CODILITY'S DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**this Agreement**") is made between you (the "**Customer**") and Codility Limited, a private limited company organised and existing under the laws of England and Wales and having its registered office at 107 Cheapside London, UK EC2V 6DN and having its subsidiaries Codility Polska sp. z.o.o, Codility US Inc and Codility Germany GmbH ("**Codility**"), each a "**Party**" and together the "**Parties**".

1. Definitions

In this Agreement the following defined terms shall have the meanings given below:

Applicable Law	means the following to the extent forming part of the law of United Kingdom (or a part of the United Kingdom) as applicable and binding on either party or the Services: a) any law, statute, regulation, byelaw or subordinate legislation in force from time to time; b) the common law and laws of equity as applicable to the parties from time to time; c) any binding court order, judgment or decree; or d) any applicable direction, policy, rule or order made or given by any regulatory body having jurisdiction over a party or any of that party's assets, resources or business;
CCPA	means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100, et seq. as amended by California Privacy Rights Act of 2020
Controller	has the meaning given to that term in Data Protection Laws
Data Protection Laws	means as applicable and binding on either party or the Services: a) the GDPR; b) the Data Protection Act 2018; c) the UK GDPR; d) the CCPA; e) any laws which implement or supplement any such laws; and f) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing.

Data Protection Losses	means all liabilities, including all: a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and b) to the extent permitted by Applicable Law: (i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Data Protection Supervisory Authority; (ii) compensation which is ordered by a court or Data Protection Supervisory Authority to be paid to a Data Subject; and the reasonable costs of compliance with investigations by a Data Protection Supervisory Authority;
Data Protection Supervisory Authority	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws
Data Subject	has the meaning given to that term in Data Protection Laws
Data Subject Request	means a request made by a Data Subject to exercise any rights of Data Subjects under Chapter III of the GDPR in relation to any Protected Data
EU Personal Data	means Personal Data to which the data protection legislation of the European Union, including the GPDR, applies.
GDPR	means the General Data Protection Regulation (Regulation (EU) 2016/679) on the protection of natural persons with regard to the processing of Personal Data and on the movement of such data, and repealing Directive 95/46/EC
Lawful Safeguards	means such legally enforceable mechanism(s) for Transfers of Personal Data as may be permitted under Data Protection Laws from time to time
List of Sub-Processors	means the latest version of the list of Sub-Processors used by Codility, as updated from time to time, the latest version is attached
Personal Data	has the meaning given to that term in Data Protection Laws

Personal Data Breach	means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data
processing	has the meaning given to that term in Data Protection Laws (and related terms such as **process**, **processes** and **processed** have corresponding meanings)
Processing End Date	means the earlier of: a) the end of the provision of the relevant Services related to processing of the Protected Data; or b) once processing by Codility of any Protected Data is no longer required for the purpose of Codility's performance of its relevant obligations under this Agreement
Processing Instructions	has the meaning given to that term in clause 3.1.1
Processor	has the meaning given to that term in Data Protection Laws
Protected Data	means Personal Data received from or on behalf of the Customer in connection with the performance of Codility's obligations under this Agreement
Standard Contractual Clauses	means: ● in respect of EU Personal Data, the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 (the "**EU Standard Contractual Clauses**"); and ● in respect of UK Personal Data, a version of EU Standard Contractual Clauses as amended by the UK Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner and laid before the Parliament of the United Kingdom in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022 (the "**UK Addendum**")
Sub-Processor	means a Processor engaged by Codility or by any other Sub-Processor for carrying out processing activities in respect of the Protected Data on behalf of the Customer

Third Country	means: • in respect of EU Personal Data, a country outside the EEA not recognised by the European Commission as providing an adequate level of protection for personal data; and • in respect of UK Personal Data, a country outside the UK that has not been deemed as providing an adequate level of protection for personal data under UK law.
Transfer	bears the same meaning as the word 'transfer' in Article 44 of the GDPR. Related expressions such as **Transfers**, **Transferred** and **Transferring** shall be construed accordingly
UK GDPR	has the meaning given to it in section 3(10) of the Data Protection Act 2018
UK Personal Data	means Personal Data to which the data protection legislation of the United Kingdom, including the Data Protection Act 2018, applies

2. **Processor and Controller**

2.1. The parties agree that, for the Protected Data, the Customer shall be the Controller and Codility shall be the Processor. Nothing in this Agreement relieves the Customer of any responsibilities or liabilities under any Data Protection Laws.

