phexnet
UG (haftungsbeschränkt)

PHEXNET UG · DPA · SPECIMEN

Data Processing Agreement

Agreement under Art. 28 GDPR

This English version is a translation of the German original. In the event of any dispute, the German version shall prevail.

01 CONTRACTING PARTIES

This data processing agreement under Art. 28 GDPR is concluded between

Muster GmbH, Musterstraße 1, 20095 Hamburg, Amtsgericht Hamburg, HRB 000000, represented by the managing director Erika Mustermann (hereinafter “Controller”)

and

phexnet UG (haftungsbeschränkt), Am Pfeilshof 9A, 22393 Hamburg, Germany, Amtsgericht Hamburg (Hamburg Local Court), HRB 114863, represented by the managing director Dr. Felix Reher (hereinafter “Processor”)

– together the “Parties” –

02 SUBJECT MATTER OF THE PROCESSING

Service basis	the agreement existing between the parties on the services named in this agreement
Services	Web hosting (web server, runtime environment, database); Mail hosting (mailboxes, receipt, filtering and sending of emails); File sharing (fileshare.phexnet.de)
Nature of the processing	Collection, recording, storage, retrieval, consultation, transmission to the Controller and to the recipients it designates, backup, restoration, restriction and erasure (Art. 4(2) GDPR), in each case insofar as required for the agreed services.
Web hosting – subject matter	Operation of the web server, the runtime environment and the database for the Controller's websites (www.example.org).
Web hosting – purpose	Provision and protection of the websites, receipt of form entries and their forwarding to the Controller, error analysis and defence against attacks.
Web hosting – data	Content of the websites and their databases, form entries, accounts of website users, access and error logs of the web server with IP address, time, requested address, status code, amount of data transferred, referrer and user agent.
Web hosting – data subjects	Visitors to the websites, senders of forms, users with an account, persons named in the content.
Mail hosting – subject matter	Operation of the mail server for the Controller's domains (example.org), including receipt, checks for spam and malware, delivery, storage in mailboxes and sending.
Mail hosting – purpose	Provision of the mailboxes and protection of the Controller's email traffic.
Mail hosting – data	Content and attachments of emails, header and connection data, mailbox credentials (passwords only as Argon2id hash values), delivery and filter logs, messages held back as spam or malware (quarantine).
Mail hosting – data subjects	Mailbox holders, senders and recipients of emails, persons named in emails.
File sharing – subject matter	Provision of the file share fileshare.phexnet.de for exchanging files between the Controller and the persons it designates.
File sharing – purpose	Transmission and time-limited provision of files to the persons designated by the Controller and receipt of files via upload links, including checks for malware on receipt.
File sharing – data	Uploaded files and their names, details of shares (recipients, times, validity) and of downloads.
File sharing – data subjects	Senders and recipients of the files, persons named in the files.
Backup	Copies of the data named above in the daily encrypted backups of the servers on storage space of the data centre operator in Falkenstein (Germany) (Annex 1).

Communication – purpose	Handling support requests, receiving instructions and issuing notifications by email; personal data that the Controller communicates in this context enters the Processor's mailboxes (Annex 2).
Communication – data subjects	Contact persons and employees of the Controller and persons named in requests, instructions or notifications.
Special categories	Not intended. Such data is only processed insofar as the controller, its users or third parties introduce it into content, messages or files.
Safeguards for special categories	If special categories of personal data (Art. 9(1) GDPR) or data relating to criminal offences (Art. 10 GDPR) are processed, only administrators of the Processor access them within the scope of documented instructions, the content is not analysed and is processed only in the systems of the agreed services; the Parties agree further restrictions or safeguards in text form (standard contractual clauses under Implementing Decision (EU) 2021/915, Clause 7.5).
Location of processing	The Processor's servers in the Falkenstein (Germany) and Helsinki (Finland) data centres of the data centre operator named in Annex 2; processing outside the European Union and the European Economic Area only takes place in accordance with § 5(5).

03 PROVISIONS

§ 1 Term and termination

(1) This agreement applies from its signature by both Parties and for the duration of the service basis.

