hogrefe

Data protection at Hogrefe

Responsible handling of sensitive data



Approval page

Role / Responsible Person	Name	Approval date	Major Version
Author	Krasny, Maria	27.05.2026	3.0
Final Approver	da Cruz, Paulo	27.05.2026	3.0

Change History

Date	Version	Changed by	Description of changes
01.Jan. 2025	1.0	Maria Krasny	First Version
07.08.2025	1.1	Tim Fetzer, Maria Krasny	Update 4. Technical and organizational measures; adjustment to point 2.5
07.08.2025	2.0	Paulo da Cruz	Approval
26.05.2026	2.1	Maria Krasny, Felix Hudy	Change of 3.4 Contact persons for data protection
27.05.2026	3.0	Paulo da Cruz	Approval

Table of Contents

1. Contact 6

2. General information about Hogrefe's data protection 7

2.1 Data protection in the Hogrefe Testsystem (online portal) 7

2.2 General 7

2.3 Protection of personal data from misuse 7

2.4 EU General Data Protection Regulation (GDPR) 8

2.5 Protection of electronic data against loss or alteration 8

2.6 Test protection 9

2.7 Data protection impact assessment 9

3. Data Processing Agreement 11

3.1 Definitions 12

3.2 Subject matter, scope, type and purpose of data use, data subjects, duration 12

3.3 Responsibilities and authority to issue instructions 12

3.4 Contact persons for data protection 13

3.5 Security 13

3.6 Confidentiality obligation 14

3.7 Support for data subjects rights 14

3.8 Support for documentation and reporting obligations 14

3.9 Monitoring rights of the Controller 15

3.10 Use of other processors (subcontractors) 15

3.11 Erasure and release 16

3.12 Liability 16

3.13 Other provisions 17

4. Technical and organizational measures 18

4.1 Confidentiality (Article 32 (1) (b) GDPR) 18

4.1.1 Physical Access Control 18

4.1.2 Equipment access control 18

4.1.3 Data access control 19

4.1.4 Separability 19

4.1.5 Pseudonymization 20

4.2 Integrity (Article 32 (1) (b) GDPR) 20

4.2.1 Data transfer control 20

4.2.2 Input control 20

4.3 Availability and resilience (Article 32 (1) (b) GDPR) 21
4.3.1 Availability control 21
4.3.2 Resilience and reliability control 21
4.4 Process for regularly testing, assessing, evaluating (Article 32 (1) (d) GDPR; Article 25 (1) GDPR) 23
4.4.1 Control processes 23
4.4.2 Processing control 23
5. List of subcontractors 24

1. Contact

Hogrefe Verlag GmbH & Co. KG
Test center
Herbert-Quandt-Str. 4
D-37081 Göttingen
Tel: +49 (0)551 999 50-880
FAX: +49 (0)551 999 50-998
Email: e-tests@hogrefe.de
Internet: www.testzentrale.de

If you have any questions about Hogrefe data protection, please contact:

datenschutz@hogrefe.de

2. General information about Hogrefe's data protection

2.1 Data protection in the Hogrefe Testsystem (online portal)

Data protection comprises three overarching aspects, the observance and implementation of which are essential for the reliable handling of data within the Hogrefe Testsystem (HTS):

1. Protection of personal data against misuse
2. Protection of electronic data against loss or alteration
3. Test protection as protection of tests and principles of evaluation against general disclosure

2.2 General

In principle, it is not necessary to collect sensitive personal data in the HTS. Only age in years and gender are necessary for the application of the relevant standards in some tests – but these do not in themselves allow identification of an individual. The identification of the individual can be entered via an individual code (e.g. a number in a separate test taker administration). The documentation of a "result to a person " assignment can be done outside the HTS.

For the general use of personal data in the assessment process (entering names, date of birth, address data, etc.) the test user is responsible and must obtain consent for the processing of this personal data, and understand the legal framework that is applicable.

Data on the Hogrefe servers is not automatically deleted and must be done or activated by the test user, as the data controller. Under the heading "Evaluate" there is a delete option for individuals; in this case **all** measurements of the given person are also deleted. In the supervisor login area, an automatic deletion function for individuals and test results can also be activated.

All data is automatically archived in a backup system in order to be able to recover it in the event of a disaster. In order to be able to comply with the statutory obligation to provide evidence, we also recommend that the results be printed and archived on paper or electronically.