2.2. To the extent the Customer is not the sole Controller of any Protected Data it warrants that it has full authority and authorization of all relevant Controllers to instruct Codility to process the Protected Data in accordance with this Agreement.

2.3. Codility shall process Protected Data in compliance with:

2.3.1. the obligations of Processors under Data Protection Laws in respect of the performance of its obligations under this Agreement; and

2.3.2. the terms of this Agreement.

2.4. Codility shall ensure that:

2.4.1. the processing of all Protected Data complies in all respects with Data Protection Laws, including in terms of its collection, use and storage; and

2.4.2. it takes all reasonable steps to ensure that: (i) persons employed by Codility; and (ii) other persons engaged at Codility's place of business who may process Protected Data are aware of and comply with this Agreement.

2.5. The Customer shall ensure that it and each User shall at all times comply with:

2.5.1. the obligations of Controllers under Data Protection Laws in respect of the exercise and performance of its rights and obligations under this Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

2.5.2. the terms of this Agreement.

2.6. The Customer warrants, represents and undertakes, that, at all times:

2.6.1. the processing and transfer of all Protected Data shall comply in all respects with Data Protection Laws, including in terms of its collection, use and storage;

2.6.2. fair processing and all other appropriate notices have been provided to the Data Subjects of the Protected Data (and all necessary consents from such Data Subjects obtained and at all times maintained) to the extent required by Data Protection Laws in connection with all processing activities in respect of the Protected Data which may be undertaken by Codility and its Sub-Processors in accordance with this Agreement;

2.6.3. the Protected Data is accurate and up to date;

2.6.4. it shall maintain complete and accurate backups of all Protected Data provided to Codility (or anyone acting on Codility's behalf) so as to be able to immediately recover and reconstitute such Protected Data in the event of loss, damage or corruption of such Protected Data by Codility or any other person;

2.6.5. all instructions given by it to Codility in respect of Personal Data shall be at all times in accordance with Data Protection Laws; and

2.6.6. it will process only information that has been lawfully and validly collected and ensure that such information will be relevant and proportionate to the respective uses.

3. Instructions and Details of Processing

3.1. Insofar as Codility processes Protected Data on behalf of the Customer, Codility:

3.1.1. unless required to do otherwise by Applicable Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Customer's documented instructions as set out in this Agreement, as updated from time to time (**Processing Instructions**). The provisions of the Principal Agreement and this Agreement shall constitute the Customer's instructions to Codility with respect to Transfers of Protected Data;

3.1.2. where Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before processing the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest); and

3.1.3. shall promptly inform the Customer if Codility becomes aware of a Processing Instruction that, in Codility 's opinion, infringes Data Protection Laws, provided that:

3.1.3.1. this shall be without prejudice to clauses 2.5 and 2.6; and

3.1.3.2. to the maximum extent permitted by Applicable Law, Codility shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with the Processing Instructions following the Customer's receipt of the information required by this clause.

3.2. Subject to applicable Services or the Order Form the processing of the Protected Data by Codility under this Agreement shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in Schedule 2 to this Agreement.

4. Technical and Organisational Measures

Codility shall implement and maintain technical and organizational measures:

4.1. in relation to the processing of Protected Data by Codility, as set out in this Agreement; and

4.2. to assist the Customer insofar as is possible (taking into account the nature of the processing) in the fulfilment of the Customer's obligations to respond to Data Subject Requests relating to Protected Data. The parties have agreed that (taking into account the nature of the processing) Codility's compliance with clause 6.1 shall constitute Codility's sole obligations under this clause 4.2.

5. Sub-Processors

5.1. The Customer authorizes the appointment of:

5.1.1. each of the Sub-Processors identified on the List of Sub-Processors attached at Schedule 3 to this Agreement; and

5.1.2. provided Codility has met the requirements of clause 5.2 below, any new Sub-Processors which Codility may appoint in the future.

5.2. Codility must provide the Customer with at least 30 days' prior written notice of the appointment of any new Sub-processor, including full details of the Processing to be undertaken by the Sub-Processor. If the Customer objects to the appointment of a new Sub-Processor (or any change to any of the Sub-Processors) following receipt of such notice, Codility may terminate the Principal Agreement in accordance with the Termination provisions thereof.

