Codigo – Privacy Policy

Last updated: April 1st 2025

Codigo, Inc., a Delaware corporation and its affiliates ("**Codigo**," "**we**," "**our**," and/or "**us**") value the privacy of individuals who use our website and related services (collectively, our "**Services**"). This privacy policy (the "**Privacy Policy**") explains how we collect, use, and share information from or about you or your device as you use the Services. By using our Services, you agree to the collection, use, disclosure, and procedures this Privacy Policy describes. If you are an entity customer located in the European Economic Area ("**EEA**"), Switzerland or the United Kingdom, you also agree to be bound by the Data Processing Agreement ("**DPA**") as provided below. Beyond the Privacy Policy, your use of our Services is also subject to our Terms of Service.

1 Information We Collect

We may collect a variety of information from or about you or your devices from various sources, as described below.

If you do not provide your information when requested, you may not be able to use some or all of our Services if that information is necessary to provide you with our Services or if we are legally required to collect it.

1.1 Information You Provide to Us.

Registration and Profile Information. When you register for an account, we ask you for your email address and may also request your phone number. If you sign up using a social media account, we will also receive information from those social media services such as your name, email address, and profile photo, in accordance with your privacy settings on those social media services.

Payment Information. When you add a credit card or payment method to your account a third-party service provider that handles payments on our behalf will receive and process your payment card information.

Communications. When you communicate with us, we may receive additional information about you. For example, when you communicate with our Customer Support Team, we will receive your name, email address, phone number, the contents of a message or attachments that you may send to us, and other information you choose to provide. If you subscribe to our newsletter, then we will collect certain information from you, such as your email address. When we send you emails, we may use technologies such as web beacons to track whether you open them to learn how to deliver a better customer experience and improve our Services.

Careers. If you apply for a job with us, you may submit your contact information and your resume online. We will collect the information you choose to provide on your resume, such as your education and employment experience. For job applicants who reside in California, these supplementary conditions apply.

1.2 Information We Collect Automatically When You Use Our Services.

When you use the Services, we use a variety of electronic tools, such as cookies, pixel tags, and similar technologies (collectively referred to in this Privacy Policy as "**cookies**") to automatically generate information about how you use and interact with the Services as discussed in this section.

What are Cookies? Cookies are small files of letters and numbers that we store on your browser or the hard drive of your computer, or small graphic images placed on web pages or in emails. They can be stored either for a single browser session or more permanently. We use cookies to collect information about your browsing activities, distinguish you from other users, provide functionality, and analyze use of the Services. Our third-party partners, such as analytics and advertising partners, may use these technologies to collect information about your online activities over time and across different services. The types of cookies we and third parties may use to collect information are as follows:

- Strictly necessary cookies. Some cookies are strictly necessary to make the Services available to you. We cannot provide you with the Services without this type of cookies.
- Functional cookies. These are used to recognize you when you return to the Services. This enables us to adapt our content for you, and remember your preferences (for example, your choice of language or region).
- Analytical or Performance cookies. We also use cookies for analytics purposes in order to operate, maintain and improve our Services. We may use our own analytics cookies or use third party analytics providers such as Google Analytics to collect and process certain analytics data on our behalf. These providers may also collect information about your use of other websites, apps, and online resources. You can opt out of Google Analytics by installing Google's browser plug-in.

You can find more information about your rights and choices, and how to block the use of certain cookies in the section Your Rights and Choices below.

What information do we automatically collect as you use the Services?

Device Information. We receive information about the device and software you use to access our Services, including internet protocol (IP) address, Internet Service Provider, web browser type, operating system version, phone carrier and manufacturer, application installations, device type and identifiers, and mobile advertising identifiers.

Location Information. We may infer your general location information from other information we collect from and about you (for example, your IP address may indicate your general geographic region). We do not collect precise geolocation data.

Usage Information. To help us understand and analyze how you use our Services and to help us improve them, we automatically receive information about your interactions with our Services, like the pages or other content you view or interact with, the searches you conduct, your

comments, any content you enter or post, commands you type, and the dates and times of your visits.

1.3 Information We Receive from Third Parties.

Information from third party services. If you choose to link our Services to a third-party account, we may receive information about you, including your profile information and your photo, and your use of the third-party account, in accordance with your settings on such third-party account. If you wish to limit the information available to us, you should visit the privacy settings of your third-party accounts to learn about your options.

Other third parties. We may receive additional information about you, such as demographic data, from third parties such as data or marketing partners and combine it with other information we have about you.

