

This Data Protection Agreement, between the customer

- "Client" -

and

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

is concluded as follows.

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

1. Subject and term of the Agreement

The order comprises the following:

	iCorr® DH	iCorr® OS	iCorr® AG	iCorr® Shop	iCorr® CT	iCorr® Apps
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"/>
Administrative maintenance and support of the end devices used at the Client's premises.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Maintenance or support of a data processing procedure with the possibility of access to personal data.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Operative processing of personal data in the context of performing the service.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
The service (remote access by means of VPN) concerns an online service of BHS CORRUGATED machines, computers, automation devices (Siemens S7), drives (ELAU Max4 controller) and possible future devices of the kind named above, if technically possible and requested.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

In the process, the Processor will process personal data for the Client in the sense of Art. 4 No. 2 and Art. 28 GDPR on the basis of this Agreement.

This contractually arranged service will be performed exclusively in a member state of the European Union or in a contracting state of the Agreement on the European Economic Area. Any transfer of the service or partial processing thereof in a country that is allocated to the Client in the context of BHS

service performance may only occur if the special prerequisites of Art. 44 et. seqq. GDPR are fulfilled (e.g. adequacy decision of the Commission, standard data privacy clauses, approved code of conduct).

Term of the contract:

The contract term is determined by the respective main agreement.

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

The processing of personal data by order occurs exclusively for the given purpose.

The purpose, the scope, and the type are as follows (according to the definition of Art. 4 No. 2 GDPR):

	Purpose of processing personal data
iCorr® DH	- Authentication and authorization of user
iCorr® OS	- Authentication and authorization of user - Email notifications (alarming) to a defined set of people
iCorr® AG	- Authentication and authorization of user - Transferring video and sound recordings to the supporter - Logging calls
iCorr Shop	- Authentication and authorization of user - Electronic order processing via the iCorr Shop
iCorr® CT	- Authentication and authorization of user - Sending notifications - Logging purposes
iCorr® Apps	- Authentication and authorization of user

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
Employee data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Potential customer / 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"/>
Service provider / supplier data	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Type of personal data (according to the definition of Art. 4 No. 1, 13, 14, and 15 GDPR):

	iCorr® DH	iCorr® OS	iCorr® AG	iCorr® Shop	iCorr® CT	iCorr® Apps
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"/>
Address	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input 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"/>
Email 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"/>
Account information	<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"/>
Social security data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communications 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"/>
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"/>
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"/>
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"/>

Special categories of personal data (according to the definition of Art. 9 and 10 GDPR) are not applicable.

3. Rights and obligations, as well as authority to issue instructions, of the Client

The Client bears the sole responsibility for judging the permissibility of processing pursuant to Art. 6 para. 1 GDPR and protecting the rights of data subjects under Art. 12 to 22 GDPR. At the same time, the Processor is obligated to forward all inquiries that are recognizable as being directed exclusively to the Client on to the Client without delay. Changes in the subject of processing and process changes shall be coordinated between the Client and the Processor and set in writing or in a documented electronic form. The Client shall generally issue all orders, partial orders, and instruction in writing or in a documented electronic format. Oral instructions must be confirmed in writing or in a documented electronic format without delay. The Client is entitled to obtain conviction of compliance with the technical and organizational measures taken by the Processor and the obligations stipulated in this Agreement as set under No. 5 before the beginning of processing and then regularly in a suitable manner. The Client shall inform the Processor without delay if errors or irregularities are found when checking the results. The Client is obligated to treat all knowledge of trade secrets and data security measures of the Processor gained in the course of the contractual relationship as confidential. This obligation remains in force after the end of this Agreement.