2.3 Protection of personal data from misuse

Hogrefe attaches a particular emphasis on the confidentiality of personal data and compliance with applicable data protection laws and regulations. Personal information stored in the Hogrefe Testsystem will only be processed within the framework of the guidelines listed here.

The connections between the client (online portal administration platform) and the server (hogrefe-online.com) and the client (test site) and the server (hogrefe-online.com) are made exclusively via encrypted SSL connections.

Current security procedures have been implemented to ensure the accuracy and security of personal data and to prevent unauthorized access or improper use. These include:

- Using a form-based authentication process
- Transferring data through a TLS-encrypted connection
- Providing firewall systems secure servers
- Limiting the access to the servers to port 443

The administration space (online portal) is secured by its own user management, which ensures that only the data managed by the user is also visible to this user. Hogrefe support staff cannot view personal data without the customer's consent.

2.4 EU General Data Protection Regulation (GDPR)

The HTS complies with the data protection requirements of the GDPR. During development of the system, special emphasis continues to be placed on the privacy-friendliness of the product design and on data protection-friendly defaults in order to comply with the principles of "privacy by design" and "privacy by default" (Art. 25 GDPR). As a result, HTS can be used without the collection of personal data.

All HTS-related processing activities and internal processes are documented and regularly reviewed in order to assist the test user in fulfilling their data protection obligations (as the data controller).

All employees are regularly trained to comply with GDPR requirements and are obliged to maintain confidentiality.

2.5 Protection of electronic data against loss or alteration

To ensure the security of processing, appropriate technical and organizational measures have been taken for HTS to enable the level of protection at all times.

In particular, this includes

- the pseudonymization and encryption of personal data;
- the ability to ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing on a permanent basis;
- the ability to rapidly restore the availability of and access to personal data in the event of a physical or technical incident;
- a process for regularly reviewing, assessing and evaluating the effectiveness of the technical and organizational measures to ensure the security of the processing.

Insofar as subcontractors are used for the processing of data, they have been carefully selected, in particular taking into account the technical and organizational measures they have taken for data protection. They were checked for compliance with the statutory and contractual data protection regulations and the agreed technical and organizational protective measures before being commissioned and during the term of the contract.

In order to protect data from loss, damage, unauthorized access and improper use, the Hogrefe online portal is hosted in a data center and has a redundant data connection.

The organizational measures include

- Seamless monitoring of operations and access, around the clock.
- “Remote hands” are available during business/support hours.
- Databases are continuously backed up on separate hardware.
- Controlled destruction of data carriers.
- Commitment to data confidentiality
- Training and awareness-raising on data protection

The complete list of technical and organizational measures in accordance with Art. 32 GDPR can be found under 4. of this document.

2.6 Test protection

Please note that test protection is also part of data protection. Test items should not be made public, otherwise results may not be valid. Professional testing procedures are subject to controlled distribution conditions that provide some protection. This also applies to PC-based testing procedures. Wherever possible, you should perform important test administrations under controlled conditions. This includes:

- Identity verification of the individual (particularly when the individual is not personally known to the test user)
- Supervision of the testing process (and in remote locations, if necessary, by a designated trustee to prevent unauthorized aids and communication).

2.7 Data protection impact assessment

The data protection impact assessment (DPIA) is a procedure to ensure and demonstrate compliance with legal requirements. Art. 35 GDPR requires a DPIA if the nature of the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. In particular, this may result from

- the use of new technologies,
- the nature,
- the extent,
- the circumstances and
- the purposes

the processing of personal data. Based on the criteria in Art. 35 GDPR, a so-called threshold analysis shall be performed to determine whether a DPIA must be carried out for the relevant processing. In the following cases, the threshold is always exceeded and a DPIA must be carried out:

1. the type of processing, in particular the use of new technologies, is likely to result in a high risk to the rights and freedoms of natural persons due to the nature, scope, circumstances and purposes of the processing (Art. 35 para. 1 GDPR)
2. the processing falls under one of the standard examples in Art. 35 para. 3 GDPR. These include:

   a. The systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and which in turn serves as the basis for decisions that produce legal effects concerning natural persons or similarly significantly affect them.
   b. the large-scale processing of special categories of personal data pursuant to Art. 9 para. 1 GDPR or of personal data relating to criminal convictions and offenses pursuant to Art. 10 GDPR.
   c. The systematic and extensive monitoring of publicly accessible areas.
3. the processing is on a list pursuant to Art. 35 para. 4 GDPR.