(2) It ends with the service basis without the need for separate termination. The right of both Parties to terminate for good cause remains unaffected. Good cause exists for the Controller in particular if the Processor seriously breaches this agreement or the GDPR, fails to carry out a lawful instruction or refuses inspections under § 9.

(3) If the Processor breaches this agreement or the GDPR, the Controller may instruct it to suspend the processing until the breach has been remedied. If the breach is not remedied within a reasonable period, the Controller may terminate this agreement and the affected services without notice.

(4) The obligations under this agreement continue until all data has been erased or returned in accordance with § 8.

§ 2 Instructions

(1) The Processor processes the data only on documented instructions from the Controller, including with regard to transfers to a third country or an international organisation, unless required to do otherwise by Union or Member State law to which it is subject; in such a case, the Processor informs the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest (Art. 28(3)(a) GDPR).

(2) This agreement with its annexes, the service basis and the configuration of the services initiated by the Controller contain the instructions. The erasure periods set out in Annex 1 are instructions. The Controller issues further instructions in text form; it confirms oral instructions in text form without undue delay. The Processor retains instructions for the term of this agreement.

(3) Persons entitled to issue instructions at the Controller: Erika Mustermann, managing director, erika.mustermann@example.org

(4) Instructions are received at the Processor by: Dr. Felix Reher, managing director, info@phexnet.de

(5) The Processor does not process the data for its own purposes or for other clients.

(6) If an authority or court requests the disclosure of the Controller's data, the Processor informs the Controller without undue delay, insofar as this is legally permissible, examines the lawfulness of the request and discloses data only insofar as it is legally obliged to do so; it complies with requests from third countries only in accordance with Art. 48 GDPR.

(7) If the Processor considers that an instruction infringes the GDPR or other Union or Member State data protection provisions, it informs the Controller without undue delay (Art. 28(3), third sentence, GDPR). It may suspend execution until the Controller confirms or changes the instruction.

§ 3 Confidentiality

(1) The Processor ensures that persons authorised to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR). The obligation continues after the end of their activity and after the end of this agreement.

(2) It ensures that persons acting under its authority who have access to the data process it only on instructions from the Controller (Art. 29, Art. 32(4) GDPR). Only persons entrusted with the operation and administration of the servers and services have access to the data; the Processor names them to the Controller on request.

(3) The persons deployed for mail hosting are bound by the secrecy of telecommunications (Section 3 TDDDG); they take note of the content and detailed circumstances of communications only insofar as this is necessary for operating and protecting the service (Section 206 StGB).

§ 4

Security of processing

(1) The Processor takes the technical and organisational measures described in Annex 1 (Art. 28(3)(c), Art. 32 GDPR).

(2) It may adapt the measures to the state of the art provided that the level of protection does not decrease. It documents significant changes and notifies the Controller of them in text form.

§ 5

Further processors

(1) The Processor engages further processors only in accordance with Art. 28(2) and (4) GDPR (Art. 28(3)(d) GDPR).

(2) The Controller authorises the engagement of the further processors named in Annex 2.

(3) Otherwise, the Controller grants a general authorisation. The Processor informs it at least 30 days before engaging a new further processor or replacing one, and before a change of data centre, by email to the address under § 10(4), stating the name, registered office, service and location of processing. It publishes the current list, with its date, at https://vertrag.phexnet.de/unterauftragnehmer. The Controller may object within this period (Art. 28(2), second sentence, GDPR). Following an objection, the change does not take place; if the service is not possible without it, either Party may terminate the affected service and this agreement with 30 days' notice.

(4) The Processor imposes on each further processor by contract the same data protection obligations as set out in this agreement, in particular sufficient guarantees for appropriate technical and organisational measures. If the further processor fails to fulfil its obligations, the Processor remains liable to the Controller for this (Art. 28(4) GDPR). It presents the contracts with the further processors to the Controller on request.

(5) Processing outside the European Union and the European Economic Area only takes place if the conditions of Art. 44 et seq. GDPR are met; Annex 2 names the safeguards that apply to the further processors listed. Any further transfer to a third country requires the Controller's prior consent in text form.

