remoteroom customer data processing agreement (AVV/DPA)

Version: 2026-10-25-netcup · Effective with the Service Agreement incorporating this version

This agreement governs personal data processed on behalf of business customers of the remoteroom file-transfer service, including Free accounts. The annexes form part of the agreement. Section 10 explains when it becomes binding.

1. Parties, scope and order of precedence

1.1. This agreement is between **remoteroom GmbH**, Theodorstraße 41P, 22761 Hamburg, Germany, registered with Amtsgericht Hamburg under HRB 199300, represented by its managing directors Max Hartmann and Finn Jakob Jaeger (**remoteroom**), and the business customer that enters into the Service Agreement (**Customer**). The Customer is the account holder acting in its own business capacity, or the legal entity on whose behalf an authorized account holder contracts. Its identity and contact are those in the account and applicable order or written agreement. The service is the remoteroom file-transfer service provided under the parties' Terms of Service or other written service agreement (**Service Agreement**).

1.2. This agreement applies where remoteroom processes personal data on the Customer's behalf in providing that service (**Customer Personal Data**). It applies to both Free and Pro use; the absence of a fee does not exclude it. The Customer acts as controller or, when acting for another controller, as processor. In the latter case remoteroom acts as the Customer's subprocessor, and the Customer must have authority to give the instructions and approvals in this agreement. References to the Customer's controller duties then mean duties within its authority and its duty to involve the upstream controller.

1.3. This agreement and its annexes form part of the Service Agreement. This agreement prevails where terms conflict about the processing it covers. Mandatory data protection law and any applicable international transfer clauses take priority. References to the GDPR mean Regulation (EU) 2016/679; its definitions apply.

1.4. Processing carried out by remoteroom for its independently determined purposes, such as account administration, billing, service security, abuse investigation and compliance with legal duties, is described in the Privacy Notice. Roles depend on the actual purpose of each activity; this clause does not permit remoteroom to repurpose customer files. Technical delivery of Customer-selected files and requested transfer messages remains within this agreement even where the same service also performs controller activities.

2. Instructions and permitted use

2.1. The subject matter, data, individuals, operations and duration are set out in Annex 1. The Service Agreement, this agreement, choices made by authorized users through the service and additional documented instructions agreed through the contacts in Annex 4 constitute the Customer's instructions. These include uploading files, selecting recipients and link protections, permitting downloads, setting or changing available expiry options, and requesting deletion.

2.2. remoteroom will process Customer Personal Data only on those documented instructions, including instructions concerning international transfers, unless Union or Member State law applicable to remoteroom requires otherwise. In that case remoteroom will notify the Customer of the legal requirement before processing unless that law prohibits notice on important public-interest grounds. It will promptly inform the Customer if, in its opinion, an instruction infringes applicable data protection law, and may suspend the affected instruction while the parties resolve it. It will document additional instructions and disclosures.

2.3. remoteroom receives only the rights to customer content needed to carry out the service and lawful instructions. It will not sell customer files, use them for advertising, train AI models on them, or inspect their content for its own commercial purposes. Access needed to fulfil authorized support, investigate a security incident or comply with a legal obligation must be limited to the purpose and to authorized personnel. This is not a representation that the service is end-to-end encrypted or that technical access is impossible.

2.4. The Customer is responsible for the lawfulness of its instructions, required notices and legal bases, its authority to provide the data and the recipients it selects. The parties will assess any processing involving GDPR Article 9 special categories or Article 10 offence data before it begins and agree in writing on necessary additional safeguards. The general service does not itself establish suitability for a particular regulated or high-risk use.

3. Temporary transfer service and file copies

3.1. The service provides file delivery and temporary availability under the lifecycle in Annex 2. **It is not a backup, archiving or disaster-recovery service for customer files.** The Customer must retain its originals or its own backup and arrange for recipients to download files before their availability ends. Storage capacity or Pro access does not create a separate file-backup service.