2 How We Use The Information We Collect

We use the information we collect:

- To provide, maintain, improve, and enhance our Services;
- To communicate with you, provide you with updates and other information relating to our Services, provide information that you request, respond to comments and questions, and otherwise provide customer support;
- To facilitate the connection of third-party services or applications, such as social networks;
- For marketing purposes, such as developing and providing promotional and advertising materials that may be useful, relevant, valuable or otherwise of interest to you;
- To personalize your experience on our Services such as presenting tailored content;
- To facilitate transactions and payments;
- To detect and prevent fraud, and respond to trust and safety issues that may arise;
- For compliance purposes, including enforcing our Terms of Service or other legal rights, or as may be required by applicable laws and regulations or requested by any judicial process or governmental agency; and
- For other purposes for which we provide specific notice at the time the information is collected.

De-Identified Information. Please note that we may de-identify the information we collect from and about you so that it can no longer be reasonably linked to you or your device. Once information has been de-identified in this way, we can use and share it for any purpose at our discretion, and this Privacy Policy no longer applies to such information.

3 Your Privacy Obligations

Codigo provides you with the ability to publish content that could be used to collect personally identifiable information from its users. If you publish such content, it is your responsibility to understand your legal obligations and to comply with all applicable laws, including:

- Providing your users with appropriate notices of their privacy rights, which should incorporate this Privacy Policy by reference.
- Obtaining any necessary consent from your users for the processing, storage, use, and transfer of any of their personally identifiable information that you collect.
- If applicable, providing any required notices and obtaining any required verifiable parental consent under the Children's Online Privacy Protection Act (COPPA) or similar laws.
- Complying with your legal obligations to allow your users to correct their personally identifiable information or to have it erased.

4 Legal Bases For Processing Information

Various global privacy laws (such as those in the European Economic Area, United Kingdom, and Brazil) require that we have a "legal basis" to process your information. The legal bases on which we rely to process your information include:

- Consent. You have consented to the use of your information, for example, where legally required, to send you marketing communications.
- Contractual necessity. We need your information to provide you with the Services, for example to facilitate your registration and respond to your inquiries.
- Compliance with a legal obligation. We have a legal obligation to use your information, for example to comply with tax and accounting obligations.
- Legitimate interests. We have a legitimate interest in using your information for a business purpose that does not override your individual rights and interests. For example, we have a legitimate interest in using your information for product development and internal analytics purposes, to improve the accuracy of our machine learning technologies such as code generation, and otherwise to improve the safety, security, and performance of our Services.

4.1 How We Share the Information We Collect

We share information with the following categories of third parties.

Affiliates. We may share any information we receive with our corporate affiliates under common ownership or control for any of the purposes described in this Privacy Policy.

Service Providers. We may share any information we receive with vendors retained in connection with the provision of our Services and process your information on our behalf. These entities may

include analytics, billing, legal support, marketing, security, machine learning, and fraud prevention companies.

Other Users and Individuals. Our Services are social services in which you can find, collaborate on, and share content. Your profile, including your name, user name, profile picture, code, and other profile information (but not your email address or phone number) will always be viewable and searchable by other users and indexed by online search engines. The content you post to the Services, including your code and forum posts, will be displayed on the Services and viewable by other users by default. The "Your Preferences" section of this Privacy Policy describes the controls that you can use to limit the sharing of your code. We are not responsible for the other users' use of available information, so you should carefully consider whether and what to post or how you identify yourself on the **Services**. Please note that student profiles created by teachers using Teams for Education and students' code are never publicly viewable or searchable, and students may not post content on publicly viewable forums.

Third Party App Integrations. If you connect a third-party application to our Services, we may share information such as code with that third party.

As Required by Law and Similar Disclosures. We may access, preserve, and disclose your information if we believe in good faith that doing so is required or appropriate to: (a) comply with law enforcement requests and legal process, such as a court order or subpoenas; (b) respond to your requests; or (c) protect your, our, or others' rights, property, or safety. For the avoidance of doubt, the disclosure of your information may occur if you post any objectionable content on or through the Services.

Merger, Sale, or Other Asset Transfers. We may disclose and transfer your information to service providers, advisors, potential transactional partners, or other third parties in connection with the consideration, negotiation, or completion of a corporate transaction in which we are acquired by or merged with another company or we sell, liquidate, or transfer all or a portion of our business or assets.

Consent. We may also disclose information from or about you with your permission.

