Data Processing Agreement in Accordance with Article 28 of the General Data Protection Regulation (GDPR)

Agreement

between
International Brain Barriers Society, VUMC, Postbus 7057, 1007 MB Amsterdam, NL
- the Controller - hereafter named the "Client" -

and

Hetzner Online GmbH, Gunzenhausen
- the Processor - hereafter named the "Supplier" -

1. Subject matter and duration of the Agreement or Contract

The subject matter and duration of the Agreement or Contract shall be determined entirely according to the information provided in the respective contractual relationship.
The Supplier shall process personal data for the Client in accordance with Art. 4 No. 2 and Art. 28 GDPR on the basis of this Agreement.

2. Object, nature, and purpose of the collection, processing or use of data

The object, nature and purpose of any possible collection, processing, or use of personal data, the nature of data, and the People Affected shall be described to the Supplier by the Client in accordance with Appendix 1 of this document as completed by the Client, insofar as this is not governed by the contractual relationships described the content of Section 1 of this document. The provision of the contractually agreed upon data processing shall occur exclusively in a member state of the European Union or in another member state party to the Agreement on the European Economic Area. Any transfer to a third country shall require the prior consent of the Client and may only occur if the special conditions defined in Articles 44 et seq. of the GDPR are fulfilled.

3. Technical and organizational measures in accordance to Art. 32 GDPR (Art. 28 Para. 3 Sent. 2 Clause c of the GDPR)

(1) Before the commencement of data processing, the Supplier shall document the execution of the necessary Technical and organizational measures defined in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the Agreement

Hetzner Online GmbH
CEO: Martin Hetzner,
Stephan Konvickova, Günther Müller
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25
91710 Gunzenhausen | Germany
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

or Contract, and shall present these documented measures to the Client for inspection (See Appendix 2 of this document). Upon acceptance of said documents by the Client, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.
(2) The Supplier shall establish the security of the data in accordance with Art. 28 Para. 3 Sent. 2 Clause c, and Art. 32 GDPR in particular in conjunction with Art. 5 Para. 1 and Para. 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the technology; implementation costs; the nature, scope, and purposes of processing; as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the scope of Art. 32 Para. 1 GDPR must be taken into account.
(3) The technical and organizational measures shall be subject to technical progress and further development. In this respect, the Supplier is permitted to implement alternative adequate measures. The safety level of the specified measures must not be compromised. Substantial changes must be documented.

4. Correction, restriction, and deletion of data

(1) The Supplier is not entitled of his own authority to delete or restrict the processing of data processed on behalf of third parties. Insofar as an Affected Person contact the Supplier directly in this respect, the Supplier will immediately forward this request to the Client without delay.
(2) Insofar as the scope of services includes, the following are to be ensured without undue delay by the Supplier in accordance with the Client's documented instructions: a deletion policy, the "right to be forgotten", data correction, data portability, and data disclosure.

5. Quality assurance and other duties of the Supplier

In addition to complying with the provisions of this agreement, the Supplier shall comply with statutory obligations in accordance with Articles 28 to 33 GDPR; in this respect, the Supplier shall particularly ensure compliance with the following requirements:

- Mrs. Margit Müller, Head of Data Protection (+49 (0)9831 505-216, data-protection@hetzner.com) is appointed to the role of Data Protection Officer by the Supplier. The Client shall be immediately notified of any change of the Data Protection Officer. The Data Protection Officer's current contact details are easily accessible on the Supplier's website.
- Confidentiality in accordance with Art. 28 Para. 3 Sent. 2 Clause b, Art. 29 and Art. 32 Para. 4 GDPR. The Supplier entrusts only such employees with the data processing defined in this agreement who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data may only process that data in accordance with the instructions of

Hetzner Online GmbH
CEO: Martin Hetzner,
Stephan Konvickova, Günther Müller
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25
91710 Gunzenhausen | Germany
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

the Client (which includes the powers granted in this Agreement) unless otherwise required to do so by law.

