Data processing agreement

within the meaning of Art. 28(3) of

the General Data Protection Regulation (GDPR)

(version as of 29 June 2020)

between

the client/signatory of the offer

- hereinafter referred to as the "**Controller**" -

and

Crosscan GmbH
Ruhrstr. 48
58452 Witten

- hereinafter referred to as the "**Processor**" -

- hereinafter collectively referred to as the "**Parties**" and each individually as a "**Party**" -

Preamble

By way of an agreement concluded between the Parties (hereinafter referred to as the "**Main Agreement**"), the Controller commissioned the Processor, inter alia, to perform the services as follows*.* In the context of the provision of the services to the Controller, the Processor thereby obtains access to personal data for this purpose.

The subject matter of the agreement/order is as follows:

Crosscan Connect:

- Setup of the Controller, the branches with address, contact person with position, email and phone number
- Evaluation via web interface incl. Advanced KPI - graphical and tabular display of all counting events, PDF standard reports via email, automated

dispatch of daily and weekly reports, permissions-based access control, regulation of access and access authorisations, metadata connection, integration of cash register and personnel data

The Parties therefore conclude this data processing agreement (hereinafter referred to as the "**Agreement**") in order to ensure the lawful collection, processing and use of personal data by the Processor. In this respect, the Agreement specifies the Processor's obligations under data protection law.

§ 1 Scope of application

1.1 The Processor shall collect, process and use personal data on behalf of and on instruction of the Controller for the purpose of fulfilling the contractual obligations incumbent upon the Processor under the Main Agreement. Within the scope of this Agreement, the Controller shall be solely responsible for compliance with the statutory provisions of the data protection laws, including in particular the lawfulness of the transfer of data to the Processor as well as the lawfulness of the data processing ("Controller" within the meaning of Art. 4 No. 7 GDPR).

1.2 The scope and purpose of the collection, processing and use of personal data by the Processor as well as the type of data concerned are set out in **Annex 1** and will be, if necessary, supplemented by corresponding instructions from the Controller. The Processor is not allowed to process or use the personal data for other purposes, in particular to use it for or to disclose it to third parties or to use the personal data for its own purposes.

1.3 The Processor shall document instructions of the Controller. The instructions shall, as a rule, be in writing or in text form. The Controller may amend, supplement or replace its instructions at any time if required.

1.4 If the Processor is of the opinion that an instruction of the Controller violates the GDPR or other Union or Member State data protection provisions, the Processor shall notify the Controller thereof in writing. The Processor shall then be entitled to suspend the execution of the relevant instruction until the Controller confirms or changes the instruction.

§ 2 Duties of the Processor

2.1 The Processor collects, processes and uses personal data within the framework of the Main Agreement and the specific individual instructions of the Controller.

2.2 In connection with the fulfilment of the Controller's obligation to make notifications in accordance with Articles 33 and 34 of the GDPR, the Processor shall notify the Controller in writing without delay in case of violations by the Processor or by the personnel involved by the Processor or by its sub-processors of the data protection regulations in relation to the Controller's personal data or violations of the specifications made in the order. The same shall also apply in the event of loss or unlawful transmission or obtaining of knowledge of personal data and in the event of serious disruptions to the operational process, in case of suspicion of other violations of regulations on the protection of personal data or other irregularities in the handling of the Controller's personal data. This shall also apply in the event of inspections and measures by the supervisory authority pursuant to Art. 58 GDPR as well as if a competent authority investigates the Processor pursuant to Artt. 82, 83 GDPR.

2.3 If the Processor culpably violates its obligations to cooperate or, in addition, fails to comply with its statutory obligations as a processor, fails to comply with instructions lawfully issued by the Controller or acts contrary to such instructions, the Processor shall be obligated to compensate the Controller for the damage resulted therefrom and to indemnify the Controller against any claims asserted against it by third parties as a result of this. This shall not apply if the Processor proves that it is in no way responsible for the circumstance that caused the damage.

2.4 The Processor shall inform the Controller without undue delay about control actions and measures of the supervisory authority insofar as they relate to this Agreement. This shall also apply insofar as a competent authority investigates at the Processor in the context of administrative offence or criminal proceedings with regard to the processing of personal data commissioned by the Controller.

2.5 Insofar as the Controller, for its part, is subject to control by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with the processing commissioned with the Processor, the Processor shall assist the Controller to the best of its ability.

