Data Processing Agreement within the EU

1. The parties listed in Annex I enter into this Data Processing Agreement in order to protect personal data and to comply with Article 28 (3) and (4) of Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR).

2. The following Annexes and Annexes form an integral part of this Data Processing

   Agreement: Annex: Standard contractual clauses between controllers and processors pursuant to Article 28 (7) of Regulation (EU) 2016/679 pursuant to Commission Implementing Decision (EU) 2021/915 of 4 June 2021 ("Standard Contractual Clauses")

   Annex I: List of Parties

   Annex II: Description of Processing

   Annex III: Technical and organisational measures, including to ensure the security of the data

   Annex IV: List of sub-processors

3. In addition to and provided that the following provisions do not directly or indirectly contradict the Standard Contractual Clauses or curtail the fundamental rights or freedoms of the data subjects, the parties agree as follows:

4. This Data Processing Agreement supersedes and replaces all previous Data Processing agreements between the parties.

5. Insofar as other agreements between the Client and the Contractor result in other agreements for the protection of personal data, this contract for order processing shall take precedence, unless the parties expressly agree otherwise.

6. This data processing agreement is subject to German law. For all disputes arising from this Data Processing Agreement, the place of jurisdiction shall be Böblingen, Germany.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 .

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 .

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

Docking Clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1 Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4 Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data

against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 . At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7 Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 Days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 .

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8 International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil

a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would

result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller’s obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I: LIST OF PARTIES

Controller(s): [Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]

Name	Customer, user of the service
Adress	Details according to registration
Contact person's name, position and contact details	Details according to registration
Contact details of the data protection officer, if applicable	
accession date	Date of registration in the portal
Signature	

Processor(s): [Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer]

Name	1cc GmbH
Adress	Max-Eyth-Str. 35, 71088 Holzgerlingen
Contact person's name, position and contact details	Meike Ruoff, Geschäftsführerin E-Mail: info@1cc-consulting.com
Contact details of the data protection officer, if applicable	Michael Weinmann E-Mail: michael.weinmann@dsb-office.de, Tel.: 0173-7632962
accession date	
Signature	

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

- Users of the compliance management platform
- Persons whose legitimation data is stored for the purpose of reporting, in particular heads of the responsible body

Categories of personal data processed

- Details of the persons who are the subject of the reports (in particular heads of the responsible body)
- Data on users of the compliance management platform such as name, username, permissions, authentication data.
- Data on the use of the compliance management platform (log files, actions in connection with the use of information such as information entered, IP addresses in connection with the call to the web service, timestamps of use)

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- Not relevant

Nature of the processing:

- Within the framework of the compliance management platform, all types of processing pursuant to Art. 4 No. 2 GDPR are relevant. In particular, the collection of information on the entity responsible for the report and the content of reports, the storage of the information and the transmission to the respective registration authorityPurpose(s) for which the personal data is processed on behalf of the controller

Purpose(s) for which the personal data is processed on behalf of the controller

- Implementation of the reports to fulfill the legal compliance requirements

Duration of the processing

- - The duration of this contract (term) corresponds to the term of the service agreement
- - Notwithstanding the preceding paragraph, the contract shall apply for as long as the Contractor processes the Client's personal data (including backups).

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

M.1 Confidentiality measures

M.1.1 Description of entry control:

- Key management - Key regulation with documentation of the keys (e.g. key book)
- Locking system - Use of a locking system
- Regulations for dealing with visitors - Visitors are received and accompanied.
- Security zones with independent access control - Definition of security zones, for example server rooms, with independent access control

M.1.2 Description of admission control:

- Authentication with user + password - Authentication with user + password
- Careful staff selection - Careful selection of cleaning staff and security staff
- Encryption of data carriers - Encryption of data carriers with state-of-the-art methods
- Firewall - Use of firewalls to protect the network

M.1.3 Description of access control:

- Authorisation concept - Creation and use of an authorisation concept
- Data erasure - Secure erasure of data carriers before reuse (e.g. by multiple overwriting)
- Encryption of data carriers - Encryption of data carriers with state-of-the-art methods
- Encryption of smartphones - Encryption of smartphones with state-of-the-art methods
- Password policy - Password policy, incl. length, complexity and frequency of replacement
- Secure storage - Secure storage of data carriers
- Separation Approval & Authorization Setup - Rights to grant rights is separate from persons who set up rights administratively.

