condens

Data Processing Agreement (“DPA”) according to Art. 28 GDPR

The **Controller** (responsible for processing) and the **Processor** shall conclude the following Data Processing Agreement in accordance with Article 28 of the EU - General Data Processing Regulation (GDPR). On the basis of the Terms of Service (“Contract”) between the parties, the Processor processes personal data for the Controller. The resulting data protection rights and obligations of the parties are specified in this contract. The regulations laid down apply to all services rendered by the Processor for the Controller and all associated activities which entail and may entail the processing of personal data.

This DPA is supplemental to, and forms an integral part of, the Terms of Service (“Contract”) and is effective upon the conclusion of the Contract. The term of this DPA will be the same as the term of services under the Contract and these DPA terms will supersede any conflicting terms of the Contract. The respective rights and obligations of the parties under this DPA survive any termination or expiration of this DPA to the extent necessary to the intended preservation of such rights and obligations (including should any processing continue following such termination).

§ 1 Definitions

a) “Contractors” means natural or legal persons, authorities or other bodies that process personal data on behalf of the controller.
b) “Controller” means you, the customer
c) "Personal Data" means any information relating to an identified or identifiable natural person (data subject). Identifiable is defined as a natural person who can be identified directly or indirectly, in particular by means of an identification code such as a name, identification number, location data, an online identifier or by means of one or more specific characteristics which are expressions of the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.
d) The "processing" of data is generally understood as the use of personal data. Processing personal data shall mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. In addition, the legal definitions of Art. 4 No. 2 GDPR shall apply.
e) “Processor” means us, Condens Insights GmbH.
f) “Responsible party” means any natural or legal person, public authority or other body which, alone or jointly with others, decides on the purposes and means of processing personal data.
g) Reference is made to further definitions set forth in Art. 4 GDPR.

§ 2 Subject matter and duration of processing

a) The subject matter of the contract is the processing of Personal Data by the Processor on behalf of and in accordance with the instructions of the Controller to provide the services as defined in the Contract.
b) The duration of the DPA corresponds with the Contract.
c) The Controller may terminate this DPA and the Contract at any time without notice if the Processor has committed a serious breach of the provisions of this Agreement, in particular, if the Processor uses the data from the Controller for purposes other than those specified in this Agreement or if the Processor breaches a material obligation under this Agreement.

d) Even if the aforementioned preconditions are not met, the Controller shall be entitled to terminate this DPA and the Contract without notice if the Processor repeatedly violates this DPA. A prior written notice or a note in text form from the Controller is a prerequisite for this.

§ 3 Type of personal data and purpose of the processing

The Processor may receive the following types of data about individuals affected by the processing of personal data ("**Data subjects**") for which the purpose of the processing is as follows:

Data subjects	**Type of personal data**	**Purpose of the treatment**
Controller's users of the Software	User account information such as name, email address and related account information	Making Condens Software available to users including login, password reset and identification in the tool.
• (Potential) customers or (potential) users of the Controller's products or services • Other individuals the Controller chooses to do user research about	Data provided in research studies in the course of user research and entered into Condens by users. This may include name, demographic profile, contact information, audiovisual recordings and additional information research participants chose to share in research studies or as feedback to Controller.	Providing the Software that supports the Controller and its users in analyzing and identifying needs and wishes of (potential) customers or users and identifying opportunities for improvements in products and services.

§ 4 Rights and obligations of the Controller

a) For the assessment of the admissibility of data processing the Controller alone is responsible and thus the person responsible within the meaning of Art. 4 para. 7 GDPR.
b) Prior to the data processing, and as a rule thereafter, the Controller shall be entitled, after prior notification in good time during normal business hours, to satisfy themselves of compliance with the technical and organizational measures taken by the Processor for data security. The Controller may also have this inspection carried out by a third party at the Controller's expense.
c) The Processor must tolerate possible control measures by the data protection authority in accordance with Art. 58 GDPR. The Processor shall inform the Controller without undue delay after notification or knowledge of the implementation of the control measure as well as in the case of other inquiries, investigations or inquiries by the data protection authority, in particular also if such inquiries are made within the framework of a prior consultation pursuant to Art. 36 GDPR, insofar as the measures or inquiries may concern data processing that the Processor provides for the Controller.
d) The Controller may submit Personal Data (containing no Sensitive Data) to the Services, the extent of which is determined and controlled by the Controller in its sole discretion.

