StaySigned’s Technical and Organisational Security Measures

Technical and Organizational

Security Measure Details

Measures of pseudonymisation and encryption of personal data

The infrastructure and data are stored redundantly in multiple locations in their hosting and data storage providers. StaySigned 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.

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

StaySigned 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. StaySigned implements Best Practices as they evolve and respond promptly to cryptographic weaknesses as they are discovered.

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 StaySigned 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	StaySigned 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 StaySigned 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	StaySigned 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.

Measures for user identification and authorization Techical security assessmets (such as web applicatio peetratio testig, maual source code review ad cofiguratio audit are performed by 3rd-party security experts o a regular basis to brig idepedet expertise ad i-depth testig..

The ISMS is thoroughly reviewed through a Audit Program maitaied by the CISO. The goal of iteral ad exteral audits is to

Idetify potetial o-compliace poits with respect to Worable policies, procedures as well as regulatory requiremets (e.g.: GDPR, CCPA, etc. ad Stadards (e.g.: ISO 271, ISO 2717, AICPA TSC.

Spot opportuity for improvemets

Documet ad tracremediatio activities

All appropriate mitigatio actios such as techical security assessmets ad audit fidigs are documeted, reviewed, approved ad traced for their effective implemetatio.

As a Product

The Worable applicatio esures a strog autheticatio flow with hardeed cofiguratio (e.g.: password policy, accout locout, Captcha mechaism ad secure protocols icludig SAML v2 ad OIDC.

Appropriate Logical Access cotrols ad restrictios are i place o the accout ad user level of the applicatio while the customer ca eforce a graular authorizatio model based o the differet available user roles.

As a Compay:

Worable systems ad services use strog autheticatio meas (such as SSO, TFA ad short sessio timeouts. Credetials are maaged through a eterprise cloud vault solutio esurig password complexity ad prohibitig password reuse

Graular role-based access cotrol is i place for all Worable employees based o their positio ad eed to ow priciple. Access is maaged via a dedicated procedure while a etitlemet review process is performed durig the iteral audits.

Measures for the protection of data during transmission

Measures for the protection of data during storage

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

Measures for ensuring events logging

Data is always encrypted in-transit to ensure its confidentiality using Security Best Practices and the latest recommended secure cipher suites and protocols.

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, StaySigned laptops and mobile devices are fully encrypted.

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

StaySigned 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. StaySigned 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

StaySigned 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.

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

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.

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 StaySigned 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).

StaySigned 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.

StaySigned 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

StaySigned 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

Measures for ensuring data minimisation

StaySigned holds seurity ertifiatios ad oply with idustry-aepted stadards ad reulatios

ISO 7001:013, Iforatio Seurity Maaeet Syste ISO 7017:015, Seurity Cotrols for the Provisio ad Use of Cloud Servie

SOC Type I Repor

SOC Type II Repor

SOC 3 Report

Additioally, Tehial Seurity Assessets (suh as web appliatio peetratio testi, aual soure ode review, ofiuratio audit, et.) are perfored by 3rd-party seurity experts o a reular basis.

I opliae with the GDPR / CCPA requireet, the StaySigned produt provides its ustoers the ability to have otrol over their data. Data deletio requests are hadled throuh a dediated autoated proess.

The Appliatio efores otrols o all upload flows to esure that oly the allowed file types are stored withi the syste. Moreover, the ters of use learly state the types of iforatio that should be stored withi StaySigned as well as the ustoers' resposibility reardi its use.

Measures for ensuring data quality Users' iput is saitized ad validated by the appliatio i reards to the busiess loi of the orrespodi feature or produt. Malfored data is thus rejeted prior to be stored.

Measures for ensuring limited data retention StaySigned Custoers deterie what Custoer Data they proess via StaySigned produt. As suh, StaySigned operates o a shared resposibility odel. If a Custoer is uable to delete Custoer Data via the self-servies futioality of the Produt, the StaySigned deletes Custoer Data upo the Custoer's writte request, withi the tiefrae speified i the Data Protetio Addedu ad i aordae with Appliable Data Protetio Law.

Measures for ensuring accountability

	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. StaySigned 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 Management has defined Roles and Responsibilities to oversee implementation of the Information Security Policy across StaySigned (e.g. DPO has been appointed, Information Security Committee is in place as well as specific security responsibilities for StaySigned Team Members). New employees undergo initial training during the onboarding week to understand their key	As a Product: StaySigned 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.

Technical and organizational measures of sub-processors
AsaCompany:

WhenacriticaltoolorserviceisunsettedStaySignedasks forconfirmationinwritinreardinpermanentdata deletion

Physicaldevicessuchaslaptopsandharddrivesarewiped accordintothedevicedisposalpolicy.

ThirdpartiesandcontractorsNon-DisclosureAreements (NDA)DataProcessinAreements(DPA)andcontracts arein placeandcontainprovisionsinreardtoconfidentiality clausesandcodeofconductifapplicable.

InparticularStaySignedentersintoDataProcessinAreements withitsAuthorizedSub-Processorswithdataprotection obliationssubstantiallysimilartothosecontainedinthis Areement.

Eachsub-processorareementmustensurethatStaySignedis abletomeetitsobliationstotheCustomerandtechnical and oranisationalmeasuresshallbeimplementedinorderto safeuardtheprotectionof personaldata. Sub-processors mustwithoutlimitationa)notifyStaySignedintheevent ofa SecurityIncidentwithoutunduedelaysoStaySignedmaynotify Customeraccordinly;b)deletedatawheninstructedby StaySignedinaccordancewithCustomer’sinstructionsto StaySigned;c)notenaeadditionalsub-processorswithout authorization;d)notchanethelocationwheredatais processed;ore)processdatainamannerwhichconflictswith Customer’sinstructionstoStaySigned.e)enterintoaseparate areementcontainintheapplicable SCCswhenthisis required.

AppropriatecontractsandServiceLevelAreements(SLAs) areinplacetooutlineandcommunicatethetermsconditions andresponsibilitiesforthird-partyproviders.(e..Goole CloudAmazon).