§ 6

Assistance to the Controller

(1) Taking into account the nature of the processing, the Processor assists the Controller by appropriate technical and organisational measures, insofar as possible, in responding to requests from data subjects under Art. 12 to 22 GDPR (Art. 28(3)(e) GDPR). This includes information from data and logs and their rectification, erasure or restriction, insofar as the data can be attributed to a person.

(2) The Processor forwards requests from data subjects that it receives to the Controller without undue delay and does not answer them itself.

(3) Taking into account the nature of the processing and the information available to it, it assists the Controller in complying with the obligations under Art. 32 to 36 GDPR (Art. 28(3)(f) GDPR), in particular with the security of processing, notifications and communications under Art. 33 and 34 GDPR, a data protection impact assessment and a prior consultation of the supervisory authority.

(4) It maintains a record of all categories of processing activities carried out on behalf of controllers (Art. 30(2) GDPR) and presents it to the Controller for this engagement on request.

§ 7

Personal data breaches

(1) The Processor notifies the Controller of a personal data breach without undue delay, if possible within 24 hours of becoming aware of it (Art. 33(2) GDPR). This also applies to breaches at a further processor.

(2) The notification contains the information under Art. 33(3) GDPR known to the Processor; it provides missing information subsequently.

(3) It takes the necessary measures to secure the data and mitigate adverse consequences without undue delay and documents the breach, its effects and the remedial measures.

(4) Notwithstanding the erasure periods in Annex 1, it retains log data required for the investigation until the investigation has been concluded and informs the Controller of this.

(5) Only the Controller notifies the supervisory authority and communicates with data subjects.

§ 8

Erasure and return

(1) During the term, the Processor erases the data in accordance with the periods in Annex 1 and on the Controller's instructions.

(2) After the end of the provision of the processing services, the Processor, at the Controller's choice, erases all personal data or returns it and erases existing copies, unless Union or Member State law requires storage of the personal data (Art. 28(3)(g) GDPR). The return takes place as an export in a common format (for example website files, a database dump, mailboxes, files) within 30 days after the end of the agreement; after that, or if the Controller does not make a choice, the Processor erases the data.

(3) Copies in the backups cannot be erased individually from the encrypted full backups. The backup snapshots are overwritten according to this rotation, daily snapshots 14 days, weekly 8 weeks, monthly 12 months, yearly 3 years. The Controller therefore instructs the Processor not to erase the copies specifically after the end of the agreement, but to let them expire with the rotation; they are erased as soon as the last snapshot containing them expires, at the latest 3 years after the end of the agreement.

(4) Until then, the copies are blocked. The Processor does not use them for any purpose and restores them only on the Controller's instructions. If it has to restore a snapshot that also contains the Controller's data, it erases this data without undue delay after the restoration. The obligations under this agreement continue to apply to the copies.

(5) The Processor confirms the erasure in text form. It ensures that the further processors also erase the data.

§ 9

Evidence and inspections

(1) The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations under Art. 28 GDPR and this agreement, and allows for and contributes to audits, including inspections, conducted by the Controller or an auditor mandated by it and bound to confidentiality (Art. 28(3)(h) GDPR).

(2) Audits are announced with at least 14 days' notice, and at short notice in the event of a justified suspicion of a breach. Insofar as a review of documents, of the configuration or a remote review is sufficient, no on-site inspection takes place.

(3) For the data centres, the Processor may provide evidence by means of current attestations, certificates or audit reports of the data centre operator. The Controller's right to carry out its own audits remains unaffected.

§ 10

Obligations of the Controller and contact persons

(1) The Controller is responsible for the lawfulness of the processing, for the legal bases, for informing the data subjects and for safeguarding their rights (Art. 24 GDPR).

(2) It notifies the Processor in advance in text form of changes that alter the nature, scope or purpose of the processing; the Parties adapt this agreement and its annexes accordingly.

(3) It informs the Processor without undue delay if it discovers errors or irregularities in the processing.

