Online DPA

If you have any questions, please contact the processor.

Data protection agreement on data processing in accordance with Article 28 GDPR

between the controller:

[[Firma]]
[[Strasse]]
[[Strasse2]]
[[PLZ]] [[Ort]]
[[Land]]
(hereinafter referred to as the Principal)

and the processor:

Just Software AG
Nobistor 16
22767 Hamburg
(hereinafter referred to as the Contractor)

the following Agreement is concluded. It shall supersede any prior data processing agreements with the same objective.

Preamble

This Agreement fleshes out the parties' obligations under data protection law that arise from the data processing described in this Agreement and in **Appendix A**. It applies to all activities related to the service in the course of which employees of the Contractor or third parties commissioned by it may come into contact with personal data of the Principal.

Individual provisions in this data protection agreement take precedence over the Contractor's General Terms and Conditions of Business (GTC).

§1 Definitions

1. Personal data

   Pursuant to Article 4(1) GDPR, personal data is any information that relates to an identified or identifiable natural person (hereinafter referred to as a "data subject"). Identifiable natural persons are natural persons who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2. Processor

   Pursuant to Article 4(8) GDPR, a processor is a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

3. Instruction

   An instruction is an order, issued by the Principal, as a rule in writing, aimed at achieving particular handling of personal data by the Contractor in terms of data protection (for example storage, pseudonymisation, erasure, surrender). Instructions shall be issued by the Principal and may be changed, supplemented or replaced by individual instructions. The Principal shall issue instructions in writing or by e-mail.

§ 2 Scope of application and responsibility

1. The Contractor provides hosting services on behalf of the Principal in the form of software as a service. In this connection it cannot be ruled out that the Contractor will be given access to personal data or gain knowledge of it. Pursuant to Article 28 GDPR it is therefore necessary to conclude a data processing agreement.

2. The Principal has selected the Contractor as a service provider within the framework of the diligence obligations under Article 28 GDPR. A precondition for the permissibility of data processing is that the Principal issues the mandate to the Contractor in writing. This contract contains, in accordance with the wishes of the parties and particularly of the Principal, the written data processing mandate in the meaning of Article 28(3) GDPR and regulates the rights and obligations of the parties with regard to data protection in connection with the provision of the software as a service (SaaS).

3. The ownership title to the personal data is held exclusively by the Principal as the "controller" in the meaning of the GDPR. On the basis of that responsibility, the Principal may demand the rectification, erasure, blocking and surrender of personal data either during the term of the contract and after the termination thereof.

§ 3 Subject and duration of the mandate

1. The subject of the mandate is as specified in **Appendix A.**
2. This Agreement shall become effective upon the signing hereof by both parties and shall terminate, as a rule, upon the termination of the underlying main contract according to the GTC. Furthermore, this agreement remains valid beyond the end of the main contract as long as the contractor has personal data that was provided to him by the client or that he collected for the client. The right of extraordinary termination remains unaffected.

§ 4 Description of the processing, data and data subjects

The scope, nature and purpose of the processing, as well as the type of data and the group of data subjects, are described in **Appendix A**.

§ 5 Technical and organisational measures

The Contractor undertakes with respect to the Principal to adhere to the technical and organisational measures that are appropriate and necessary for compliance with the applicable data protection regulations

1. As the Contractor operates the software as a service for the Principal also outside the Principal's business premises, the Contractor must, without fail, document the technical and organisational measures implemented by it for that purpose, within the meaning of Article 28(3) point c) GDPR, Article 32 GDPR in conjunction with Article 5(1) and (2) GDPR, and the documentation must be handed over to the Principal for verification. The processing of personal data by employees of the Contractor outside the business premises (e.g. when working from home) is permitted, provided that the Contractor takes appropriate technical and organisational measures to ensure that the confidentiality, integrity and availability of the personal data is maintained.
2. The measures shall serve the purpose of data security and ensuring a level of protection being commensurate with the risk with regard to the confidentiality, integrity, availability and resilience of the systems related to this mandate. In this context, the state of the art of technology, the implementation costs and the type, scope and purposes of the processing, as well as the varying probability and severity of the risk for the rights and freedoms of natural persons in the meaning of Article 32(1) GDPR, must be taken into account.