- The implementation and observance of all technical and organizational measures necessary for this Agreement in accordance with Art. 28 Para. 3 Sent. 2 Claus c, Art. 32 GDPR are specified in Appendix 2 of this Agreement.
- The Supplier and the Client shall, upon request, cooperate with the supervisory authority in the performance of their duties.
- The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Agreement or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any civil or criminal law, administrative rule, or regulation regarding the processing of personal data in connection with the processing of this Agreement or Contract.
- Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim of an Affected Person or a third party or any other claim in connection with the processing of the Agreement or Contract by the Supplier, the Supplier shall make every effort to support the Client to the best of his ability.
- The Supplier shall regularly monitor the internal processes as well as the Technical and organizational measures to ensure that the processing in his area of responsibility is executed in accordance with the requirements of the applicable data protection law and that the rights of the Affected People are protected.
- The Client may request documentation to verify the execution of the Technical and organizational measures taken by the Supplier in accordance with section 3 of this Agreement by completing the form at https://www.hetzner.com/AV/TOM_en.pdf.

6. Subcontracts

For the purposes of this Agreement, subcontracting relationships are defined as those services which relate directly to the provision of the principal commission. This does not include ancillary services which the Supplier uses, e.g. telecommunications services; postal/ transport services; maintenance and user support services; as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Supplier is obligated to make appropriate and legally binding contractual arrangements and implement appropriate inspection measures to guarantee data protection and data security of the Client's data, even in the case of outsourced ancillary services.
If the Client selects a location outside of Germany for his dedicated servers, colocation servers, and Hetzner Cloud servers, he thereby accepts the Supplier's subcontractor as the data center operator and subcontractor at this location. A product-specific list of the subcontractors operating at each location can be found at: https://hetzner.com/AV/subcontractors.pdf.

Hetzner Online GmbH
CEO: Martin Hetzner,
Stephan Konvickova, Günther Müller
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25
91710 Gunzenhausen | Germany
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

7. The Client's inspection rights

(1) The Client shall have the right to implement inspections in consultation with the Supplier or to have them implemented by inspectors designated in individual cases. The Client shall have the right to verify compliance with this Agreement by the Supplier in his business operations by means of spot inspections, which shall as a general rule be announced in good time.
(2) The Supplier shall ensure that the Client can verify the Supplier's compliance with the obligations under Article 28 of the GDPR. The Supplier is obligated to provide the Client with the necessary information upon request and in particular to provide proof of the implementation of the Technical and organizational measures.
(3) Evidence of such measures which concern not only this specific Agreement or Contract may be provided by compliance with approved codes of conduct pursuant to Article 40 GDPR; certification according to an approved certification procedure in accordance with Article 42 GDPR; current auditor's certificates, reports, or excerpts from reports provided by independent bodies (e.g. an auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor); or a suitable certification by IT security or data protection auditing, e.g. according to "BSI-Grundschutz" (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology [BSI]).
(4) The Supplier may assert a claim for remuneration for enabling the Client's inspections.

8. Communication in the case of infringement by the Supplier

(1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments, and prior consultations referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an adequate level of protection with the Technical and organizational measures that take into account the circumstances and purposes of the data processing, the projected probability and severity of potential breaches of the law due to security vulnerabilities, and measures that enable relevant breaches of the law to be detected immediately.
b) The obligation to immediately report violations of personal data to the Client.
c) The duty to assist the Client with regard to the Client's own obligation to provide information to the Affected People and, in this context, to immediately inform the Client of its own obligations.
d) Assisting the Client with his data protection impact assessment.
e) Assisting the Client with regard to prior consultation with the supervisory authority.

(2) The Supplier may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.

9. The Client's authority to issue instructions

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).

Hetzner Online GmbH
CEO: Martin Hetzner,
Stephan Konvickova, Günther Müller
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25
91710 Gunzenhausen | Germany
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

(2) The Supplier shall inform the Client immediately if he believes that an instruction violates data protection regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or alters said instructions.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall not be created without the knowledge of the Client, with the exception of backup copies as far as they are necessary to ensure proper data processing as well as data required for compliance with statutory storage obligations.
(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement, the Supplier shall submit to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession in accordance with data protection law. The same applies to any and all connected test and scrap material. Upon request, the Supplier shall provide the Client with information on nature and the time of the data's deletion.
(3) The Supplier shall retain documentation that proves that data was processed in an orderly and contractual manner after the respective contract period has elapsed in accordance with respective retention periods beyond the end of the contract. Alternatively, the Supplier may be absolved of this duty by transferring said documentation to the Client upon the termination of the contract.

