Codility Whitepapers

Overview of Codility security practice

Codility Limited, 107 Cheapside, London EC2V

Introduction

At Codility we believe trust is not only rooted in products that help find and unlock the potential of engineering talent, but also in how we manage information we collect on the way.

Being integrated with our clients' hiring processes we don't just learn of their hiring needs, but also of what strategic objectives the new hires will support. That's why we have introduced the strictest, globally acknowledged measures, processes and training to ensure all client information is safe with us.

Besides our clients we bear the trust of the thousands of candidates who complete tests on our platform. We never ask candidates to create an account with us, because we only collect their data to support the actual hiring process they take part in. This data is stored on segregated US and EU servers, and under no circumstances is shared with other companies looking for engineering hires, or recorded for future by any third party not involved in the actual hiring process.

We believe candidate privacy is a value all businesses in the hiring process should share.
That's why we never compromise when it comes to data protection.

In this document you will find the description of security practices supporting this spirit.

Compliance

Industry standards

Compliance with applicable regulations, standards and industry best practices protect us and our customers' sensitive information in ways that are testable and verifiable. The following security-related audits and certifications are applicable to Codility services:

- **Service Organization Control (SOC)**: Codility has undergone a SOC 2 audit, and a copy of the most recent report is available upon request.
- **General Data Protection Regulation (GDPR)**: Codility has introduced tools and processes to ensure our compliance with requirements imposed by the GDPR. Our Data Protection Impact Assessment (DPIA) report is available upon request
- **ISO 27001**: Codility has undergone ISO 27001 and has been certified as a company that is compliant with ISO 27001 standard. Copies of security policies and certification can be shared upon request.
- **CCPA**: Codility acknowledges and is compliant with the clauses of the CCPA.

Codility is hosted in Amazon Web Services (AWS) data centers, which are highly scalable, secure, and reliable. AWS complies with leading security policies and frameworks, including SSAE 16, SOC framework, ISO 27001 and PCI DSS. More information can be found at https://aws.amazon.com/compliance/.

Anti bribery

It is our policy to conduct all of our business in an honest and ethical manner. We take a zero-tolerance approach to bribery and corruption and are committed to acting professionally, fairly and with integrity in all our business dealings and relationships.

Copy of our policy can be shared upon request. We have implemented a set of controls for our employees, vendors and notice to clients about how Codility acts upon bribes.

People Security

All Codility employees are required to understand and follow internal policies and standards. Security training is mandated as part of the onboarding process. Topics covered include device security, acceptable use, preventing spyware/malware, physical security, data privacy, account management, and incident reporting, among others.

Codility is also performing regular phishing campaigns to check how our employees are responding to suspicious mails. Results of these campaigns are later shared with the whole company. Summary reports can be also shared upon request.

Codility employees are also using 1password manager for creating strong and unique passwords.

Physical Security

Currently Codility has a data center in North Virginia, USA and Frankfurt, DE.

Codility leverages Amazon Web Services (AWS) data centers for all production systems and customer data. AWS offers state-of-the-art physical protection for the servers and complies with an impressive array of standards. For more information on AWS Data Center Physical Security, see the AWS Security Whitepaper: https://aws.amazon.com/architecture/security-identity-compliance.

Besides the safety of our data center Codility also takes security measures when it comes to the safety of our offices.

Access to our offices is secured with cards, all buildings are secured with CCTV cameras and 24/7 security guard monitoring. All visitors must be written into the visitors log at the reception desk and also cannot be left unattended. Computers are kept in secured cabinets when unattended. Employees also must follow the Clear Desk Policy.

Data security

We know that in the digital era data security is one of the most important things in companies. Codility wants to ensure our customers that their data is safe and secure with us.

Data in transit

The access to our service as well as the user data are encrypted with TLS 1.2 (AES256). Codility is securing it's connection to the internet.

Data at rest

For better protection all the data is encrypted while at rest. Secured with OS-level encryption (AES 256). Also all of our employees' workstations are encrypted and can be securely wiped if necessary.

All of the workstation has also antivirus protection and antimalware. Both are managed centrally.

Secure logging

Securing logging is also part of data protection. In Codility users need to login using SSO provided to us via the JumpCloud portal.

In our application we are supporting integration with your authentication center via SAML.