3.2. **Customer file payloads are not included in remoteroom's database or its Proxmox/PBS/cloud database backups.** File payloads are stored in Cloudflare R2 and delivered through the download service. The database contains operational records, including file names, transfer messages, addresses and access-related records, which may themselves be personal data. The authorized database-backup locations and the operational limits of those arrangements are described in Annex 4. Database recovery does not provide an independent backup of the file payloads or a guaranteed recovery point or recovery time.

3.3. No independent file-backup or archive copy is created by remoteroom for later recovery. This does not mean only one physical copy exists: R2 uses its own storage redundancy, the service uses short deletion-recovery copies in R2, downloads can produce temporary edge-cache copies, and ZIP delivery uses temporary manifests. Annex 2 describes these processing stages. They are not customer-accessible backup repositories or a promise of successful recovery.

3.4. The service cannot restore a file after all service-controlled copies have been purged; a database backup cannot reconstruct the file payload. Files already downloaded or retained by the Customer or its recipients remain under their control. These scope limits do not exclude remoteroom's duties under Article 32 GDPR, responsibility for performing the agreed service, or mandatory liability.

4. Personnel and security

4.1. remoteroom will allow access to Customer Personal Data only to personnel who need it for authorized duties, are bound by confidentiality or an appropriate statutory duty, and are instructed in handling the data securely. Access will be withdrawn when no longer required.

4.2. remoteroom will implement and maintain the technical and organisational measures in Annex 2 and the backup/security arrangements in Annex 4, appropriate to the risks, nature, scope, context and purposes of processing. It will review their effectiveness and may update them without materially reducing the agreed protection. Material changes will be documented and made available to the Customer. If a proposed use requires additional measures, the parties must agree them before that processing begins.

4.3. The parties acknowledge the actual link-access model: a person holding an unprotected share link may access the transfer. Password protection is available where described by the service. Previously issued signed download links have their own validity period; deletion or a password change does not promise their instant revocation. The Customer should use available protections appropriate to its data and share passwords through a separate channel.

5. Subprocessors and processing locations

5.1. The Customer grants general written authorization to the subprocessors identified, with their activities and locations, in Annex 3. remoteroom will bind each subprocessor to data protection obligations providing in substance the protection required by this agreement and Article 28 GDPR, verify sufficient guarantees, and remain responsible to the Customer for the subprocessor's performance of those obligations.

5.2. remoteroom will give the Customer at least **30 calendar days' advance written notice** of an intended addition or replacement, identifying the entity, purpose, relevant processing locations, transfer safeguards and intended start date. The Customer may object during that period on reasonable data protection grounds. The parties will seek a suitable solution. The new subprocessor will not process that Customer's data while an unresolved objection is being assessed; if no solution is possible, either party may terminate the affected service before the change, with return/deletion under section 8 and a proportionate refund of unused prepaid charges for the affected period.

5.3. On request, remoteroom will provide relevant subprocessor-contract evidence, with proportionate redactions for secrets, security details and other customers' data. Such redactions must not prevent verification of the required obligations.

5.4. Customer Personal Data may be processed only at the locations and under the transfer arrangements disclosed in Annexes 3 and 4 and in accordance with documented instructions. A transfer requiring GDPR Chapter V safeguards may occur only with an applicable adequacy decision or other valid safeguard, including required assessments and supplementary measures. A storage location hint is not an EU-only residency guarantee. This agreement does not itself constitute an international-transfer safeguard or authorize undisclosed backup destinations. Recipient delivery to the Customer's chosen destination remains subject to the Customer's lawful instructions and applicable transfer rules.

6. Assistance and individual rights

6.1. remoteroom will promptly forward requests it receives from individuals concerning Customer Personal Data and will not answer on the Customer's behalf unless instructed or legally required. It will assist the Customer with access, rectification, deletion, restriction, portability and other applicable rights, using available technical and organisational measures appropriate to the processing. It will not disclose one customer's data to another requester.

