Data Privacy Impact Assessment

Description of Coderbyte:

Coderbyte Enterprise Inc. (‘Coderbyte’) was founded in June 2012 with the objective of enabling organizations to evaluate candidates. Coderbyte has created a technical assessment and interviewing Software as a Service (SaaS) platform that services 2,000+ customers.

Disclaimer:

Supervisory Authorities will be notified If the results of the data protection impact assessment (DPIA) result in a high risk in the absence of measures taken by the controller to mitigate the risk. The relevant supervisory authorities will be contacted through the respective agencies. Notifying these authorities is the responsibility of the CEO, Daniel Borowski.

DPIA Explained:

The GDPR requires controllers to implement appropriate measures to ensure and be able to demonstrate compliance with the GDPR, taking into account among others the “the risks of varying likelihood and severity for the rights and freedoms of natural persons” (article 24 (1)). The obligation for controllers to conduct a DPIA in certain circumstances should be understood against the background of their general obligation to appropriately manage risks presented by the processing of personal data.

A “risk” is a scenario describing an event and its consequences, estimated in terms of severity and likelihood. “Risk management”, on the other hand, can be defined as the coordinated activities to direct and control an organization with regard to risk.

Article 35 refers to a likely high risk “to the rights and freedoms of individuals”. As indicated in the Article 29 Data Protection Working Party Statement on the role of a risk-based approach in data protection legal frameworks, the reference to “the rights and freedoms” of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. Instead, a DPIA is only required where a type of processing is “likely to result in a high risk to the rights and freedoms of natural persons” (Article 35(1)). The mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish controllers’ general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects. In practice, this means that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is “likely to result in a high risk to the rights and freedoms of natural persons”.

A single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks. Indeed, DPIAs aim at systematically studying new situations that could lead to high risks on the rights and freedoms of natural persons, and there is no need to carry out a DPIA in cases (i.e. processing operations performed in a specific context and for a specific purpose) that have already been studied. This might be the case where similar technology is used to collect the same sort of data for the same purposes. For example, a group of municipal authorities that are each setting up a similar CCTV system could carry out a single DPIA covering the processing by these separate controllers, or a railway operator (single controller) could cover video surveillance in all its train stations with one DPIA. This may also be applicable to similar processing operations implemented by various data controllers. In those cases, a reference DPIA should be shared or made publicly accessible, measures described in the DPIA must be implemented, and a justification for conducting a single DPIA has to be provided.

When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights and freedoms of the data subjects. Each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities.

Contents

1. DPIA setup and changelog
2. About the processing activity in scope
3. Data necessity, proportionality and transparency
   3.1 Lawfulness, Fairness and Transparency
   3.2 Purpose Limitation
   3.3 Data Accuracy and Data Minimization
   3.4 Accountability
   3.5 Data Subject Rights
4. Data Protection Risk Identification, Assessment and Mitigation

1. DPIA setup and changelog

This section provides introductory information about the DPIA being conducted, including high level descriptions of the processing activity, key dates, and stakeholders involved.

Title	Description
1.1 Project Title	Coderbyte DPIA
1.2 DPIA prepared by and person responsible for upkeep of this DPIA (indicate if they are separate)	Daniel Borowski, CEO
1.3 Date of review of this DPIA	June 16, 2025
1.3a Date of next review of this DPIA	June 16, 2026
1.4 DPIA change log (dates of changes made to this DPIA and	June 16, 2025 - Initial Document Creation