Secure Software Development Life Cycle

Standard best-practices are used throughout our software development cycle from design to implementation, testing, and deployment. All code is checked into a permanent version-controlled repository. Code changes are always subject to peer review and continuous integration testing to screen for potential security issues. All changes released into production are logged and archived, and alerts are sent to the engineering team automatically. Access to Codility source code repositories requires strong credentials and two-factor authentication.

Testing

Codility is performing penetration testing once a year in search of vulnerabilities. Summary reports of those tests can be shared upon request.

Once a week we perform vulnerability scans using Qualys.

Our developers are also checking code using SonarQube.

Audit trails

All actions taken to make changes to the infrastructure or to access customer data for specific business needs are logged for auditing purposes. In order to protect end user privacy and security, only a small number of senior engineers on the infrastructure team have direct access to production servers and databases.

API

More information about APIs can be found here: API Documentation | Connect Your Recruitment Data

Data retention

Customer data is kept while the customer has an active contract, and for up to 90 days after a contract ends or is terminated. Application logs are kept while the customer has an active contract, and for up to 1 year after a contract ends or is terminated.

As Codility is defined as the Data Processor of Candidates' data the company is obliged to handle data in line with the instructions given by the Data Controller (the Customer). Codility expects to return and/or delete Candidate data at a time defined by the contract governing the provision of Codility's services to the customer. In some cases, personal data are anonymised for statistical analysis and research purposes.

Disaster recovery and business continuity

Codility customer data is regularly backed up each day to guard against data loss scenarios.

All backups are encrypted both in transit and at rest using strong industry encryption techniques. All backups are also geographically distributed to maintain redundancy in the event of a natural disaster or a location-specific failure.

Codility uses third-party monitoring services to track availability, with engineers on call to address any outages.

Codility is set up to operate from geographically distributed locations. By leveraging cloud resources, Codility infrastructure and customer support teams can support your business at any time.

Data Used in Codility

1. What type of data does Codility collect?

The personal data of Candidates processed by Codility are predominantly contact details and may include details relating to the candidates' education and current professional role. This data are either entered by the customer (ie. a recruiter) and/or by the Candidate directly. This information is provided to the customer (ie. a recruiter) by the Candidate.

Customers may specify that candidate data be anonymised. Data likely includes:

- First name
- Last name
- Email address

Data may also include (at the request of the customer):

- School attended
- Degree/Field
- Years of experience
- Profile URL (for example, their GitLab account, Linkedin profile)
- Phone number

The level of detail is configured by the customer (ie. account admin).
Only the email address is required for invites to be sent to Candidates.

2. Where does Codility store the collected data?

Data are stored on Amazon Web Services' US East region production servers (production database and its backups) and in Rackspace (other backups). When no longer required, all data is deleted from the production servers. Amazon Web Services implemented best in market standards for data center security and data handling.

A high quality of service is maintained by Amazon, this includes regular checks and annual audits.

For EU-based hosting, data is stored on Amazon Web Services EU Central 1 region, Frankfurt (production database and its backups). Please note, when data is no longer required, it is deleted from the production servers. Amazon Web Services implemented best in market standards for data center security and data handling. Codility makes sure that a high quality of service is maintained by Amazon, this includes regular checks and annual audits.

3. What is the purpose of collecting data by Codility?

This data are used for several of purposes including:

- Inviting Candidates to participate in tasks that assess their skills and competence in relevant areas such as coding and software development
- Inviting Candidates to online interviews with customers / recruiters
- Providing feedback to customers / recruiters on Candidates' performance in assessments and online interviews.

4. What is the source of the collected data?

Candidates provide their personal data themselves including their contact details directly, through Codility's platform, as part of their recruitment process. Candidates' personal data (contact information) are collected from Customers who have signed a contract of sale with Codility outlining Codility's Terms of Service.

5. Does Codility share data with any third parties?

Codility does not share Candidate data with any individuals or organisations external to Codility Limited and its subsidiaries for any purpose that involves further usage, manipulation or interpretation.

Data will be transferred to external platforms to facilitate Codility's service delivery. Codility ensures that all such transfers are lawful and are subject to adequate safeguards as defined by relevant global Data Protection laws.

Conclusion

We take security seriously at Codility Customers using our service expect their data to be secure and confidential. Safeguarding this data is a critical responsibility we have, and we work hard | to maintain that trust.

If after reading this whitepaper you have any further questions, please don't hesitate to contact our security team at security@codility.com.