4. Right to issue instructions of the Client, instruction recipient of the Processor

The Client's roles authorized to issue instructions are:

	Client's roles authorized to issue instructions
iCorr® DH	
iCorr® OS	
iCorr® AG	
iCorr® Shop	
iCorr® CT	
iCorr® Apps	

The Processor's recipients for instructions are:

	Processor's recipients for instructions
iCorr® DH	Project Manager 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, ITS Department, Lifecycle Parts E-Commerce
iCorr® CT	Product Manager iCorr® Control Tower, Digital Solutions Department
iCorr® Apps	Product Manager iCorr® Apps, Digital Solutions Department

Communication methods to be used for instructions:

	Communication methods
iCorr® DH	- By email to the following address: icorr@bhs-world.com
iCorr® OS	- By email to the following address: operations-support@icorr.io
iCorr® AG	- By email to the following address: icorrassist@bhs-world.com
iCorr® Shop	- By email to the following address: info@icorr.shop
iCorr® CT	- By email to the following address: icorr@bhs-world.com
iCorr® Apps	- By email to the following address: iCorr@bhs-world.com

In the event of a change or ongoing absence of a contact person, the other contracting party must be informed without delay and told of their successor or substitute in writing or by electronic means. The instructions must be followed for their valid period and subsequently for three full calendar years.

5. Obligations of the Processor

The Processor processes personal data exclusively in the context of the set agreements and according to the instructions of the Client, inasmuch as it is not obligated to perform other processing by the law of the Union or the member states to which the Processor is subject (e.g. decrees from public prosecutors or state officials); in such a case, the Processor shall communicate these legal requirements to the Controller/Client before processing, provided that the law concerned does not prohibit such communication due to an important public interest (Art. 28 para. 3 clause 2 lit. a GDPR). The Processor will not use the personal data submitted for processing for any other purpose, and particularly not for its own purposes. No copies or duplicates of the personal data may be created without the Client's knowledge. In the field of correct processing of personal data, the Processor warrants that all stipulated measures will be performed as contractually stipulated. It warrants that the data processed for the Client will be strictly separated from other data.

The Processor shall particularly conduct the following checks in its field during the whole course of the service for the Client:

- Ensuring data availability through at least daily data backups

In the fulfillment the rights of data subjects pursuant to Art. 12 to 22 GDPR by the Client, the creation of the list of data processing activities and in the event of necessary data protection impact assessments of the Client, the Processor shall cooperate to the necessary extent and shall appropriately support the Client as far as possible (Art. 28 para. 3 clause 2 lit. e and f GDPR). It must also send the necessary information to the following entity of the Client without delay:

- The roles authorized to issue instructions named in clause 4

The Processor will inform the Client without delay if, in its opinion, an instruction issued by the Client would infringe against a statutory provision (Art. 28 para. 3 clause 3 GDPR). The Processor is entitled to delay the execution of such an instruction until it has been reviewed by the Controller of the Client

and confirmed or changed. The Processor shall correct, delete, or restrict processing of personal data from the contractual relationship if the Client requests this by means of an instruction and legitimate interests of the Processor do not prohibit it. The Processor may only give information about personal data from the contractual relationship to third parties or data subjects after previous instruction or approval by the Client. The Processor declares its agreement that the Client - always after scheduling a time - is entitled to check compliance with the provisions of data privacy and data security and the contractual agreements personally or through a third party commissioned by the Client, especially by receiving information and viewing stored data and the data processing programs, as well as through monitoring and inspections on site (Art. 28 para. 3 clause 2 lit. h GDPR). The Processor warrants that it, inasmuch as this is necessary, will cooperate supportively with these inspections. The processing of data in teleworking or home office environments by employees of the Processor is only permitted with the approval of the Client. Provided that the data will be processed in the prescribed manner, this will be regulated in advance in a separate agreement between BHS Corrugated and the employee in question. The measures pursuant to Art. 32 GDPR must also be upheld in this case. The Processor confirms that the relevant data privacy provisions of the GDPR are known to it. The Processor undertakes to maintain confidentiality in processing the personal data of the Client. This will also continue after the end of the Agreement.

The Processor warrants that it will make the employees used for the execution of the works familiar with the provisions of data privacy that are relevant for them before their activities begin and will obligate them to maintain confidentiality for the period of their activities and also after the end of the employment relationship in a suitable manner (Art. 28 para. 3 clause 2 lit. b and Art. 29 GDPR). The Processor shall monitor compliance with data protection regulations in its operations.

- The Processor has appointed the following Data Protection Officer(s):
Last name, first name: Dr. Kraska, Sebastian
Organizational unit: IITR GmbH
Contact information: Tel: +49 89 1891 7360, Email: skraska@iitr.de
Any change in the Data Protection Officers must be reported to the Client without delay.

6. Communication obligations of the Processor in the event of disturbances in processing and breach of the protection of personal data

The Processor shall notify the Client without undue delay of any disruptions, violations by the Processor or the persons employed by it and of any violations of data protection provisions or of the stipulations made by order as well as of any suspected data protection violations or irregularities in the processing of personal data. This also applies in particular with regard to any reporting and notification obligations of the Client pursuant to Art. 33 and Art. 34 GDPR. The Processor warrants to appropriately support the Client in its obligations pursuant to Art. 33 and 34 GDPR if necessary (Art. 28 para. 3 clause 2 lit. f GDPR). Notifications pursuant to Art. 33 or 34 of the GDPR for the Client may only be carried out by the Processor after prior instruction pursuant to Sec. 4 of this Agreement.

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

- The future use of subcontractors to process data of the Client is permitted for the Processor **without special authorization** by the Client, Art. 28 para. 2 clause 2 GDPR. The Processor must take care to select the subcontractor with particular consideration of suitability for the technical and organizational measures they must undertake in the sense of Art. 32 GDPR. The relevant test documents for this shall be made available to the Client upon request. In this case, the Processor will also always inform the Controller of any intended change with regard to additional processors or the replacement of other processors.

Subcontractors may only be used in third party countries if the particular requirements of Art. 44 et. seqq GDPR are fulfilled (e.g. adequacy decision of the Commission, standard data protection clauses, approved codes of conduct).

The Processor shall contractually ensure that the agreed provisions between the Client and the Processor also apply to subcontractors. The contract with the subcontractor shall specify the information in a concrete manner, such that the responsibilities of the Processor and the subcontractor are clearly delineated. If multiple subcontractors are used, this also applies for the division of responsibilities between these subcontractors. The Client must particularly be entitled to conduct suitable reviews and inspections of subcontractors if necessary, also on site, or to have them conducted by third parties. The contract with the subcontractor must be concluded in writing, which can also occur in an electronic form (Art. 28 para. 4 and para. 9 GDPR). Data may only be sent to the subcontractor after the subcontractor has fulfilled the obligations pursuant to Art. 29 and Art. 32 para. 4 GDPR with regard to its employees. The Processor shall review compliance with the obligations of the subcontractor(s) as follows:

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

The result of the review must be documented and provided to the Client upon request. The Processor shall be liable to the Client for ensuring that the subcontractor complies with the data protection obligations contractually imposed on it by the Processor in accordance with this section of the Agreement.

Currently, the Processor employs...	iCorr® DH	iCorr® OS	iCorr® AG	iCorr® Shop	iCorr® CT	iCorr® Apps
no subcontractors	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
the subcontractor documented in Annex 1 is commissioned with processing personal data in the scope described there. The Client declares its agreement with the use of the subcontractor named in Annex 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"/>

The Processor will always inform the Controller of any intended change with regard to the addition of new processors or the replacement of previous processors. The Client will have the opportunity to make an objection against such changes, if the previously agreed technical and organizational measures warranted by the Processor cannot be guaranteed in full (Art. 28 para. 2 clause 2 GDPR). In this case, the intended change may not take place.

