

This Data Protection Agreement is entered into between the Customer

- "Client" -

and

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

- "Processor" -

closed.

- iCorr® Digital Hub (DH)
- iCorr® Operations Support (OS)
- iCorr® Assist Glasses (AG)
- iCorr® Shop
- iCorr® Control Tower (CT)
- iCorr® Apps
- iCorr® MOS

1. Subject matter and duration of the agreement

The order includes the following:

	iCorr® DH	iCorr® OS	iCorr® AG	iCorr® Shop	iCorr® CT	iCorr® Apps	iCorr® MOS
Administrative maintenance and support of the IT infrastructure installed at the client's premises.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Administrative maintenance and support of the end devices used by the client	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Maintaining or supporting a data processing process with the possibility of accessing personal data	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Operational processing of personal data in the context of the provision of services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
The service (remote access via VPN) is an online service for BHS CORRUGATED machines, computers, automation devices (Siemens S7), drives (ELAU Max4 controllers) and possibly future technical devices of the aforementioned type, if technically possible and desired.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

In doing so, the processor processes personal data for the client within the meaning of Art. 4 No. 2 and Art. 28 GDPR on the basis of this contract.

The contractually agreed service is provided exclusively in a member state of the European Union or in a state party to the Agreement on the European Economic Area. Any relocation of the service or part of the work to a country to which the customer is assigned as part of the BHS service provision may only take place if the special requirements of Art. 44 et seq. GDPR are met (e.g. adequacy decision of the Commission, standard data protection clauses, approved rules of conduct).

Duration of the job:

The term of the contract depends on the respective main contract.

2. Purpose, scope and type of processing, type of personal data and categories of data subjects

The processing of personal data on behalf of the individual is exclusively for a specific purpose. The purpose, scope and nature are as follows (as defined in Art. 4 No. 2 GDPR):

	Purpose of the processing of personal data
iCorr® DH	- User authentication and authorization
iCorr® OS	- User authentication and authorization - E-mail notifications (alerting) to defined groups of people
iCorr® AG	- User authentication and authorization - Transmission of video and sound recordings to the supporter - Call logging
iCorr Shop	- User authentication and authorization - Electronic order processing via the iCorr Shop
iCorr® CT	- User authentication and authorization - Sending notifications - Logging Purposes
iCorr® Apps	- User authentication and authorization
iCorr® MOS	- User authentication and authorization - E-mail notifications (alerting) to defined groups of people - Sending notifications - Work Order Management - Parts Management

Categories of data subjects (according to the definition of Art. 4 No. 1 GDPR):

	iCorr® DH	iCorr® OS	iCorr® AG	iCorr® Shop	iCorr® CT	iCorr® Apps	iCorr® MOS
Employment data	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Prospect / customer data	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service Provider / Supplier Data	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Type of personal data (as defined in Art. 4 Nos. 1, 13, 14 and 15 GDPR):

	iCorr® DH	iCorr® OS	iCorr® AG	iCorr® Shop	iCorr® CT	iCorr® Apps	iCorr® MOS
Last name, first name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Address	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Telephone number	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
E-mail address	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Account	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tax data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Social Security Data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communication data (e.g. email, internet, telephone)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Contract master data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Contract transaction data (e.g. billing data and payment data)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Job Title	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Special categories of personal data (as defined in Articles 9 and 10 of the GDPR) are not applicable.

3. Rights and obligations as well as authority of the client

The client is solely responsible for assessing the permissibility of the processing in accordance with Art. 6 (1) GDPR and for safeguarding the rights of the data subjects under Art. 12 to 22 GDPR. Nevertheless, the Processor is obliged to forward all such inquiries to the Client without delay, provided that they are recognisably addressed exclusively to the Client.

Changes to the object of processing and changes to the process must be jointly agreed between the client and the processor and determined in writing or in a documented electronic format.

As a rule, the Client issues all orders, partial orders and instructions in writing or in a documented electronic format. Verbal instructions must be confirmed immediately in writing or in a documented electronic format.

The Client is entitled, as stipulated in No. 5, to satisfy itself in an appropriate manner of compliance with the technical and organisational measures taken by the Processor and the obligations set out in this Agreement before the start of the processing and on a regular basis.

The Client shall inform the Processor immediately if it discovers errors or irregularities in the examination of the order results.

The Client is obliged to treat confidentially all knowledge of the Processor's trade secrets and data security measures acquired in the context of the contractual relationship. This obligation shall survive the termination of this Agreement.