11. Other agreements

11.1. Reimbursement

A fee for this contract is not required.
If the Client requires assistance in answering inquiries from Affected People as described in section 4 of this Agreement, the Client shall be required to reimburse the Supplier for such assistance.
If the Client exercises monitoring rights as described in section 7 of this Agreement, the amount of remuneration to be agreed upon will be based on the fixed hourly rate of the Supplier's employee who is instructed to supervise the auditor.
If the Client issues instructions to the Supplier as described in section 9 of this Agreement, the Client shall be required to pay any costs that result from these instructions.

11.2. Duration of contract

This Agreement is dependent on the existence of a principal contractual relationship as described in section 1 of this document. The cancellation or other termination of the principal contractual relationship as described in section 1 shall simultaneously invalidate this Agreement.
The right to isolated extraordinary notice of cancellation hereby remains intact as do statutory rights of rescission.

11.3. Choice of law

The laws of the Federal Republic of Germany shall apply.

Hetzner Online GmbH
CEO: Martin Hetzner,
Stephan Konvickova, Günther Müller
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25
91710 Gunzenhausen | Germany
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

11.4. Place of jurisdiction

The parties agree that the place of jurisdiction shall be the location of the court responsible for Gunzenhausen.

Signatures

_____, date _____

Client

Gunzenhausen, date 16.03.18

Supplier

Hetzner Online GmbH
CEO: Martin Hetzner,
Stephan Konvickova, Günther Müller
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25
91710 Gunzenhausen | Germany
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

Appendix 1 Pursuant to Art. 28 GDPR:

List of Personal Data and the Purpose of Their Being Processed

Types of data

The following types and categories of data are the object of this additional agreement:

- Personal master data
- Communication data (e. g. telephone, email)
- Contractual master data
- Log data

Affected People

Those affected as a result of this additional agreement include:

- IBBS Members

Hetzner Online GmbH
CEO: Martin Hetzner,
Stephan Konvickova, Günther Müller
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25
91710 Gunzenhausen | Germany
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

Appendix 2 of the Agreement Pursuant to Art. 28 GDPR: Technical and Organizational Measures in Accordance with Art. 32 GDPR and Amendments

I. Confidentiality

- Physical access control
  - Data center parks in Nürnberg and Falkenstein
    - electronic physical entry control system with log
    - high security perimeter fencing around the entire data center park
    - documented distribution of keys to employees and colocation customers for colocation racks (each Client only for his rack)
    - policies for accompanying and designating guests in the building
    - data center staff present 24/7
    - video monitoring at entrances and exits; security door interlocking systems and server rooms
    - For people outside of the employment of Hetzner Online GmbH (data center visitors), entrance to the building is only permitted in the company of a Hetzner Online employee.
  - Monitoring
    - electronic physical access control system with log
    - video surveillance for all entrances and exits
- Electronic access control
  - for dedicated root server, colocation server, cloud server, and storage box principal commissions
    - server passwords, which, after the initial deployment, can only be changed by Client and are not known to the Supplier
    - The Client's password for the administration interface is determined by the Client himself; the password must comply with predefined guidelines. In addition, the Client may employ two-factor authentication to further secure his account.
  - for managed server, web hosting, and Nextcloud principal commissions
    - Access is password-protected and only employees of the Supplier have access to the passwords. Passwords must meet a minimum length, and new passwords shall be changed on a regular basis.
- Internal access control
  - for the Supplier's internal administration systems
    - The Supplier shall prevent unauthorized access by applying security updates regularly by using state of the art technology.
    - a revision-proof, compulsory process for allocating authorization for Supplier employees
  - for dedicated root server, colocation server, cloud server, and storage box principal commissions

Hetzner Online GmbH
CEO: Martin Hetzner,
Stephan Konvickova, Günther Müller
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25
91710 Gunzenhausen | Germany
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