8. Technical and organizational measures pursuant to Art. 32 GDPR (Art. 28 para. 3 clause 2 lit. c GDPR)

A level of protection appropriate to the risk to the rights and freedoms of the data subjects concerned by the processing must be ensured for the specific commissioned processing. To this end, the protection objectives of Article 32 para. 1 GDPR, such as confidentiality, integrity and availability of the systems and services, as well as their resilience in relation to the type, scope, circumstances and purpose of the processing operations, shall be taken into account in such a way that the risk is permanently contained by appropriate technical and organizational remedies. For the contractual processing of personal data, a suitable and traceable method for risk evaluation will be used, one which considers the likeliness of occurrence and severity of the risks for the rights and freedoms of the data subjects affected by the processing. The data protection concept described in Annex 2 depicts the minimum requirements of the technical and organizational measures appropriate for the determined risks under consideration of the protection goals according to the state of the art in detail and under special consideration of the IT

systems and processing procedures used by the Processor. The procedure for regular monitoring, assessment, and evaluation of the technical and organizational measures to ensure processing in compliance with data protection is also described.

There are the following option for documentation through certification:

- The Processor shall, as the occasion arises, but at least annually, carry out a review, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the security of the processing (Art. 32 para. 1 lit. d GDPR). The results shall be shared with the Client "upon request." Decisions relevant to security regarding the organization of data processing and the procedures used shall be agreed between the Processor and the Client. If the measures taken by the Processor do not satisfy the requirements of the Client, the Processor shall inform the Client without delay. The measures taken by the Processor can be adjusted over the course of the contract relationship to technical and organizational developments, but must not fall below the agreed standards. Significant changes must be agreed between the Processor and the Client in a documented form (written, electronic). Such agreements shall be retained for the term of this Agreement.

9. Obligations of the Processor after the end of processing, Art. 28 para. 3 clause 2 lit. g GDPR

After the conclusion of the contractual works, the Processor shall have all data, documents, and created processing or use results in connection with the contractual relationship in its possession or that of the subcontractors deleted or destroyed as described below:

	Handling data after the end of the order
iCorr® DH	- iCorr® Digital Hub User will be deleted from User Management.
iCorr® OS	- iCorr® OS User will be removed using the delete function in User Management. - iCorr® OS contacts will be removed in the iCorr® OS administration area by the iCorr® or Remote Service Team. - The daily backups of the User database and Contact database will be stored for 60 days on a separate physical storage system before being deleted.
iCorr® AG	- iCorr® AG user accounts will be removed in the iCorr® AG Administration area by the iCorr® AG Product Management Team.
iCorr® Shop	- iCorr® Shop user accounts will be removed in the back office (SAP Hybris administration area) by the Lifecycle E-Commerce Team.
iCorr® CT	- Personal data will be deleted immediately after the end of the contractual relationship.
iCorr® Apps	- iCorr® Apps User will be deleted from User Management.



10. Other provisions

Agreements about the technical and organizational measures and checking and review documents (also about subcontractors) shall be retained by both contracting parties for their terms and afterwards for three full calendar years. The written form or a documented electronic form is always necessary for ancillary agreements. The court locally responsible for the Client is agreed as the court of jurisdiction. If the property or the personal data to be processed by the Processor of the Client is endangered by the measured of third parties (such as attachment or seizure), through insolvency or similar proceedings or other events the Processor must inform the Client without delay. The defense of the right of retention within the meaning of Sec. 273 BGB (German Civil Code) is excluded with regard to the data processed for the Client and the associated data storage media. If some parts of this Agreement are ineffective, this shall not affect the effectiveness of the rest of the Agreement.

_____, on _____
City of the Client, Date

For the Client:

Name: _____


Position: _____

Signature: _____

For the Processor:

Name: Lars Engel

Position: Managing Director

Signature: 