4. Authorized Persons of the Client, Recipients of Instructions of the Processor

The functions of the client authorised to issue instructions are:

	Functions of the client authorised to issue instructions
iCorr® DH	
iCorr® OS	
iCorr® AG	
iCorr® Shop	
iCorr® CT	
iCorr® Apps	
iCorr® MOS	

The processor's recipients of instructions are:

	Recipients of instructions at the processor
iCorr® DH	Product Owner iCorr® Digital Hub; Digital Solutions Department
iCorr® OS	Product Manager iCorr® Operations Support, Digital Solutions Department
iCorr® AG	Product Manager iCorr® Assist Glasses, Digital Solutions Department
iCorr® Shop	Team Lead eBusiness, Department ITS, Lifecycle Parts E-Commerce
iCorr® CT	Product Manager iCorr® Control Tower, Digital Solutions Department
iCorr® Apps	Product Owner iCorr® Apps, Digital Solutions Department
iCorr® MOS	Product Manager M2P®, Department M2P®

Communication channels to be used for instruction:

	Communication channels
iCorr® DH	- by e-mail to the following address: icorr@bhs-world.com
iCorr® OS	- by e-mail to the following address: operations-support@icorr.io
iCorr® AG	- by e-mail to the following address: icorrassist@bhs-world.com
iCorr® Shop	- by e-mail to the following address: info@icorr.shop
iCorr® CT	- by e-mail to the following address: icorr@bhs-world.com
iCorr® Apps	- by e-mail to the following address: icorr@bhs-world.com
iCorr® MOS	- by e-mail to the following address: icorrmos@bhs-world.com

In the event of a change or a long-term impediment of the contact persons, the successors or representatives must be notified to the contractual partner immediately and in principle in writing or electronically. The instructions shall be kept for their period of validity and thereafter for three full calendar years.

5. Obligations of the processor

The processor processes personal data only within the framework of the agreements concluded and in accordance with the instructions of the client, unless it is obliged to process it differently by Union or national law to which the processor is subject (e.g. investigations by law enforcement or state security authorities); in such a case, the processor shall inform the controller/client of these legal requirements prior to processing, unless the relevant law prohibits such notification on the grounds of an important public interest (Art. 28 (3) sentence 2 (a) GDPR).

The processor does not use the personal data provided for processing for any other purposes, in particular not for its own purposes. Copies or duplicates of personal data will not be made without the knowledge of the Client.

In the area of the processing of personal data in accordance with the order, the processor ensures that all agreed measures will be carried out in accordance with the contract. He assures that the data processed for the client will be strictly separated from other databases.

The processor shall in particular carry out the following checks in its area of responsibility throughout the entire processing of the service for the Client:

Data availability control through at least daily data backup

The processor must cooperate to the extent necessary in the fulfilment of the rights of data subjects under Art. 12 to 22 GDPR by the Client, in the preparation of the records of processing activities and in the necessary data protection impact assessments by the Client and provide the Client with appropriate

support as far as possible (Art. 28 (3) sentence 2 lit. e and f GDPR). He must forward the information required for this purpose immediately to the following department of the client:

The function authorised to issue instructions referred to in number 4

The processor will immediately draw the Client's attention to it if, in its opinion, an instruction given by the Client violates statutory provisions (Art. 28 (3) sentence 3 GDPR). The Processor shall be entitled to suspend the implementation of the corresponding instruction until it is confirmed or amended by the Controller at the Client after review.

The processor must correct, delete or restrict the processing of personal data from the contract relationship if the client requests this by means of an instruction and the legitimate interests of the processor do not conflict with this.

The processor may only provide information about personal data from the contractual relationship to third parties or the data subject after prior instruction or consent by the client.

The Processor agrees that the Client is entitled - in principle by appointment - to monitor compliance with the regulations on data protection and data security as well as the contractual agreements to an appropriate and necessary extent itself or through third parties commissioned by the Client, in particular by obtaining information and inspecting the stored data and the data processing programs, as well as through on-site inspections and inspections (Art. 28 para. 3 sentence 2 lit. h GDPR).

The Processor warrants that it will assist in these checks where necessary.

The processing of data in teleworking or home/home office by employees of the processor is permitted.

The measures under Art. 32 GDPR must also be ensured in this case.

The processor confirms that it is aware of the data protection provisions of the GDPR that are relevant to order processing. The Processor undertakes to maintain confidentiality in the processing of the Client's personal data in accordance with the order. This continues even after the termination of the contract.

