DATA PROCESSING AGREEMENT BETWEEN JOINT CONTROLLERS

This Data Processing Agreement ("**DPA**") between Joint Controllers shall apply to you, i.e. the contracting party signing up for an account at WorkMotion Platform via our website www.workmotion.com and using our Internet HR tech platform (hereinafter "**Platform**") and our digital services as described in more detail in the Terms & Conditions (hereinafter "**Client**") and WorkMotion Software GmbH, registered at Richard-Ermisch-Str. 7, 10247 Berlin, Germany, (hereinafter "**WorkMotion**")

Hereinafter collectively referred to as « Joint Controllers » or the « Parties », and individually referred to as « Party ».

This Data Processing Agreement is part of the WorkMotion T&C ("**T&C**") for the use of the Platform

THE FOLLOWING HAS BEEN AGREED:

1. Definitions

All terms and expressions related to the protection of Personal Data that are used in this DPA and identified by capital letters, whether used in singular or in plural, shall be interpreted in accordance with Data Protection Regulation.

Joint Controllers: Client, WorkMotion

Joint Processing: the Personal Data Processing activity/ies which purposes and means are jointly determined by the Joint Controllers, and described in Annex 1. For the sake of simplicity, the term is used in the singular despite the fact that it could cover several Joint Processing defined and implemented.

The Data Protection Regulation: any provision of a legislative or regulatory nature, European or national, resulting in particular from Regulation (EU) 2016/679 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), as well as any other EU or domestic regulations applicable in this field.

"Personal Data", "Controller", "Data Controller", "Data Processor", "Data Subject", "Personal Data Breach", "Process", "Processing", "Processor", "Supervisory Authority" and "Third Country", written in singular or in plural, shall bear the respective meanings given to them in the Data Protection Regulation.

2. Purpose of the DPA

The purpose of this DPA is to determine the respective obligations of the Joint Controllers in order to ensure compliance with the Data Protection Regulation when carrying out the Joint Processing.

The nature and purpose of the Joint Processing is related to the hiring, onboarding, managing and paying international employees via the Platform.

Categories of Personal Data:

Contact data (e.g. email, phone number), Content data (e.g. texts, photographs, videos), Payment data (e.g. bank account, payment history), Usage data (e.g. access times, log files), Employee master data (e.g. names, addresses, salary group, tax classification), Application data (e.g. names, contact data, qualifications, application relevant data)

Special categories of Personal Data:

Personal data revealing religious or philosophical beliefs; Data concerning health

Categories of Data Subjects:

Applicants, Employees, Freelancers

3. Duration of the DPA

This DPA enters into force upon acceptance by the Parties and shall apply until the T&C will remain in force.

4. Obligations of the Joint Controllers

4.1. Compliance with the Data Protection Regulation by each Joint Controller

The Joint Controllers recognise that they have full knowledge of the obligations that apply to them pursuant to the Data Protection Regulation in their role of Joint Controllers for the Joint Processing described in Annex 1.

For this reason, the Joint Controllers undertake to:

- respect and comply with these obligations in every country where the Joint Processing is carried out;
- implement a register of the Joint Processing of Personal Data as required under the Data Protection Regulation;
- document their compliance and make the documentation available to the other Party upon simple request;
- inform each other of any proven or potential error, irregularity, omission or alleged Personal Data Breach to Data Protection Regulation to which the present DPA applies;
- update the conditions for carrying out the Joint Processing when needed, having regards to the changes in the Data Protection Regulation.

Each Party undertakes to ensure its own compliance and the compliance of its staff and its processors (where applicable) with the following obligations:

- to process Personal Data for the sole purposes of the Joint Processing;
- to ensure the confidentiality of Personal Data processed under this DPA;
- to make sure that the people authorised to process Personal Data:
  - Only access the Personal Data necessary for the fulfilment of their duties according to their roles and to the needs of the present DPA;
  - Are subject to an adequate confidentiality obligation;
  - Have received appropriate training in data protection.
- to communicate to the other Party, upon simple request and without delay, all the information and documents proving compliance with its obligations under the Data Protection Regulation;
- to define, adopt and keep updated the necessary technical and organisational measures to ensure an appropriate level of data security and confidentiality for the part of the Joint Processing that is under its responsibility. The measures thus implemented are described in Annex 2;
- to define and adopt the internal procedures that are necessary for complying with its obligations;
- to ensure, where appropriate, the deletion of Personal Data at the end of the retention period.