2.6 The Processor shall, taking into account the nature of the processing and the information available to it, assist the Controller free of charge in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR. This shall include, inter alia

a. ensuring an appropriate level of security through technical and organisational measures that take into account the context and purposes of the processing as well as the predicted likelihood and severity of a potential infringement due to security vulnerabilities and allow for the immediate detection of relevant violations,

b. the obligation to notify the Controller without undue delay about personal data breaches,

c. the obligation to assist the Controller in fulfilling its obligation to inform the data subject and, in this context, to provide it with all relevant information without delay,

d. the assistance to the Controller in conducting its data protection impact assessment,

e. the assistance to the Controller in the context of prior consultations with the supervisory authority.

2.7 The Controller shall be entitled at any time to demand the correction, deletion and blocking of personal data. The Processor shall implement corresponding instructions of the Controller without undue delay, unless the Processor has a legal obligation to store the personal data.

2.8 After the end of the provision of the services relating to processing, the Processor shall, in accordance with the Controller's instructions, destroy in a data protection compliant manner or return the personal data or data carriers that were handed over to the Processor for the fulfilment of its obligations under the Main Agreement. Copies or duplicates of the data shall not be made without the Controller's knowledge. This shall not apply to backup copies where they are required to ensure proper data processing or to any data required to comply with statutory retention obligations. After completion of the contractually agreed work or earlier upon Controller’s request - at the latest upon termination of the Main Agreement - the Processor shall hand over to the Controller or, after prior consent, destroy in a data protection compliant matter all documents, processing and utilisation results produced and data files which have come into its possession and which relate to the contractual relationship. The same applies to test and reject material. The protocol of the deletion shall be submitted upon request. Documentation which serves as proof of orderly and proper data processing shall be kept by the Processor beyond the end of the Agreement in accordance with the respective retention periods. The Processor may hand them over to the Controller at the end of the Agreement to discharge the Processor.

2.9 The Processor shall document the data processing and shall, upon request, make the documentation available to the Controller without delay.

2.10 The Processor undertakes to maintain a record of processing activities in accordance with Art. 30(2) GDPR. The record shall be maintained in writing or in an electronic format and shall be presented to the Controller and/or its data protection officer at any time upon request.

§ 3 Technical and organisational measures

3.1 The Processor shall design its internal organisation in such a way that it meets the special requirements of data protection. The Processor shall establish security pursuant to Art. 28(3) lit. c) and Art. 32 GDPR, in particular in connection with Art. 5(1), (2) GDPR. Overall, the measures to be implemented are data security measures and to ensure a level of security appropriate to the risk with respect to the confidentiality, integrity, availability and the resilience of the systems. In this context, the state of the art, the costs of implementation and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32(1) GDPR shall be taken into account. To this end, the Processor shall in particular take the technical and organisational measures defined in **Annex 2** to adequately secure the personal data against misuse and loss.

3.2 The technical and organisational measures are subject to technical progress and further development. In this respect, the Processor may implement alternative adequate measures, provided that the new measures do not fall short of the level of security provided by the specified measures. Substantial changes must be documented and the Controller must be notified in writing. The Processor also undertakes to adapt the technical and organisational measures to the applicable statutory provisions. If the Controller requests a change to the contractually agreed technical and organisational measures, the Parties shall mutually agree on the further procedure. In the event of a change, **Annex 2** shall be adjusted accordingly.

§ 4 Controller’s rights of control

4.1 The Controller shall have the right, before the Processor commences the data processing and thereafter on a regular basis, to conduct an order control regarding the data processing operations to be carried out by the Processor. The Controller shall have the right to satisfy itself of the Processor's compliance with this Agreement in its business operations by means of spot checks. Within the scope of the order control, the Processor shall make available to the Controller all necessary rights of information, inspection and access. The Processor may make the performance of an on-site inspection dependent on prior notification with an appropriate lead time and on the signing of a confidentiality agreement with regard to the data of other customers and the technical and organisational measures set up. Should the auditor appointed by the Controller be in a competitive relationship with the Processor, the Processor shall have a right of objection against such auditor.

4.2 The Processor undertakes to provide the Controller, upon request, with the information required to carry out a comprehensive order control and to make the relevant evidence available. Proof of the implementation of appropriate measures can also be provided by submitting current test certificates as well as reports from independent bodies (auditor, revision, data protection officer, IT security department, etc.).

