This data protection agreement according to Art. 28 GDPR is concluded between the customer

.....

.....

.....

- »Controller« -

and

BHS Corrugated Maschinen- und Anlagenbau GmbH
Paul-Engel-Str. 1
92729 Weiherhammer

- »Processor« -

as a complement for iCorr® Assist Glasses (iCorr® AG).

1. Subject and term of the Agreement

The following services are commissioned:

☒ Administrative maintenance and support of the IT infrastructure installed at the Controller site
☐ Administrative maintenance and support of terminal devices used by Controller
☒ Maintenance or support of a data processing method with the possibility of access to personal data
☒ Operational processing of personal data within the context of service provision
☐ Other: _____

Processor will process personal data for Controller within the meaning of Art. 4 (2) and Art. 28 GDPR on the basis of this Agreement. The contracted service will be provided exclusively in a member state of the European Union or the European Economic Area. Any transfer of the service or of part thereof to a country to which the Customer is assigned within the scope of BHS service provision may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled (e.g. Commission's decision on appropriateness, standard data protection clauses, approved rules of conduct).

Term of the commission:

☒ The contract period is based on the main contract.

2. Purpose, extent and nature of the processing, type of personal data and categories of data subjects

The commissioned processing of personal data may only take place for a specific purpose. The purpose, scope and nature of the data are as follows (as defined in Art. 4 No. 2 GDPR): Via the Glasses an audiovisual live connection between customer and supporter is established by means of appropriate software, so that the customer can receive help from the helpdesk. In the course of the support, video and sound are transmitted to the supporter, and recordings can be made of the user's field of vision, which are stored in the system. During the call, the duration of the call is also documented, as well as which images, messages and documents were sent.

Categories of data subjects (as defined in Art. 4 (1) GDPR):

☒ Employee data
☒ Prospect/customer data
☒ Service provider/supplier data

Type of personal data (as defined in Art. 4 (1), (13), (14) and (15) GDPR):
☒ Last name, first name
☒ Address
☒ Phone number
☒ E-mail address
☐ Bank account data
☐ Tax data
☐ Social security data
☒ Communication data (e.g. e-mail, internet, telephone)
☒ Master contract data
☐ Transaction contract data (such as invoicing data and payment data)
☒ Job Title
☐ _____

Special categories of personal data (in accordance with the definition in Art. 9 and 10 GDPR) are not applicable.

3. Rights and obligations as well as instructions of Controller

Controller alone is responsible for assessing the admissibility of processing in accordance with Art. 6 (1) GDPR as well as for protecting the rights of data subjects in accordance with Art. 12 to 22 GDPR. Nevertheless, Processor must forward all such inquiries, provided that they are identifiably directed exclusively to Controller, immediately to Controller. Changes to the processed data and procedural changes must be agreed jointly between Controller and Processor and must be set down in writing or in a documented electronic format. Generally, Controller will issue all processing requests, partial requests and instructions in writing or in a documented electronic format. Verbal instructions must be confirmed immediately in writing or in a documented electronic format. Controller has the right, as stated in number 5 above, prior to the start of the processing and thereafter on a regular basis, to verify the compliance of the technical and organizational measures taken by Processor as well as Processor's compliance with the obligations specified in this Agreement. Controller must inform Processor immediately if it detects any errors or irregularities in verifying the results of the processing. Controller must handle with confidentiality all knowledge of Processor's business secrets and data security measures obtained as part of the contractual relationship. This obligation remains valid even after termination of this Agreement.

4. Controller employees authorized to give instructions and Processor employees authorized to receive instructions

The following Controller employees are authorized to give instructions:

.....

.....