Annex 1 – Subcontracting Relationships

	Subcontracting relationships & subcontractors
iCorr® DH	<p>Currently, the following subcontractor relationships exist in connection with the data processing:</p> <ul style="list-style-type: none"> - Amazon Web Services Emea Sarl 38, Avenue John F. Kennedy L-1855 Luxembourg Luxembourg - Microsoft Corporation 1 Microsoft Way Redmond, WA 98052 USA - Atlassian. Pty Ltd
iCorr® OS	<p>Currently, the following subcontractor relationships exist in connection with the data processing:</p> <ul style="list-style-type: none"> - Amazon Web Services Emea Sarl 38, Avenue John F. Kennedy L-1855 Luxembourg Luxembourg - Atlassian. Pty Ltd
iCorr® AG	<p>Currently, the following subcontractor relationships exist in connection with the data processing:</p> <ul style="list-style-type: none"> - TeamViewer Germany AG Bahnhofsplatz 2 73033 Göppingen Germany - Microsoft Corporation 1 Microsoft Way Redmond, WA 98052 USA - Atlassian. Pty Ltd
iCorr® Shop	<p>Currently, the following subcontractor relationships exist in connection with the data processing:</p> <ul style="list-style-type: none"> - DotSource E-Commerce & Digitalagentur GmbH Goethestrasse 1 07743 Jena Germany - Microsoft Corporation 1 Microsoft Way Redmond, WA 9805 USA

iCorr® CT	<p>Currently, the following subcontractor relationships exist in connection with the data processing:</p> <ul style="list-style-type: none"> - Amazon Web Services, Inc. 410 Terry Avenue North Seattle, WA 98109-5210 USA - Microsoft Corporation 1 Microsoft Way Redmond, WA 98052 USA - Atlassian. Pty Ltd
iCorr® Apps	<p>Currently, the following subcontractor relationships exist in connection with the data processing:</p> <ul style="list-style-type: none"> - Amazon Web Services Emea Sarl 38, Avenue John F. Kennedy L-1855 Luxembourg Luxembourg - Atlassian. Pty Ltd

Annex 2 – Technical and Organizational Measures / Data Protection Concept

In this Data Protection Concept, the requirements and the implementation of the measures for safe processing in conformity with the protection of personal data will be described. In the process, the requirements of Articles 24, 25 and 32 GDPR will be considered as far as possible.

1. Confidentiality

1.1 Controlled physical access

The rooms in which personal data is processed or data processing systems are installed must not be accessible to the public. They must be locked when the employees are not present. The access authorizations must be issued in a set procedure according to the "need to know principle" and must be regularly monitored as to their necessity. Rooms in which data processing systems (data centers, servers, network distributors, etc.) are housed must be particularly protected against unauthorized access and may only be accessible for employees of the IT administration (and management if relevant). Alternatively, the devices must be placed in suitable locked cabinets. Visitors and people who are not part of the company must be registered in a documented procedure and supervised within the business premises.

The company has implemented the requirements in the following manner:

- | | |
|--|--|
| <input checked="" type="checkbox"/> Locked building | <input checked="" type="checkbox"/> Locked server rooms with controlled access |
| <input checked="" type="checkbox"/> Locked offices | <input checked="" type="checkbox"/> Locked server cabinets |
| <input checked="" type="checkbox"/> Electronic security locking system | <input checked="" type="checkbox"/> Alarm system for buildings / offices |
| <input checked="" type="checkbox"/> Mechanical security locking system | <input checked="" type="checkbox"/> Alarm system for server room |
| <input checked="" type="checkbox"/> Documentation of keys issued | <input checked="" type="checkbox"/> Electronic controlled access |
| <input checked="" type="checkbox"/> Visitor registration | |
| <input checked="" type="checkbox"/> Area-specific authorization cards | |

1.2 Controlled electronic access

For each network user, a personally assigned user must be set up with a password of at least 10 characters with upper and lower case letters, number and special characters. Users shall be required by the system to change passwords at least every 90 days. Network users shall be required to comply with the user access policy in a documented manner. The creation, alteration, and removal of access authorizations must occur in a documented procedure. Established access authorizations must be reviewed regularly with regard to their necessity in a documented manner. Network accesses must be monitored and logged; this also includes unsuccessful attempts at access. Access to the network must be automatically blocked by the system no later than after 10 failed attempts.

The company has implemented the requirements in the following manner:

- | | |
|--|--|
| <input checked="" type="checkbox"/> Password conventions with complex passwords of min. 12/16 characters | <input checked="" type="checkbox"/> Encrypted notebooks |
| <input checked="" type="checkbox"/> Central authentication with user name and password | <input checked="" type="checkbox"/> Secure line connection for external access |
| <input checked="" type="checkbox"/> Locking access after multiple incorrect entries of the login data | <input checked="" type="checkbox"/> Use of a current firewall |
| | <input checked="" type="checkbox"/> Use of a mobile device management software |

1.3 Controlled physical access

A documented, role-based authorization concept must be in place for access to personal data, which restricts access in such a way that only authorized persons can access the personal data required for their task (minimum principle). The password regulations from controlled electronic access must also be implemented for controlled physical access. The administrative activities must be limited to a small circle of administrators. The activities of the administrators must be monitored and logged within the scope of technically justifiable effort.

The company has implemented the requirements in the following manner:

- | | |
|---|---|
| <input checked="" type="checkbox"/> Role-based authorization concept | <input checked="" type="checkbox"/> Allocation of authorizations only after approval by the data owner |
| <input checked="" type="checkbox"/> Application-linked authentication with user name and password | <input checked="" type="checkbox"/> Administrative users should be limited to a minimum and documented. |
| <input checked="" type="checkbox"/> Logging user accesses | |

1.4 Controlled separation

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

The company has implemented the requirements in the following manner:

- Separation of clients within the data processing system
- Separation of productive and test systems

2. Integrity

2.1 Controlled transmission

As part of controlled transmission, it must be ensured that only authorized persons can view the personal data. For transmission by email, corresponding protective measures (e.g. encryption of the 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 requirements in the following manner:

- VPN connections
- Leased lines
- Prohibition against the use of private storage media

2.2 Controlled input

It must be possible to assign the entry, modification and deletion of personal data to the employee that performed it. The change and deletion of data sets must be restricted by the system to effectively prevent accidental changes or deletions.

The company has implemented the requirements in the following manner:

- | | |
|--|--|
| <input checked="" type="checkbox"/> Traceability of entries, changes and deletions by personalized users | <input checked="" type="checkbox"/> Monitoring and logging of automated data processing operations |
| <input checked="" type="checkbox"/> Traceability when assigning, changing and deleting user authorizations | <input checked="" type="checkbox"/> Sampling of automated data processing operations |

2.3 Controlled processing

As part of controlled processing, it must be ensured that the data processing operations carried out under the order are carried out exclusively according to the instructions of the Client. The employees involved in data processing must be trained and instructed for this purpose. The data processing must be monitored through internal controls. The results of the controls must be documented.

Subcontractors may only be used on the basis of the requirements coordinated with the Client. The transfer of or access to personal data may only take place after the subcontractor has signed a data processing agreement in accordance with Article 28 GDPR and has confirmed compliance with the regulations of the data protection concept. The Contractor's duty to audit its subcontractor results from the data processing agreement concluded with the Client.

The company has implemented the requirements in the following manner:

- No use of processors that have not been obligated in accordance with Art. 28 GDPR

3. Availability and resilience

The processing of personal data must occur on data processing systems that undergo regular, documented patch management. No systems may be connected in the network that are outside the maintenance cycles of the manufacturers (esp. no Windows XP, Windows Server 2003, etc.). Security-related patches must be installed within 72 hours after being announced. 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 correspond to the state of the art (temperature regulation, protection against fire, water penetration, etc.). The servers must have an uninterruptible power supply (UPS) that ensures a controlled shutdown without data loss.

The company has implemented the requirements in the following manner:

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

4. Procedure for regular monitoring, assessment, and evaluation

A procedure for monitoring data protection in the company must be implemented. This must include employee commitment to data confidentiality, employee training and awareness, and regular auditing of data processing procedures. The documentation of the processing procedures performed for the Client must also take place before data processing begins. A consistent notification and handling process must be in place for data privacy violations and the protection of data subjects' rights. This must also include the information of the Client.

The company has implemented the requirements in the following manner:

- Appointing a Data Protection Officer