3. A description of the status of the technical and organisational measures as of the conclusion of the contract is attached to this Agreement as **Appendix B "Technical and organisational measures for data protection"** . The parties agree that changes to the technical and organisational measures may become necessary for the purpose of adjustment to technical and legal circumstances. The Contractor shall seek the Principal's prior approval for any significant changes that may impair the integrity, confidentiality or availability of the personal data. Measures that only involve minor technical or organisational changes and do not adversely affect the integrity, confidentiality and availability of the personal data may be implemented by the Contractor without any consultation with the Principal. The security level specified in Annex B "Technical and organizational measures for data protection" must not be undercut. The Principal may at any time request a current version of the technical and organisational measures implemented by the Contractor.

§ 6 Processing of data

1. The Contractor shall only process the data on the documented instructions of the client. They may not, for example, correct, delete or restrict the processing of the data processed on behalf of the Principal without authorization. If a data subject directly contacts the Contractor in this respect, it shall promptly pass that request on to the Principal for approval.

2. The implementation of erasure, the right to be forgotten and the right to rectification, data portability and access shall only be effected directly by the Contractor following a documented instruction issued by the Principal.

3. Copies or duplicates of the data shall not be prepared without the Principal's knowledge, except for back-up copies insofar as they are necessary for the purpose of ensuring correct data processing, as well as data which is necessary in the interests of compliance with statutory retention requirements.

4. After the completion of the contractually agreed work or earlier at the Principal's request, but no later than upon the termination of the service agreement, the Contractor shall hand over to the Principal all documents that have come

into its possession, any created processing or utilisation outcomes and data records related to the contractual relationship or, with the Principal’s prior consent, destroy them in line with data protection requirements. The same applies for test and waste materials. The erasure report must be submitted on request and no later than upon termination of the service relationship.

5. Documentation that serves the purpose of proving that the data processing is carried out in accordance with the mandate and properly must be filed by the Contractor after the end of the contract in accordance with the respective statutory retention periods. It may fulfil its obligation by handing them over to the Principal at the end of the contract.

§ 7 Obligations of the Contractor

1. The Contractor is not permitted to carry out any processing of personal data that does not relate to the provision of SaaS services or support, unless the Principal has agreed to this in writing.

2. The Contractor confirms that – insofar as it is legally obliged to do so – it has appointed a company data protection officer in the meaning of Articles 38, 39 GDPR. The Contractor has appointed Carsten Knoop, audatis Consulting GmbH, Luisenstr. 1, 32052 Herford, datenschutz@just.social as its data protection officer. Any change of the data protection officer must be promptly reported to the Principal.
3. Unless the Principal informs the Contractor otherwise, the persons authorised to issue instructions are the up to four persons for whom the Contractor provides support. The Principal is obliged to name these persons in writing at the start of the project and to inform the Contractor immediately of any changes. The persons authorised to receive instructions from the Principal are the members of the Customer Success Team, who the Contractor shall name at the start of the project and communicate to the Principal.
4. The Contractor shall promptly inform the Principal if, in its opinion, an instruction issued by the Principal violates provisions of law. The Contractor shall have the right to suspend the execution of the relevant instruction until the Principal has confirmed or changed it.

5. The Contractor shall promptly notify the authorised persons of the Principal in the event of serious disruptions of its operations or in the event of a suspicion of data protection violations or other irregularities in the processing of the Principal’s personal data.

6. The Contractor shall support the Principal in fulfilling its obligations to respond to requests from data subjects in accordance with Articles 12 to 22 GDPR. The Contractor is not authorised to respond directly to requests from data subjects unless the Principal has explicitly authorised it to do so in writing. The Contractor shall forward such requests in writing (e.g. by email) to the Principal's authorised persons without delay, at the latest within 24 hours of receipt.