Under certain circumstances, the test user, as the controller under data protection law, must carry out a data protection impact assessment for the use of HTS. As a processor, Hogrefe is obliged to support the controller in carrying out the data protection impact assessment in accordance with Art. 28 para. 3 f) GDPR. Hogrefe cannot anticipate the exact circumstances of the processing of personal data by the test user in HTS and any associated high risks to the rights and freedoms of the data subjects. For the data protection impact assessment, not only the processing within the HTS is relevant, but also operations that take place outside the HTS at the test user's site as part of the execution of the assessments, of which Hogrefe has neither knowledge nor influence.

In principle, it is possible to use HTS entirely without entering any personal data, so that a high risk can be virtually ruled out. On the other hand, it is also possible to process personal data and special categories of personal data within the HTS. This is in the responsibility of the test-user.

If the test user is therefore obliged to carry out a data protection impact assessment as the controller under data protection law, a large number of suitable countermeasures are provided in this document under sections 2. 2. to 2.6. as well as 4. and 5. in order to reduce any risks to an adequate level. These measures are continuously reviewed and further developed by Hogrefe. It is not to be expected that high risks for the data subjects will arise from the use of the HTS, nor that there is an obligation to consult a supervisory authority in advance in accordance with Art. 36 GDPR, insofar as the aforementioned remedial measures are taken by the test user.

3. Data Processing Agreement

Data protection agreement in accordance with Article 28 GDPR
regarding the provision of IT services

Between

[Ange organisationens fullständiga namn]
[Ange organisationens postadress]
[Ange organisationens organisationsnummer]
[Ange kontaktpersonens e-postadress]

(hereinafter referred **to as the Controller)**

And

Hogrefe Psykologiförlaget AB
Gävlegatan 12B
113 30 Stockholm
556711-8202
pubavtal@hogrefe.se

(hereinafter referred to **as the Processor)**

Preamble

In accordance with Article 28 of EU General Data Protection Regulation 2016/679 (hereinafter referred to as the GDPR), this agreement specifies the data protection obligations of the parties with respect to the provision of IT services.

It applies to all activities in which employees of the Processor or third parties engaged by the Processor may come into contact with personal data of the Controller.

3.1 Definitions

The definitions of Article 4 GDPR apply.

3.2 Subject matter, scope, type and purpose of data use, data subjects, duration

(1) The purpose of this document is to specify the agreement between the Controller and the Processor on the provision of information technology services, which comes into force upon accessing the Hogrefe online portal. The provision of information technology services involves the processing of personal data by the Processor on behalf of the Controller in accordance with instructions given by the Controller.

(2) The object of this agreement is, in particular, the provision of the following services by the Processor:
- Hosting the HTS online portal and ensuring operability
- Provision of server infrastructure for completion of online testing
- Keeping the test results in PDF format available on the online portal for the duration of the contractual relationship or the Controller deletes the files

(3) In the context of the provision of the services, the following personal data may be affected:
- Name
- Age
- Gender
- E-mail address (in individual cases)
- Test results and evaluations

(4) Affected by the use of data may be (depending on the Controller's area of responsibility):
- Employees
- Applicants
- Coaches
- Test users
- Other:.....

(5) The validity of this Annex corresponds with the duration of the main agreement.

(6) The processing of personal data takes place exclusively in the territory of the Federal Republic of Germany, in a Member State of the European Union or in another Contracting State of the Agreement on the European Economic Area. Any transfer to a third country requires the prior documented instructions of the Controller (Art. 28 sec. 3 lit. a GDPR) and may only take place if the special requirements of Art. 44-49 GDPR are met.

3.3 Responsibilities and authority to issue instructions

(1) The Controller is solely responsible for compliance with data protection laws and regulations, in particular with respect to the lawfulness of disclosure of data to the Processor and the lawfulness of data processing (Article 4 (7) GDPR).

(2) The Processor reserves the right to anonymize or aggregate the personal data, so that it is no longer possible to identify individual data subjects, and in this form to use it for the purpose of designing, developing and optimizing the service agreed in accordance with the main agreement. The parties agree that anonymized or aggregated personal data according to the above conditions will no longer be considered personal data within the meaning of this Agreement.
(3) The Processor shall only process personal data on documented instructions from the Controller, unless required under EU law or the laws of the member state or country to which the Processor is subject. In the event of any other obligation, the Processor shall notify the contractor of the relevant legal requirements prior to processing.

(4) If the Processor believes that an instruction from the Controller violates data protection regulations, he shall immediately inform the Controller in accordance with Article 28 (3) GDPR. Pending confirmation or amendment of the relevant instruction, the Processor is entitled to suspend the execution of the instruction.

3.4 Contact persons for data protection

The Processor is not obliged to appoint a data protection officer. The Processor is not obliged to appoint a data protection officer. A point of contact for data protection issues at the Processor has been set up at privacy@hogrefe.com.

The persons responsible for the data protection contact point are able, upon the Controller's request, to provide proof that the Processor complies with the requirements of international and national data protection laws.

3.5 Security

(1) The Processor shall take appropriate technical and organizational measures to adequately protect the personal data in accordance with Article 28 (3) GDPR in conjunction with Article 32 (1) GDPR in order to ensure the security of the processing on behalf of the court. To this end, the Processor will

- ensure the confidentiality, integrity, availability and resilience of the systems and services associated with processing in the long term;
- ensure the ability to rapidly restore the availability and access to personal data in the event of a physical or technical incident;
- maintain a procedure for the regular review, evaluation and evaluation of the effectiveness of technical and organizational measures to ensure the safety of processing.

The state of the art, the implementation costs and the nature, scope and purposes of the processing, as well as the different probability and severity of the risk to the rights and freedoms of individuals within the meaning of Article 32(1) GDPR must be taken into account.

(2) The Parties agree on the specific data security measures set out in Section IV of this Agreement, "Technical and Organizational Measures".

(3) Technical and organizational measures shall be subject to technical progress and development. In this respect, the Processor is permitted to implement alternative adequate measures. The level of safety of the measures laid down must not be lowered. Substantial changes must be documented and notified to the Controller in writing.

3.6 Confidentiality obligation

The Processor shall only use employees who have been obliged to maintain confidentiality in accordance with Article 28 (3) (b) GDPR and who have previously been familiarized with the relevant provisions on data protection in accordance with Article 28 (3) (2) (b) GDPR. The Processor and any individuals under the authority of the Processor who have access to personal data should process such data exclusively in accordance with the instructions of the Controller, including the powers conferred in this Agreement, unless they are legally obliged to process them in another manner.

3.7 Support for data subjects rights

(1) The Processor is obliged to support the client with appropriate technical and organizational measures in the protection of the rights of the data subjects referred to in Articles 12 to 22 GDPR (Article 28 (3) GDPR). In particular, the Processor will assist the Controller in fulfilling requests of individuals for deletion of their personal data in accordance with Article 17 GDPR.

(2) Insofar as individuals may exercise a right to data portability vis-a-vis the Contractor, the Processor shall ensure that they can obtain the data they have provided to the Contractor in a structured, common and machine-readable format.

(3) The Processor may only correct, delete or restrict the processing of personal data in accordance with documented instructions of the Controller. The Processor may only provide information to third parties or individuals with the prior written consent of the Controller.

(4) Insofar as an individual contacts the Processor directly in order to assert his or her rights under Articles 12 to 22 GDPR, the Processor shall immediately forward the request to the Controller.

3.8 Support for documentation and reporting obligations

(1) If the Processor becomes aware of a breach of the protection of personal data, he shall immediately notify the Controller of Article 28 (3) (f), Article 33 (2) GDPR. The same shall apply if individuals employed by the Processor violate this Agreement.

(2) After consultation with the Controller, the Processor shall immediately take the necessary measures to secure the data and to reduce possible adverse consequences for the parties concerned.

(3) The Processor shall assist the Controller with all the information available in the fulfilment of the information obligations to the competent supervisory authority in accordance with Article 33 GDPR and, if necessary, to those affected by the breach of the protection of personal data in accordance with Article 34 GDPR.

(4) The Processor shall assist the Controller with all the information available in the data protection impact assessment in accordance with Article 35 GDPR and, if necessary, in a prior consultation with the competent supervisory authority in accordance with Article 36 GDPR.

(5) The Processor shall immediately inform the Controller of controls and measures taken by the supervisory authority in so far as they relate to this Agreement.