4.2. Obligation of information

Each Joint Controller shall provide to Data Subjects the information required by the Data Protection Regulation, according to the conditions and deadlines prescribed by the Data Protection Regulation.

4.3. Managing Data Subjects' rights

In this section, the term « rights » shall mean any right granted to Data Subjects by the Data Protection Regulation, such as the right to access, to rectify, to delete and, where appropriate, to limit, to make portable, to object and to withdraw consent.

In compliance with the Data Protection Regulation, a Data Subject may exercise their rights against each Joint Controller or against both Joint Controllers.

Notwithstanding the above, the Parties agree that it shall fall upon:

- WorkMotion to follow up and to manage relations with Data Subjects pursuant to any enquiries that are related to the Joint Processing, according to the conditions and deadlines prescribed by the Data Protection Regulation;

In order to allow for a correct management of enquiries, Client undertakes to:

- transfer without delay any request or enquiry that was directly received to the Party that is responsible for managing enquiries (mentioned above);
- where appropriate, provide all information relating to the part of the Joint Processing that is under its responsibility, where such information is necessary to the follow-up and the management of a Data Subject's request;
- ensure necessary measures are implemented.

4.4. Management of Data Breaches

Joint Controllers undertake to define and implement internal procedures necessary to manage Personal Data Breach according to Data Protection Regulation.

The Joint Controllers undertake to inform each other without delay of any Personal Data Breach affecting the Joint Processing in whole or in part and

to cooperate together when notification to the Supervisory Authority and/or, where appropriate, to the Data Subjects is required.

4.5. Cooperation in carrying out Privacy Impact Assessments

The Joint Controllers undertake to cooperate in order to identify the need to carry out a data protection impact assessment for the Joint Processing, and where appropriate, to jointly carry out this impact assessment under the direction of the referents designated in article 6.

Each Party bears its own costs for carrying out the impact assessment.

4.6. Cooperation regarding Supervisory Authorities

The Joint Controllers shall inform each other of any requests, enquiries, follow-up activities and any similar measures taken by the Supervisory Authority or any other authority regarding the Joint Processing.

The Joint Controllers shall assist each other in answering and complying with every request or enquiry coming from the Supervisory Authority or any other authority and relating, in whole or in part, to the Joint Processing.

4.7. International Transfers of Personal Data

Where appropriate, any international transfer of Personal Data undertaken by either Party must comply with Data Protection Regulation and be made pursuant either on the grounds of an Adequacy Decision or Appropriate Safeguards such as Standard Contractual Clauses made public by the European Commission

5. Data Processors

5.1. Conditions to contract with a Data Processor

Each Party may subcontract all or part of its obligations, subject to prior information of the other Party. Any change in Data Processors shall enter into application in the absence of objection by the other Party within eight (8) calendar days from receipt of the above mentioned prior information.

All contractual agreements with the subcontractor(s) and the performance of the contractual relationship must be designed in such a way that they comply with the requirements of the GDPR and other data protection provisions, where applicable.

In the case of subcontracting, the Parties shall be granted control and inspections rights by the subcontractor in accordance with this DPA, The Parties undertake to ensure that each of their Data Processors respect the obligations provided for in this DPA, in particular by expressly including the same obligations in the contract binding this or these Data Processors and by carrying out a regular audit or having it carried out to verify the compliance of these Data Processors.

5.2. Obligations when using a Data Processor

The Parties undertake to only resort to Data Processors who have taken sufficient safeguards, in particular when they intervene in order to implement appropriate technical and organisational measures for the Joint Processing.

They also undertake to ensure that each of their Data Processors respect the obligations provided for in this DPA, in particular by expressly including the same obligations in the contract binding this or these Data Processors and by carrying out a regular audit or having it carried out to verify the compliance of these Data Processors.

Each Party shall remain fully liable to the other Party for the performance by the Data Processor(s) of its (their) obligations.