The processor assures that it familiarizes the employees employed in the execution of the work with the provisions of data protection that apply to them before commencing their work and that it obliges them to maintain confidentiality in an appropriate manner for the duration of their work as well as after the termination of the employment relationship (Art. 28 para. 3 sentence 2 lit. b and Art. 29 GDPR). The processor monitors compliance with data protection regulations in its company.

The processor is appointed as the data protection officer:

Last name, first name: RA Dr. Kraska, Sebastian

Organizational unit: IITR Privacy Ltd

Contact details: datenschutz@bhs-world.com

Any change of the data protection officer must be communicated to the client as soon as possible.

6. Obligations of the processor to notify in the event of disruptions to processing and personal data breaches

The Processor shall immediately inform the Client of any disruptions or violations by the Processor or the persons employed by the Processor as well as of data protection regulations or the stipulations made in the Order, as well as of the suspicion of data protection violations or irregularities in the processing of personal data. This applies in particular with regard to any reporting and notification obligations of the client under Art. 33 and Art. 34 GDPR. The processor assures that it will provide the Client with appropriate support in its obligations under Articles 33 and 34 of the GDPR if necessary (Article 28 (3) sentence 2 (f) of the GDPR). Reports pursuant to Art. 33 or 34 GDPR for the Client may only be submitted by the Processor after prior instruction pursuant to No. 4 of this contract.

7. Subcontracting relationships with subcontractors for core services (Art. 28 para. 3 sentence 2 lit. d GDPR)

- The future commissioning of subcontractors to process the Client's data is the responsibility of the Processor **without a separate permit** of the client, Art. 28 (2) sentence 2 GDPR. The processor must ensure that it carefully selects the subcontractor, taking particular account of the suitability of the technical and organisational measures taken by the subcontractor within the meaning of Art. 32 GDPR. The relevant test documents shall be made available to the Client upon request. In this case, the Processor shall also always inform the Controller of any intended change in relation to the involvement or replacement of other Processors.

Subcontractors may only be commissioned in third countries if the special requirements of Art. 44 et seq. GDPR are met (e.g. adequacy decision of the Commission, standard data protection clauses, approved rules of conduct).

The processor must contractually ensure that the agreed provisions between the client and the processor also apply to subcontractors. In the contract with the subcontractor, the information must be specified in such a way that the responsibilities of the processor and the subcontractor are clearly demarcated from each other. If several subcontractors are used, this also applies to the responsibilities between these subcontractors. In particular, the client must be entitled, if necessary, to carry out appropriate checks and inspections, including on site, at subcontractors or to have them carried out by third parties commissioned by him.

The contract with the subcontractor must be drawn up in writing, which can also be done in an electronic format (Art. 28 para. 4 and para. 9 GDPR).

The forwarding of data to the subcontractor is only permissible if the subcontractor has fulfilled the obligations under Art. 29 and Art. 32 (4) GDPR with regard to its employees.

The Processor shall verify compliance with the obligations of the Subcontractor(s) as follows:

- Regular review of the data protection concept set up at the subcontractor (at least every 2 years)

The result of the inspections must be documented and made available to the client on request. The Processor shall be liable to the Client for the Subcontractor's compliance with the data protection obligations contractually imposed on it by the Processor in accordance with this Section.

At present, the processor...	iCorr [®] DH	iCorr [®] OS	iCorr [®] AG	iCorr [®] Shop	iCorr [®] CT	iCorr [®] Apps	iCorr [®] MOS
no subcontractors employed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
employs the subcontractors documented in Appendix 1 with the processing of personal data to the extent specified therein. The Client agrees to the commissioning of the subcontractors listed in Appendix 1.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

The Processor shall always inform the Controller of any intended change in relation to the use of new subcontractors or the replacement of existing ones. The client is given the opportunity to object to such changes if the technical and organisational measures previously agreed and assured by the processor cannot be fully guaranteed (Art. 28 (2) sentence 2 GDPR). In this case, the intended change may not be carried out.

8. Technical and organisational measures in accordance with Art. 32 GDPR (Art. 28 para. 3 sentence 2 lit. c GDPR)

A level of protection appropriate to the risk to the rights and freedoms of the natural persons affected by the processing is guaranteed for the specific order processing. To this end, the protection objectives of Art. 32 (1) GDPR, such as confidentiality, integrity and availability of the systems and services as well as their resilience with regard to the type, scope, circumstances and purpose of the processing, are taken into account in such a way that the risk is contained in the long term by means of suitable technical and organisational remedial measures. For the legitimate processing of personal data, an appropriate and comprehensible risk assessment methodology is used, which takes into account the likelihood and severity of the risks to the rights and freedoms of the data subjects.