(4) Forwarded requests under § 6(2) and notifications under § 7 are sent to: datenschutz@example.org

(5) Data protection officer of the Controller: _____

(6) The Processor has not appointed a data protection officer. Contact for data protection: info@phexnet.de. Competent supervisory authority of the Processor: The Hamburg Commissioner for Data Protection and Freedom of Information.

§ 11

Liability and remuneration

(1) The Parties are liable to data subjects in accordance with Art. 82 GDPR. The Processor is liable for damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the Controller (Art. 82(2), second sentence, GDPR). This agreement does not limit liability towards data subjects.

(2) Where a Party has paid full compensation, it may claim back from the other Party that part of the compensation corresponding to the other Party's part of responsibility for the damage (Art. 82(5) GDPR).

(3) Otherwise, the Parties are liable to each other in accordance with the service basis and the statutory provisions.

(4) The Processor may charge for assistance under §§ 6 and 9 that goes beyond the service basis and is not caused by a breach on the part of the Processor, according to effort and after prior notice. Notifications and assistance under § 7 are not remunerated separately.

§ 12

Final provisions

(1) This agreement is in writing, which may be in electronic form (Art. 28(9) GDPR). An electronic signature is sufficient. Amendments and additions require text form.

(2) This agreement is in version 2026-11-21.1; Annexes 1 and 2 form part of this agreement. In the event of conflict, this agreement takes precedence over the service basis in matters of data protection.

(3) Both Parties retain this agreement until the end of the third calendar year after its termination (evidence under Art. 5(2), Art. 28 GDPR).

(4) If any provision of this agreement is invalid, the remainder of the agreement remains valid. The invalid provision is replaced by the statutory provision.

(5) German law applies. The place of jurisdiction is Hamburg, insofar as an agreement on jurisdiction is permissible (Section 38 ZPO).

04 SIGNATURES

Controller	Muster GmbH
Signed by	Erika Mustermann, managing director
Place, date	
Processor	phexnet UG (haftungsbeschränkt)
Signed by	Dr. Felix Reher, managing director
Place, date	