6. Referents for the protection of Personal Data

Each Party undertakes to appoint a referent for the protection of Personal Data, with the required skills to manage the proper performance of this DPA and to answer the other Party's requests.

WorkMotion Referent: Dr. Jonas Jacobsen, jacobsen@comtection.com
Responsibility of the Joint Controllers

The Joint Controllers shall bear reciprocal liability for breach of duty in accordance with the T&C. Exclusions or limitations of liability contained in the T&C should only apply between the Joint Controllers. In any case, statutory liability with regard to the Data Subject shall remain unaffected.

7. Communication of the DPA

Following a Data Subject's request, the Joint Controllers are authorised to communicate to this Data Subject a summary of this DPA.

8. Miscellaneous

- The Parties are not allowed to unilaterally modify or suspend the performance of this DPA, unless otherwise specified in an express manner. Any amendment to the provisions of this DPA shall be subject to a written amendment between the Parties.
- In the case where a provision of this DPA is deemed or judged entirely or partially invalid or inapplicable by a competent court or in accordance with a law, the invalidity of this provision shall have no effect on the other provisions, and they will continue to apply.
- The DPA shall be subject and be interpreted in accordance with the laws of Germany.
- All and any disputes arising from and/or in connection with this DPA shall be decided exclusively by the courts of Berlin, Germany.

Annex 1: Main characteristics of the Joint Processing

Subject matter:

The Joint Controllers shall cooperate on the basis of individual mandates given to WorkMotion, or on the basis of individual contracts concluded between Client and WorkMotion.

Nature and purpose of the Joint Processing:

The nature and purpose of the Joint Processing is related to the hiring, onboarding, managing and paying international employees via a Software Platform.

Categories of Personal Data:

- Contact data (e.g. email, phone number)
- Content data (e.g. texts, photographs, videos)
- Payment data (e.g. bank account, payment history)
- Usage data (e.g. access times, log files)
- Employee master data (e.g. names, addresses, salary group, tax classification)
- Application data (e.g. names, contact data, qualifications, application relevant data)

Special categories of Personal Data:

- Personal data revealing religious or philosophical beliefs;
- Data concerning health

Categories of Data Subjects:

- Applicants
- Employees
- Freelancers

Annex 2: TOMs

Technical and organisational measures (TOM)
according to Art. 32 GDPR

WorkMotion Software GmbH

1. Encryption and pseudonymisation of personal data

Ensuring that personal data is only stored in the system in a way that does not allow third parties to identify the data subject.

Measures	Description	Suitability (taking into account the requirements of Article 32 of the GDPR)
Encryption of data records	*Use of database software that enables the encrypted storage of data records*	*Selection of the software corresponds to the current specifications of the BSI*

2. Confidentiality and integrity

2.1. Access control

Denying unauthorised persons access to processing equipment with which the processing is carried out.

Measures	Description	Suitability (taking into account the requirements of Article 32 of the GDPR)
All personal data is stored in data centers of external service providers.	*The data centers used are secured in accordance with current security standards:* *ISO 27001/27017/27018*	*The measures correspond to the state of the art.*

2.2. Access control

Prevention of the use of data processing systems by unauthorised persons

Measures	Description	Suitability

		(taking into account the requirements of Article 32 of the GDPR)
Individual log-in and log-in protocol	*Logging on to the system or company network is done with a separate log-in and is logged (user name and password); use of user-profiles and assignment of user rights*	▪ *There are minimum requirements for the assignment of passwords (minimum number of characters)* ▪ *Access to data processing systems can bKe traced via individual log-ins and is thus suitable for clarifying unauthorised access in retrospect and thus already acts as a deterrent in advance.*
Software Firewall	*A state of the art firewall is enabled by default and is kept up to date.*	*The software is regularly updated and corresponds to the state of the art*
Lock screen	*The automatic lock screen on all computers; automatic pausing of screens*	*Access by unauthorized persons is made more difficult.*

2.3. Data medium control

Prevention of unauthorized reading, copying, modification or deletion of data carriers.