4.3 If the Controller identifies deficiencies in compliance with the technical and organisational measures within the scope of the order control, the Processor shall remedy the deficiencies without delay. The Processor shall bear the costs required to remedy the deficiencies.

§ 5 Subcontracting

5.1 The Processor may not involve subprocessors without the Controller’s consent. Subcontracting may only be carried out with the prior written consent of the Controller for the individual case. Subcontracting relationships within the meaning of this provision shall be understood to be those services which relate directly to the provision of the main service. This does not include ancillary services used by the Processor including for example telecommunication services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. Also in case of outsourced ancillary services, the Processor is, however, obligated to implement appropriate and legally compliant contractual agreements as well as control measures to ensure data protection and data security of the Controller's data.

5.2 If the Controller consents to the use of a subprocessor, the Processor shall ensure that the same data protection obligations as set out in this Agreement shall be imposed on that subprocessor. At the Controller's request, the Processor shall provide appropriate evidence of the subprocessor’s corresponding obligation. The Processor shall ensure that the subprocessor complies with the technical and organisational measures by obtaining sufficient guarantees from the subprocessor. The Processor shall be liable to the Controller for the performance of the subprocessor’s obligations.

5.3 The Controller consents to the Processor engaging the subprocessors specified in **Annex 3** for the areas of activity described therein.

§ 6 Data secrecy

6.1 The Processor ensures that the persons authorised to process the personal data have committed themselves to data secrecy and confidentiality or are under an appropriate statutory obligation of confidentiality.

6.2 The obligation to maintain data secrecy and confidentiality shall survive the termination of this Agreement.

§ 7 Transmission to non-EEA countries

7.1 The Processor will collect, process and use personal data exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every transfer of data to a state which is not a Member State of either the EU or the EEA shall only occur if the conditions of the statutory provisions are fulfilled and with the separate written consent of the Controller. Deviations from the aforementioned rule are only permitted in the cases specified in Art. 28(3) lit. a) GDPR under the additional conditions mentioned in this provision.

7.2 If the Processor is obligated under the applicable law of a Member State or of the European Union to transfer data to an entity located outside the EEA, the Processor shall, in accordance with its obligation under Art. 28(3) lit. a) GDPR, inform the Controller thereof before the processing, unless the applicable law prohibits such information on important grounds of public interest.

§ 8 Data subjects’ rights

8.1 The Processor may not correct or delete personal data or restrict its processing on its own authority, but only in accordance with documented instructions from the Controller. Insofar as a data subject contacts the Processor directly in this regard, the Processor shall forward this request to the Controller without delay.

8.2 The Processor shall, at the Controller's request, assist the Controller to the best of its ability in fulfilling the rights of the data subjects, in particular with regard to the right to be forgotten and the right to data portability.

§ 9 Data protection officer

The Processor has designated a data protection officer. At the time of the conclusion of the contract this is:

Dipl. Inform. Olaf Tenti
GDI
Gesellschaft für Datenschutz und Informationssicherheit mbH
Fleyer Str. 61
58097 Hagen
Phone: + 49 (0) 2331/ 35 68 32 - 0
Email: tenti@gdi-mbh.eu

The Processor shall immediately inform the Controller in writing of any dismissal or designation of a new data protection officer.

§ 10 Duration of the Agreement

10.1 The Agreement shall enter into force with the main agreement and shall be concluded for an indefinite period. The Agreement shall terminate automatically upon termination of the Main Agreement on which the data processing by the Processor is based, without the need for a separate termination of the Agreement.

10.2 All existing data processing agreements shall be fully replaced by this Agreement with its entry into force.

§ 11 Miscellaneous

11.1 Insofar as the data of the Controller is endangered by confiscation or seizure, by insolvency or settlement proceedings or by other events or measures of third parties taken at or towards the Processor, the Processor shall inform the Controller without delay. The Processor will inform all parties involved in this regard without delay that the sovereignty and ownership of the data lies exclusively with the Controller as the "controller" within the meaning of the GDPR.

11.2 In the event of changes to the actual form of the service relationship between the Parties, the Parties shall amend the Annexes accordingly and exchange them by mutual agreement. Upon signature of the amended Annex by the Parties, it shall become effective and replace the previously applicable Annex.

11.3 The Agreement is governed by the law of the Federal Republic of Germany. The place of jurisdiction for all disputes in connection with this agreement is Hamburg.

11.4 Amendments or additions to the Agreement require a written form. This also applies to the waiver of this form requirement.