6.2. Taking account of the processing and information available, remoteroom will assist the Customer with its obligations under Articles 32-36 GDPR, including security assessments, breach notifications, data protection impact assessments and prior consultation. It will provide relevant processing and subprocessor information and cooperate with competent supervisory authorities as required.

6.3. Any separately chargeable, exceptional assistance must be described and agreed in advance. Fees must not obstruct mandatory assistance, urgent breach response, statutory rights or correction of remoteroom's own non-compliance.

7. Personal-data breaches

7.1. remoteroom will notify the Customer **without undue delay after becoming aware of a personal-data breach** affecting Customer Personal Data, using the Customer's designated contact and the escalation arrangements in Annex 4. It will not wait for a complete investigation before notifying.

7.2. The notice will include information available about the nature of the breach, affected data and categories and approximate numbers of individuals and records, likely consequences, mitigation and remedial steps, and a contact for further information. Missing information will follow without undue further delay. remoteroom will preserve a proportionate incident record, take reasonable steps to contain and remedy the breach, and assist the Customer

with required notices.

7.3. The Customer remains responsible for notifications for which it is the controller, including the applicable Article 33 deadline. Nothing in this agreement gives remoteroom a general 72-hour waiting period or represents that a continuously staffed response service exists.

8. Return, deletion, backups and restoration

8.1. The Customer instructs remoteroom to apply the selected lifecycle and deletion operations in Annex 2. At the end of the affected service, the Customer may choose return of its remaining Customer Personal Data followed by deletion, or deletion, unless applicable law requires continued storage. Return of files uses the available download facilities; the account-data export does not include file payloads. Routine expiry remains a documented deletion instruction.

8.2. The Customer must arrange return before the agreed expiry/deletion date and tell remoteroom promptly if assistance is required. If remoteroom ends the service early, it will give a reasonable opportunity to retrieve remaining data where legally and technically possible. This agreement does not require recovery of previously purged files or indefinite preservation while no return instructions are provided. remoteroom will confirm completion of deletion on request, stating any remaining backup or legally retained categories and their deletion dates.

8.3. Database backups can contain previously deleted metadata until the last copy containing it is erased under the deletion instructions and handling in Annex 4. They are restricted to security, continuity and recovery, not routine access or a new use of that data. Selective removal from an immutable backup is not promised; the deletion obligation still applies; technical difficulty is not permission for indefinite storage. remoteroom will inform the Customer of any necessary residual retention, its reason and the proposed deletion date. Copies retained under a legal duty must be isolated, limited to that duty, and deleted when it ends; remoteroom will explain the basis and period where permitted. This is not blanket authorization to retain backups indefinitely.

8.4. Before a restored database returns to ordinary operation, remoteroom will reapply relevant deletion, expiry, access-restriction and account-closure instructions recorded since the backup and reconcile outstanding object-cleanup work. Restoring metadata must not silently reactivate expired or deleted transfers, revive access credentials or restart retention clocks. Any data restored solely to carry out deletion remains restricted to that purpose.

9. Evidence, audits and non-compliance

9.1. remoteroom will make available information needed to demonstrate compliance with this agreement and Article 28 GDPR, and allow and contribute to audits, including inspections, by the Customer or an independent auditor it appoints. The parties will coordinate reasonable scope, notice and confidentiality to protect security, availability and others' data. Existing reports may be used where adequate, but do not remove inspection rights. Urgent incidents, credible non-compliance or an authority's request may require shorter notice or further checks. No certification is implied by use of a certified infrastructure vendor.

9.2. Where remoteroom cannot fulfil a material obligation it will promptly inform the Customer. The Customer may suspend the affected processing and terminate it if adequate protection cannot be restored, without prejudice to other remedies. Return and deletion obligations continue after termination.