Contractor's agents authorized to receive instructions:
Michael Froschauer, Department Digital Solutions, Project Leader Digital Platform Business

Communication channels to be used for giving instruction:
☒ by post to the following address:
BHS Corrugated Maschinen- und Anlagenbau GmbH, Paul-Engel-Straße 1, 92729 Weiherhammer
☒ by e-mail to the following address:
MFroschauer@bhs-world.com

In the event of a change in or long-term unavailability of a point of contact, the parties must notify each other immediately and in writing or electronically of the replacement or alternate point of contact. Instructions are to be kept on file for the remainder of their validity and thereafter for three full calendar years.

5. Obligations of Processor

Processor must process personal data only in accordance with prior arrangements and the instructions of Controller, unless required to otherwise process the data by European Union or Member State law to which Processor is subject (such as investigations by law enforcement or national security agencies); in such a case, Processor must inform the Controller of these legal requirements prior to processing the data, unless the relevant law prohibits such information on important grounds of public interest (Article 28 (3) sentence 2 (a) GDPR). Processor may not use the personal data provided for processing for any other purpose, particularly for its own purposes. Copies or duplicates of the personal data must not be created without Controller's knowledge. Processor guarantees performance of all the agreed measures for commissioned processing of personal data. Processor guarantees that the data processed for Controller will be strictly separated from other data.

Processor must carry out, at a minimum, the following controls on all data processing performed on Controller's behalf:

☒ Data availability control through, at a minimum, daily data backups

Processor must cooperate to the extent necessary and adequately assist Controller as much as possible in fulfilling the rights of the data subjects per Art. 12 to 22 GDPR, preparing directories of processing activities and conducting the required data protection impact assessments (Article 28 (3) sentence 2 (e) and (f) GDPR). Processor must forward all information required for these purposes immediately to the following parties at the Controller:

☒ The authorized instruction giver named in section 4

Processor must notify Controller immediately if, in its opinion, an instruction given by Controller violates legal provisions (Article 28 (3) sentence 3 GDPR). Processor has the right to suspend the execution of the relevant instruction until it has been confirmed or changed by Controller after verification. Processor must correct, delete or limit the processing of personal data under the contractual relationship if Controller instructs Processor to do so and doing so does not go against the legitimate interests of Processor. Processor may only share information about personal data under the contractual relationship with third parties or the data subject after prior instruction or approval by Controller. Processor hereby agrees that Controller is entitled, generally by appointment, to check compliance with the provisions on data protection and data security as well as the contractual agreements, or to hire a third party to do so, to the appropriate and necessary extent, including but not limited to by obtaining information and access to the stored data and data processing programs as well as through on-site audits and inspections (Art. 28 (3) sentence 2 (h) GDPR). Processor assures that it will support such checks to the extent necessary. The processing of data in remote/home-office employees of Processor is permitted only with the consent of Controller. To the extent that data is processed in the described manner, this was previously regulated in a separate agreement between BHS Corrugated and the respective employees. The measures under Art. 32 GDPR are to be ensured in this case as well. The processor confirms that he is familiar with the relevant data protection regulations of the GDPR for the contract data processing. Processor agrees to maintain confidentiality in the commissioned processing of Controller's personal data. This obligation continues after the end of the Agreement. Processor guarantees that it will familiarize employees involved in the execution of the work with the data protection rules relevant to their job before commencing the activity and require them to maintain confidentiality during as well as after termination of their employment (Art. 28 (3) sentence 2 (b) and Art. 29 GDPR). Processor will supervise compliance with the data protection regulations within its operation.

☒ The following person is the designated data protection officer for Processor:
Last name, first name: Dr. Kraska, Sebastian
Organizational unit: IITR GmbH
Contact information: Tel: +49 89 1891 7360, E-Mail: skraska@iitr.de
Any changes in the identity of the data protection officer are to be communicated to Controller immediately.

6. Notification obligations of Processor in case of processing disruptions and personal data breaches

Processor must inform Controller immediately of any disruptions, violations by Processor or persons employed by Processor of data protection provisions or provisions established in processing requests, and any suspected data breaches or irregularities in the processing of personal data. This applies especially to any reporting or notification obligations of Controller under Art. 33 and Art. 34 GDPR. Processor agrees to adequately support Controller in performing its duties under Art. 33 and 34 GDPR if necessary (Art. 28 (3) sentence 2 (f) GDPR). Notifications pursuant to Art. 33 or 34 GDPR on behalf of Controller may be issued by Processor only after prior instruction in accordance with section 4 of this Agreement.