The data protection concept described in [Appendix 2](#) presents the minimum requirements of the technical and organisational measures in accordance with the identified risk in detail, taking into account the protection objectives according to the state of the art and with special consideration of the IT systems and processing processes used by the processor. The procedure for regularly reviewing, evaluating and evaluating the effectiveness of the technical and organisational measures to ensure data protection-compliant processing is also described.

The following option for proof by certification exists:

- The processor must carry out a review, evaluation and evaluation of the effectiveness of the technical and organisational measures to ensure the security of processing if necessary, but at least annually (Art. 32 para. 1 lit. d GDPR). The result must be communicated to the client "on request". Decisions on the organisation of data processing and the procedures used that are relevant for security must be agreed between the processor and the client. If the measures taken by the processor do not meet the requirements of the Client, the Client shall notify the Client without delay. The measures taken by the processor can be adapted to technical and organisational developments in the course of the contract relationship, but must not fall below the agreed standards. The processor must coordinate significant changes with the client in documented form (in writing, electronically). Such votes shall be retained for the duration of this contract.

9. Obligations of the processor after termination of the order, Art. 28 para. 3 sentence 2 lit. g GDPR

After completion of the contractual work, the processor must delete or have destroyed/destroyed all data, documents and processing or usage results in connection with the contract that have come into its possession and subcontractors as described below:

	Handling of data after the end of the order
iCorr® DH	- iCorr® Digital Hub users will be deleted from user management.
iCorr® OS	- iCorr® OS users are removed by the delete function in User Management. - iCorr® OS contacts are removed in the iCorr® OS administration area by the iCorr® or Remote Service Team. - The daily backups of the user database and contact database are kept on a separate physical storage system for 60 days before they are deleted. - BHS OEE App Contacts are overwritten with random names in the OEE App's User Management.
iCorr® AG	- iCorr® AG user accounts are removed in the iCorr® AG administration area by iCorr® AG Product Management.



iCorr® Shop	- iCorr® Shop user accounts are removed in the back office (SAP Hybris administration area) by the Lifecycle E-Commerce team.
iCorr® CT	- Personal data will be deleted immediately upon termination of the contractual relationship.
iCorr® Apps	- iCorr® Apps Users are deleted from User Management.
iCorr® MOS	- iCorr® MOS user accounts will be removed by the iCorr® MOS Key User.

10. Miscellaneous

Agreements on technical and organisational measures as well as control and audit documents (including those relating to subcontractors) must be retained by both contracting parties for their period of validity and thereafter for three full calendar years.

For ancillary agreements, the written form or a documented electronic format is generally required. The place of jurisdiction is agreed to be the court with territorial jurisdiction for the client.

If the property or the personal data of the Client to be processed by the Processor is endangered by measures taken by third parties (e.g. by seizure or seizure), by insolvency or composition proceedings or by other events, the Processor must inform the Client without delay.

The defence of the right of retention within the meaning of Section 273 of the German Civil Code (BGB) is excluded with regard to the data processed for the Client and the associated data carriers.

Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of the agreement.

_____ the _____
Place of the client, date

For the client:

Name: _____


Position: _____

Signature: _____

For the processor:

Name: Lars Engel

Position: Manager

Signature: 



Appendix 1 – Subcontracting

Subcontracting & Subcontractors	
iCorr® DH iCorr® Apps	<p>Currently, the following subcontracting relationships exist in connection with order processing:</p> <ul style="list-style-type: none"> - Cloud provider that provides the environment for the operation of the iCorr® Apps: Amazon Web Services Emea Sàrl 38, Avenue John F. Kennedy L-1855 Luxembourg Luxembourg - Provision and operation of a cloud-based platform and system infrastructure for technical support in the provision, operation and use of the client's applications. openpack GmbH Böttgerstr. 40 92637 Weiden Deutschland - Atlassian. Pty Ltd, Ticketing - Office 365 Products
iCorr® OS	<p>Currently, the following subcontracting relationships exist in connection with order processing:</p> <ul style="list-style-type: none"> - Cloud provider Amazon Web Services Emea Sàrl 38, Avenue John F. Kennedy L-1855 Luxembourg Luxembourg - Cloud provider Microsoft Corporation 1 Microsoft Way Redmond, WA 98052 United States - Atlassian. Pty Ltd, Ticketing - Office 365 Products

