

# Agreement on the processing of personal data on behalf according to Art. 28 GDPR (DPA)

between:

<COMPANY\_CUSTOMER>  
represented by: <NAME>  
<ADDRESS\_CUSTOMER>

- hereinafter referred to as the **Customer** -

and

Papershift GmbH, Register Court of Mannheim, HRB 722151  
Lange Straße 2, 76199 Karlsruhe  
represented by its management :  
Michael Emaschow, Florian Suchan

- hereinafter referred to as the **Contractor** -

## 1. Subject matter and duration of the agreement

### 1.1. Subject matter of the agreement

This agreement specifies the data protection obligations of the contracting parties, which result from the contract concluded between the parties via the website [app.papershift.com](https://app.papershift.com) (hereinafter: licence agreement). It applies to all activities related to the service contract and to all personal data that employees of the Contractor or agents commissioned by the Contractor come into contact with, for which the Customer is the controller or a Contractor itself (hereinafter: personal data of the Customer). If the provisions of this agreement contradict the provisions of the licence agreement, the provisions of this agreement take precedence.

The Contractor provides the following service: The paid provision of services by the Contractor within the framework of the licence agreement, in particular the provision of duty planning and personnel planning software as Software as a Service (SaaS).

The subject matter of the contract is, however, not the original processing of personal data by the Contractor. In the course of the provision of the services rendered by the Contractor as a service provider, however, personal data of the Customer will be accessed.

Thus, the Contractor (processor) will process personal data on behalf of the Customer (controller) (processing on behalf within the meaning of Article 28 GDPR).

## **1.2. Duration of the agreement**

The duration of this agreement is based on the term of the licence agreement. Regardless of the stipulated regulations on the duration of the order, the obligations to data secrecy, the duty of confidentiality, and the agreed retention periods apply beyond the termination of this agreement.

## **2. Purpose and data**

### **2.1. Nature and purpose of processing**

The Customer processes personal data as part of its activities described in the licence agreement. The data categories described below are affected by the activities to the extent and purpose resulting from the licence agreement: The system allows the collection of personal data, in particular data relevant to billing, such as working hours, time recording, vacation days, sick leave, other absenteeism, contractual conditions, hourly wages. The Customer can also configure their own data fields in the system.

### **2.2. Categories of data subjects**

Staff, i.e. applicants, employees.

### 3. Obligations and rights of the Customer

- 3.1. The Customer is responsible for assessing the admissibility of data processing and safeguarding the rights of the data subjects. The Customer is the controller within the meaning of Art. 4 no. 7 GDPR for the processing of data on behalf by the Contractor.
- 3.2. All instructions must be in writing.
- 3.3. The Customer has the right to issue instructions that relate to data processing, in particular those mentioned under 7 as well as the return of data. The right to issue instructions to permanently delete data remains with the Customer until the end of the agreement.
- 3.4. If instructions change, repeal, or supplement the provisions of this agreement, they are only permissible if a corresponding new regulation is made.

### 4. Obligations of the Contractor

- 4.1. The Contractor exclusively processes personal data within the framework of the agreements made and according to the Customer's documented instructions. The Contractor is not permitted to process or use the data provided for processing for other purposes. The Contractor is not authorised to make changes to the data at its own discretion.
- 4.2. Instructions are generally issued in text form. In justified urgent cases, instructions can also be issued verbally by authorised individuals of the Customer. The Customer will immediately confirm verbal instructions in writing.
- 4.3. The processing and use of the data takes place, as far as possible, in the territory of the Federal Republic of Germany, in a member state of the European Union, or in another contracting state of the Agreement on the European Economic Area (EEA). If cloud services (e.g. Amazon Cloud) are used, the Contractor ensures that the data stay within the EEA or that corresponding guarantees are made in accordance with Chapter V of the GDPR. Any relocation to a third country that goes beyond what has been approved thus far, must be reported to the Customer with a notice period of six weeks.
- 4.4. The Contractor undertakes to maintain confidentiality when processing the Customer's data. The Contractor furthermore assures that it obligates the employees involved in the execution of the work to confidentiality in accordance

with Art. 29 GDPR (formerly data secrecy in accordance with § 5 BDSG) (German Federal Data Protection Act). The Contractor confirms that it is aware of the relevant data protection regulations and monitors compliance with them. To do so, the Contractor uses the form "Obligation to maintain data secrecy" in the Annex and familiarises itself with the relevant data protection provisions.

- 4.5. The Contractor regularly checks the obligation to maintain data secrecy as well as compliance with technical and organisational measures.
- 4.6. If the Contractor is of the opinion that an instruction issued by the Customer violates a regulation, it must inform the Customer thereof immediately. The Contractor can suspend the execution of the relevant instruction until it has been confirmed or changed by the Customer.
- 4.7. The contractor may not store the data for longer than the duration specified by the Customer in writing (exclusion of retention obligations, e.g. according to the HGB (German Commercial Code)).
- 4.8. The Contractor must appoint a data protection officer. The contact details of said data protection officer, as well as any changes to the data protection officer, must be reported to the Customer. See Annex "Appointed persons".