7. Relationships with subcontractors for core services (Article 28 (3) sentence 2 (d) GDPR)

☒ Processor may engage future subcontractors for processing controller data **without separate approval** from Controller (Art. 28 (2) sentence 2 GDPR). Processor must ensure that the subcontractor is carefully selected with due regard for the suitability of the technical and organizational measures taken by the subcontractor in accordance with Art. 32 GDPR. The relevant audit documentation is to be made available to Controller on request. In this case, Processor must always inform Controller of any intended changes concerning the addition or replacement of other processors.

Subcontractors in third countries may only be engaged if the special requirements of Article 44 et seq. GDPR are met (adequacy decision of the Commission, standard data protection clauses, approved codes of conduct, etc.).

Processor must contractually ensure that the rules agreed between Controller and Processor also apply to subcontractors. The subcontractor agreement must be worded in such a way that the responsibilities of Processor and the subcontractor are clearly separated. If several subcontractors are used, this also applies to the responsibilities between these subcontractors. In particular, Controller must be entitled, if necessary, to carry out, or hire third parties to carry out, appropriate audits and inspections, including on-site, of subcontractors. The subcontractor agreement must be in writing, including in electronic form (Art. 28 (4) and (9) DS-GVO). Data may be forwarded to the subcontractor only if the subcontractor has fulfilled the obligations under Art. 29 and Art. 32 (4) GDPR with regard to its employees.

Processor must verify compliance with the obligations of the subcontractor(s) as follows:

☒ Regular examination of the technical and organizational measures implemented by the subcontractor (at least every 2 years)

The result of these checks must be documented and made available to Controller upon request.
Processor is liable to Controller for the subcontractor's compliance with the data protection obligations contractually imposed by Processor in accordance with this section.

Currently,

☒ the subcontractors listed in Annex 1 are engaged by Processor fort he processing of personal data tot he extent specified therein.
Controller agrees to the engagement of the subcontractos listed in Annex 1.

Processor must always inform Controller of any intended changes concerning the addition or replacement of subcontractors. Controller will be given the opportunity to object to such changes, provided that the technical and organizational measures agreed to date and promised by Processor cannot be fully guaranteed (Art. 28 (2) sentence 2 GDPR). In this case, the intended change is not allowed.

8. Technical and organizational measures according to Art. 32 GDPR (Article 28 (3) sentence 2 (c) GDPR)

A level of security appropriate to the risk for the rights and freedoms of natural persons whose data is subject to processing must be guaranteed. For this purpose, the protection objectives of Art. 32 (1) GDPR, such as the confidentiality, integrity and availability of the systems and services and their resilience in terms of the nature, extent, circumstances and purpose of the processing, must be taken into account in such a way that appropriate technical and organizational remedial measures are taken to permanently reduce the risk. An appropriate and comprehensible methodology that takes into account the likelihood and severity of the risks to the rights and freedoms of the data subjects must be used to assess the risk of the commissioned processing of personal data. The data protection policy described in Annex 2 details the minimum requirements of the technical and organizational measures appropriate to the identified risk, taking into account the protection objectives based on current technology and with special consideration of the IT systems and processes used by Processor. It also describes the procedure for periodically auditing, measuring and evaluating the effectiveness of the technical and organizational measures to ensure compliance with data protection standards.

The following options for demonstrating compliance through certification exist:

☒ Processor must audit, measure and evaluate the effectiveness of its technical and organizational measures to ensure the safety of the processing as needed but at least annually (Article 32 (1) (d) GDPR). The results, along with the complete audit report, must be communicated to Controller on request. Security-relevant decisions regarding the organization of data processing and the procedures used must be agreed upon between Processor and Controller. If the measures taken by Processor do not meet the requirements of Controller, Processor must inform Controller immediately. The measures taken by Processor may be adapted to technical and organizational developments over the course of the contractual relationship but must not fall below the agreed standards. Significant changes must be agreed upon between Processor and Controller in documented form (printed or electronic). Such arrangements are to be kept on file for the duration of this Agreement.

9. Obligations of Processor after the end of commissioned processing (Art. 28 (3) sentence 2 (g) GDPR)

Upon completion of the contractual work, all data, records and processing or use results related to the contractual relationship either in the possession of Processor or its subcontractors must be:

☐ deleted or destroyed by Processor or a hired party in accordance with data protection laws as described below:
Personal data is deleted from the iCorr® AG system as follows: iCorr® AG user accounts are removed in the iCorr® AG administration area by iCorr® AG product management. The deletion or destruction must be confirmed to Controller, including the date, in writing or in a documented electronic format.

10.Miscellaneous

Any special arrangements regarding technical and organizational measures as well as control and audit documentation (including with regard to subcontractors) must be kept on file by both contracting parties for the remainder of their validity and thereafter for three full calendar years.Collateral agreements must generally be set down in writing or a documented electronic format. The court of jurisdiction is the local competent court of Controller. Should the ownership or the personal data of Controller to be processed by Processor become endangered as a result of third-party measures (such as seizure or attachment), bankruptcy or settlement proceedings or other events, Processor must notify Controller immediately. Processor may not invoke the right of retention within the meaning of section 273 of the German Civil Code (BGB) with regard to data processed for Controller or the associated data carriers. Should individual parts of this Agreement be ineffective, this does not affect the validity of the rest of the Agreement.

Annex 1 – Subcontractors
The following subcontracting relationships currently exist in connection with order processing:
TeamViewer Germany GmbH, Bahnhofsplatz 2, 73033 Göppingen: Provider of the software, via which the audiovisual support is provided.

Annex 2 – Technical and organizational measures/data protection policy
The policy describes the measures that Processor must take with regard to commissioned processing to ensure the safe the handling of personal data. The requirements of Articles 24, 25 and 32 GDPR are taken into account where applicable.

1. Confidentiality

1.1 Entry control

The rooms in which personal data are processed or data processing systems are installed may not be freely accessible. They must be locked when employees are away. Entry authorizations must be assigned in a regulated procedure on a need-to-know basis and are generally monitored in terms of whether they are necessary. Rooms in which data processing systems (datacenter, server, network distributor, etc.) are located must have particular entry protections and may be accessible only to employees in IT administration (management, if necessary). Alternately, the devices must be stored in suitable and locked cabinets. Visitors and non-company individuals must be registered in a documented procedure and monitored while visiting the offices.

The company has implemented the requirement as follows:

☒ Locked building
☒ Locked offices
☒ Electronic security locking system
☒ Mechanical security locking system
☒ Documented key assignment process
☒ Visitor registration
☒ Area-dependent authorization IDs
☒ Locked server rooms with electronic entry control
☒ Locked server cabinets
☒ Alarm system for building / offices
☒ Alarm system for server room
☒ Electronic entry control

1.2. Access control

For every network user, a personally assigned user must be set up with a minimum 10-digit password featuring both uppercase and lowercase letters, numbers, and special characters. The system must require users to change passwords at least every 90 days. Network users are to be required to comply with the user access policy in a manner subject to documentation. Creating, changing, and removing access authorizations must occur in a documented procedure. The establishment, modification and withdrawal of system access authorization must follow a documented procedure.
Established system access authorizations must be regularly reviewed for their necessity and the review documented. Network access must be monitored and logged, including unsuccessful login attempts. Network access must be automatically blocked by the system after 10 failed attempts.