<p>iCorr® AG</p>	<p>Currently, the following subcontracting relationships exist in connection with order processing:</p> <ul style="list-style-type: none"> - Providers of the software through which audiovisual support is provided: TeamViewer Germany AG Bahnhofsplatz 2 73033 Göppingen Germany - Cloud provider that provides the environment for authenticating users: Microsoft Corporation 1 Microsoft Way Redmond, WA 98052 United States
<p>iCorr® Shop</p>	<p>Currently, the following subcontracting relationships exist in connection with order processing:</p> <ul style="list-style-type: none"> - Development: DotSource E-Commerce & Digitalagentur GmbH Goethestraße 1 07743 Jena Germany - Cloud provider that provides the environment for authenticating users: Microsoft Corporation 1 Microsoft Way Redmond, WA 9805 United States - Cloud provider that provides the environment for the operation of the iCorr® Shop Tower: SAP Deutschland SE & CO. KG Hasso-Plattner-Ring 7 69190 Walldorf - Atlassian, Ticketing

<p>iCorr® CT</p>	<p>Currently, the following subcontracting relationships exist in connection with order processing:</p> <ul style="list-style-type: none"> - Cloud provider that provides the environment for the operation of the iCorr® Control Tower: Amazon Web Services, Inc. 410 Terry Avenue North Seattle, WA 98109-5210 United States - Cloud provider that provides the environment for authenticating users: Microsoft Corporation 1 Microsoft Way Redmond, WA 98052 United States
<p>iCorr® MOS</p>	<p>Currently, the following subcontracting relationships exist in connection with order processing:</p> <ul style="list-style-type: none"> - Software hosting partners : Hexagon AB (Publ) Lilla Bantorget 15 SE-103 59 Stockholm Sweden - Implementation partners: aomation GmbH Schloßstraße 8f 22041 Hamburg Germany - Cloud provider that provides the environment for authenticating users: Microsoft Corporation 1 Microsoft Way Redmond, WA 98052 United States - Atlassian. Pty Ltd, Ticketing - Office 365 Products (Excel, Word, PowerBI)

In addition to the subcontractors mentioned above, the companies affiliated with the processor within the meaning of Section 15 of the German Stock Corporation Act ("BHS Group") are also among the subcontractors that may be used.

Appendix 2 – Technical and Organizational Measures / Data Protection Concept / August 2025

This data protection concept describes the requirements and implementation of the measures for the secure and data protection-compliant processing of personal data. In doing so, the requirements of Articles 24, 25 and 32 of the GDPR are taken into account to the extent applicable.

1. Confidentiality

1.1 Access control

The rooms in which personal data is processed or data processing equipment is installed must not be freely accessible. They must be locked when employees are absent. Access authorisations must be assigned in a regulated procedure according to the "need to know principle" and regularly monitored with regard to their necessity. Rooms in which data processing systems (data centre, servers, network distributors, etc.) are housed must be particularly protected and may only be accessible to employees of IT administration (if necessary, management). Alternatively, the devices must be housed in suitable and locked cabinets. Visitors and persons outside the company must be registered in a documented procedure and supervised within the business premises.

The company has implemented the demands as follows:

- | | |
|---|---|
| <input checked="" type="checkbox"/> Implemented access controls for buildings and rooms | <input checked="" type="checkbox"/> Sectoral Credentials |
| <input checked="" type="checkbox"/> Electronic security locking system | <input checked="" type="checkbox"/> Locked server rooms with access control |
| <input checked="" type="checkbox"/> Mechanical security locking system | <input checked="" type="checkbox"/> Locked server cabinets |
| <input checked="" type="checkbox"/> Documented key issuance | <input checked="" type="checkbox"/> Alarm system for buildings / offices |
| <input checked="" type="checkbox"/> Visitor Registration | <input checked="" type="checkbox"/> Alarm system for server room |
| | <input checked="" type="checkbox"/> Electronic access control |

1.2 Access control

For each network user, a user must be set up with a password of at least 10 digits with uppercase and lowercase letters, at least one digit, and at least one special character. Users must be obliged by the system to change the passwords at least every 360 days. Network access must be monitored and logged, including unsuccessful login attempts. Network access must be automatically blocked by the system after 15 failed attempts at the latest.