11.5 Should any provision of this Agreement be or become invalid, this shall not affect the validity of the remaining terms. The invalid provision shall be deemed replaced by a valid provision which comes closest to the commercial purpose of the invalid provision. The above shall apply accordingly in case of a contractual gap.

Witten, 26.10.2021
p. p. Michael Hedtke, COO

Annex 1: Personal data concerned and purpose of the processing
Annex 2: Technical and organisational measures
Annex 3: Approved subprocessors and areas of activities of subprocessors

Annex 1: Personal data concerned and purpose of the processing

The Processor processes the personal data of the following **data subjects**:

- *Contact persons in the branches*
- *Contact person at the head office*

The Processor processes the following **personal data** under the Main Agreement:

- *Controller data: contact person, title, street, house number, postal code, city, phone number*
- *Addresses and other data of employees: name, address, email, telephone number*

Data processing by the Processor is carried out exclusively for the following **purpose**:

- *For contacting according to the service order of the Main Agreement.*

Annex 2: Technical and organisational measures (status: 12 April 2018)

The Processor is obligated to ensure data protection. The Contactor shall implement and maintain the following technical and organisational measures during the term of the Agreement:

1. Physical access control

Appropriate measures to prevent unauthorised persons from gaining access to the data processing equipment, through

- Access control for employees and third parties
- Rules on handling of keys
- Securing the building also outside working hours by alarm system
- Definition of security areas
- Security locks
- Window security (especially ground floor)

2. Electronic access control

Appropriate measures to ensure that those engaged in processing only have access to data covered by their respective access authorisation by means of:

- Rules for user authorisation
- Use of encryption methods
- Firewalls
- Identification and authentication including procedural rules for password assignment (minimum length, special characters, regular change of password)
- Logging of accesses

3. Internal access control

Appropriate measures to prevent unauthorised persons from accessing the data processing systems by means of:

- Automatic deactivation of the user ID if the password is entered incorrectly several times
- Lockability of data processing facilities (rooms, buildings, computer hardware and related equipment)
- Control of files, controlled and documented destruction of data carriers
- Use of encryption methods

4. Disclosure control

Appropriate measures to ensure that, in the event of further transmission of the data (electronically or transport on data carriers), no unauthorised third parties read, delete, modify, copy the data by means of:

- Designation of authorised persons and authorisation policies
- Documentation of the bodies to which transmission is planned and the transmission paths
- Use of encryption methods

5. Input control

The Processor shall ensure that it is possible to check and establish retrospectively whether and when personal data has been entered into data processing systems by means of:

- Proof of the organisationally defined responsibilities for the input at the Processor
- Use of log files

6. Order control

The data processed and used by the Processor may only be processed in accordance with the Controller's instructions. This is ensured by means of:

- Clear contractual provisions
- Verification of compliance with contractual provisions
- Binding policies and procedures that have been approved in advance by the Controller

7. Availability control

Appropriate measures to protect the data against accidental destruction or loss by means of:

- Internal data processing policies and procedures, guidelines, work instructions
- Daily backups
- UPS
- Hard disk mirroring

8. Isolation control

Appropriate measures to ensure the isolated processing of data transmitted or accessed for different purposes by means of:

- Backup of data
- Setting up anti-virus/firewall systems

9. Pseudonymisation and encryption

Measures for pseudonymisation and encryption

10. Measures to restore the availability and access to personal data in the event of a physical or technical incident in a timely manner

Recovery plan through

- Daily backups
- Mirroring of hard disks

11. Procedures for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

- Annual data protection audit by external company
- Continuous sensitisation of employees with respect to data protection

Annex 3: Approved subprocessors and areas of activities of the subprocessors

Subprocessors (name, legal form, registered office)	**Place of processing**	**Description of service**
Hetzner Online GmbH, Register Court Ansbach, HRB 6089	Industriestr. 25, 91710 Gunzenhausen Email: support@hetzner.com Phone: +49 9831 505 0	Server hosting
Credativ GmbH, Register Court District Court Mönchen-gladbach HRB 12080	Trompeterallee 108 41189 Mönchengladbach Email: info@credativ.de Phone: +49 2166 9901 0	Server maintenance
INX Netzwerktechnik GmbH HRB 108409	Wolfener Straße 32i 12681 Berlin Email:info@inx-netzwerktechnik.de Phone: +49 (0)30 914 279 110	1st level hotline support outside Crosscan office hours