7. In the event that the Contractor establishes or specific circumstances indicate that personal data processed by it for the Principal is subject to a violation of the statutory protection of personal data under Article 33 GDPR (data protection violation / data breach), for example if it is unlawfully transmitted or otherwise unlawfully disclosed to third parties, the Contractor must promptly and fully inform the Principal about the time, type and scope of the incident(s) in writing or text form via e-mail. The notification to the Principal must contain at least the following information:

a) a description of the type of violation of the protection of personal data, if possible specifying the categories and the approximate number of data subjects affected, the affected categories and the approximate number of affected personal data records.

b) the name and contact details of the data protection officer or a different point of contact for further information.

c) a description of the likely consequences of the personal data breach.

d) a description of the measures implemented or proposed for the elimination of the personal data breach and any measures aimed at mitigating its possible adverse effects. The Contractor must also promptly notify the Principal as to what measures have been implemented by the Contractor in order to prevent any unlawful transmission / unauthorised access by third parties in the future.

8. The Contractor shall provide the Principal, at its request, with the information necessary for the purpose of maintaining a record of processing activities in accordance with Article 30(1) GDPR and shall itself, as the processor, maintain a record of processing activities in accordance with Article 30(2) GDPR.

9. The Contractor shall ensure that the employees involved in the processing of the Principal’s personal data are obligated to maintain confidentiality in accordance with Article 28(3) sentence 2 point b), 29, 32(4) GDPR and are familiarised in advance with the data protection regulations being relevant for them. The Contractor and each person subordinate to it who has access to personal data may only process that data in accordance with the Principal’s instructions, including the authorisations granted in this Agreement, unless they are legally obliged to carry out the processing. This confidentiality obligation shall continue to exist after the completion of the work.

10. The fulfilment of the above-mentioned obligations must be monitored by the Contractor and proved in an appropriate manner, for example through regular auditing and certification by an external data protection company.

11. Furthermore, the Contractor undertakes to support the Principal in accordance with Article 28(3) point f) GDPR in ensuring compliance with the obligations referred to in Articles 32 – 36 GDPR, i.e.:

    a) as part of its notification obligation with respect to data subjects and the Principal in this connection it shall promptly make all relevant information available.

    b) it shall support the Principal in carrying out its data protection impact assessment.

    c) it shall support the Principal in the course of prior consultation with the supervisory authority.

12. The Principal and the Contractor shall cooperate with the supervisory authority in the performance of its tasks, as requested.

13. The Contractor must promptly inform the Principal of any monitoring or measures conducted by the supervisory authority insofar as they relate to this mandate. This shall also apply insofar as a competent authority is conducting

an investigation at the Contractor as part of administrative offence proceedings or criminal proceedings with regard to the processing of personal data in the course of the data processing.

14. Insofar as the Principal is subject to monitoring by the supervisory authority, administrative offence proceedings or criminal proceedings, a liability claim asserted by a data subject or a third party or a different claim in connection with the data processing conducted by the Contractor, the Contractor must do everything in its power to support the Principal.

15. The Contractor shall regularly verify internal processes as well as technical and organisational measures in order to ensure that the processing in its area of responsibility is conducted in line with the requirements of applicable data protection laws and that the protection of the rights of data subjects is ensured.

§ 8 Rights and obligations of the Principal

1. The Principal shall have the right to issue at any time supplementary instructions with respect to the Contractor concerning the type and scope of and the procedure for the development, care and maintenance of software and/or IT systems. Such instructions may be issued in writing or orally. The Principal shall promptly confirm any oral instructions with respect to the Contractor in text form via e-mail.

2. The Principal shall promptly and fully inform the Contractor if it identifies any errors or irregularities in light of data protection laws in the course of verifying the outcomes of the mandate.

3. The Principal is subject to the notification requirements arising from Article 33(1) GDPR.

4. The Principal shall stipulate, either contractually or in an instruction, the arrangements for the return of provided data carriers and/or the erasure of stored personal data after the completion of the mandate.

5. If the Principal issues individual instructions that extend beyond the contractually agreed scope of performance and the statutory obligations of the Contractor, the costs that arise as a result shall be borne by the Principal. The cost is 125 euros (net) per hour or part thereof.