5.3. With respect to each Sub-Processor, Codility shall:

5.3.1. prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, ensure the Sub-Processor is appointed under a written contract containing terms which offer at least the same level of protection for Personal Data as those set out in this Agreement and which meet the requirements of article 28(3) of the GDPR and/or the UK GDPR; and

5.3.2. ensure each new Sub-Processor identified on the List of Sub-Processors meets the following criteria at the time the addition of that Sub-Processor is first made: it has been

operating for at least two years, has not been sanctioned by any Data Protection Supervisory Authority in relation to any breach of any Data Protection Laws and by reference to pre-tax revenues in the most recent year has filed publicly available accounts.

5.4. Codility shall ensure that each Sub-Processor performs the obligations in accordance with this Agreement as if the Sub-Processor were a party hereto in place of the Processor. The Processor shall remain fully liable to the Customer for the performance of the Sub-Processor's obligations.

6. Assistance with Customer's Compliance and Data Subject rights

6.1. Codility shall refer all Data Subject Requests it receives to the Customer without undue delay and in any case within five (5) business days of receipt of the request.

6.2. Codility shall provide such assistance as the Customer reasonably requires (taking into account the nature of processing and the information available to Codility) to the Customer in ensuring compliance with the Customer's obligations under Data Protection Laws with respect to:

6.2.1. security of processing;

6.2.2. data protection impact assessments (as such term is defined in Data Protection Laws);

6.2.3. prior consultation with a Data Protection Supervisory Authority regarding high-risk processing; and

6.2.4. notifications to the Data Protection Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach.

7. International Transfers

7.1. The Customer acknowledges and agrees that Codility, and/or its Sub-Processors, may Transfer Protected Data in accordance with this Agreement and Applicable Law, to a country outside of the EEA and/or the UK. In such circumstances, Codility agrees that any such Transfers (including any onward transfer and to the extent required under Data Protection Laws) shall:

7.1.1. be effected by way of the Lawful Safeguards referred to in clause 7.2 below; and

7.1.2. be in accordance with Data Protection Laws and this Agreement.

7.2. The Lawful Safeguards employed by Codility in connection with Transfers pursuant to this clause 7 shall be as follows:

7.2.1. Transfers to a country approved by the European Commission or its UK equivalent as having an adequate level of protection for personal data; or

7.2.2. Codility's agreement to use the Standard Contractual Clauses in the manner set out in clause 8 below.

8. Standard Contractual Clauses

8.1. The parties agree that in the case of Transfers of Protected Data either (i) directly by Codility or (ii) by way of onward transfer permitted by Codility, to a Third Country, the Standard Contractual Clauses shall be incorporated by reference into this Agreement.

8.2. As the Customer acts as Controller and Codility acts as Processor, Module 2 of the Standard Contractual Clauses (*Controller-Processor*) shall apply, unless the parties agree that the circumstances are otherwise, in which case the parties will determine the appropriate Module of the Standard Contractual Clauses that is applicable.

8.3. Where applicable in each case, and unless otherwise agreed by the parties, with regards to the specific clauses of the Standard Contractual Clauses:

8.3.1. Optional Clause 7 (*Docking Clause*) shall apply.

8.3.2. Clause 9a (*Use of sub-processors*) – Option 2 (*GENERAL WRITTEN AUTHORISATION*) shall apply, and the time period to be given as notice for any change of Sub-Processor shall be as specified in clause 5 of this Agreement.

8.3.3. Clause 11 (*Redress*) – the optional text shall not apply.

8.3.4. Clause 17 (*Governing Law*) – Option 2 shall apply.

8.3.5. Clause 18 (*Choice of forum and jurisdiction*) – any disputes arising from the Standard Contractual Clauses shall be resolved by the courts of the country selected under Clause 17 as the jurisdiction of governing law.

8.3.6. Annex I(A)(*List of Parties*) – the Controller shall be the Data Exporter and the Processor (or its Sub-Processor, as the case may be) shall be the Data Importer, and the contact and other details of the Controller and Processor as shared or agreed between the parties shall be deemed the contact and other details of the Data Exporter and Data Importer.

8.3.7. Annex I(B)(*Description of Transfer*) – Schedule 1 to this Agreement shall be deemed to be Annex I(B) of the Standard Contractual Clauses.

8.3.8. Annex I(C) (*Competent Supervisory Authority*)– The competent supervisory authority in accordance with Clause 13 of the Standard Contractual Clauses shall be the competent supervisory authority in the jurisdiction in which the data exporter is established.

8.3.9. Annex II (*Technical and Organisational Measures*) – Schedule 2 to this Agreement shall be deemed to be Annex II of the Standard Contractual Clauses.