5 Your Rights and Choices

Sharing Preferences. If you prefer to not have others see your code, you can set the relevant repository as private, which may require that you purchase a subscription service from us. If you import code from GitHub and your repository is public, it will remain public by default. If you wish to import code from GitHub and your repository is private, you can upgrade to ensure that your code will also remain private on Codigo.

Marketing Communications. You can unsubscribe from our promotional emails via the link provided in the emails. Even if you opt-out of receiving promotional messages from us, you will continue to receive administrative messages from us.

How to Block Cookies. You can change your browser settings to block, disable, or notify you when you receive a Cookie, delete Cookies, or browse our Services using your browser's anonymous usage setting. However, if you use your browser settings to block all Cookies (including essential Cookies) you may not be able to access all or parts of our Services, or some portions of the Services may not function properly.

Your European Privacy Rights. If you are located in the European Economic Area or the United Kingdom, you have the additional rights described below.

- You may request access to the information we maintain about you, update and correct inaccuracies in your information, restrict or object to the processing of your information, have the information anonymized or deleted, as appropriate, or exercise your right to data portability to easily transfer your information to another company (where technically feasible). In addition, you also have the right to lodge a complaint with a supervisory authority, including in your country of residence, place of work or where an incident took place.
- You may withdraw any consent you previously provided to us regarding the processing of your information, at any time and free of charge. We will apply your preferences going forward and this will not affect the lawfulness of the processing before you withdrew your consent.

You may exercise these rights by contacting us using the contact details at the end of this Privacy Policy. Before responding to your request, we may ask you to provide reasonable information to verify your identity. Please note that there are exceptions and limitations to each of these rights, and that while any changes you make will be reflected in active user databases instantly or within a reasonable period of time, we may retain information for backups, archiving, prevention of fraud and abuse, analytics, satisfaction of legal obligations, or where we otherwise reasonably believe that we have a legitimate reason to do so.

Third Parties

Our Services may contain links to other websites, products, or services that we do not own or operate. We are not responsible for the privacy practices of these third parties. Please be aware that this Privacy Policy does not apply to your activities on these third-party services or any information you disclose to these third parties. We encourage you to read their privacy policies before providing any information to them.

Retention

We take measures to delete your information or maintain it in a de-identified form when it is no longer necessary to be kept in identifiable form for the purposes for which we process it, unless we are required by law to keep this information for a longer period. When determining the specific retention period, we take into account various criteria, such as the type of service provided to you, the nature and length of our relationship with you, and mandatory retention

periods provided by applicable law and any statute of limitations. When you request to delete your account, we delete your data within 30 days.

Security

We use a variety of technical, organizational, and physical safeguards designed to safeguard the information we maintain. However, as our Services are hosted electronically, we can make no guarantees as to the security or privacy of your information.

Children's and Students' Privacy

Our Services are directed to a general audience and are not directed to children under the age of 13. By agreeing to our Privacy Policy and Terms of Service, you represent that you are allowed to use our Services according to your country's applicable age limits. If we learn that a child is under the age of 13 in the United States, or is under the applicable age requirement in another jurisdiction, we will take reasonable steps to obtain parental consent or delete the user's personal information from our files as soon as is practicable. Please contact us at support@codigo.ai if you believe that a user has provided us with representations in violation of this Privacy Policy.

Notice at collection

The following table summarizes the categories of "personal information" (as defined under relevant state laws cited below) that we collect from and about you, the purposes for which we use each category, and the third parties to which we share each category for a business purpose. Please find this information in the following chart and see the various sections above in this Privacy Policy for more information on each category.

Category of Personal Information	**Purposes of Use**	**Categories of Third Parties**
Registration and profile information	● Provide the Services ● Communicate with you ● Facilitate 3rd-party connections ● Marketing and advertising ● Personalization ● Legal and compliance purposes ● With consent	● Affiliates ● Service providers ● Third-party app integrations ● Entities for legal compliance ● Entities for business transactions
Payment information	● Facilitate transactions ● Legal and compliance purposes	● Service providers ● Entities for legal compliance