3.9 Monitoring rights of the Controller

(1) The Controller is entitled to assess the Processor with regard to the technical and organizational measures taken as well as the compliance with this Agreement and the data protection regulations, either on their own or by another auditor commissioned by the Controller. For this purpose, it can alternatively:

- obtain self-information from the Processor, or
- obtain an existing certificate from an external expert or the company DPO, or
- in the event of reasonable doubt about the documents submitted or an incident relevant to data protection law, after timely notification and by stating the reasons, at normal business hours and without disrupting the operation, the Controller can carry out an audit.

(2) The Processor undertakes to provide the Controller with all the information necessary for an assessment.

(3) The Processor is obliged to tolerate assessments by the Controller with regard to compliance with this Agreement and the associated compliance with data protection regulations, in particular by obtaining information requested. The Processor shall provide information on the specific individual case immediately upon request of the Controller and shall provide appropriate evidence of compliance with this Agreement.

3.10 Use of other processors (subcontractors)

(1) The use of subcontractors must be permitted by the Controller. However, the Controller gives the Processor general permission to involve subcontractors, if these are affiliated companies of the Processor. Ten weeks before the use of affiliated company as a subcontractor, the Processor must inform the Controller. The subcontractors approved by the Controller at the time of conclusion of this Agreement are listed under section 5. For the purposes of this Agreement subcontractors shall be defined as services which relate directly to the provision of the main service. This does not include ancillary services which the Processor uses, such as telecommunications services, postal/transport services, cleaning, etc.

(2) In individual cases, the Controller has the right to object to the appointment of a subcontractor. The Controller shall exercise the right of opposition only for objective reasons, taking into account reasonable discretion, without undue delay, at the latest within a period of 2 weeks after receipt of the information. The opposition must be given in text form and provide all the reasons which, in the opinion of the Controller, preclude the use of the subcontractor. In the event that the subcontractor's use is necessary to eliminate the risk of a material adverse effect on the interests of another client or individuals, the Processor shall be entitled to provisionally appoint the subcontractor whose use the Controller has been informed of before the expiry of the opposition period. In such cases, the subcontractor's provisional use shall be based on an opposition from the Controller which meets reasonable discretion and the abovementioned requirements in terms of form and justification. Significant impairments within the meaning of the above rules exist, for example, where the involvement of a subcontractor is required for reasons of data security or if, without the subcontractor's use, the Processor would suffer a disproportionate effort or damage.

(3) Subcontractors must be carefully selected, in particular with particular regard to the technical and organizational data protection measures they have taken within the meaning of Article 32 GDPR. They must be checked for compliance with statutory and contractual data protection regulations as well as the agreed technical and organizational protective measures before commissioning and during the term of the contract. The results of this inspection shall be documented and transmitted to the Controller upon request.

(4) Contractual agreements between the Processor and subcontractors shall comply with the confidentiality, data protection and data security requirements of this Agreement. The transfer of personal data to the subcontractor is only permitted if the subcontractor fulfils the obligations under Article 28 GDPR.

(5) Further outsourcing by the subcontractor requires the express consent of the Processor (minimum text form). All contractual provisions in the contract chain must also be ordered to the additional subcontractor.

3.11 Erasure and release

(1) The Processor will only retain the personal data for as long as instructed by the Controller. In the absence of a specific instruction, the personal data will only be retained before destruction for as long as is necessary for the execution of the processing commissioned under this Agreement.

(2) At the request of the Controller and after termination of this agreement, the Processor will delete all personal data related to this Agreement for processing, as well as any copies thereof within 14 days after the Controller's request and instruction or termination of the order processing, in compliance with relevant data protection regulations.

(3) Documentation that serves as proof of proper data processing must be kept by the Processor in accordance with the respective statutory or contractually agreed upon retention periods beyond the end of this Agreement. The Processor can hand over the documentation to the Controller upon termination of this Agreement without discharge.

(4) The Processor shall notify the Controller of the cancellation in writing upon request.

3.12 Liability

Pursuant to Art. 82 (1) and (4) GDPR, the controller and the processor shall be liable to third parties for any material and non-material damage suffered by a person as a result of a breach of the GDPR. If both the client and the contractor are responsible for such damage, the parties are liable internally for this damage in proportion to their share of responsibility. If, in such a case, a person makes a claim for damages against one party in whole or in part, that party may demand indemnification or hold harmless from the other party to the extent that it corresponds to its share of responsibility for the damage.