8.3.10. Annex III (*List of Sub-processors*) – Schedule 3 to this Agreement shall be deemed to be Annex III of the Standard Contractual Clauses.

8.4. The information contained in this Agreement and referenced in clauses 8.3.6-8.3.10 above shall be deemed to be Tables 1 and 3 of the UK Addendum (where applicable).

8.5. For the purpose of Table 2 of the UK Addendum, the version of the Approved EU SCCs to which the UK Addendum is appended shall be the EU Standard Contractual Clauses (as defined in this Agreement), with the options thereunder being as selected in this clause 8.

8.6. For the purposes of Table 4 of the UK Addendum, neither party shall have the right to end the UK Addendum when a revised version is issued by the ICO.

9. California Consumer Privacy Act

In the event that the Personal Data of residents of California, United States of America is collected, then the Parties agree that Exhibit I shall apply and shall form part of this Agreement.

10. Records, Information and Audit

10.1. Codility shall maintain, in accordance with Data Protection Laws binding on Codility, written records of all categories of processing activities carried out on behalf of the Customer.

10.2. Codility agrees, in accordance with Data Protection Laws, at the request of Customer, to submit to audits to ascertain and/or monitor Codility's compliance with this DPA, provided that:

10.2.1. the Customer shall bear the fees of any auditor and any work, time, costs and expenses incurred by Codility and/or any Sub-Processors in complying with this clause;

10.2.2. any audits shall be carried out:

10.2.2.1. no more than once in any 12-month period;

10.2.2.2. with reasonable notice of same provided to Codility;

10.2.2.3. during regular business hours and in a manner which is not disruptive to Codility's business (or the business of any Sub-Processors or customers of Codility or the Sub-Processors);

10.2.2.4. under a duty of strict confidentiality (save for any information which is required to be disclosed to a Data Protection Supervisory Authority or as otherwise required by Applicable Law); and

10.2.2.5. by the Customer and/or by a third party appointed by Customer and accepted by Codility.

10.3. The scope of any audit will be agreed in advance and shall not involve physical access to the servers on which the Protected Data is hosted. On request, Codility shall provide the Customer (or auditors mandated by the Customer) with a copy of the third-party certifications and audits to the extent made generally available to its customers. Such information shall be confidential to Codility and shall be Codility's confidential information and shall be treated in accordance with applicable terms.

11. Breach Notification

11.1. In respect of any Personal Data Breach, Codility shall, without undue delay (and in any event within 24 hours):

11.1.1. notify the Customer of the Personal Data Breach; and

11.1.2. provide the Customer with details of the Personal Data Breach.

12. Deletion of Protected Data and Copies

12.1. Subject to clause 12.2, Codility shall (and shall ensure that each of the Sub-Processors shall) delete the Protected Data (and all copies) within a reasonable time and in any event within 90 days of the Processing End Date, or such other period of time as may be agreed between the parties, except to the extent that storage of any such data is required by Applicable Law (and if so, Codility shall inform the Customer of any such requirement and shall (and shall ensure any relevant Sub-Processor shall) securely delete such data promptly once it is permitted to do so under Applicable Law.

12.2. Codility shall promptly comply with any reasonable requests from time to time from the Customer for the secure return or transfer of Protected Data to the Customer within a reasonable time provided:

12.2.1. such request is received within five (5) business days of the relevant Processing End Date; and

12.2.2. the Customer shall pay Codility for all work, time, costs and expenses incurred by Codility or any Sub-Processor(s) in connection with such activity.

12.3. Codility shall have no liability (howsoever arising, including in negligence) for any deletion or destruction of any such Protected Data undertaken in accordance with this Agreement.

13. Liability, Indemnities and Compensation Claims

13.1. The Customer shall indemnify and keep indemnified Codility in respect of all Data Protection Losses suffered or incurred by, awarded against, or agreed to be paid by, Codility and any Sub-Processor arising from or in connection with any:

13.1.1. non-compliance by the Customer with Data Protection Laws;

13.1.2. processing carried out by Codility or any Sub-Processor pursuant to any Processing Instruction that infringes any Data Protection Law; or

13.1.3. breach by the Customer of any of its obligations under this Agreement.

13.2. Codility shall be liable for Data Protection Losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with this Agreement:

13.2.1. only to the extent caused by the processing of Protected Data under this Agreement and directly resulting from Codility ’s breach of this Agreement; and

13.2.2. in no circumstances to the extent that any Data Protection Losses (or the circumstances giving rise to them) are contributed to or caused by any breach of this Agreement by the Customer (including in accordance with clause 3.1.3.2).