§ 9 Protection of data subjects’ rights

1. The Principal is responsible for the protection of data subjects’ rights.

2. Insofar as cooperation by the Contractor is necessary for the protection of data subject rights by the Principal – particularly their rights to information, rectification, restriction, data portability or erasure – the Contractor shall take the necessary action following an instruction issued by the Principal.

3. If a data subject directly contacts the Contractor for the purpose of the rectification, erasure, restriction or portability of its data, the Contractor shall promptly pass that request on to the Principal.

§ 10 Control authorisations

1. The Principal has the right to verify, at any time and to the necessary extent, compliance with the statutory regulations concerning data protection and compliance with the contractual provisions agreed between the parties, as well as compliance with the Principal’s instructions by the Contractor.

2. The Contractor must provide information to the Principal insofar as this is necessary for the purpose of conducting verification in the meaning of paragraph 1.

3. The Principal may, following a prior announcement giving reasonable advance notice, carry out an inspection himself or through auditors commissioned by him in the meaning of paragraph 1 in the Contractor’s business premises during normal business hours. The Principal shall ensure in this context that the inspections are only carried out to the necessary extent, insofar as the Contractor’s operational procedures are disrupted by them.

4. The Contractor must provide the Principal with the necessary information in the event of measures implemented by the supervisory authority with respect to the Principal in the meaning of Article 58 GDPR, particularly with respect to notification and control obligations.

5. The Contractor shall provide proof of technical and organisational measures that do not relate solely and specifically to the mandate in question. This may be done through:

   a) compliance with approved codes of conduct in accordance with Article 40 GDPR.

   b) certification according to an approved certification procedure in accordance with Article 42 GDPR.

   c) current attestations, reports or report extracts of independent agencies (for example public auditor, auditing unit, data protection officer, IT security officer, data protection auditors).

   d) a suitable certification through an IT security or data protection audit (for example according to ISO 27001 or BSI Grundschutz).

6. The Contractor may claim from the Principal any costs incurred in connection with control measures at the Contractor referred to in paragraphs 3 and 4, which exceed the statutory obligations of the Contractor. The cost is 125 euros (net) per hour or part thereof.
7. Where applicable, the contractor undertakes to inform the client immediately of the exclusion from approved codes of conduct pursuant to Art. 41 para. 4 GDPR and the revocation of a certification pursuant to Art. 42 para. 7 GDPR.

§ 11 Subcontractor relationships

1. For the provision of SaaS services on behalf of the Principal, the Contractor shall not make use of any services of third parties which are not specified in paragraph 2 that process data on its behalf in accordance with Article 28 GDPR ("subcontractors").

2. The Principal agrees to the Contractor engaging service companies for the purpose of performing its contractually agreed services or commissioning them to perform services as subcontractors. Those companies are currently:

   Approved subcontractors for services hosted by Just Software AG:
   - Netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe (data centre)
   - Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen (data centre)
   The Just platforms of the Principal are hosted in these two data centres. The locations of the data centres are in Germany (Nürnberg and Falkenstein).

3. In the event that it commissions a subcontractor, the Contractor must carefully select it and before engaging it verify whether it is able to comply with the agreements concluded between the Principal and the Contractor. In particular, the Contractor must verify, in advance and at regular intervals during the term of the contract, that the subcontractor has implemented the necessary technical and organisational measures for the protection of personal data in accordance with Articles 28(3) point c), 32 GDPR in conjunction with Article 5(1), (2) GDPR. The result of the verification must be documented by the Contractor and sent to the Principal at its request. The Contractor must ask the subcontractors to confirm that they have appointed a company data protection officer in the meaning of Articles 37 – 39 GDPR.

4. The Contractor must ensure that the provisions agreed in this contract and any supplementary instructions of the Principal also apply with respect to the subcontractor. The Contractor must regularly monitor compliance with those obligations.

5. As a rule, the subcontractor must be obligated in writing insofar as no other form is appropriate. A copy of the undertaking must be sent to the Principal at its request.

6. In particular, the Contractor must ensure, through contractual provisions, that the control authorisations (section 10 of this Agreement) of the Principal and supervisory authorities also apply with respect to the subcontractor and that appropriate control rights of the Principal and supervisory authorities are agreed. It must also be contractually stipulated that the subcontractor must tolerate these control measures and any on-site inspections.