summary of key changes)	
1.5 Data Controllership: ☑ Customer is Controller ❏ Customer is a joint controller ❏ Customer is Processor ❏ Not yet known	**Service 1 Description:** Description: This is a service offered by Coderbyte where customers such as employers deploy evaluation services to their employees and job candidates. In this case the Controller is the Employer & the Processor is Coderbyte. **Service 2 Description:** Description: This is a service offered by Coderbyte where the general public can receive services with no involvement from their employer. In this case the Controller is Coderbyte. ***For the purpose of this DPIA exercise, we are focused on the service side of the business. As such,*** Coderbyte ***is the Data Controller in all cases.***
1.6 Third parties responsible for processing personal data	AWS
1.7 Is this a 'Mandatory' or 'Good Practice' DPIA	This is a 'Good Practice' DPIA as Coderbyte's data processing is not likely to result in a high risk to the rights and freedoms of individuals.
1.10 External reference materials relied upon (version or publication date if applicable)	Coderbyte Privacy Policy - https://coderbyte.com/privacy-org Coderbyte Terms of Service - https://coderbyte.com/terms-org and https://coderbyte.com/terms-ai

2. About the processing activity in scope

Title	Description
2.1 Provide a description of what the data processing is intended to accomplish (i.e., the primary purposes for which the data are collected and used). Generally, this can be a high-level description of the services. This can **briefly** describe the service, the data subjects whose personal data is processed as well as the purpose/value derived from the processing system. Put simply, why does this exist?	Coderbyte Enterprise Inc. (“Coderbyte”) provides a Software as a Service (SaaS) platform designed to help organizations make informed hiring and workforce decisions for technical roles, particularly in software development and engineering. The primary purpose of data processing is to support and enhance the recruitment and upskilling process through features such as auto-graded technical assessments, interview tools, performance analytics, and fraud detection. The platform processes personal data from job applicants (data subjects) on behalf of clients who use the service to evaluate technical aptitude and suitability for specific roles. Data processing enables core functionalities such as account management, personalized service delivery, reporting, support, and system security. Additionally, Coderbyte uses analytics and research to improve the platform’s performance and user experience. In summary, the processing exists to provide secure, efficient, and data-driven evaluation tools that enable organizations across industries to identify qualified technical talent while ensuring fairness, compliance, and continuous service improvement.

2.2 Explain and provide a narrative overview of the personal data processing in detail and highlight any steps that are high risk. ❏ sourced ❏ processed ❏ stored ❏ shared ❏ deleted This needs to contain sufficient detail to understand what and how the personal data will be processed and by whom. The narrative should allow a reader, such as a regulator, to understand how the data flows.	Below is a description of how Coderbyte Data is processed including how data is sourced, processed, stored, shared, and deleted. **Sourced** - Coderbyte data is sourced directly from customers which they provide for Coderbyte to assist them in evaluating employees and candidates. **Processed:** Coderbyte processes customer requests. The application also processes PII information needed for conducting evaluation services. **Stored:** Data is stored within the secured databases of AWS. **Shared**: Coderbyte may use aggregated, de-identified or anonymized data and share it with third parties for our lawful business purposes, including to analyze, build and improve the Services and promote our business. **Deleted:** Data is deleted upon a customer's request or after the relevant record retention period has passed.
2.3 List personal data being processed.	**Coderbyte Customer Data** **Customer Data Collected** ➢ First and last name ➢ Email ➢ Unique identifiers such as passwords ➢ Payment card type ➢ Last 4 digits of payment card ➢ IP address ➢ Type of device/operating system/browser used to access the Services ➢ Web page interactions ➢ Referring webpage/source through which you accessed the Services ➢ Non-identifiable request IDs ➢ Statistics associated with the interaction between device or browser and the Services ➢ IP-address-based location information ➢ Identifying information in emails, letters, texts, or other communication you send us

2.4 Approximate number of individual data subjects whose personal data is envisaged to be processed	There are approximately 2,000 customers in Coderbyte's system.
2.6 What categories of data subjects are impacted and exist by the data processing/whose personal data is being processed, what is the nature of your relationship with the individuals? Examples: employee; contractor; supplier; member of employee's household; member of public; children or other vulnerable groups	Coderbyte Data Subjects who are customers of the Coderbyte Service are classified as follows: - **Customers:** Any persons using Coderbyte as a provider for its services or candidate being evaluated by a Coderbyte customer. **Note 1:** Coderbyte does not classify customers based on their racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences that might warrant special thought and consideration. **Note 2:** Coderbyte also does not collect data for anyone under the age of 16.