13.3. If a party receives a compensation claim from a person relating to processing of Protected Data, it shall promptly provide the other party with notice and full details of such claim.

13.4. The parties agree that the Customer shall not be entitled to claim back from Codility any part of any compensation paid by the Customer in respect of such damage to the extent that the Customer is liable to indemnify or otherwise compensate Codility in accordance with the wider contractual terms agreed between the parties.

13.5. This clause 13 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

13.5.1. to the extent not permitted by Applicable Law (including Data Protection Laws); and

13.5.2. that it does not affect the liability of either party to any Data Subject.

14. Survival

This Data Protection Agreement shall survive termination (for any reason) or expiry of the contractual relationship between the parties and continue until no Protected Data remains in the possession or control of Codility or any Sub-Processor, except that clauses 12 to 14 (inclusive) shall survive termination (for any reason) or expiry of this Agreement and continue indefinitely.

SCHEDULE 1

Data Processing Details

1. Subject-matter of the Processing of Personal Data:

The Protected Data may be subject to the following processing activities: providing Codility's Services, communicating with Customers and candidates, creating and sending candidate evaluation reports, providing technical support, and storing information for the duration of the Customer relationship.

2. Duration of the Processing of Personal Data:

Until the earlier of final termination or final expiry of the terms or agreement governing the contractual relationship between the parties, except as otherwise expressly stated in such terms or agreement;

3. Nature and purpose of the Processing of Personal Data:

The Protected Data transferred by Customer will be processed by Codility to provide the Services to Customer and Customer's individual employees, potential employees/candidates, contractors, or agents in accordance with the terms or agreement governing the contractual relationship between the parties and Customer may make Protected Data available to Codility in connection with this purpose;

The processing is in accordance with the rights and obligations of the parties under the terms or agreement governing the contractual relationship between the parties and the processing as reasonably required to provide the Services; and

The Processing as initiated, requested or instructed by Users in connection with their use of the Services, or by the Customer, in each case in a manner consistent with the terms or agreement governing the contractual relationship between the parties.

4. Types of Personal Data to be Processed:

Customer and/or Customer's individual employees, potential employees/candidates, contractors, or agents may submit Protected Data to Codility through the Services, which may include information relating the following types of data: contact information; titles, personal identifiers, such as first name, last name and email addresses, educational information, employer, ID data, and professional experience; and other identifiers such as IP address.

5. Categories of Data Subjects to whom Personal Data relates:

Users, employees, potential employees/candidates, contractors or agents of the Customer.

SCHEDULE 2

Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

1. **Confidentiality** (Article 32 sec. 1 lit. b) GDPR)

a. Physical Access Control: Codility ensures with proper measures that unauthorized persons do not get access to the Codility premises and data processing facilities (in particular phone systems, data bases, application servers and connected hardware) that are utilized for the processing of personal data. This must especially be ensured by:

Physical Access Control	**Implemented**
Codility premises are monitored 24/7 by security cameras at all entry points.	Yes
Codility premises are secured by an alarm system and security locks with electronic locking system (transponder keys).	Yes

Codility hands out transponder keys to authorized personnel only, keeps records of all transponder key holders and follows a strict return policy.	Yes
Codility limits access to facilities where personal data are stored, e.g. with password or key controlled access for authorized personnel.	Yes
Visitors to Codility premises must be accompanied by authorized personnel at all times.	Yes
Codility cleaning personnel is selected with care and diligence.	Yes

a. Electronic Access Control: Codility ensures that the IT systems utilized for the data processing allows authorized users only limited access, specified by their individual authorization rights. Codility must take adequate measures to ensure that personal data cannot be read, copied, modified or deleted in an unauthorized manner. This must especially be ensured by:

Electronic Access Control	**Implemented**
User accounts for Codility personnel are allocated to all IT systems. User accounts are solely accessible with an access user ID, consisting of username and password.	Yes
The password associated with an access user ID is the primary means of verifying identity and subsequently allowing access to Codility personnel's computer and to the information. Identity verification password is kept secret and not shared with anyone else.	Yes
Identity verification passwords must not be trivial or predictable and must: ● Be at least 8 positions in length ● Contain a mix of alphabetic and non-alphabetic characters (numbers, punctuation or special characters) or a mix of at least two types of non-alphabetic characters ● Not contain the access user ID as part of the password	Yes
A password protected keyboard / screen lock that is automatically activated by a period of inactivity is set.	Yes
The access rights of personnel to personal data is restricted to the necessary minimum required for their job functions.	Yes
Personal data may only be printed in physically secure areas controlled by Codility and only shared with personnel on a need to know basis.	N/A
Antivirus program is installed and run on the workstation.	Yes
Hardware firewall program is installed and run on the workstation.	Yes
Personnel with workstations using Microsoft Windows operating systems will install security patches for their respective version (but only the patches approved by CODILITY's infrastructure team).	Yes
Any media that contains personal data is securely stored at Codility's facilities.	N/A (no physical media)
In order to access Codility servers from outside of the premises, Codility has established VPN tunnels. VPN access requires an access user ID and associated VPN password, set up under the following requirements:	Yes

• Has a length of minimum 8 and maximum 32 characters / digits • Contains at least 1 uppercase and 1 lowercase character • Contains at least 1 digit • Is not identical with identity verification password	
Codility has established rules for the safe and permanent destruction of data that is no longer required.	Yes
Codility has established rules for the safe and permanent deletion and destruction of data from devices that are no longer in use.	Yes

b. Internal Access Control: Codility prevents with appropriate measures that the data processing systems cannot be used by unauthorized persons. This must especially be ensured by:

Internal Access Control	**Implemented**
Codility applies an authorization concept with need-based access rights and reduction of number of administrators to necessary ones (management of rights by system administrator). Codility has implemented measures to prevent unauthorized personnel from accessing data processing systems.	Yes
Codility ensures that access control is supported by an authentication system.	Yes

c. Separation Control: Codility ensures with applicable measures that data that was collected for different purposes will be processed separately. This must be ensured by:

Separation Control	**Implemented**
Codility has determined an authorization concept and rights management for databases.	Yes
Data records are provided with purpose attributes / data fields.	Yes
Codility has established a separation between test data and productive system.	Yes
Codility has established logical client separation in terms of software and databases.	Yes
Codility has introduced spatial and organisational separation of departments.	Yes
Codility's partners (including their affiliates) have access only to their own partner instance(s).	Yes

d. Pseudonymisation (Article 32 sec. 1 lit. a GDPR; Article 25 sec. 1 GDPR):

Pseudonymisation	**Implemented**

Codility has implemented a method that the data cannot be associated with a specific data subject without the assistance of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.	Yes

2. **Integrity** (Art. 32 sec. 1 lit. b GDPR)

a. Data Transfer Control: Codility ensures with applicable measures that during data transfer personal data cannot be unauthorized read, copied, modified or deleted. This must especially be ensured by:

Data Transmission Control	**Implemented**
VPN tunnels	Yes
Emails sent from Codility are encrypted.	Yes

a. Data Entry Control: Codility ensures with applicable measures, that it can reproduce who entered personal data in data processing systems or by whom personal data was deleted from data processing systems. Codility is only allowed to process personal data subject to the contract on behalf of its data controllers and according to contract with and/or further instructions of data controllers. This must especially be ensured by:

Data Entry Control	**Implemented**
Codility has implemented an authorization concept for data entry, modification and deletion.	Yes
Codility has established logging mechanisms that record data entry, modification and deletion.	Yes

b. Order Control: Codility ensures with applicable measures, that personal data processed on behalf of it can only be processed by the processor in accordance with the instructions of the controller. This must especially be ensured by:

Order Control	**Implemented**
Processors are selected carefully with respect to diligence and data security.	Yes
Security measures taken by the processor checked and documented prior to the collaboration.	Yes
Codility gives documented instructions to the processor and maintains ongoing monitoring of the processing activities.	Yes
Agreements ensure the effective control rights of Codility, the commitment of the processor and its employees to data secrecy and the destruction of data after completion of the collaboration.	Yes

3. **Availability and Resilience** (Art. 32 sec. 1 lit. b GDPR)

a. Availability Control and Rapid Recovery: Codility ensures with applicable measures that personal data cannot be unintentionally lost or destroyed and that personal data can be restored. This must be ensured by:

Availability Control	**Implemented**
Codility has business continuity plans.	Yes
Codility has implemented backup processes and other measures that ensure rapid restoration of business-critical systems as and when necessary.	Yes
Codility has an uninterrupted power supply to ensure power availability to the data centres.	Yes
Codility has sufficient capacity for data storage.	Yes
Codility has a disaster recovery plan in place.	Yes
Codility facilities and server rooms are equipped with smoke detectors and fire alarm systems.	Yes
Codility server rooms are equipped with temperature and humidity monitoring, air conditioning and protective socket strips.	Yes