## 5. Technical and organisational measures

- 5.1. The Contractor complies with the principles of proper data processing. It guarantees the contractually agreed and legally prescribed data security measures.
- 5.2. The technical and organisational measures described in the Annex (according to Art. 32 GDPR) are binding.
- 5.3. The technical and organisational measures can be adjusted to technical and organisational developments in the course of the contractual relationship. If the level of protection is maintained or improved during this adjustment, the Customer does not need to be notified separately; the Customer must be notified of significant changes in writing. Decisions, which are significant for security, on the organisation of the data processing and the procedures used are to be agreed with the Customer.
- 5.4. The Customer can request a supplement to the technical and organisational

measures by issuing instructions. The Customer must bear any resulting costs.

## 6. Subcontractors

The commissioning of subcontractors is only permitted under the following conditions:

- 6.1. The Contractor will inform the Customer of the name, address, and nature of the services rendered by the subcontractor. The subcontractors listed in the Annex “Subcontractors” have been approved.
- 6.2. Furthermore, the Contractor must ensure that it has selected the subcontractors with special consideration of suitability as well as the organisational and technical measures taken. The Contractor must regularly check compliance of the subcontractor with the same provisions it is subject to: The result of the compliance checks must be documented and forwarded to the Customer on request.
- 6.3. The Contractor must contractually ensure that the regulations agreed between the Customer and the Contractor also apply to subcontractors. In particular, the Customer must be entitled to carry out on-site checks at the subcontractor or to commission third parties to carry out said on-site checks.
- 6.4. In the contract concluded with the subcontractor, the responsibilities of the Contractor and the subcontractor must be clearly delimited. If several subcontractors are commissioned, this also applies to the responsibilities between these subcontractors.
- 6.5. The Contractor always informs the Customer of any intended change in relation to the involvement or replacement of subcontractors, whereby the Customer can object to such changes in writing. In the event of such an objection, the contracting parties will endeavour to come to an amicable agreement. The Customer can switch off the non-operationally necessary tools of the subcontractors, by having the Contractor switch the Customer to the “eu-only” option. If this is not an adequate solution for the Customer, it has a special right of termination.
- 6.6. The forwarding of data is only permitted if the subcontractor has fulfilled its obligation under Art. 28 GDPR. If a subcontractor does not comply with its data protection obligations, the Contractor is liable to the Customer for compliance with the obligations of that subcontractor.

**6.7.** Services of third parties that the Contractor uses as ancillary services to facilitate the execution of the order are not to be understood as subcontracting relations within the meaning of this agreement. These include e.g. telecommunication services, cleaning staff, postal and courier services, transport services, maintenance services (if access to personal data of the Customer is excluded), and security services.

## **7. Rights of data subjects**

**7.1.** The Contractor must correct, delete, or block personal data, as well as support the Customer in its obligations to provide information, further details, or data portability, and accommodate objection, if the Customer issues an instruction and requests this. Corresponding inquiries from data subjects or third parties must be forwarded to the Customer.

**7.2.** Unless otherwise agreed, the Customer bears the costs incurred. The Customer is to be notified of these in advance.

## **8. Supporting the Customer in its obligations**

**8.1.** The Contractor supports the Customer in complying with the obligations specified in Articles 32 to 36 GDPR. These are:

- Security of processing
- Reporting personal data breaches to the supervisory authority
- Notification of a data subject who has been affected by the breach of protection
- Data protection impact assessment
- Prior consultation

**8.2.** If the Contractor is not responsible for the circumstance, the Customer bears the costs. The Customer is to be notified of these in advance. In the case of Art. 32 GDPR, it can be assumed that the Contractor is responsible for this; in the event of a data protection breach, the Contractor is responsible if the breach occurred at the Contractor.

## **9. Erasure at contractual end**

**9.1.** After completion of the contractual work, the Contractor must hand over to the Customer and/or erase/destroy all documents that have come into its possession

and any processing or usage results that were created (data and data carriers) in connection with the contractual relationship.

- 9.2. All data and additional personal data/documents of the Customer that are located in the Contractor's systems and are no longer required must be irrevocably erased or destroyed. The erasure not only affects the user systems, but all associated files and data in all systems and on all storage media of the Contractor, in particular backups. Data carriers (paper, hard drives, CD's, USB sticks, etc. including all misprints or incorrect storage) that contain data of the Customer must be destroyed in accordance with DIN standard 66399.
- 9.3. The Contractor is obligated to organisationally ensure that the Customer's data can actually be erased or destroyed. The Contractor must inform all employees of these erasure obligations.
- 9.4. Confirmation of this erasure must be sent to the Customer in writing within four weeks at the latest.