Communications	• Communicate with you • Legal and compliance purposes • With consent	• Affiliates • Service providers • Entities for legal compliance • Entities for business transactions
Careers information	• To facilitate your application for employment with us	• Affiliates • Service providers • Entities for legal compliance
Device information	• Provide the Services • Marketing and advertising • Personalization • Legal and compliance purposes • With consent	• Affiliates • Service providers • Entities for legal compliance • Entities for business transactions
Location information	• Provide the Services • Marketing and advertising • Personalization • Legal and compliance purposes • With consent	• Affiliates • Service providers • Entities for legal compliance • Entities for business transactions
Usage information	• Provide the Services • Marketing and advertising • Personalization • Legal and compliance purposes • With consent	• Affiliates • Service providers • Entities for legal compliance • Entities for business transactions
User-generated content (e.g., code)	• Provide the Services • Facilitate 3rd-party connections • Personalization • Legal and compliance purposes • With consent	• Affiliates • Service providers • Other users and individuals • Third-party app integrations

		● Entities for legal compliance ● Entities for business transactions
Third-party information	● Provide the Services ● Marketing and advertising ● Personalization ● Legal and compliance purposes ● With consent	● Affiliates ● Service providers ● Entities for legal compliance ● Entities for business transactions

Additional information for California residents

If you are a California resident, the California Consumer Privacy Act ("**CCPA**") requires us to provide you with a summary of the categories of "personal information" (as defined under the CCPA) that we collect from and about you, the purposes for which we use each category, and the third parties to which we share each category for a business purpose. You may find this summary in the section "Notice at collection" above.

If you are a California resident, you may exercise the following rights with regard to data where we determine the purposes and means of processing:

- The right to request a copy of the personal information that we have collected about you in the prior 12 months.
- The right to request details about the categories of personal information we collect, the categories of sources, the business or commercial purposes for collecting information, and the categories of third parties with which we share information.
- The right to request deletion of the personal information that we have collected about you, subject to certain exemptions.
- The right to opt out of the sale of your personal information. We do not "sell" personal information as such term is defined in the CCPA.
- The right to opt out from profiling, defined as the automated processing of personal information to assess or forecast aspects of your behavior.
- The right to request us to correct errors in the personal information that we hold about you.

California residents can submit access and deletion requests by emailing us at support@codigo.ai. California residents can also request that we delete your information through

your account settings. You have the right not to receive discriminatory treatment for the exercise of your CCPA privacy rights, subject to certain limitations.

An authorized agent may submit an access or deletion request on your behalf by sending a written authorization signed by you to support@codigo.ai. We may still require you to directly verify your identity and confirm that you provided the authorized agent permission to submit the request.

Additional information for Colorado residents

If you are a Colorado resident, the Colorado Privacy Act ("**CPA**") requires us to provide you with a summary of the categories of "personal information" (as defined under the CPA) that we collect from and about you, the purposes for which we use each category, and the third parties to which we share each category for a business purpose. You may find this summary in the section "Notice at collection" above.

If you are a Colorado resident, you may exercise the following rights with regard to data where we determine the purposes and means of processing:

- The right to request a copy of the personal information that we have collected about you in the prior 12 months. We will not charge a fee for up to two requests per year.
- The right to request details about the categories of personal information we collect, the categories of sources, the business or commercial purposes for collecting information, and the categories of third parties with which we share information.
- The right to request deletion of the personal information that we have collected about you, subject to certain exemptions.
- The right to opt out of the sale of your personal information. We do not "sell" personal information as such term is defined in the CPA.
- The right to opt out from profiling, defined as the automated processing of personal information to assess or forecast aspects of your behavior.
- The right to request us to correct errors in the personal information that we hold about you.
- The right to appeal if we decline a request that you have made.

Colorado residents can submit access and deletion requests by emailing us at support@codigo.ai. California residents can also request that we delete your information through your account settings. You have the right not to receive discriminatory treatment for the exercise of your CPA privacy rights, subject to certain limitations.

An authorized agent may submit an access or deletion request on your behalf by sending a written authorization signed by you to support@codigo.ai. We may still require you to directly verify your identity and confirm that you provided the authorized agent permission to submit the request.

Additional information for Connecticut residents

If you are a Connecticut resident, the Connecticut Data Privacy Act ("**CDPA**") requires us to provide you with a summary of the categories of "personal information" (as defined under the CDPA) that we collect from and about you, the purposes for which we use each category, and the third parties to which we share each category for a business purpose. You may find this summary in the section "Notice at collection" above.