9.3. Nothing here restricts the rights of individuals or supervisory authorities, liability under Article 82 GDPR, or obligations which applicable law does not permit the parties to exclude. The Service Agreement governs other matters only to the extent consistent with this agreement and mandatory law. The governing law is German law, subject to mandatory applicable data protection law.

Annex 1 - description of processing

Item	Agreed scope
Subject matter and purpose	Receiving and making available Customer-selected files for delivery; administering transfers and incoming request-link packages; authorizing downloads and ZIP delivery; sending requested transfer notifications; implementing deletion and the separate database-recovery arrangements.
Operations	Collection, recording, temporary storage, retrieval, transmission, access control, organization into packages/ZIP streams, integrity checking, restriction and deletion; backing up and restoring database records only. Processing occurs as the Customer uses the service, not as a one-off batch.
Personal data	Any personal data the Customer lawfully includes in files; file names, paths, sizes and checksums; titles/messages; sender and recipient contact data; transfer/access events and identifiers to the extent processed on the Customer's behalf. Own-purpose controller records remain subject to section 1.4.
Individuals	Customer personnel, clients, suppliers, contractors, collaborators, recipients, request-link contributors and identifiable people included in files, images, audio or video.
Sensitive data	Not authorized by this general agreement without the prior assessment and written safeguards under section 2.4.
Duration	The selected transfer lifecycle in Annex 2, plus residual operational copies and the database-backup handling in Annex 4. The relationship continues while relevant processing remains; ending a subscription does not erase all copies instantly.
Customer duties and rights	Select lawful files and recipients, retain its own file copies, manage authorized users/link protections, issue instructions, exercise verification rights, and satisfy the controller or upstream-processor duties applicable to it.

Annex 2 - file lifecycle and service measures

The following describes the service implementation reviewed on 25 October 2026. Availability remains subject to service incidents and outages. Cleanup failures must be retried and investigated; the stated recovery intervals are not a promise of physical erasure at an exact instant.

Stage or measure	Behavior and boundary
Upload and storage	Browser and native clients send payloads directly to presigned operations in private R2 object storage. The control-plane database stores records, not file payloads.
New outgoing Free transfers	Default link life 24 hours; maximum selectable life 14 days. API callers can select a permitted whole-hour lifetime. Expired share links do not provide new download authorization.
New outgoing Pro transfers	Default link life 72 hours; maximum selectable life 60 days. A permitted expiry edit starts the chosen interval from the edit, so total storage can exceed 60 days after upload.
Incoming request-link packages and older Pro transfers	Incoming packages currently have no automatic link expiry, and older Pro transfers can also lack an expiry. They remain until owner deletion or expiry imposed when Pro ends. Temporary-transfer scope is not a representation of a universal age limit; a maximum age for every file would require a separately implemented lifecycle change.