The company has implemented the demands as follows:

- | | |
|---|--|
| <input checked="" type="checkbox"/> Password convention with complex password with min. 12/16 Sign | <input checked="" type="checkbox"/> Encrypted notebooks |
| <input checked="" type="checkbox"/> Central authentication with username and password | <input checked="" type="checkbox"/> Secure line connection when accessed from external sources |
| <input checked="" type="checkbox"/> Blocking of access after multiple incorrect entry of login data | <input checked="" type="checkbox"/> Use of an up-to-date firewall |
| | <input checked="" type="checkbox"/> Use of mobile device management software |

1.3 Access control

For access to personal data, there must be a documented, role-based authorization concept that restricts access in such a way that only authorized persons can access the personal data necessary for their task (minimum principle). The password regulations from access control must also be implemented within the framework of access control. Administrative activities must be limited to a small circle of administrators. The activities of the administrators must be monitored and logged within the framework of technically justifiable effort.

The company has implemented the demands as follows:

- | | |
|--|---|
| <input checked="" type="checkbox"/> Role-based authorization concept | <input checked="" type="checkbox"/> Administrative users are kept to a minimum and documented |
| <input checked="" type="checkbox"/> Application-related authentication with username and password | <input checked="" type="checkbox"/> Mandatory use of multi-factor authentication (MFA) |
| <input checked="" type="checkbox"/> Logging of user access | |
| <input checked="" type="checkbox"/> Assignment of authorizations only after approval by the data owner | |

1.4 Separation control

The separation of personal data must be ensured by different storage locations or by client separation.

The company has implemented the demands as follows:

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

2. Integrity

2.1 Transfer control

As part of the transfer control, it must be ensured that only authorised persons can take note of the personal data. When transmitting by e-mail, appropriate protective measures (e.g. encryption of communication between the mail servers) must be taken. Mobile devices or mobile storage media must be encrypted if personal data is stored on them.

The company has implemented the demands as follows:

- VPN Connections
- Leased lines
- Prohibition of the use of private storage media

2.2 Input control

It must be possible to assign the input, modification and deletion of personal data to the employee carrying out the work. The modification and deletion of records must be restricted by the system to effectively prevent accidental modification or deletion.

The company has implemented the demands as follows:

- Traceability of entries, changes and deletions by personalized users
- Traceability in the assignment, modification and deletion of user authorizations
- Monitoring and logging of automated data processing
- Random Sampling of Automated Data Processing

2.3 Order control

As part of the order control, it must be ensured that the data processing operations carried out on behalf of the client are carried out exclusively on the instructions of the client. To this end, those involved in data processing must be trained and instructed. Order processing must be monitored by internal controls. The results of the inspections must be documented.

Subcontractors may only be commissioned on the basis of the regulations agreed with the client. The transfer or access to personal data may only take place if the subcontractor has signed a contract processing agreement in accordance with Article 28 of the GDPR and has confirmed compliance with the provisions of the data protection concept. The Contractor's obligation to inspect its subcontractor results from the contract processing agreement concluded with the Client.

The company has implemented the demands as follows:

- No use of processors who have not been obliged under Art. 28 GDPR

3. Availability and resilience

The processing of personal data must take place on data processing systems that are subject to regular and documented patch management. No systems may be connected in the network that are outside the maintenance cycles of the manufacturers (especially not Windows XP, Windows Server 2003, etc.). Security-relevant patches must be applied within 72 hours of notification. The continuous availability of personal data must be ensured by means of redundant storage media and data backups in accordance with the state of the art. Data centers and server rooms must be state-of-the-art (temperature control, fire protection, water ingress, etc.). The servers must have an uninterruptible power supply (UPS) that ensures a regulated shutdown without data loss.

The company has implemented the demands as follows:

- | | |
|---|--|
| <input checked="" type="checkbox"/> Regular documented patch management for servers | <input checked="" type="checkbox"/> Spatially separated redundant data storage |
| <input checked="" type="checkbox"/> Install security-critical patches within 72 hours | <input checked="" type="checkbox"/> Uninterruptible power supply |
| <input checked="" type="checkbox"/> Data storage on storage system | <input checked="" type="checkbox"/> Redundant air conditioning of the servers |
| | <input checked="" type="checkbox"/> Early fire detection |

4. Procedures for periodic review, evaluation and evaluation

A procedure for monitoring data protection in the company must be implemented. This must include the obligation of employees to data secrecy, the training and sensitization of employees and the regular auditing of data processing procedures. Likewise, the documentation of the processing procedure carried out for the client must be carried out before the data processing begins. For data protection violations and the protection of the rights of data subjects, a consistent reporting process and processing process must be introduced. This must also contain the information of the client.

The company has implemented the demands as follows:

- Appointment of a data protection officer