Measures	**Description**	**Suitability** (taking into account the requirements of Article 32 of the GDPR)
Authorization concept	*Due to the authorization concept, only authorized persons have the possibility to process personal data.*	*Risk of unauthorized data access is effectively minimized by restricting access rights.*

2.4. Memory Control

Prevention of unauthorised input of personal data as well as unauthorised knowledge, modification and deletion of stored personal data.

Measures	**Description**	**Suitability** (taking into account the requirements of Article 32 of the GDPR)
Authorization concept	*Due to the authorization concept, only authorized persons have the possibility to process personal data.*	*Risk of unauthorized data access is effectively minimized by restricting access rights.*

Software Firewall	*Windows firewall is enabled by default and is kept up to date.*	*The software is regularly updated and corresponds to the state of the art*

2.5. User control

Prevention of the use of automated processing systems by means of data transmission equipment by unauthorised persons.

Measures	Description	Suitability (taking into account the requirements of Article 32 of the GDPR)
Firewall and VPN access. Admission only from identified devices	*Sealing off the system against access by unauthorised persons*	*The selected technical solution corresponds to the state of the art and is continuously updated*

2.6. Access control

Ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation.

Measures	Description	Suitability (taking into account the requirements of Article 32 of the GDPR)
Authorization concept	*Due to the authorization concept, only authorized persons have the possibility to process personal data.*	*The measure is proportionate to the risk.*

2.7. Transmission control

Ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available by means of data communication equipment.

Measures	Description	Suitability (taking into account the requirements of Article 32 of the GDPR)
Storage of all outgoing and incoming emails	*Automated archiving of e-mail communication documents all data transmissions.* *The access to the archive system is strictly regulated*	*The measure taken is proportionate to the risk.*

2.8. Transport control

Ensure that the confidentiality and integrity of personal data is protected during the transmission of personal data and during the transport of data media.

Measures	Description	Suitability (taking into account the requirements of Article 32 of the GDPR)
Signature of e-mails *No shipping of data carriers*	*The sending of signed e-mails is offered*	*Measure is commensurate with the risk.*

2.9. Input control

Ensure that it is possible to verify and establish ex post which personal data have been entered or modified in automated processing systems, at what time and by whom.

Measures	Description	Suitability (taking into account the requirements of Article 32 of the GDPR)
Traceability of entries, changes and deletions	*File system captures changes.*	*Measure is commensurate with the risk.*

2.10. Data integrity

Ensure that stored personal data cannot be damaged by system malfunctions.

Measures	Description	Suitability (taking into account the requirements of Article 32 of the GDPR)
Data backup	*Regular backups enable the restoration of an error-free system.*	*Measure is commensurate with the risk.*

2.11. Order control

Ensure that personal data processed on behalf can only be processed in accordance with instructions.

Measures	Description	Suitability (taking into account the requirements of Article 32 of the GDPR)

AV agreements according to DSGVO	*Selection of service providers that implement the requirements of the GDPR and obligation to comply with the requirements of Art. 32 GDPR.*	*Measure is commensurate with the risk.*

3. Availability

Ensure that personal data is protected against destruction or loss.

Measures	Description	Suitability (taking into account the requirements of Article 32 of the GDPR)
Data backup	*Regular backups*	*Measure is commensurate with the risk.*

4. Recoverability

Ensure that deployed systems can be restored in the event of a failure.

Measures	Description	Suitability (taking into account the requirements of Article 32 of the GDPR)
Data backup	*Creating backups*	*Measures are commensurate with the risk.*

5. Separability

Ensure that personal data collected for different purposes can be processed separately.

Measures	Description	Suitability (taking into account the requirements of Article 32 of the GDPR)
Separate storage of personal data for different purposes	*A breakdown of records by purpose was made.*	*Measures are commensurate with the risk.*

6. Review and evaluation

Presentation of the procedure for the regular review, assessment and evaluation of the effectiveness of the technical and organisational measures.

Measures	Description	Suitability

		(taking into account the requirements of Article 32 of the GDPR)
Testing and documentation	*TOMs are assessed and evaluated on a quarterly basis.* *The completion is documented and presented to the management.*	*Quarterly audit is appropriate and sufficient for the risk*

Status: December 2021