3.13 Other provisions

(1) In the event of a conflict between any other contract and this Agreement, this Agreement shall take precedence with respect to the processing of personal data.

(2) Should one or more provisions of this Agreement be or become ineffective, the validity of the remaining agreement shall remain unaffected. The invalid provision(s) shall be replaced by a provision which ultimately is as close as possible to that which the parties had sought with the ineffective provision. The same applies in the case of contractual gaps.

_____ Location, Date _____ Signature Controller	_____ Location, Date _____ Signature Processor

4. Technical and organizational measures

4.1 Confidentiality (Article 32 (1) (b) GDPR)

4.1.1 Physical Access Control

Scope
The objective of physical access control is to prevent unauthorized persons from getting close to data processing equipment, thereby gaining physical access to the systems used to process or use personal data by implementing various structural, organizational and personnel measures, which shall be laid down in a physical access control policy.

Technical and organizational measures
The purpose of the following measures is to deny an unauthorized individual physical access to data processing equipment:

- Electronic access code cards / access transponders
- Rules for granting access authorisation
- Video surveillance
- Alarm system
- Keys policy
- Visitors must always be accompanied by employees
- Visitor check-in/check-out records
- Tiered security areas and controlled access
- Separately secured access to the data center
- Servers are kept in locked rooms
- Storage of data carriers under lock and key or in locked rooms

4.1.2 Equipment access control

Scope
The objective of equipment access control is to deny an unauthorized individual access to data processing equipment by implementing appropriate measures to ensure that only users who have the appropriate authorization can gain access to data and IT applications. If a user fails to demonstrate that he or she has the necessary authorization, the equipment access control will deny the user access to the IT system.

Technical and organizational measures
The purpose of the following measures is to deny an unauthorized individual access to data processing systems:

- Password protection of workstation screens
- Functional and/or temporary allocation of user authorisations
- Use of individual passwords
- Automatic blocking of user accounts after entering the wrong password multiple times

- Automatic password-protected screen lock after a period of inactivity (screensaver)
- Password policy and minimum password complexity requirements:
  – At least 12 characters, upper and lower case letters, special characters, numbers
  – Password history (no reuse of the last 3 passwords)
- Procedure for granting authorizations to new employees
- Procedure for withdrawing authorizations from employees who move to a different department
- Procedure for withdrawing authorizations from employees who leave the company
- Confidentiality obligation
- Logging and evaluation of system use
- Controlled destruction of data carriers

4.1.3 Data access control

Scope
The objective of data access control is to ensure that those authorized to use a data processing system can only access data covered by their access authorization, and personal data is not read, copied, modified, or removed by an unauthorized user during processing, use or after it has been stored.

Technical and organizational measures
The purpose of the following measures is to deny an unauthorized individual access to data processing systems:

- Formulation of access authorization policy
- Procedure for the recovery of data from backups (who, when, at whose request)
- Regular review of authorizations
- Restriction of free and uncontrolled query options for databases
- Regular analysis of logs (log files)
- Partial access to databases and functions (read, write, execute)
- Logging of file access
- Logging of file erasures
- The company uses adequate security systems (software/hardware), including:
  - Virus scanner
  - Firewalls
  - SPAM filter
  - Intrusion prevention (IPS)
  - Intrusion detection (IDS)
- Encrypted storage of data
- Use of hash function – SHA2 (256, 384, 512 bit)

4.1.4 Separability

Scope
The objective of the principle of separability is to ensure that data collected for different purposes can be processed separately. Among other things, the purpose is to have the ability to associate data with a specific department, individual, branch or customer, and to comply with the principle of purpose limitation, which is one of the basic principles of data protection. The objective can be achieved in many ways, for example, by implementing a suitable application authorization policy.

Technical and organizational measures
The purpose of the following measures is to ensure that data collected for different purposes is processed separately:

- Requirements for rights management
- Separation of customers (multi-controller capability of the system used)
- Logical data separation (e.g. based on customer or Controller numbers)
- The Controller's and other customers' data are processed by different employees of the Processor
- Access authorisation policy which takes into account the requirement of processing Controller's data separately from other customers' data
- Segregation of functions
- Separation of development, testing and production systems
- Dedicated system

4.1.5 Pseudonymization

The Controller can configure the system settings to ensure that the processing of personal data takes place in a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.

4.2 Integrity (Article 32 (1) (b) GDPR)

4.2.1 Data transfer control

Scope
The objective of data transfer control is to ensure that personal data cannot be read, copied, modified or removed without authorisation during their transfer or transport or when storing the data on data carriers, and that it can be checked and determined who are the recipients of the personal data transfer.

Technical and organizational measures
The following measures have been implemented to achieve this objective:

Data exchange is cryptographically encrypted via a secure HTTPS connection.
Secure destruction of paper documents using document shredders or locked metal containers (known as data protection bins) and documented disposal by a certified service provider.

4.2.2 Input control

Scope
The objective of input control is to ensure that it is possible to check and establish whether and by whom personal data has been input into data processing systems, modified or removed.

Technical and organizational measures
The following measures have been implemented to achieve this objective:

- Identification of acquired data
- Definition of user authorizations (profiles)
- Differentiated user access authorizations:
    - Read, change, delete
    - Partial access to data or functions
    - Field access to databases
- Organisational specification of input responsibilities
- Logging of entries/erasures
- Obligation to maintain data confidentiality
- Log policy that goes beyond the OS standard

4.3 Availability and resilience (Article 32 (1) (b) GDPR)

4.3.1 Availability control

Scope
The objective of availability control is to ensure that personal data are protected against accidental destruction or loss.

Technical and organizational measures
The availability of the Hogrefe test system is guaranteed by the data center operator in terms of hardware. In addition, the following are implemented to ensure availability.

- Data backup and recovery concepts
- Implementation of data backup and recovery concepts
- Access restriction to server rooms limited to essential personnel
- Processes for secure development
- Patch and change management

4.3.2 Resilience and reliability control

Scope
The objective of resilience and reliability control is to ensure that systems can handle risk-related changes and have the ability to tolerate and withstand disruptions.

Technical and organizational measures
The availability of the Hogrefe test system is ensured on the hardware side by the data center operations.

In addition, the following are implemented to ensure availability:
- Disk mirroring
- Data storage on RAID systems (RAID 1 and above)

- Segregation of critical components
- Execution of penetration tests
- System hardening (disabling non-essential components)
- Immediate and regular activation of available software and firmware updates, including:

  – Identification of the various devices that make up the network, and determination of their hardware versions as well as current software and firmware versions
  – Establishment of communication channels with manufacturers to stay informed about new updates and patches released for owned devices
  – Definition of timeframes for implementing updates (e.g., periods of low activity, maintenance windows)
  – Use of redundant systems to maintain operations while primary devices are being updated
  – Progressive rollout of updates/patches to detect issues early without affecting multiple devices
  – Specification of a testing period to verify correct implementation of updates and ensure smooth operation with the new versions

- Security is considered a primary concern during the system design phase, including:

  – Restriction of permissions based on necessity
  – External contractors and maintenance personnel receive specific access that is only active during the intervention and deactivated at all other times

- Periodic awareness campaigns to educate users about security concepts specific to both dedicated systems and traditional IT systems

4.4 Process for regularly testing, assessing, evaluating (Article 32 (1) (d) GDPR; Article 25 (1) GDPR)

4.4.1 Control processes

We have implemented the following processes for regularly testing, assessing and evaluating the effectiveness of data security measures:

- Reporting of new/changed data processing procedures to the DPO
- Recording of processes for reporting new/changed procedures
- Selection of data protection-friendly default settings
- Subjecting the implemented protection measures to regular internal controls

4.4.2 Processing control

Scope
The objective of processing control is to ensure that personal data processed by service providers on behalf of the Controller (subprocessors) can only be processed in compliance with the Processor's instructions.

Technical and organizational measures
The following measures have been implemented to achieve this objective:

- Contracts drafted in accordance with legal requirements (Article 28 GDPR)
- Central recording of existing service providers (standard contract management)
- Regular checks by the Processor after the contract start date (during the term of the contract)
- Inspections at the premises of the Processor
- Verification of the Processor's data security concept
- Review of the Processor’s existing IT security certificates

5. List of subcontractors

The following subcontractors are engaged for processing, but only under the condition of a contractual agreement in accordance with Art. 28 (2) to (4) GDPR:

Company (subcontractor) and address	Processing location	Nature of the service
Hogrefe Verlag GmbH & Co. KG Merkelstr. 3 D-37085 Göttingen	Göttingen, Germany	Hosting, operation, support and development of the HTS online portal