3. Data necessity, proportionality and transparency

3.1 Lawfulness, Fairness and Transparency

Title	Description
3.1.1 What is the lawful basis for this processing?	Coderbyte's processing is considered lawful based on the following grounds: - Data subjects have given consent when they sign up for Coderbyte's services - The processing of customer data is necessary for the performance of a contract with the data subject or client organization, as the functionality of Coderbyte's platform—such as delivering technical assessments, managing candidate interactions, and generating analytics—relies on the collection and use of such data to fulfill its core service obligations.
3.1.2 Are there other less privacy impacting ways to achieve the same outcome?	Coderbyte collects the least amount of information possible to make evaluation services available, and even offers a method for Customers to evaluate candidates without providing any PII.
3.1.3 What information or privacy impacting notices are provided to data subjects in relation to the processing?	Coderbyte provides notice to Data Subject through the following means: 1. When signing up for Coderbyte's services, all users are presented with the Terms, Privacy Policy, and DPA. 2. When invited to an evaluation, Customer's employees and job candidates are presented with the Terms and DPA that the Customer has agreed to. Customer can also add their own additional consent language.
3.1.4 If processing is based on consent,how is this obtained / withdrawn?	As stated above in Section 3.1.3, Coderbyte collects consents when users sign-up for the web application. If a user wanted to withdraw consent, they would need to initiate the data deletion process which is outlined in section **3.5** below. To do so, they would need to contact our user support email address: support@coderbyte.com and request for their information to be deleted.

3.2 Purpose Limitation

Title	Description
3.2 What controls are in place to prevent personal data being used for another purpose incompatible with the primary purpose of collection or those falling under the lawful basis for collection and processing?	Coderbyte has implemented the following controls to prevent data from being used for reasons other than the primary rationale: **Identity & Access Management:** Coderbyte has designed RBAC controls in the application and supporting infrastructure which implements the principle of least privilege and prevents employees from being able to access data that is not relevant to the primary purpose. **Network Security:** Coderbyte's network infrastructure is protected by firewalls and backend infrastructure. In addition, Coderbyte has threat management tools which monitor the network for irregular traffic. **Mobile Device Management:** Devices used by employees are managed through a GRC tool with MDM capabilities. These devices are encrypted and required to follow good security practices such as screen lock and auto updates. In addition, mobile devices have Anti-Virus installed and are updated regularly to help the organization detect new threats. **AI Features:** Coderbyte relies on existing sub-processors for AI-powered capabilities, and neither stores prompts nor allows aforementioned sub-processors to train on Customer data. PII is not transmitted via prompts to AI models.

3.3 Data Accuracy and Data Minimization

Title	Description
3.3 What controls are in place to ensure (i) data quality and (ii) data minimization?	Coderbyte will only accept the minimum number of data fields required for Coderbyte to perform required activities. In addition, data types collected are also limited. This is done by limiting the number of required fields and not asking for more information than necessary. Data quality is maintained as customers have the ability to change their own data quality.

	With regard to AI-powered capabilities, Coderbyte uses the latest models available from sub-processors and allows Customers to bring their own API key instead. Customers must agree to amended terms and manually enable individual features. Users are reminded to manually verify outputs from AI models.