05 ANNEX 1 – TECHNICAL AND ORGANISATIONAL MEASURES

	The measures apply to all services under this agreement (Art. 32 GDPR). Information as of 18.11.2026; the values were measured on the Processor's servers.
Location of processing	Servers in the Falkenstein (Germany) and Helsinki (Finland) data centres of the data centre operator named in Annex 2.
Physical access	The servers are located in the data centres of the data centre operator. Physical access is governed by its technical and organisational measures under the agreement pursuant to § 5(4).
System access	Administrative access to the servers from outside is only possible via a central management access point with sign-in; sign-ins to servers only with SSH keys. Management applications can only be reached after sign-in via the central sign-in service with password and second factor, and only for accounts authorised for the respective service. Administrator sign-ins are logged.
Data access	Each application has its own database accounts with the permissions it requires. Credential files are stored outside the web directories and can only be read by the system administrator and the respective service.
Separation	Websites run in their own virtual hosts with their own web directories and databases, application instances are separated per customer; data of different clients is not merged.
Transfer	The services are delivered via TLS. The TLS connection terminates at the processor's reverse proxy in Falkenstein (Germany); from there, requests are forwarded to the application servers in Helsinki (Finland), that is, between two data centres. The processor does not commit to additional transport encryption for this forwarding. Backups are transferred in encrypted form.
Pseudonymisation	Pseudonymisation by the Processor is not provided for; the Controller determines the content and form of the data through its use of the services.
Storage media	The servers' storage media are not encrypted. The backups are stored encrypted, as is data that an application encrypts itself.
Key management	The processor generates and keeps the backup keys (repository key and passphrase) itself on the server that writes the backup, readable only by the system administrator; the data centre operator receives backups and copies of these keys only in encrypted form. Keys with which an application encrypts data itself are kept by the processor separately from that data, per instance with an identifier; older keys are retained as long as backups made with them exist.
Availability	Daily backup of all servers, encrypted (Borg) on storage space of the data centre operator (Storage Box) in the Falkenstein (Germany) data centre; retention of snapshots, daily snapshots 14 days, weekly 8 weeks, monthly 12 months, yearly 3 years; after the end of the agreement, the Controller's copies are blocked until they expire (§ 8). Availability and load of the servers and services are monitored.
Resilience and recovery	The services run on individual servers without automatic failover to a second server; high availability is not part of the services. After an outage, the Processor restores from the most recent daily backup. A documented recovery test in an isolated environment and a guaranteed recovery time are not yet available; the processor carries out the test at least once a year and discloses the result and measured duration on request.
Protection against malware	Incoming emails are checked for spam and malware, files in the file share on receipt; the servers receive automatic security updates.
Security updates	Security updates are installed automatically; a security update that remains outstanding for more than 7 days triggers an alert.
Email transport	Submission by users only encrypted (submission with enforced TLS, SMTPS); mailbox retrieval (IMAP, POP3) only encrypted; TLS is used between mail servers if the other side offers it; MTA-STS and TLS reporting can be enabled per domain.
Input control	Access and changes can be traced via the logs of the web servers, the mail server, the system journal and the administrators' sign-in log.
Erasure periods	Web server access and error logs 14 days; block logs (fail2ban) 4 weeks; mail server logs 4 weeks; server system journal 30 days; administrator sign-in log 365 days; backups according to the rotation under “Availability”, at most 3 years. Contents of the services (websites, mailboxes, files, application data) are kept until erased by the Controller or on its instructions and in accordance with § 8.
Personnel	Persons with access are bound to confidentiality before starting their work (§ 3) and instructed in data protection; they receive access only to the extent required, and access is revoked without undue delay when they leave or change roles.
Incidents	Security incidents are detected through monitoring or reports, assessed, resolved and documented with cause, impact and remedy; the Processor reports personal data breaches in accordance with § 7.

Destruction of storage media	Decommissioned server storage media are erased or destroyed by the data centre operator in accordance with its technical and organisational measures (agreement pursuant to § 5(4)).
Processing control	Processing only on documented instructions pursuant to § 2; further processors only pursuant to § 5 and with an agreement under Art. 28(4) GDPR.
Review	The Processor reviews these measures at least once a year and in the event of significant changes, documents the result and presents it on request (Art. 32(1)(d) GDPR).

06 ANNEX 2 – FURTHER PROCESSORS

	The Controller authorises the engagement of the following further processors (§ 5(2)). List as of 21.11.2026; the current version is available at https://vertrag.phexnet.de/unterauftragnehmer.
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Germany; contact: the data protection officer of Hetzner Online GmbH at the address given. Service: Servers in the data centre and storage space for the backups (Storage Box). Location of processing: Falkenstein (Germany) and Helsinki (Finland) data centres; storage space for the backups (Storage Box) in Falkenstein (Germany); under the agreement with Hetzner, processing exclusively within the European Union or the EEA. Agreement under Art. 28(4) GDPR dated 19 November 2026.
Nanosystems S.r.l.	Via del Commercio, 76/A, 63100 Ascoli Piceno (AP), Italy; contact: Nanosystems S.r.l. at the address given. Service: Brokering the connection for remote support via the support tool (Supremo); sessions are not recorded. Location of processing: Servers in the European Union; Registered office and processing in the European Union.
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland; contact: Microsoft's data protection officer in the EU via https://aka.ms/privacyresponse. Service: Email mailboxes and office communication of the processor (Microsoft 365), exclusively for communication with the controller (support requests, instructions, notifications). Location of processing: Data centres in the European Union (EU Data Boundary); access from third countries, in particular by Microsoft Corporation (USA), is possible in exceptional cases and is safeguarded by certification under the EU-US Data Privacy Framework (Art. 45 GDPR) and by standard contractual clauses (Art. 46(2)(c) GDPR) in Microsoft's data protection addendum. Agreement under Art. 28(4) GDPR: Microsoft Products and Services Data Protection Addendum, version according to the Product Terms as of the conclusion of the contract.