Security Addendum & Annex III of the Data Processing Addendum

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by Workpath as the processor (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. The term "Customer Data" as defined in the Agreement includes personal data subjected to the Services by Customer who is the controller.

Measures of pseudonymisation* and encryption of personal data

- Encryption at rest: Workpath encrypts data at rest using AES-256 bit algorithm. Workpath uses Amazon Aurora for storing Customer Data.
- Encryption in transit: Workpath uses TLS 1.2 and 1.3 for encrypting data in transit.
- HTTPS: Workpath's application is accessible only via HTTPS.

*Note that the features of the Subscription Service are tied to the identity of a User so full pseudonymization is not possible. However, only personal data strictly necessary for the use of the Subscription Service are required.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- Workpath is ISO 27001:2022 and certified and implemented all controls from the standard.
- Workpath is also TISAX certified, with participant number PVVYK4.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Business Continuity (BC) and Disaster Recovery (DR). Workpath implements and maintains industry standard BC and DR plans. These plans include, without limitation:

- Redundant systems for zero-downtime bridging of partial failures of the server infrastructure
- Database backups in a separate data centre (at least daily, retention 30 days)
- Restoration testing performed in a biannual rhythm
- Recovery Point Objective of at least 12 hours and Recovery Time Objective of at least 24 hours
- In case of a disaster, Customer Data is restored from separate back-up data centre to servers in main operations data centre

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- Audits: Workpath conducts security audits internally and by independent external auditors at least annually. The audits are conducted to certify compliance with the standards and best practises of ISO 27001:2022.
- Penetration Testing: To increase security by identifying risks and remediation options, Workpath performs internal penetration tests on the Workpath platform at least once a year by contracting an independent third party to execute a penetration test. Upon request, the summary of the report of these penetration tests can be made available to Customer (provided that an adequate non-disclosure obligation is in place).
- Vulnerability Scanning: Workpath performs regular vulnerability scanning on the platform that processes Customer Data to identify threats and potential vulnerabilities and to remediate them.

Measures for user identification and authorisation

- Internal Access Control: In normal operation of the SaaS platform, Workpath employees do not access Customer Data. Workpath provides access to its employees on the basis principle of least privilege ("need-to-know"). Access is granted based on job roles and by following a proper approval process based on Workpath's Access Rights Management Policy. Access privileges are reviewed regularly.
- Password: Workpath has a strong password policy implemented, including password complexity requirements, locked account after 5 failed attempts, etc. Passwords are salted and hashed.
- Users: Customer administrators are responsible for managing User accounts within the Subscription Service.

Measures for the protection of data during transmission

- Encryption in transit: Workpath uses TLS 1.2 and 1.3 for encrypting data in transit.

Measures for the protection of data during storage

- Encryption at rest: Workpath encrypts data at rest using AES-256 bit algorithm.
- Separation Control: Customer Data is separated from data of other customers by using a dedicated database schema per customer.

Measures for ensuring physical security of locations at which personal data are processed

- Workpath premises: physical access to Workpath premises is restricted using personalized digital keys and restricted access to sensitive areas. Periodic review of access allowances is conducted in formal procedures.
- AWS: Workpath is hosted in AWS datacenter in Frankfurt, Germany which is among others certified according to ISO 27001, SOC 1, 2, 3 and TISAX.
- Hetzner: Customer Data is backed up with Hetzner Online GmbH in Nürnberg, Germany. Hetzner is certified according to the ISO 27001 standard.

Measures for ensuring events logging

- Logs: Logging is enabled on the Workpath platform, including application servers, network, operating system, database, web servers and security assets.
- Log retention: Logs are stored according to Workpath's retention policy.

Measures for ensuring system configuration, including default configuration

- Systems are configured and hardened according to Workpath's standards.

Measures for internal IT and IT security governance and management

- Incident and change management: Workpath implements a formal incident and change management process. All requests are logged and processed with a formal process.
- Risk management: Workpath established a defined risk management methodology within its ISMS.
- Security Training: all Workpath' employees are required to take regular security and privacy trainings.
- Supplier management: Workpath maintains a process to ensure that all suppliers provide appropriate security controls with regards to information security and data protection, including re-assessments.

Measures for certification/assurance of processes and products

- Policies: Workpath maintains policies, processes, procedures and controls to guarantee compliance with the ISO 27001:2022 standard.

Measures for ensuring data minimisation

- Data Minimisation: the Customer is responsible for uploading Customer Data on the SaaS platform. The SaaS platform is designed to only require the input of the personal information directly relevant and necessary to accomplish the relevant purpose. Also, Workpath will retain the data only for as long as it is necessary to fulfil that purpose or until the contract ends.

Measures for ensuring limited data retention

- Deletion after termination/expiration: Customer Data is deleted 30 days after the termination or expiration of the Agreement.
- Deletion as part of back-ups: Customer Data is deleted as part of backups in the regular process within 30 days.

Measures for ensuring accountability

- Accountability: Workpath is accountable and responsible for operation and maintenance of the Workpath platform, including availability, upgrades, backups, and patching. Ownership of the data within the platform is with the Customer.

Measures for allowing data portability and ensuring erasure

- Customer Data export: Customers can export their Data themselves by using the available APIs or csv-export functionality anytime during the Subscription Period.
- Deletion: Workpath is responsible for deleting Customer Data from the infrastructure involved in the delivery of the Services. Workpath cannot wipe the hardware servers as Workpath uses a multi-tenant Subscription Service. AWS wipes the servers in line with industry standards.