        - The responsibility for access control is incumbent upon the Client.
    - for managed server, web hosting, and Nextcloud principal commissions
        - The Supplier shall prevent unauthorized access by applying security updates regularly by using state of the art technology.
        - a revision-proof, compulsory process for allocating authorization for Supplier employees
        - Only the Client is responsible for transferred data/software with regard to security and updates.
- Transfer control
    - Data center parks in Nürnberg and Falkenstein
        - Drives that were in operation on canceled servers will be swiped multiple times (deleted) in accordance with data protection polices upon termination of the contract. After thorough testing, the swiped drives will be reused.
        - Defective drives that cannot be securely deleted shall be destroyed (shredded) directly in the Falkenstein data center.
- Isolation control
    - for the Supplier's internal administration systems
        - Data shall be physically or logically isolated and saved separately from other data.
        - Backups of data shall also be performed using a similar system of physical or logical isolation.
    - for dedicated root server, colocation server, cloud server, and storage box principal commissions
        - The Client is responsible for isolation control.
    - for managed server, web hosting, and Nextcloud principal commissions
        - Data shall be physically or logically isolated and saved separately from other data.
        - Backups of data shall also be performed using a similar system of physical or logical isolation.
- Pseudonymization
    - The Client is responsible for pseudonymization.

II. Integrity (Art. 32 Para.1 Clause b GDPR)

- Data transfer control
    - All employees are trained in accordance with Art. 32 Para. 4 GDPR and are obliged to ensure that personal data is handled in accordance with data protection regulations.
    - Deletion of data in accordance with data protection regulations after termination of the contract.
    - Encrypted data transmission options are provided within the scope of the service description of the principal commission.

Hetzner Online GmbH
CEO: Martin Hetzner,
Stephan Konvickova, Günther Müller
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25
91710 Gunzenhausen | Germany
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

- Data entry control
  - for the Supplier's internal administration systems
    - Data is entered or collected by the Client.
    - Changes in data are logged.
  - for dedicated root server, colocation server, cloud server, and storage box principal commissions
    - The responsibility for input control is incumbent upon the Client.
  - for managed server, web hosting, and Nextcloud principal commissions
    - Data is entered or collected by the Client.
    - Changes in data are logged.

III. Availability and Resilience (Art. 32 Para. 1 Clause b GDPR)

- Availability control
  - for the Supplier's internal administration systems
    - backup and recovery concept with daily backups of all relevant data
    - professional employment of security programs (virus scanners, firewalls, encryption programs, spam filters)
    - employment of disk mirroring on all relevant servers
    - monitoring of all relevant servers
    - employment of an uninterruptible power supply system or emergency power supply system
    - permanently active DDoS protection
  - for dedicated root server, colocation server, cloud server, and storage box principal commissions
    - Data backup is incumbent upon the Client.
    - employment of an uninterruptible power supply system or emergency power supply system
    - permanently active DDoS protection
  - for managed server, web hosting, and Nextcloud principal commissions
    - backup and recovery concept with daily backups of all relevant data depending upgon the services booked for the principal commission
    - employment of disk mirroring
    - employment of an uninterruptible power supply system or emergency power supply system
    - employment of software firewalls and restricted ports
    - permanently active DDoS protection
- Rapid recovery measures (Art. 32 Para. 1 Clause c GDPR)
  - For all internal systems, there is a defined escalation chain which specifies who is to be informed in the event of an error in order to restore the system as quickly as possible.

Hetzner Online GmbH
CEO: Martin Hetzner,
Stephan Konvickova, Günther Müller
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25
91710 Gunzenhausen | Germany
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

IV. Procedures for regular testing, assessment, and evaluation (Art. 32 Para. 1 Clause d GDPR; Art. 25 Para. 1 GDPR)

- The data protection management system and the information security management system have been combined into a DIMS (data protection information security management system).
- Incident response management is available.
- Data-protection-friendly default settings are taken into account for software development (Art. 25 Para. 2 GDPR).

- Agreement or contract control
  - Hetzner Onling GmbH employees are regularly instructed in data protection law and are familiar with the procedural instructions and user guidelines for data processing on behalf of the Client also with regard to the Client's right of instruction. The General Terms and Conditions contain detailed information on the type and scope of the commissioned data processing and use of the Client's personal data.
  - The General Terms and Conditions contain detailed information about the purpose limitation of Client’s personal data.
  - Hetzner Online GmbH has appointed a company Data Protection Officer and an Information Security Officer. The data protection organization and the information security management systems integrate both officers into the relevant operational procedures.

Hetzner Online GmbH
CEO: Martin Hetzner,
Stephan Konvickova, Günther Müller
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25
91710 Gunzenhausen | Germany
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760