Stage or measure	Behavior and boundary
Pro ending	Pro transfers expire no later than seven days after Pro ends; a sooner existing expiry remains sooner. This includes incoming packages and older transfers without an expiry.
Expiry and deletion	Free expiry schedules permanent object purge after a 12-hour recovery interval; Pro expiry, sender deletion and operator disabling ordinarily use a 24-hour interval. The service removes active references and purges recovery objects through durable cleanup jobs. Sweeps, retries and provider outages can delay completion; recovery is not guaranteed.
Abandoned uploads	Drafts inactive for more than 48 hours are eligible for cleanup only where no continuing file/session activity or live upload session protects them. Expired upload sessions are failed and multipart uploads aborted. Terminal failed/aborted session records are pruned after seven days.
Temporary download copies	Eligible single-file downloads up to 256 MiB can be cached for up to 24 hours. Signed download URLs are checked by the Worker before serving cached content and have their own expiry. A cache copy can outlast removal from active object storage; link revocation is not instantaneous. ZIP job manifests are also temporary operational records.
Storage fallback cleanup	The last recorded bucket configuration aborts incomplete multipart uploads after two days, removes trash objects after seven days and ZIP job objects after two days. These are fallback object rules, not an extension of customer link access or a universal live-file age limit. These fallbacks are secondary to the durable deletion jobs and do not set a live-file lifetime.
Download metadata	Download-event records are pruned after 90 days or earlier with deletion of their transfer. Their presence in database backups is governed by Annex 4. Transfer metadata can contain personal data independently of the files.
Encryption and integrity	HTTPS for deployed transport, provider-managed R2 encryption at rest, scoped signed operations, token-gated downloads, CRC verification and ZIP integrity checks. The service does not provide end-to-end encryption or general malware scanning.
Authorization and separation	Account ownership checks, scoped API keys/sender tokens, private incoming packages and optional link passwords. The download service validates signed requests; an unprotected share link is a bearer-access mechanism.
Deletion reliability	Object-cleanup pointers can survive removal of account/transfer records and track retry work. The short recovery copy is in R2, outside the Proxmox backup chain. Administrative monitoring, backup deletion and restoration procedures must also satisfy Annex 4.
Local copies	Sender originals, downloaded files and local client working files are controlled by the relevant device user; server deletion does not remove them.

Annex 3 - authorized subprocessors and locations

The following services are authorized only for the activities described below. An authorization is not a representation that every service holds every Customer's data. In particular, listing a backup destination does not establish that an automatic backup job for this service is active. Additional or replacement subprocessors are subject to section 5.

Provider	Processing	Location and safeguards
netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe, Germany	Virtual-server infrastructure for the application and PostgreSQL database, administered by remoteroom. Customer transfer-file payloads remain in R2.	Selected server location: Nürnberg, Germany. Infrastructure processing is subject to the applicable Article 28 processing agreement with netcup.
Cloudflare, Inc.	Private R2 file storage, short recovery copies, Worker downloads, edge caches, ZIP manifests and website ingress through Tunnel/proxy.	US-headquartered provider with a global delivery/support network. The currently recorded R2 bucket has default jurisdiction and a Western Europe location hint; it is not an EU-only residency guarantee. Processing is subject to Cloudflare's applicable customer DPA and Chapter V safeguards, including applicable adequacy coverage or Standard Contractual Clauses.
Plus Five Five, Inc. (Resend)	Requested transfer emails and associated addresses, subjects, message bodies and delivery records. Transferred file payloads are not attached to these emails.	United States; the sending region does not establish EU-only storage. Processing is subject to the applicable Resend DPA and applicable adequacy coverage or Standard Contractual Clauses.
LenoIT SARL (Cloud-PBS), 1 rue Anita Conti, 56000 Vannes, France; SIREN/RCS Vannes 941 951 667	Offsite storage and recovery of database backups; excludes customer file payloads in R2.	Published DPA limits EU-customer backup processing/storage to the EU; published Privacy Policy identifies France/Germany and infrastructure providers OVHcloud, Hetzner and Equinix. Processing must remain within the applicable agreement and authorized locations. Client-side encryption is available but no enabled configuration or provider inability to read our backups is asserted by this agreement.

The application and database are hosted on a netcup virtual server in Nürnberg, Germany. The PostgreSQL backup repository and separate local PBS infrastructure are operated by remoteroom itself at Theodorstraße 41P, 22761 Hamburg, Germany. The Hamburg infrastructure is internal infrastructure, not an additional external subprocessor. Proxmox software use does not itself make its software publisher a recipient of Customer Personal Data.

The provider will maintain applicable subprocessor agreements and location/transfer evidence and supply relevant information under sections 5 and 9. Identity providers, desktop-distribution services and payment providers are not automatically subprocessors of customer file content; their own activities are described in the Privacy Notice and assessed according to their actual roles.