§5 Duties of the Processor

a) The Processor is obliged to process personal data exclusively in accordance with the instructions and in accordance with the stipulations of this DPA. The processing of personal data for own purposes or

for third parties is prohibited. In particular, no copies may be made unless this is the subject of the data processing or the Controller has given its express consent**.**

b) The Processor will maintain the confidentiality of all data of the Controller and will not disclose data of the Controller to third parties unless Controller or this DPA specifically authorizes the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires Processor to process or disclose personal data, Processor must first inform Controller of the legal or regulatory requirement and give Controller an opportunity to object or challenge the requirement, unless the law prohibits such notice.

c) In granting the rights of the persons concerned in accordance with Art. 15 et seq. GDPR (correction, restriction of processing, deletion, notification and provision of information) the Processor will support the Controller at first request within the scope of its possibilities. The Processor will take appropriate technical and organizational measures for this purpose. The Processor shall, on instruction, correct, delete or restrict the processing of personal data processed on behalf of the Controller.

d) If the data collected on behalf of the Controller is subject to a request for data portability in accordance with Art. 20 of the GDPR, the Processor shall make the data set available to the Controller without delay, upon request, within the set time limit, otherwise within 5 working days, in a structured, common and machine-readable format.

e) When a data subject makes direct contact with the Processor to exercise rights, the Processor shall forward this request to the Controller without delay.

f) The Processor shall inform the Controller without delay if the Processor is of the opinion that an instruction given violates legal regulations. The Processor may suspend the execution of the corresponding instruction until it has been confirmed or modified by the Controller.

g) The Processor shall be obliged to notify the Controller no later than 24 (twenty-four) hours after any breach of data protection regulations, of the provisions made in the Contract and the Agreement and/or instructions given by the persons employed by the Controller or other third parties involved in the processing of data by the Processor.

h) After termination of the Contract, the Processor is obliged to hand over to the Controller all personal data, documents and processed and used results which are in connection with the contractual relationship, as well as to delete them in compliance with data protection and data security regulations and in accordance with the instructions.

i) The Processor shall ensure that employees and other persons working for the Processor involved in the processing of the Controller's data are prohibited from processing the data except on the instructions of the Controller. Furthermore, the Processor guarantees that the persons authorized to process personal data have committed themselves to confidentiality or are subject to an appropriate statutory obligation of secrecy. The confidentiality/non-disclosure agreement remains in force even after it has been terminated.

§ 6 Place of service

a) The processing and use of the data take place exclusively in a member state of the European Union or in another contracting state of the DPA on the European Economic Area. Any transfer to a third country shall require the prior consent of the Controller and may only take place if the special conditions laid down in Articles 44 et seq. GDPR are fulfilled.

b) If the processing of personal data is carried out outside the EU, the Processor guarantees that the special conditions laid down in Articles 44 et seq. GDPR are fulfilled. This is the case, on the one hand, if and to the extent that the EU Commission has certified an appropriate level of protection for the latter. Furthermore, if the processing of personal data outside the EU takes place exclusively within the framework of a program that has been certified by the EU Commission as having an

appropriate level of protection, and if it fulfills the formal and substantive prerequisites required for participation in the program, if it has qualified for this purpose and if it remains uninterruptedly qualified for the program during the duration of the contract.

§ 7 Subcontracting

a) The Controller agrees that the Processor may involve subcontractors and authorizes the use of the subcontractors list as described in § 7h of this DPA.
b) The Processor shall be responsible for all acts and omissions of appointed subcontractors. The Processor will communicate the name, address and field of activity as well as the purpose of the contract in writing or in text form to the Controller. The Controller has the right to convince themselves of the suitability of the subcontractor.
c) Where a subcontractor is involved, a level of protection comparable to that provided for in this DPA shall be ensured at all times. However, the Processor shall at all times remain responsible for any act or omission of the subcontractor commissioned by the Processor in the same way as the Processor is responsible for the Processor's own acts and omissions.
d) In the contract with the subcontractor, the Processor shall ensure that the provisions contained in this DPA shall also apply in their entirety to the contract with its subcontractors. This includes, in particular, the obligation to maintain confidentiality, the guarantee of technical and organizational measures to ensure an appropriate level of processing security, the participation in the processing of inquiries from interested parties and the fulfillment of the agreed documentation obligations.
e) The Processor shall regularly verify compliance with the obligations of the subcontractor. In particular, the Processor shall check in advance and on a regular basis during the term of the DPA that the subcontractor has taken the promised and required technical and organizational measures to protect personal data.
f) The Processor will terminate any access to Controller Data promptly when such access is no longer required (including upon termination of subcontractors and personnel).
g) Processor will notify the Controller of any change in subcontractors at least 15 ("fifteen") days before any services of the new subcontractor are used. The Controller has the right to object to the use of new subcontractors resulting in either Processor not using the new subcontractors or the Controller's right to terminate the Contract.
h) A list of the subcontractors the Processor is currently cooperating with in the performance of the Contract can be found here: https://www.condens.io/subprocessors The subprocessors relevant for processing data on behalf of the Controller are listed under "Infrastructure Subprocessors".