The company has implemented the requirement as follows:

☒ Password convention with complex password having a minimum 12/16 of characters
☒ Central authentication with user name and password
☒ Blocking access after repeated failed attempts of logging in
☒ Encrypted Notebooks
☒ Secure link for external access
☒ Use of an updated firewall
☒ Use of a Mobile Device Management Software

1.3 Usage control

A documented, role-based authorization concept must be provided for use of personal data which limits the use so that only authorized individuals can use the personal data necessary for their task (De Minimis Principal). The password rules for access control must also be followed for usage control.
Administrative activities must be limited to a small group of administrators. Administrator activities must be monitored and logged to the extent that the effort involved is technically supportable.

The company has implemented the requirement as follows:

☒ Role-based authorization concept
☒ User-dependent authentication with username and password
☒ Logging of user usage
☒ Assignment of authorizations only after approval by the data owner
☒ Administrative users are kept to a minimum and documented

1.4 Pseudonymization

Evaluations must be pseudonymized in so far as the connection to the individual is not absolutely necessary for the result.

The company has implemented the requirement as follows:

☒ Client separation within the data processing system
☒ Separation of production and test systems

2. Integrity

2.1 Transfer control

Transfer control requires that only authorized individuals can inspect the personal data. For transmission by e-mail, appropriate protective measures (e.g., encryption of communication between the e-mail servers) are required. Mobile devices or mobile storage media must be encrypted if personal data are stored on them.

The company has implemented the requirements as follows:

☒ VPN connections
☒ Dedicated lines
☒ Prohibition of the use of mobile storage media

2.2 Input control

It must be possible to assign the input, change, and deletion of personal data to the acting employee. The system must limit the change and deletion of datasets in order to effectively prevent accidental change or deletion.
The company has implemented the requirements as follows:

☒ Traceability of inputs, changes, and deletions by personalized users
☒ Traceability in assigning, changing, and deleting user authorizations
☒ Monitoring and logging automated data processing
☒ Random check of automated data processing

2.3 Commissioned processing control

As part of commissioned processing control, commissioned data processing operations can only be carried out on the instructions of Controller. For this purpose, employees tasked with data processing must be trained and instructed on how to perform this task. Commissioned processing must be monitored through internal controls. The results of the controls must be documented. Subcontractors may only be hired on the basis of the rules agreed upon with Controller.

Transmission or access to personal data may not take place until the subcontractor has signed a commissioned processing agreement in accordance with Article 28 GDPR and has confirmed compliance with the data protection policy. Processor’s obligation to audit its subcontractors results from the commissioned processing agreement established with Controller.

The company has implemented the requirement as follows:
☒ No use of processors that are not subject to obligations imposed in accordance with Article 28 GDPR.

3. Availability and reliability
Personal data must be processed on data processing systems that are subject to regular and documented patch management. No systems may be linked on the network that are outside of the manufacturer's maintenance cycles (especially not any Windows XP, Windows Server 2003, etc.). Security-related patches must be installed within 72 hours after being announced. Continuous availability of personal data must be guaranteed by means of redundant storage media and backups according to the latest technical standards. Data centers and server rooms must be state of the art (temperature control, fire protection, water penetration, etc.). Servers must have uninterrupted power supply (UPS) ensuring controlled shutdown without any loss of data.

The company has implemented the requirement as follows:
☒ Regular documented patch management for servers
☒ Installation of security-critical patches within 72 hours
☒ Data storage on storage system
☒ Physically separate redundant data storage
☒ Uninterrupted power supply
☒ Redundant climate control for servers
☒ Early fire detection

4. Procedures for periodic auditing, measurement and evaluation
A procedure must be implemented for reviewing data protection in the company. It must include the obligation of employees to maintain data secrecy, training and education of employees, and regular auditing of data processing procedures. The processing procedure performed for the Controller must also be documented before data processing begins. A complete reporting and management process must be introduced for data breaches and the protection of data subjects' rights. It must also include notification of the Controller.

The company has implemented the requirement as follows:
☒ Appointment of a data protection officer