3.4 Accountability

Accountable Person	Accountability for the Data Privacy Program is assigned to the CEO. Daniel Borowski is Coderbyte's CEO and is responsible for all privacy practices. He is responsible for ensuring controls related to GDPR are in place. Coderbyte does not need a Data Protection Officer under the UK GDPR because it is not a public authority or body, it does not require regular and systemic monitoring of individuals on a large scale, and it does not process "special categories" or personal data or criminal convictions/offenses data.
3.4 What measures do you have in place to demonstrate compliance with the GDPR principles	Broad measures undertaken by Coderbyte in relation to compliance with the GDPR are set out below, including Coderbyte's 5 privacy principles as listed below: ● Control: We will put you in control of your privacy with easy-to-use tools and clear choices. ● Transparency: We will be transparent about data collection and use so that you can make informed decisions. ● Security: We will protect the data that you entrust to us via strong security and encryption. ● Strong legal protections: We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right. ● Benefits to you: When we do collect data, we will use it to benefit you and to make your experiences better. To demonstrate compliance with the principles listed above, Coderbyte has the following measures in place: **Policies and procedures**: Coderbyte has documented policies and procedures that outline how personal data is collected, processed, stored, and protected. These policies and procedures are reviewed and updated regularly to

	ensure they align with the GDPR principles. **Data protection impact assessments (DPIAs):** Coderbyte conducts DPIAs to assess the privacy risks associated with the processing of personal data, and to identify and mitigate potential privacy risks. This includes assessing the necessity and proportionality of the data processing, as well as identifying any additional privacy risks that may arise due to the use of new technology or changes to the processing Activities. **Training and awareness**: Coderbyte provides regular training and awareness programs to employees to ensure they are aware of their Information Security responsibilities and the importance of protecting personal data. This can include training on security measures such as encryption and access controls. **Privacy notices**: Coderbyte provides privacy notices to data subjects, outlining how their personal data will be collected, used, and protected. These privacy notices are clear and concise and include information on the lawful basis for processing personal data and the categories of personal data being processed. **Data subject rights**: Coderbyte provides data subjects with the right to access, restrict, file a complaint, correct, and delete their personal data, as well as the right to object to the processing of their personal data. Coderbyte has procedures in place to ensure that data subject rights are respected and responded to in a in a timely manner.
What organizational measures (such as training) have you implemented?	Coderbyte employees receive Security Awareness training which emphasizes the importance of least privilege and employees responsibility to properly manage customer data.

3.5 Data Subject Rights

Title	Description

3.5 How will the rights of the data subjects impacted by this be supported?	Coderbyte supports the rights of data subjects and has created defined procedures in the event a data subject chooses to exercise their rights. Refer to the links below for detailed procedures of what would be done in each instance: - **Access:** You can request more information about the Personal Data we hold about you and request a copy of such Personal Data. You can also access certain of your Personal Data by logging on to your account. - **Rectification**: If you believe that any Personal Data we are holding about you is incorrect or incomplete, you can request that we correct or supplement such data. You can also correct some of this information directly by logging on to your account. - **Erasure**: You can request that we erase some or all of your Personal Data from our systems. - **Withdrawal of Consent**: If we are processing your Personal Data based on your consent (as indicated at the time of collection of such data), you have the right to withdraw your consent at any time. Please note, however, that if you exercise this right, you may have to then provide express consent on a case-by-case basis for the use or disclosure of certain of your Personal Data, if such use or disclosure is necessary to enable you to utilize some or all of our Services. - **Portability:** You can ask for a copy of your Personal Data in a machine-readable format. You can also request that we transmit the data to another controller where technically feasible. - **Objection**: You can contact us to let us know that you object to the further use or disclosure of your Personal Data for certain purposes, such as for direct marketing purposes. - **Restriction of Processing:** You can ask us to restrict further processing of your Personal Data. - **Right to File Complaint**: You have the right to lodge a complaint about Coderbyte's practices with respect to your Personal Data with the supervisory authority of your country or EU Member State. A list of Supervisory Authorities is available here:https://edpb.europa.eu/about-edpb/board/members_en.

4. Risk Assessment & Mitigating Factors

Coderbyte management has performed a risk assessment over the rights and freedoms of data subjects and also identified mitigating factors to address those risks. Results from the Risk Assessment can be found here: https://docs.google.com/spreadsheets/d/1ALi0l7qlPzYlXXqQ-ICIsH6mWGl0I-AT/edit#gid=338661081.