§ 8 Technical and organizational measures

a) The Processor is obliged to comply with the principles of proper data processing pursuant to Art. 32 in conjunction with Art. 5 para. 1 GDPR. The Processor will take all necessary measures to secure the data or the security of the processing, in particular taking into account the state of the art, as well as to reduce possible adverse consequences for the affected parties. Measures to be taken include, in particular, measures to ensure appropriate pseudonymization or encryption, measures to protect the confidentiality, integrity, availability and resilience of systems and measures to ensure continuity of processing after incidents.

§ 9 Records

The Processor will keep accurate and up-to-date written records regarding any processing of Personal Data it carries out for the Controller.

§ 10 Liability/Contractual Penalty

a) The Processor shall be liable to the Controller in accordance with the statutory provisions for all damages arising from culpable breaches of this DPA, as well as from the statutory data protection provisions applicable to it, which the Processor, its employees or those appointed by the Processor cause in connection with the performance of the contractual service.
a) The liability in the case of damages to a person as a result of inadmissible or incorrect data processing is handled according to Art. 82 GDPR. The Processor shall indemnify the Controller internally against all claims for damages asserted against the Controller due to a culpable breach of the obligations arising from this contract by the Processor.

§ 11 Miscellaneous

a) Amendments and additions to this DPA must be made in writing and require the express statement that the present provisions will be amended and/or supplemented. This also applies to the waiver of this formal requirement.
b) Should a provision of this DPA be or become invalid or unenforceable, the remaining provisions of this DPA shall remain unaffected. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision that comes closest to the purpose of the replacement provision.
c) This DPA is subject to German law and German jurisdiction.

Annex 1 - Technical and Organizational Measures

	Requirements	Minimum Controls
1.	**Physical Access Controls** preventing unauthorized persons from getting physical access to the information systems, data processing devices and to confidential files, including:	● Processor doesn't operate any hardware for hosting or data storage, instead trusted ISO 27001/27017 certified sub-processors are used. ● The server facilities of these subprocessors require badge and/or biometric access and have 24x7 Security Guards and CCTV. ● Access to the subprocessor facilities is managed by the subprocessor security team and is only authorized to personnel with a business need.
2.	**Logical Access Controls** preventing data processing systems from being used without authorization, including:	● A formal access management process to request, review and approve assignment of access privileges based on least-access principles. ● Access to production systems is controlled and maintained by Processor's security team. ● Access is role-based and granted after demonstrated business need.
3.	**Data Access Controls** ensuring that users who are entitled to use a data processing system have access only to the data to which they have a right to access, including:	● Access to the environment is role-based and access rights are maintained by the Processor information security team which monitors access usage through access logs. ● Access privileges are enforced using technical access restrictions.
4.	**Transmission Controls** ensuring that personal data cannot be read, copied, modified or deleted without authorization during the electronic transmission, transport or storage, including:	● Processor´s production environment is logically separated from the Processor´s other environments. ● Data communications between facilities and into facilities occur only via secure channels ● Processor maintains a change management system to submit, authorize, and review any changes made in the production environment. ● Encryption of any storage and transmissions of passwords, usernames, access credentials and other sensitive data. ● Processor (or Processor's subprocessors) maintains a log management system and monitors for changes 24/7.
5.	**Input Controls** ensuring the assessment of who has entered, modified or removed any data from the system, including:	● Processor maintains access logs to monitor access to the production systems. ● All raw log data is stored for 12 months. ● Monitoring system alerts are configured to notify management of any potential system configuration issues. Identified issues are resolved by the Operations team or monitoring system. An Intrusion Detection System (IDS) and Security Incident and Event Management (SIEM) has been configured to notify Security personnel of any potential security events. High priority alerts are reviewed by Security personnel and appropriate action is taken. Physical and logical user access logs are restricted to authorized personnel.

6.	**Job Controls** ensuring that in case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the data exporter, including:	● Binding policies and procedures for the Processor's employees ● There are procedures in place that formalize data processing ● Processor personnel with access to production systems are required to follow applicable Instructions.
7.	**Availability Controls** ensuring that no accidental loss or destruction of electronic data files and data mediums can take place, including:	● Production systems are monitored 24/7 to ensure the integrity and availability of data. ● Processor performs daily backups which are tested regularly.
8.	**Segregation Controls** guaranteeing that personal data is separated from other data and systems so that no accidental use of the data for another purpose is possible, including:	● Processor enforces logical segmentation and encryption of customer data.