4. **Procedures for regular testing, assessment and evaluation** (Art. 32 sec. 1 lit. d and 25 sec. 1 GDPR)

a. Data Protection and Incident Response Management

Management, Testing, Assessment and Evaluation	**Implemented**
Codility personnel with access to personal data are subject to confidentiality obligations.	Yes
Codility regularly audits its data protection implementation and documents.	Yes
Codility provides security guidelines ensuring its personnel are informed of security policies, procedures, and their respective roles.	Yes
Codility informs personnel of the possible consequences resulting from not following security policies and procedures.	Yes
Codility maintains a record of security incidents with a description of the incident, the time period, the consequences, the name of the reporter or service, to whom the incident was reported, and the remediation, in the event of a security incident.	Yes

a. Privacy by Design and Default

Privacy by Design and Default	Implemented
The software, service, product, application or comparable means used for the processing of personal data is designed and / or developed in accordance with the principles of privacy by design and privacy by default under GDPR (e.g. implementation to the extent applicable of pseudonymising, encrypting, minimising personal data processing as a default setting or/and defining the period).	Yes

SCHEDULE 3

Codility List of Sub-Processors 2022

The table below lists the sub-processors Codility uses with the service the sub-processor provides, the data type, the country or location of the destination of the transfer and the measures in place to ensure compliance with the GDPR. Further information regarding the security measures put in place by Codility's processors and sub-processors can be viewed at the relevant corporate websites.

Sub-Processor	Use Case	Data Type	Location	Measures	Notes

Miro	Whiteboard		US	Binding Contract, Data Processing Agreement, Standard Clauses,	GDPR compliance
Elastic	Logs Storage	Anonymous	US	Binding Contract, Data Processing Agreement, Standard Clauses,	
Hotjar	Usage analytics	Anonymous	EU	Binding Contract, Data Processing Agreement, Standard Clauses,	ISO 27001 certified
Satismeter	Customer feedback	Anonymous	EU		Registered In the Czech Republic
Typeform	Candidate feedback	Personal	EU		Registered In Barcelona, Spain
Amazon (AWS)	Database and back-ups	Personal	US	Binding Contract, Data Processing Agreement, Standard Clauses,	ISO 27001 certified
Rackspace	Back-ups	Anonymous	US		
Sendgrid	E-mails	Personal	US		Acquired by Twilio (below)
Google Analytics	Usage analytics	Anonymous	US		ISO 27001 certified
Mixpanel	Usage analytics	Anonymous	US		US & EU offices
Twilio	Video conferencing	Personal	US		ISO 27001 certified
Mailchimp	Newsletters	Personal	US		SOC II Compliant
Salesforce	Customer Relationship Management	Personal	EU & US		ISO 27001/17/18 certified, SOC Compliant
SalesLoft	Sales Management	Personal	US		ISO 27001/17/18 certified, SOC II Compliant
Zendesk	Customer Service Software	Personal	US		ISO 27001 certified, SOC II compliant

ChurnZero	Sales Management	Personal	US		SOC II Compliant

EXHIBIT I

California Consumer Privacy Act

Codility's Processing of Personal Information will be governed by the Agreement, which may set out certain terms regarding the subject matter, duration, nature, and purpose of the Processing, type of Personal Information and categories of Data Subjects, instructions for Processing Personal Information, and obligations and rights of the Parties. To the extent there is a conflict between this Exhibit and the Agreement, this Exhibit will prevail.

1. Representations, Warranties, and Covenants.

1.1. Codility's use, Collection, disclosure, storage, or Processing of Personal Information will be governed by the terms of this Exhibit. Capitalized terms not defined in the Agreement or this Exhibit have the meaning given in the California Consumer Protection Act, the California Privacy Rights Act (Cal. Civ. Code §§ 1798.100 – 1798.199), the Colorado Privacy Act (Colo. Rev. Stat. §§ 6-1-1301 – 6-1-1313), the Utah Consumer Privacy Act (Utah Code Ann. §§ 13-61-101–404), the Virginia Consumer Data Protection Act (Va. Code Ann. §§ 59.1-575 – 59.1-585), any implementing regulations thereof or modifications thereto, and any comparable legislation in any other states (collectively, the "**US Data Protection Laws**").