7. If the Contractor uses the services of a new additional processor (main service), it shall inform the Principal of this in writing and give the Principal 30 days to object to the processing by the new processor. If an amicable solution cannot be reached, this agreement or the data processing will be restricted or terminated.
8. The contractor is liable to the client for ensuring that the subcontractor complies with the data protection obligations contractually imposed on it by the contractor in accordance with this section (Art. 28 para. 4 sentence 2 GDPR).
9. The engagement of subcontractors in third countries is only permitted if the specific requirements of Art. 44 et seq. GDPR are met and the client gives prior consent.

§ 12 Data secrecy and confidentiality obligations

1. The Contractor undertakes to comply with the same secrecy provisions as those which the Principal is obliged to

observe. The Principal must notify the Contractor of any special secrecy provisions.

2. The Contractor warrants that it is familiar with the currently applicable data protection regulations and the application thereof.

3. Both parties undertake to treat as confidential any information that they obtain in connection with the performance of this Agreement, without any time limitation, and to use it solely for the purpose of the performance of the contract. Neither party shall have the right to use that information, either entirely or partially, for any purposes other than those referred to above or to make that information available to third parties.

4. The above obligation does not apply to information that one party demonstrably obtains from third parties, without being obliged to maintain secrecy, or which is publicly known.

§ 13 Liability

Reference is made to the liability provisions under Article 82 GDPR.

§ 14 Notification obligations, written form clause, governing law

1. If the Principal’s personal data at the Contractor or in the case of subcontractors is jeopardised due to attachment or seizure, to insolvency or arrangement proceedings or to other events or measures of third parties, the Contractor must promptly notify the Principal to that effect. The Contractor shall promptly inform all responsible persons in this connection that the Principal has exclusive authority over the personal data and holds the exclusive ownership title to it as the "controller" in the meaning of the GDPR.

2. Any amendments or additions to this Agreement or any of its components – including any warranties of the Contractor – shall require a written agreement and an explicit reference to the fact that it is an amendment / addition to these terms and conditions. This also applies to any waiver of this formal requirement.

3. In the event of the ineffectiveness of a provision of these contractual terms and conditions, the other provisions hereof shall nevertheless remain effective. The parties shall replace any ineffective provision or fill in any unintended gap/omission, in good faith, with a provision that comes closest to the parties’ jointly pursued objective.

4. Furthermore, insofar as legally permissible, Hamburg is agreed as the place of jurisdiction and German law applies.
5. The defense of the right of retention pursuant to Section 273 of the German Civil Code (BGB) is excluded with regard to the data processed for the client and the associated data carriers.

[[Ort]], 2026-05-18

signed [[Name]] (Principal’s authorised representative)

Hamburg, 2026-05-18

signed Dr. Thomas Kreye (Member of the Executive Board, Just Software AG)

[This Agreement is effective without a signature]

Appendix A: Details on the contract

The mandate issued by the Principal to the Contractor includes the following work and/or services:

☑ **Maintenance of the social software "Just"**

☐ Access to the Principal’s IT systems (specifically the social software "Just") via remote maintenance.

☑ Provision of the social software "Just" as hosted software in the Contractor’s computer centre or that of a subcontractor.

Appendix A: Details on the contract

The scope of the processing and therefore the quantity of data used are variable and depend on the intensity of use by the Principal. The purpose served is the management of data protection tasks and measures, documentation of digital / digitalised documents and documentation relating to implemented training measures for individual employees of the Principal. The contractually agreed data processing shall be provided exclusively 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 county shall require the prior consent of the Principal and may only occur if the special conditions under Article 44 et seq. GDPR are fulfilled. The service to be provided under the mandate involves the following types of automated processing of personal data using data processing systems:

☑ **Alteration (e.g. through changes to the data records by users)**
☑ **Transmission (e.g. through transmission of messages by e-mail)**
☑ **Storage (e.g. through backing up and archiving on hard drives, other storage systems or data carriers)**
☑ **Erasure (e.g. through the erasure of data records or the destruction of data carriers)**
☑ **Restriction (e.g. through the deactivation of individual data records)**
☐ Use (e.g. through carrying out evaluations)
☐ Collection (e.g. through inputting of employee lists and other data)

