Alva’s information security and privacy practices

In the age of cyberattacks and data breaches, it’s never been more important to protect information – especially considering it’s at the heart of every business process and relationship.

Alva is wholly committed to being responsible and trustworthy with customer data. Our robust information security and privacy policy promotes a culture of data safety and security throughout the entire organisation, ensuring your information is in safe hands.

Organisational controls around security & privacy practices

We have a dedicated security team in place to handle issues that may crop up at any stage of the software development and maintenance process. The following controls are taken internally to ensure our customers' data are kept safe and secure.

Security-first protocol with risk assessments

We routinely run risk assessments with all departments at Alva, training them to approach each task with a security mindset. Internally, our teams are constantly testing and optimising our processes to ensure continued information security. We've also partnered with an independent third party assessor to help us identify potential vulnerabilities in our information infrastructure and mitigate accordingly.

Security awareness training

Alva regularly runs security awareness training to ensure our employees are aware of cyber threats and how they can contribute to lower the risk of a threat at all times.

Access privileges are controlled

Alva practises "least privilege" – meaning user permissions are strict and routinely updated to ensure employees only have access to information that helps them get their jobs done. Rolling out a least privilege policy has helped us keep data secure and minimise risk. Finally, it is mandatory for Alva employees to use Google SSO with a two-factor authentication when accessing authenticated information.

Suppliers are carefully vetted

For each new supplier and partnership, Alva does a cost and risk analysis to determine whether a potential collaboration is viable. In the event that a critical risk is identified, further information security requirements may be applied.

Results are protected and all third-party transfers are constantly evaluated

Alva constantly evaluates all third-party transfers between Alva and our sub-processors to ensure that they try to live up to a similar security level as inside the EU/EEA. All assessment results stay within Google and will never be shared with any other sub-processor.

Strategising ahead with incident handling procedures

At Alva, we've established incident handling procedures, where we approach each risk with structure and refer to a playbook for handling security breaches. In the event that a situation escalates, we refer to our business continuity plan, with special reference to our action plan in the event of a cyber threat or data breach.

Technical controls of information security and privacy

For every new feature, update, or maintenance, Alva implements organisational-wide security controls, which consists of the following:

Hosting with modern cloud infrastructure

We are hosted on the Google Cloud Platform (GCP) which is backed by the same infrastructure and security that Google uses for its own services. GCP is compliant and compatible with most major security standards and certifications. All our servers and data are hosted primarily in Belgium, Europe.

Backups are conducted every night and activity is monitored regularly

We create backups for our databases every night which we store for 7 days. All activity on our platform is logged and monitored. Generally, we store logs in our systems for 30 days. Additionally we store audit logs for all API requests for 450 days (15 months).

Software is regularly updated and tested by third-party vendors

Our team regularly gets together and plans for software updates, assessing changes that might impact the confidentiality and stability of our platform. We also conduct annual penetration testing to ensure our software runs smoothly.

Quality-controlled, zero trust security model

Alva's security model is based on a zero-trust security model. This means that all requests are required to be authorised in order to be accepted. This is true regardless if the request originates from any of Alva's servers or if it originates from the public internet. One practical consequence of the zero-trust security model is that its effectiveness does not depend on network perimeter boundaries.

Securing personal data with a third-party encryption broker

Personal identifiable information (PII) and all other data is encrypted, both in transit and at rest.

→ Encryption in transit

All information in transit is encrypted by a Secure Sockets Layer (SSL) certificate. We use Transport Layer Security (TLS) to enable strong encryption for all data that is sent between the customer and server.

→ Encryption at rest

All databases and services on Google Cloud that handle PII are encrypted with externally managed encryption keys using Cloud EKM and Thales Key Broker. This is done to make it as difficult as possible for Google to be able to access the PII. For other, non-PII data, Google managed encryption keys are used.

→ User credential encryption

For all registered users, we enforce a password complexity standard (thanks to Dropbox) to safeguard our users accounts. Passwords and credentials are stored using a PBKDF2 function.

Data retention and disposal

Data retention allows us to anonymise data, safeguarding against data misuse and minimising internal exploitation risks. Our customers can set their own retention time for candidate test results. The default time is 24 months. If the customer chooses to, they can anonymise specific candidates on-demand.

Well tested access control to separate customer environments

Alva uses a multi-tenant environment with access control used to separate customer environments. This is tested annually by a third-party vendor through a security assessment. We consider the risk as low, as customers cannot execute any code nor any other configurations in our platform.

Our availability and Service-Level Agreements (SLAs)

All of our services are configured with automatic failovers, which means that our services will still function even if a data center should fail. Our services are classified and have assigned internal SLAs depending on what purpose they fill in our product. Primary user flows such as candidate job positions, create candidates and take tests guarantees 99.9 %, 24/7 availability, with Recovery Point Objective and Recovery Time Objective of 30 minutes. Scheduled maintenance is excluded, but should not exceed four hours per quarter. Current and planned maintenance is shown at Alva’s status page.