Annex 4 - database backups, deletion and operational contacts

Subject	Arrangement and contractual boundary
Scope	Only database/operational records are included in the database-backup arrangements described here. Customer transfer-file payloads remain in R2 and are excluded from these backups. Database records may nevertheless contain personal data, including names, messages, addresses and access-related information.
Locations	Internal copies are held on remoteroom-operated infrastructure at its Hamburg company site. The separate local PBS host is also operated by remoteroom. Cloud-PBS by LenoIT SARL is the authorized external database-backup destination under Annex 3 when used.
Current backup handling	Scheduled PostgreSQL base backups and continuous transaction-log archiving send database recovery data to the separately operated repository in Hamburg. Local and offsite VM backups protect that repository. These arrangements do not provide customer-accessible file backups or reconstruct purged R2 payloads. Backup frequency, monitoring and tested restoration procedures are maintained in the operational recovery plan. This agreement does not promise a fixed recovery point, recovery time or uninterrupted availability.
Retention and deletion	Automated retention selects recent full, differential and VM backups. These selection rules do not establish a fixed maximum age for every copy; historical manual database copies have no service-wide fixed age. This does not authorize permanent retention: copies containing Customer Personal Data remain subject to the Customer's deletion instructions, necessity and section 8. remoteroom will identify affected copies, remove them without undue delay when no longer required or when deletion is instructed, and tell the Customer any remaining lawful retention and expected deletion date. If a shared recovery copy cannot immediately be selectively erased, it must be restricted from ordinary use while deletion is completed. A configurable Cloud-PBS pruning policy or a post-contract retrieval window is not a general per-backup lifetime.
Access and security	Access is limited to authorized operational personnel under confidentiality duties and the security requirements in section 4. Backup transfers and stored copies must be protected appropriately to risk; encryption/key custody, access separation and restoration must be included in that assessment. No assertion of independently audited controls, enabled client-side encryption, immutable copies or 24/7 staffing is made.
Restoration	The responsible operator must apply section 8.4 before returning a restored database to normal service, including deletion/restriction replay, credential/access review and object-cleanup reconciliation. This is a contractual operating duty, not a claim that automatic restore replay already exists.
Contacts	Finn Jakob Jaeger, finn@remoteroom.io, is the primary operational privacy/security contact. Public service contact: yasync@remoteroom.io. Max Hartmann handles these matters when Finn is unavailable; the same service address reaches the responsible operator. These are operational responsibilities, not a DPO appointment.
Customer contact	Notices and instructions use the Customer's verified account contact or a replacement contact it designates in writing. The Customer must keep that contact current and identify authorized instruction representatives.

10. Incorporation, acceptance and changes

10.1. remoteroom offers this agreement as part of the Service Agreement. Where the Customer accepts Terms that expressly incorporate this version, this agreement becomes binding for processing on the Customer's behalf. An authorized person accepting for an entity represents that they have authority to bind it. The agreement also may be concluded by a separate written agreement identifying this version and the Customer. No separate handwritten signature is required for an electronic agreement.

10.2. An account's versioned Terms acceptance records the acceptance of the incorporated agreement. Publication alone does not accept it for existing customers or backdate an acknowledgement. Returning customers must accept the current Terms through the service's existing acknowledgement process before new sending. Customer account identity, contact, accepted Terms version and date/time identify the contracting record; a downloadable copy of this DPA remains available for that version.

10.3. Material changes require notice and the applicable contractual acceptance process; a website edit does not silently rewrite an already agreed version. Changes must preserve mandatory data protection rights. Technical updates under section 4 and subprocessor changes under section 5 follow those sections.

Legal references

- GDPR, especially Articles 4, 28 and 32-36.

- Commission Decision (EU) 2021/915: controller/processor contract requirements.

- Cloud-PBS provider identity, DPA and Privacy Policy.

This is a service-specific agreement, not the Commission's unmodified standard contractual clauses or a certification of the service.

- netcup provider identity and privacy information and processing-agreement procedure.