Appendix A: Details on the contract

☑ **Employee data (e.g. photographs, names, contact details, position, date of birth).**

☑ **Usage data (e.g. logging user activities, log files).**

Appendix A: Details on the contract

☑ **Employees and former employees of the Principal**

☐ Employees and former employees of affiliated companies of the Principal

☐ Clients

☐ Association members

☐ External persons

Appendix B: Technical and organisational measures for data protection

Massnahme	Schutzziel
Audits	Vertraulichkeit, Integrität, Verfügbarkeit
Appointment of a data protection officer	Vertraulichkeit, Integrität, Verfügbarkeit
Regular data protection audits by the company data protection officer	Vertraulichkeit, Integrität, Verfügbarkeit
Written data processing agreement in accordance with Article 28 GDPR, with provisions on the Contractor’s rights and obligations	Vertraulichkeit, Integrität, Verfügbarkeit
Training for all employees with an access authorisation. Regularly held follow-up training.	Vertraulichkeit, Integrität, Verfügbarkeit
Software-based tools	Vertraulichkeit, Integrität, Verfügbarkeit
Confidentiality obligation in accordance with Article 28(3) sentence 2 point b), 29, 32(4) GDPR	Vertraulichkeit, Integrität, Verfügbarkeit
Alarm system	Vertraulichkeit
Automatic access control system	Vertraulichkeit
Visitors book / log	Vertraulichkeit
Visitor control	Vertraulichkeit
Motion detector	Vertraulichkeit
Chip cards / transponder systems	Vertraulichkeit
The backups of the private cloud servers are encrypted before transmission and transferred to separate backup servers via SSH/SCP and stored there.	Vertraulichkeit
Differentiated authorizations	Vertraulichkeit
Documentation of authorizations	Vertraulichkeit
Reception / gatekeeper	Vertraulichkeit
Separate systems (logical client separation)	Vertraulichkeit
Tunnelled remote data connections (VPN=virtual private network)	Vertraulichkeit
Additional protection through a VPN tunnel if necessary	Vertraulichkeit
Password procedure (specifying password parameters with regard to complexity and the updating interval)	Vertraulichkeit

manual lock system	Vertraulichkeit
Personal and individual user login upon registration in the system / company network	Vertraulichkeit
Profile and role concept	Vertraulichkeit
Key management	Vertraulichkeit
Secure transfer of the data via the internet through SSL encryption (https) or SSH connection	Vertraulichkeit
If the contractor extracts exports or other data from the server at the request of the client, the transfer and local storage is exclusively encrypted.	Vertraulichkeit
Careful selection of cleaning services	Vertraulichkeit
Blocking clients after a certain period of time without any user activity (including a password-protected screensaver or automatic timeout)	Vertraulichkeit
SSH with personalized SSH keys for server maintenance	Vertraulichkeit
SSL(https) / TLS >= 1.2 for using the software	Vertraulichkeit
Separation of contact details	Vertraulichkeit
Separation of master data	Vertraulichkeit
Separation of test and development systems	Vertraulichkeit
Doors with an external doorknob	Vertraulichkeit
Locking up the work laptop in the home office	Vertraulichkeit
Encryption of data carriers using a state-of-the-art procedure.	Vertraulichkeit
Management of authorizations	Vertraulichkeit
Use of code numbers for clients or personnel instead of names	Vertraulichkeit
Video surveillance of entrances	Vertraulichkeit
Access authorizations	Vertraulichkeit
The possibility of tracking inputting, alteration and erasure of data through individual login data	Integrität
Logging by the system	Integrität
Access rights	Integrität

(UPS) uninterruptible power supply	Verfügbarkeit
Storing backups on an outsourced server in the computer centre	Verfügbarkeit
Backup procedure	Verfügbarkeit
IT emergency plans and recovery plans	Verfügbarkeit
Air-conditioning system in server rooms	Verfügbarkeit
Regular, documented data recovery	Verfügbarkeit
Mirroring hard drives	Verfügbarkeit

18.05.2026