Standard Contractual Clauses

Last updated: October 30, 2026

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

The customer

(the data controller)

and

Workfeed ApS
VAT no.: DK38921746

(the data processor)

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble 3

3. The rights and obligations of the data controller 3

4. The data processor acts according to instructions 3

5. Confidentiality 4

6. Security of processing 4

7. Use of sub-processors 4

8. Transfer of data to third countries or international organisations 5

9. Assistance to the data controller 6

10. Notification of personal data breach 6

11. Erasure and return of data 7

12. Audit and inspection 7

13. The parties' agreement on other terms 7

14. Commencement and termination 8

Appendix A Information about the processing 9

Appendix B Authorised sub-processors 9

Appendix C Instruction pertaining to the use of personal data 10

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In the context of the provision of Workfeed's scheduling platform or other software, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Three appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains information about the data processor's use of sub-processors.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

10. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Additional provisions and explanatory details are set out in Appendix C.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data controller is responsible for staying up to date on the list of sub-processors as described in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

   a. transfer personal data to a data controller or a data processor in a third country or in an international organization

   b. transfer the processing of personal data to a sub-processor in a third country

   c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.5.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 72 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall, if so requested by the data controller, be under an obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so, unless Union or Member State law requires storage of the personal data. Nothing in this clause shall prevent the data processor from deleting such personal data in the absence of such a request.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.6. and C.7.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of the customer's acceptance of this agreement. This acceptance will take place within the platform as part of the signup process.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

On behalf of the data controller	On behalf of the data processor
Name	Name
Date	Date
Signature	Signature

Appendix A Information about the processing

A.1 Purpose of Processing

The data processor processes personal data solely to provide the data controller with Workfeed's workforce management SaaS services. These include, but are not limited to, employee scheduling, time and attendance tracking, leave management, communication tools, payroll and POS integrations, and related HR functionalities designed to support the data controller's workforce operations.

A.2 Nature of Processing

The processing operations may include:

- Collection: Receiving personal data provided by the data controller, its staff, or via authorized third-party integrations.
- Storage & Management: Securely storing and processing such data within the Workfeed platform to enable features such as shift scheduling, availability visualization, absence and leave management, time clocking, and internal communications.
- Monitoring & Tracking: Recording time and attendance data, including location data when employees clock in and out, in order to validate working hours and workplace presence.
- Integration: Facilitating synchronization with third-party systems (e.g., payroll, POS, booking tools) and exporting relevant data at the request of the data controller.

A.3 Categories and Types of Personal Data

Personal data processed may include (without limitation):

- Basic identifiers: Name, contact details (email, phone), profile images, national identification number (e.g. CPR number)
- Employment details: Roles, departments, availability, contract details
- Scheduling & attendance: Shift assignments, check-in/out times, absence records, overtime
- Payroll-related: Salary or wage information, payroll export data
- Location & system metadata: Geolocation data from check-in/out, IP address, device and usage logs as required to provide the service

A.4 Categories of Data Subjects

The processing concerns staff, employees, and contractors of the data controller whose personal data is entered into or generated within the Workfeed platform.

A.5 Duration of Processing

The processing continues for as long as the data controller has an account with the data processor, and until the personal data has been deleted or returned as set out in Clause 11 and Appendix C.4.

Appendix B Authorised sub-processors

The current list of authorised sub-processors can always be obtained at https://workfeed.io/list-of-sub-processors/, and it is the responsibility of the data controller to stay up to date with the list.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing
This Appendix C constitutes the data controller's documented instructions to the data processor regarding the processing of personal data. The processing shall be carried out solely for the purposes and within the scope described in Appendix A – Information about the Processing, and in accordance with the Agreement.

C.2. Security of processing
The level of security shall take into account that the processing may involve personal data subject to Article 9 GDPR and national identification numbers. Accordingly, a level of security appropriate to such data shall be established.

The data processor shall be entitled and is under an obligation to determine and maintain the technical and organisational security measures necessary to ensure the agreed level of security.

At a minimum, the data processor shall implement and maintain the following measures:

- Secure infrastructure: The Workfeed platform is hosted on Google Cloud Platform (GCP), which provides state-of-the-art security, redundancy, backup, and recovery capabilities, and maintains internationally recognised certifications (including ISO 27001 and SOC2).
- Sub-processors: Customer support and other auxiliary services are provided through established third-party SaaS providers (e.g. Intercom), each engaged under appropriate data processing agreements and with their own security certifications.
- Access control: Access to personal data is restricted to a small, stable group of employees and contractors who require it to perform their duties and who are bound by confidentiality obligations.
- Authentication: Authentication and identity management are handled through GCP's secure services, which apply industry-standard protections (including hashing and salting of credentials, and support for multi-factor authentication).
- Encryption: Personal data is encrypted both in transit and at rest.
- Practical safeguards: The data processor relies on sensible, industry-standard security practices, such as applying updates, limiting exposure of systems to the internet, and ensuring customer data is handled responsibly at all times.

These measures may be updated and supplemented by the data processor from time to time to maintain an appropriate level of protection.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

The data processor shall assist the data controller as described in the Clauses to the best of its ability. If the assistance comprises a significant workload for the data processor, the data processor will charge a fee of 1,500.00 DKK per hour.

C.4. Storage period/erasure procedures
The processing continues for as long as the data controller has an account with the data processor. The data controller instructs the data processor to delete all personal data processed on its behalf (a) without undue delay when the data controller requests it in writing, or (b) five (5) years after the last activity on the account.

The five-year period reflects the data controller's typical statutory retention duties (e.g. bookkeeping and working-time records). Until deletion, the data controller may request a copy or return of the data, charged as set out in Appendix C.3.

C.5. Instruction on the transfer of personal data to third countries

The data processor will transfer personal data to sub-processors in a third country for processing and storage of personal data. The transfer of personal data to a third country can only take place following the rules applying to transfer of personal data to third countries following the General Data Protection Regulation and in specific the obligation for a legal basis for this transfer. The transfer tool for each sub-processor is stated in the list referred to in Appendix B.

C.6. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data controller or the data controller's representative may every second year perform a physical or written inspection of the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing to ascertain the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

In addition to the planned inspection, the data controller may perform an inspection of the data processor when the data controller deems it required

All costs, if applicable, relating to physical or written inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

C.7 Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor shall at the data controller's request and expense obtain an auditor's / inspection report from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of auditor's report may be used in compliance with the Clauses:

- ISO/IEC 27001

The report shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor or the data processor's representative shall in addition have access to inspect, including physically inspect, the places where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data processor deems it required.

Documentation for such inspections shall without delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology.