Workable's Technical and Organisational Security Measures

Technical and Organizational Security Measure	Details
Measures of pseudonymisation and encryption of personal data	All Application data - including personal data such as candidates information - is always encrypted at-rest and in-transit in order to ensure its confidentiality across all its lifecycle (e.g.: storage means, data flows). Personal data is stored on a microservice level to apply segregation and segmentation across the Application storage resources(e.g.: databases). Randomly generated and long UUIDs are used to correlate data to an individual.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Workable data is encrypted at rest and in transit using Security Best Practices and the latest recommended secure cipher suites and protocols Appropriate safeguards have been implemented to protect the creation, storage, retrieval and destruction of secrets. Workable implements Best Practices as they evolve and respond promptly to cryptographic weaknesses as they are discovered. The infrastructure and data are stored redundantly in multiple locations in their hosting and data storage providers. Workable uses multiple relational databases for its applications. Each database server has an independent synchronous replica in a different availability zone within the same AWS region to mitigate the risk of data lost due to hardware failure.

	In the unlikely event of a major disaster, a Business Continuity Plan (BCP) is in place to help guarantee a smooth and organized transition towards a full recovery. To ensure that production services are highly available, teams have designed infrastructure so as to have replicas/ fallbacks for all critical resources. To ensure that Workable infrastructure is resilient against single node or instance failure, for all critical services multiple instances are available and running. This guarantees that if a single instance fails there is at least an extra instance to serve traffic until the failure is recovered. In order to protect services from single zone failure of cloud providers, all critical resources have multi-zone availability. This means that when teams provision production resources they make sure that they have replicas in multiple zones, so if a single zone fails the replicas in the other zones can still serve traffic
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	Workable has documented and follows specific policies and procedures to securely take, maintain, test and restore backups of production data. Backup data includes but is not limited to customers' and candidates' data, application logs and systems' configuration, and has a retention period of at least 18 months. The backup configuration of a new resource is not limited to availability factors (e.g.: retention period, frequency) but also includes restoration aspects such as integrity tests and restore periodic procedure and timeline.. The enterprise cloud platforms (e.g.: GCP and AWS), where Workable infrastructure is hosted, offer strong and out of the box managed backup services ensuring data availability and integrity.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Workable has identified a suitable, systematic approach and framework for risk assessment which is appropriate for its business, legal, regulatory and contractual requirements, and this is described in the Risk Assessment Report. Assessment (analysis and evaluation) of risks is carried out at least once a year, options for risk treatment are identified and evaluated in line with the Risk Assessment process.

	Technical security assessments (such as web application penetration testing, manual source code review and configuration audit) are performed by 3rd-party security experts on a regular basis to bring independent expertise and in-depth testing.. The ISMS is thoroughly reviewed through an Audit Program maintained by the CISO. The goal of internal and external audits is to: • Identify potential non-compliance points with respect to Workable policies, procedures as well as regulatory requirements (e.g.: GDPR, CCPA, etc.) and Standards (e.g.: ISO 27001, ISO 27017, AICPA TSC.) • Spot opportunity for improvements • Document and track remediation activities All appropriate mitigation actions such as technical security assessments and audit findings are documented, reviewed, approved and tracked for their effective implementation.
Measures for user identification and authorization	As a Product: • The Workable application ensures a strong authentication flow with hardened configuration (e.g.: password policy, account lockout, Captcha mechanism) and secure protocols including SAML v2 and OIDC. • Appropriate Logical Access controls and restrictions are in place on the account and user level of the application while the customer can enforce a granular authorization model based on the different available user roles. As a Company: • Workable systems and services use strong authentication means (such as SSO, TFA and short session timeouts). Credentials are managed through an enterprise cloud vault solution ensuring password complexity and prohibiting password reuse. • Granular role-based access control is in place for all Workable employees based on their position and need to know principle. Access is managed via a dedicated procedure while an entitlement review process is performed during the internal audits.

Measures for the protection of data during transmission	Data is always encrypted in-transit to ensure its confidentiality using Security Best Practices and the latest recommended secure cipher suites and protocols.
Measures for the protection of data during storage	Data is always encrypted at-rest to ensure its confidentiality and integrity using Security Best Practices and the latest recommended secure cipher suites and protocols. On top of all cloud storage resources, Workable laptops and mobile devices are fully encrypted.
Measures for ensuring physical security of locations at which personal data are processed	Offices: • Access to the premises is protected by physical access controls such as security guards, access cards, CCTV and alarm system.Guest and external visitors' access is handled securely through a dedicated procedure. Cloud resources: • Workable uses subservice organizations (Google Cloud Platform and Amazon Web Services) for cloud hosting services and for providing physical controls, environmental controls, infrastructure support and storage services. Workable reviews the reports and/ or certifications (e.g. SOC 2, ISO) of the subservice contractors in regard to security controls including data centers physical and environmental controls
Measures for ensuring events logging	Workable maintains an extensive, centralized logging system in the production environment. It contains information pertaining to security, monitoring, availability and access, as well as other metrics about our application ecosystem and its microservices. Production log retention is set to 18 months. These logs are analyzed for security events and abnormalities via logical and technical controls. Further, alerts and monitors automatically notify appropriate internal teams 24/7/365 to ensure visibility and responsiveness. These alerts also include the product availability, capacity and performance metrics.

	Production operation actions (such as major system configuration update and product deployments) are performed in a controlled (segregated responsibilities, approval step) and tracked (audit logs) manner.
Measures for ensuring system configuration, including default configuration	Security best practices are taken into account during the installation of any resource in the cloud infrastructure in order to ensure that cloud infrastructure complies with Workable Security Policies. A production readiness checklist depicts the high level controls (e.g.: access controls requirements, encryption, patch management, backup strategy, logging requirements, etc.) that have to be met for all production systems. Each control is detailed for each type of resource (e.g.: vm, database).
Measures for internal IT and IT security governance and management	Workable maintains reasonable and appropriate technical and organizational controls (based on best practices, i.e. ISO 27001, ISO 27017 and SOC 2 requirements) in order to protect customer data against accidental loss, destruction or alteration, unauthorized disclosure or unlawful destruction. Workable compliance requirements are continuously monitored and reviewed and appropriate changes to Information Security Policies and technical controls are performed as needed. The Legal Department and DPO are responsible to ensure that all requirements from applicable legislation are communicated to the Security department. The Security Department is responsible to review the policies and procedures in order to achieve compliance with the regulatory requirements Workable undertakes management review of the ISMS on a regular basis (are held at not greater than six-monthly intervals) to ensure that the scope remains adequate and improvements in the ISMS process are identified. The agenda of Management Review Meetings covers all the items that are required by the relative standards (i.e. ISO 27001:2013, ISO 27017:2015, AICPA Trust Services Criteria, etc.). All actions that are decided during the management review meeting are monitored in order to ensure their implementation and effectiveness.

Measures for certification/ assurance of processes and products	Workable holds security certifications and comply with industry-accepted standards and regulations: • ISO 27001:2013, Information Security Management System • ISO 27017:2015, Security Controls for the Provision and Use of Cloud Services • SOC 2 Type I Report • SOC 2 Type II Report • SOC 3 Report Additionally, Technical Security Assessments (such as web application penetration testing, manual source code review, configuration audit, etc.) are performed by 3rd-party security experts on a regular basis.
Measures for ensuring data minimisation	In compliance with the GDPR / CCPA requirement, the Workable product provides its customers the ability to have control over their data. Data deletion requests are handled through a dedicated automated process. The Application enforces controls on all upload flows to ensure that only the allowed file types are stored within the system. Moreover, the terms of use clearly state the types of information that should be stored within Workable as well as the customers' responsibility regarding its use.
Measures for ensuring data quality	Users' input is sanitized and validated by the application in regards to the business logic of the corresponding feature or product. Malformed data is thus rejected prior to be stored.
Measures for ensuring limited data retention	Workable Customers determine what Customer Data they process via Workable product. As such, Workable operates on a shared responsibility model. If a Customer is unable to delete Customer Data via the self-services functionality of the Product, then Workable deletes Customer Data upon the Customer's written request, within the timeframe specified in the Data Protection Addendum and in accordance with Applicable Data Protection Law.

Measures for ensuring accountability	Management has defined Roles and Responsibilities to oversee implementation of the Information Security Policy across Workable (e.g. DPO has been appointed, Information Security Committee is in place as well as specific security responsibilities for Workable Team Members). New employees undergo initial training during the onboarding week to understand their key responsibilities, tasks and Team's process. The Employment Agreement and the Acceptable Use Policy are signed by the end of the first week. Employees are evaluated on a periodic basis based on their role specific goals and overall performance. Regular meetings on SVPs / VPs level as well as Management Review Meetings (MRMs) are conducted regarding information security. The topics of these meetings include results from risk assessments, internal and external audits, security assessments,other feedback from interested parties and appropriate corrective and preventive decisions are taken. Major gaps are communicated to the Board of Directors through Management Review Meetings (MRMs). Internal & external information security audits are performed at least on an annual basis in order to ensure compliance with Data Protection (e.g. GDPR, CCPA) and Information Security requirements (e.g. Workable policies & procedures, ISO 27001, ISO 27017, TSC, Security Best Practices). All identified gaps are investigated, and appropriate corrective and preventive actions are implemented via formal procedures. Major gaps are communicated to the Board of Directors through Management Review Meetings (MRMs).
Measures for allowing data portability and ensuring erasure	As a Product: • Workable provides the appropriate tools that give Customer control over their data, ensuring compliance with GDPR / CCPA requirements. Additionally, appropriate operation procedures are in place internally in order to handle GDPR / CCPA requests in case Customer is not able to handle any data subject request.

	As a Company: • When a critical tool or service is sunsetted, Workable asks for confirmation in writing regarding permanent data deletion. • Physical devices such as laptops and hard drives are wiped according to the device disposal policy.
Technical and organizational measures of sub-processors	Third parties and contractors Non-Disclosure Agreements (NDA), Data Processing Agreements (DPA) and contracts are in place and contain provisions in regard to confidentiality clauses and code of conduct if applicable. In particular Workable enters into Data Processing Agreements with its Authorized Sub-Processors with data protection obligations substantially similar to those contained in this Agreement. Each sub-processor agreement must ensure that Workable is able to meet its obligations to the Customer and technical and organisational measures shall be implemented in order to safeguard the protection of personal data. Sub-processors must without limitation a) notify Workable in the event of a Security Incident without undue delay so Workable may notify Customer accordingly; b) delete data when instructed by Workable in accordance with Customer's instructions to Workable; c) not engage additional sub-processors without authorization; d) not change the location where data is processed; or e) process data in a manner which conflicts with Customer's instructions to Workable. e) enter into a separate agreement containing the applicable SCCs, when this is required. Appropriate contracts and Service Level Agreements (SLAs) are in place to outline and communicate the terms, conditions and responsibilities for third-party providers. (e.g. Google Cloud, Amazon).