## 10. Right to control

**10.1.** The Customer is permitted and obligated to track the technical and organisational measures taken by the Contractor (see Annex) before the start of data processing and regularly thereafter.

**10.2.** This is done by submitting an up-to-date audit opinion, reports from independent bodies, certification through IT security or data protection audits, or through an inspection at the Contractor.

**10.3.** The Contractor will provide all relevant information.

**10.4.** The Customer is entitled to carry out an inspection at the Contractor. Controls by the Customer must be carried out without avoidable disruptions to the business operations of the Contractor. This is to be carried out, after written notification, in consultation with the Contractor or by an inspector who is appointed on a case-by-case basis. The Customer has the right to track the Contractor's compliance with this agreement in its business operations by means of random checks, which the Contractor must be notified of in writing with a reasonable deadline. The Contractor undertakes, upon written request, to provide the Customer with the information

required to comply with its obligation to monitor and to make the corresponding verification available within a reasonable deadline. Controls take place once every 12 months at the most.

10.5. Within the framework of this control, the Customer may view process-related documents as well as its stored data and the data-processing programs.

## 11. Reporting a breach of the protection of personal data to the Customer

11.1. After becoming aware of a breach, the Contractor will immediately inform the Customer of the following:

- the suspicion of breaches to the confidentiality of the data,
- violations by the Contractor or its employees against data protection regulations,
- the specifications laid out with commissioning or
- the irrecoverable loss or defectiveness of data.

For this purpose, the information must be given in the Annex “Reporting data protection breaches”.

11.2. The Contractor takes the necessary measures to secure the data and to mitigate possible negative consequences for the data subjects. It supports the Customer in fulfilling information obligations in accordance with Art. 33 and 34 GDPR.

## 12. Duty of confidentiality

The Customer is obligated to treat confidentially all information of business secrets and data security measures of the Contractor, which it becomes aware of within the framework of the contractual relationship.

## 13. Relation to the principal contract/Termination

- 13.1.** A separate termination of this agreement without simultaneous termination of the principal contract is excluded.
- 13.2.** The Customer can terminate this agreement at any time without adhering to a notice period if the Contractor has seriously violated the provisions of this agreement, if the Contractor cannot or does not want to execute a legally compliant instruction issued by the Customer, or if the Contractor refuses access to the Customer in breach of the contract.

## 14. Attachment, seizure at the Contractor

If the Customer's property at the Contractor is endangered by measures of third parties (such as attachment or seizure), insolvency or settlement proceedings, or other incidents, the Contractor must inform the Customer thereof immediately.

## 15. Right of retention of the personal data

An objection to the right of retention within the meaning of § 273 BGB is excluded with regard to the data to be processed and the associated data carriers.

## 16. Place of processing, security

**16.1.** As far as possible, the processing of data only takes place within the EU or the EEA (cf. 4.3).

**16.2.** The processing of data in private homes is permitted if a right to control is guaranteed.

**16.3.** The transmission channels must be secured (encrypted). The way in which these channels are to be secured is specified in the Annex "Technical and organisational measures".

## 17. Liability, compensation for damages, and contractual penalty

**17.1.** Liability and compensation for damages are based on the statutory regulations (Art. 82 GDPR).

**17.2.** The Contractor is liable to the Customer for any damages caused by the Contractor, its employees, or any individuals commissioned by it with the execution of the contract when providing the contractual service.

## 18. List of processing activities at the Contractor

This agreement contains all specifications for the order processing in accordance with Art. 30 para. 2 GDPR:

- Processor: See information on the Contractor (at the beginning of this agreement)
- Controller: See information on the Customer (at the beginning of this agreement)
- Categories of processing: See Chapter 2 "Purpose and data"
- Transfers to a third country: See Chapter 4.3 and Chapter 16 "Place of processing, security"

- Technical and organisational measures: See Annex “Technical and organisational measures by the contractor”

## 19. Severability clause

Should individual parts of this agreement be ineffective, this does not affect the effectiveness of the rest of the agreement. Instead, the parties undertake to agree on a substitute provision which comes as close as possible to the invalid or unenforceable provision in terms of its effects in a legally permissible and economical manner. The above stipulations apply accordingly in the event that the ancillary agreement proves to be incomplete.

## 20. Persons authorised to issue instructions

The recipients of instructions at the Contractor are Mr Florian Suchan and Mr Michael Emaschow. The persons authorised to issue instructions at the Customer are the authorised representatives specified in the applicable section of this agreement as well as the persons specified by them in writing.

## 21. Ancillary agreements

At the time of contract conclusion, there are no ancillary agreements. The written form is required for ancillary agreements to this contract. This also includes the repeal of this written form clause.

The following Annexes are part of this agreement:

- Annex Description of the technical and organisational measures
- Annex Subcontractors
- Annex Appointed persons
- Annex Reporting data protection breaches
- Annex Data protection goals