the following address:

ZREALITY GmbH
Zollamtstr. 11
67663 Kaiserslautern
Germany
support@zreality.com

Data Processing Agreement (DPA)

Agreement between Customer ("Client") and ZREALITY GmbH, Zollamstrasse 11, 67663 Kaiserslautern ("Contractor"; collectively the "Parties" or each a "Party") on the processing of personal data on behalf of the "DPA". The terms "personal data", "process", "data subject", "controller" and "processor" are defined in Art. 4 of the General Data Protection Regulation (Regulation (EU) 2016/679 ("GDPR").

1. Subject matter and duration of the assignment

1.1. Subject of the contract

The subject matter of the data processing order by the Contractor results from the software or SaaS contract between the parties ("Main Agreement"). In doing so, the Contractor processes personal data on behalf of the Client. As the controller, the Client is responsible for the processing of personal data, for assessing the legal admissibility of the processing of personal data and for safeguarding the rights of data subjects.

1.2. Duration of the job

This DPA is agreed between the parties for the duration during which the Contractor processes personal data on behalf of the Client on the basis of the main contract.

2. Specification of the content of the contract

2.1. Scope, nature and purpose

The scope, nature and purpose of the processing of personal data by the Contractor for the Client are specifically described in the main contract.

2.2. Type of data

The subject matter of the processing of personal data is the following data types/categories ("Client Data")

- Name
- the contact data (e-mail / phone),
- Internet usage data generated when using the Contractor's SaaS solution,
- Data generated when using the chat or video chat function.

2.3. Circle of those affected

The group of data subjects affected by the processing of personal data in the context of this assignment includes:

- Employees/employees of the client (this includes management, interns, temporary employees and similar persons),
- Employees / employees of the Client's business partners,
- Customers and contact persons at the client's customer.

3. Authority of the Client / Place of Data Processing

- 3.1. The processing of client data is carried out exclusively in accordance with documented instructions of the client. The Client shall immediately confirm verbal instructions in writing or by e-mail (in text form). Changes to the object

of processing and changes to the process must be jointly agreed and documented. Any additional expenses incurred shall be reimbursed by the Client on a time and material basis.

- 3.2. The Contractor shall only process Client data outside the instructions of the Client to the extent that it is obliged to do so by applicable law. In such a case, the Contractor shall inform the Client of this circumstance in advance, unless the relevant law prohibits this.

- 3.3. The Contractor shall inform the Client if it is of the opinion that an instruction violates relevant data protection regulations. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller at the Client.

- 3.4. The processing of the Client data by the Contractor takes place within the EU / EEA. A relocation of processing to countries outside the EU / EEA by the Contractor will only take place after consultation with the Client.

4. Confidentiality

The persons authorised to process the Client's data have committed themselves to confidentiality or are subject to a statutory duty of confidentiality.

5. Technical and organisational measures

- 5.1. The Contractor shall take technical and organisational measures to protect the Client's data that meet the requirements of Art. 32 GDPR. These technical and organisational measures are described in Annex 1 to this GCU. The Client is aware of these technical and organisational measures and is responsible for ensuring that they provide an appropriate level of protection for the risks of the data to be processed.

- 5.2. The technical and organizational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. The safety level of the defined measures must not be undercut. Significant changes must be documented.

6. Subcontracting

- 6.1. The Client agrees to the use of subcontractors by the Contractor:

- 6.1.1. The Client agrees to the use of the subcontractors listed in Annex 2 to this DPA when concluding this DPA.

- 6.1.2. The Client agrees to the use of additional subcontractors or the modification of existing subcontractors if the Contractor notifies the Client of the use or change in writing (e-mail sufficient) fourteen (14) days before the start of the data processing. The Client may object to the use of a new subcontractor or the change for important data protection reasons within ten (10) days. If no objection is made within the deadline, consent to the assignment or modification shall be deemed to have been given. The Client acknowledges that in certain cases the service can no longer be provided without the use of a specific subcontractor. If there is an

important reason for the objection under data protection law and it is not possible for the parties to find an amicable solution, the parties each have a special right of termination with regard to the performance of the contractor concerning the rejected subcontractor.

- 6.2. The Contractor shall conclude written (this includes the electronic form) order processing agreements with the subcontractor(s), taking into account the nature and scope of data processing within the scope of the subcontract, the content of which corresponds to this DPA.

7. Rights of data subjects

The Contractor shall support the Client within the scope of its possibilities in fulfilling the requests and claims of data subjects under Chapter III of the GDPR.

8. Obligations of the Contractor to Cooperate

The Contractor shall support the Client in complying with the obligations set out in Articles 32 to 36 of the GDPR regarding the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations.

9. Client's right to information and review

- 9.1. The Client shall have the right to request the necessary information to prove compliance with the agreed obligations of the Contractor and to carry out inspections in agreement with the Contractor or to have them carried out by auditors to be appointed in individual cases.
- 9.2. The parties agree that the Contractor is entitled to submit meaningful documentation to the Client in order to prove compliance with its obligations and implement the technical and organisational measures. Meaningful documentation can be provided by submitting a current attestation, reports or report excerpts from independent bodies (e.g. auditors, auditors, data protection officers), suitable certification by IT security or data protection audit (e.g. according to ISO 27001) or certification approved by the competent supervisory authorities.
- 9.3. This does not affect the contracting authority's right to carry out on-the-spot checks. However, the Client will weigh up whether an on-site inspection is still necessary after the submission of meaningful documentation, in particular taking into account the maintenance of the orderly operation of the Contractor. The Client will only carry out on-site checks in consultation with the Contractor.

10. Deletion of data and return of data carriers

At the Client's discretion and request – at the latest upon termination of the order processing – the Contractor shall, at the discretion of the Client, hand over to the Client all documents that have come into its possession, the processing and usage results created as well as data sets in connection with the contractual relationship or, subject to prior consent, destroy them in accordance with data protection regulations.

Documentation that serves to prove that data processing has been carried out in accordance with the order and in

accordance with the order, or which the Contractor is legally obliged to retain, may be retained by the Contractor beyond the end of the contract in accordance with the respective retention periods.

11. Liability

The Contractor's liability in connection with this DPA shall be subject to the limitations of liability agreed in the main contract.

Appendix 1 to the Data Processing Agreement:

Technical and organizational measures in accordance with Art. 32 GDPR.

Description of the technical and organizational security measures taken by ZREALITY GmbH ("Processor")

The Contractor has implemented the following technical and organizational security measures ("TOMs") to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services. The TOMs are complemented, where appropriate, by the security measures taken by the subcontractors used:

1. Confidentiality

The Contractor has taken the following technical and organisational security precautions, in particular to ensure the confidentiality of the processing systems and services:

- The Contractor shall take appropriate measures to prevent its data processing systems from being used by unauthorised persons. This is achieved by:
 - Authentication with username and password;
 - key control (key issuance of buildings only to authorized personnel, etc.) and security locks;
 - Careful selection of external service providers and conclusion of confidentiality obligations;
 - Alarm messages in case of unauthorized access to server rooms;
 - Automatic timeout of the user terminal if it remains idle, identification and password required to access again?
 - Issuing and securing identification codes and using two-factor authentication
 - industry-standard encryption and password requirements (password policy, incl. minimum length, use of special characters, etc., password change);
 - blocking of security-relevant access after faulty login attempts;
 - Physically separate storage on separate systems and data carriers;
 - Regular security updates for data processing systems.
- The Contractor's employees who are authorized to use its data processing systems may access personal data only to the extent and to the extent covered by their respective access authorization (authorization).

Specifically, access rights and levels are based on the function and role of employees, using the concepts of least privilege and knowledge need to align access rights with defined responsibilities. This is achieved in particular by:

- Mandatory employee policies and training;
- Obligation of employees to confidentiality and secrecy;
- Creation of user profiles and assignment of user rights;
- Restricted access to personal data only for authorized persons;
- blocking of user access after incorrect login attempts;
- Centralized storage of log files and limited access for authorized persons;
- Logical client separation;
- Limited access to servers only for authorized persons;
- Industry-standard encryption;
- Use of VPN technology;
- Physical deletion of data carriers before reuse.

2. Integrity

The Contractor has taken the following technical and organisational safeguards, in particular to ensure the integrity of the processing systems and services:

- The Contractor shall take appropriate measures to prevent personal data from being read, copied, altered or deleted by unauthorised persons during transmission or transport of the data carriers. This is achieved by:
 - Establishment of leased lines or VPN tunnels;
 - The use of firewall and encryption technologies for software and hardware;
 - Conducting vulnerability tests on a monthly basis;
 - avoiding the storage of personal data on portable storage media for transport purposes and on company-owned laptops or other mobile devices;
 - In the case of physical transport: careful selection of transport personnel and vehicles; safe transport containers and packaging.

- Secure destruction and disposal of data carriers.
- The Contractor will not access any Customer Content unless it is necessary to provide the Customer with the products and professional services it has selected. The Contractor does not access Customer Content for any other purpose.

3. Availability

The Contractor has implemented the following technical and organisational security measures, in particular to ensure the availability of processing systems and services:

- The processor shall take appropriate measures to ensure that personal data is protected against accidental destruction or loss. This is achieved by:
 - Creation of backup and recovery concept;
 - Infrastructure redundancy;
 - use of anti-virus software;
 - Use of hardware firewall;
 - Fire and smoke alarm systems;
 - Protective power strips in server rooms;
 - Fire extinguishing equipment in server rooms;
 - Regular security updates for data processing systems;
 - Alarm messages in case of unauthorized access to server rooms;
 - Carrying out regular data backups;
 - Keeping backups in a secure, outsourced location;
 - Separation of production and test system.

- Incident detection system and project-related management of incident response;
- Regular (external) auditing;
- Regular review of scale and infrastructure;
- Privacy-friendly defaults;
- Secure development cycle
- Test.

4. Resilience

The Contractor has implemented the following technical and organisational security measures, in particular to ensure the resilience of the processing systems and services:

- Data protection management and definition of roles and responsibilities;
- Business continuity management and contingency plan;
- Project-related risk management;
- Conducting vulnerability tests on a monthly basis and implementing the results immediately;

Annex 2 to the Data Processing Agreement

Approved subcontractors

#	Name	Address	Area of application within the scope of the contract
1	Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855, Luxemburg	IT infrastructure / hosting (EU servers only)
2	Open AI Inc.	3180 18th St, San Francisco, California 94110, US	Integrated Third-Party Service Support: Operation of AI Functionality

Updated: April 2024