1.2. Where definitions of such terms vary between such statutes, the most comprehensive and restrictive definition will apply herein. As used herein, "**Personal Information**" means personal information, personal data, sensitive personal information, and sensitive data, collectively, as those terms are defined by the US Data Protection Laws.

1.3. Codility represents, warrants, and covenants that it will:

1.3.1. Process Personal Information received or Collected from or on behalf of Customer solely to provide the Service, including any Order Form, and only in compliance with the US Data Protection Laws. For the avoidance of doubt, the provision of Personal Information by Customer is not a Sale or Share of such Personal Information to Codility;

1.3.2. not otherwise Sell, Share, retain, use, or disclose Personal Information received or Collected from or on behalf of Customer, except:

1.3.2.1. to engage a subcontractor in compliance with Section 1.7 of this Exhibit;

1.3.2.2. for internal use in improving the quality of Codility's Service, provided that such use does not include:

1.3.2.2.1. building or modifying household or consumer profiles;

1.3.2.2.2. cleaning/augmenting data acquired from another source; or

1.3.2.2.3. creating de-identified or anonymized data, and

1.3.2.3. as otherwise permitted by the US Data Protection Laws.

1.3.3. assist Customer in complying with Consumer requests under the Data Protection Laws, including by deleting, correcting, providing access to, or stopping the Sale, Sharing, or other disclosure/use of Personal Information. Codility will notify Customer within 48 hours of its receipt of a Consumer request and will comply with Customer's direction regarding whether and how to respond thereto;

1.3.4. provide information to Customer as necessary to enable Customer to conduct and document data protection impact assessments required by Data Protection Law;

1.3.5. return or delete any Personal Information upon Customer's request, unless retention is required by law;

1.3.6. ensure that each person, including employees and subcontractors Processing Personal Information subject to the Agreement, is subject to a duty of confidentiality with respect to such Personal Information;

1.3.7. not disclose Personal Information to or engage subcontractors (including affiliates) to Process Personal Information without prior written approval of Customer. If authorized by Customer to engage a subcontractor, Codility will ensure that the subcontractor agrees in writing to:

1.3.7.1. comply with this Exhibit and the US Data Protection Laws;

1.3.7.2. be trained to handle Personal Information; and

1.3.7.3. comply with applicable Customer policies and procedures.

Codility will be responsible for subcontractor's noncompliance therewith, which will constitute a breach as if committed by Codility. Codility will indemnify Customer for all losses resulting therefrom, and

1.3.8. implement and maintain reasonable security procedures and practices appropriate to the nature of the Personal Information processed under this Agreement and required by the US Data Protection Laws, including all applicable requirements described in the most recent version of the Center for Internet Security Controls. Codility agrees that Customer may take reasonable and appropriate steps as it, in its sole discretion, deems warranted to stop and remediate unauthorized use of Personal Information.

2. Notification.

If Codility becomes aware of a breach or potential breach of security, or any unauthorized access, use, or disclosure, or loss of any Personal Information (a "**Data Incident**"), Codility will promptly, at its expense:

2.1. notify Customer;

2.2. investigate the breach or potential breach;

2.3. take reasonable steps to mitigate the effects thereof; and

2.4. perform any post-incident assessments as required by Customer.

3. Audit Rights.

3.1. Customer, or any agency, representative, or third party working on its behalf, will have the right to audit Codility during normal business hours and on reasonable notice to monitor compliance with this Exhibit.

3.2. Codility agrees to make available to Customer all information necessary to demonstrate its compliance with this Exhibit and with the US Data Protection Laws.

3.3. Each Party will bear their own expenses in relation to such audit.

4. Indemnification

In the event of a Data Incident, Codility will defend and indemnify Customer for:

4.1. the costs of remedying any Data Incident caused by Codility, or on Codility's network, including costs to provide notices and credit services required by applicable law to third parties, and all associated support to such third parties (e.g., call center support);

4.2. any claims, fines, penalties, fees or other charges imposed upon or assessed against Customer by a governmental authority, arising out of an alleged violation of applicable law; and

4.3. any third party claims for damages (including attorneys' fees) or penalties (including payment card brand fines) arising out of an alleged violation of applicable law or contract.

5. **Certification**

5.1. Codility certifies that it understands and will comply with the restrictions and obligations in this Exhibit.

5.2. Codility agrees that it will promptly inform Customer if it makes a determination that it or its subcontractors can no longer meet their obligations under this Exhibit or under the US Data Protection Laws.

5.3. This Section 5 will survive the termination of the Agreement.