M.1.4 Description of the transfer / transport control:

- SSL/TLS encryption - Use of SSL/TLS encryption when transferring data on the Internet
- VPN tunnel - Set up VPN tunnels for external access to the network

M.1.5 Description of the separation rule:

- Logical client separation - Logical client separation (software side)
- Productive and test system - Separation of productive and test system

M.1.6 Description of the encryption:

- Mobile systems are encrypted - Mobile devices (e.g. notebooks, tablets, phones, USB sticks) are encrypted according to the state of the art.
- Transfer - Encrypted transfer of data (e.g. email encryption according to PGP or S/Mime, VPN, encrypted Internet connections using TLS/SSL, use of FTAPI data transfer tool)

M.2 Integrity measures

M.2.1 Description of the input control:

- Access rights - Personal access rights for tracking access.
- Logging - Logging the entry, amendment and erasure of data
- Personalised usernames - Traceability of the entry, amendment and erasure of data by individual usernames (not user groups)

M.3 Availability and resilience measures

M.3.1 Description of the availability control:

- Air-conditioning system - Air-conditioning system in server rooms
- Antivirus software - Use of antivirus software to protect against malware
- Backup and recovery concept - Creation of a backup and recovery concept
- Emergency IT plan - Preparation and application of emergency IT plans
- Fire extinguishers - CO2 fire extinguishers in server rooms
- Outsource data backup - Storage of data backup at a secure, external location
- Redundant data retention - Redundant data retention (e.g. mirrored hard drives, RAID 1 or higher, mirrored server room)
- Uninterruptible power supply - (UPS) uninterruptible power supply

M.3.2 Description of the rapid recoverability:

- Data recoveries - Regular and documented data recoveries

M.4 Additional data protection measures

M.4.1 Description of the order control:

- Ongoing review - Ongoing review of the contractor and its activities
- Processing contract - Conclusion of a processing contract pursuant to Art. 28 GDPR.
- Selection - Contractor selection from due diligence perspectives (especially with regard to privacy)

M.4.2 Description of the data protection management system:

Appointment of a Data Protection Officer - A Data Protection Officer is appointed and reported to the supervisory authority.

- Privacy management system - Management system for protecting data (e.g. based on ISO 27701)
- Software-based tools - Use of software-based tools to comply with privacy requirements (e.g. audatis MANAGER)
- Training - Training sessions for all authorised employees. Regular follow-up training.
- Binding directive/organisation to meet the legal requirements - To meet the legal requirements, binding regulations have been set out in operational instructions (e.g. data

protection guidelines, process regulations on data protection violations, enquiries from data subjects...).

Comments on the description of the measures:

The servers for operating the compliance management platform are operated by the subcontractor Hetzner Online GmbH. In this regard, explicit reference is made to document https://www.hetzner.com/AV/TOM.pdf .

ANNEX IV: LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).

The controller has authorised the use of the following sub-processors:

- Hosting Web-Server:
  HubSpot, Inc., Two Canal Park, MA 02141, Cambridge, USA
  Suitable guarantees: Standard Contractual Clauses, Registration EU-U.S. DPF

- Automation of the platform
  HubSpot, Inc., Two Canal Park, MA 02141, Cambridge, USA
  Suitable guarantees: Standard Contractual Clauses, Registration EU-U.S. DPF

- Creation of documents and drawing processes
  PandaDoc, Inc.; 3739 Balboa St.; #1083; CA 94121; San Francisco; USA
  Suitable guarantees: Standard Contractual Clauses, Registration EU-U.S. DPF

- Payment services
  Stripe, Legal Process, 510, Townsend St., San Francisco, CA 94103, USA
  Suitable guarantees: Standard Contractual Clauses, Registration EU-U.S. DPF