If you are a Connecticut resident, you may exercise the following rights with regard to data where we determine the purposes and means of processing:

- The right to request a copy of the personal information that we have collected about you in the prior 12 months. We will not charge a fee for up to one request per year.
- The right to request details about the categories of personal information we collect, the categories of sources, the business or commercial purposes for collecting information, and the categories of third parties with which we share information.
- The right to request deletion of the personal information that we have collected about you, subject to certain exemptions.
- The right to opt out of the sale of your personal information. We do not "sell" personal information as such term is defined in the CDPA.
- The right to opt out from profiling, defined as the automated processing of personal information to assess or forecast aspects of your behavior.
- The right to request us to correct errors in the personal information that we hold about you.
- The right to appeal if we decline a request that you have made.

Connecticut residents can submit access and deletion requests by emailing us at support@codigo.ai. Connecticut residents can also request that we delete your information through your account settings. You have the right not to receive discriminatory treatment for the exercise of your CDPA privacy rights, subject to certain limitations.

An authorized agent may submit an access or deletion request on your behalf by sending a written authorization signed by you to support@codigo.ai. We may still require you to directly verify your identity and confirm that you provided the authorized agent permission to submit the request.

Additional information for Iowa residents

If you are an Iowa resident, the Iowa Consumer Data Protection Act ("**ICDPA**") requires us to provide you with a summary of the categories of "personal information" (as defined under the ICDPA) that we collect from and about you, the purposes for which we use each category, and the third parties to which we share each category for a business purpose. You may find this summary in the section "Notice at collection" above.

If you are an Iowa resident, you may exercise the following rights with regard to data where we determine the purposes and means of processing:

- The right to request a copy of the personal information that we have collected about you in the prior 12 months. We will not charge a fee for up to two requests per year.
- The right to request details about the categories of personal information we collect, the categories of sources, the business or commercial purposes for collecting information, and the categories of third parties with which we share information.
- The right to request deletion of the personal information that we have collected about you, subject to certain exemptions.
- The right to opt out of the sale of your personal information. We do not "sell" personal information as such term is defined in the ICDPA.
- The right to opt out from profiling, defined as the automated processing of personal information to assess or forecast aspects of your behavior.
- The right to appeal if we decline a request that you have made.

Iowa residents can submit access and deletion requests by emailing us at support@codigo.ai. Iowa residents can also request that we delete your information through your account settings. You have the right not to receive discriminatory treatment for the exercise of your ICDPA privacy rights, subject to certain limitations.

An authorized agent may submit an access or deletion request on your behalf by sending a written authorization signed by you to support@codigo.ai. We may still require you to directly verify your identity and confirm that you provided the authorized agent permission to submit the request.

Additional information for Utah residents

If you are a Utah resident, the Utah Consumer Privacy Act ("**UCPA**") requires us to provide you with a summary of the categories of "personal information" (as defined under the UCPA) that we collect from and about you, the purposes for which we use each category, and the third parties to which we share each category for a business purpose. You may find this summary in the section "Notice at collection" above.

If you are a Utah resident, you may exercise the following rights with regard to data where we determine the purposes and means of processing:

- The right to request a copy of the personal information that we have collected about you in the prior 12 months. We will not charge a fee for up to one request per year.
- The right to request details about the categories of personal information we collect, the categories of sources, the business or commercial purposes for collecting information, and the categories of third parties with which we share information.

- The right to request deletion of the personal information that we have collected about you, subject to certain exemptions.
- The right to opt out of the sale of your personal information. We do not “sell” personal information as such term is defined in the UCPA.

Utah residents can submit access and deletion requests by emailing us at support@codigo.ai. Utah residents can also request that we delete your information through your account settings. You have the right not to receive discriminatory treatment for the exercise of your UCPA privacy rights, subject to certain limitations.

An authorized agent may submit an access or deletion request on your behalf by sending a written authorization signed by you to support@codigo.ai. We may still require you to directly verify your identity and confirm that you provided the authorized agent permission to submit the request.

Additional information for Virginia residents

If you are a Virginia resident, the Virginia Consumer Data Protection Act ("**VCDPA**") requires us to provide you with a summary of the categories of “personal information” (as defined under the VCDPA) that we collect from and about you, the purposes for which we use each category, and the third parties to which we share each category for a business purpose. You may find this summary in the section “Notice at collection” above.

If you are a Virginia resident, you may exercise the following rights with regard to data where we determine the purposes and means of processing:

- The right to request a copy of the personal information that we have collected about you in the prior 12 months. We will not charge a fee for up to two requests per year.
- The right to request details about the categories of personal information we collect, the categories of sources, the business or commercial purposes for collecting information, and the categories of third parties with which we share information.
- The right to request deletion of the personal information that we have collected about you, subject to certain exemptions.
- The right to opt out of the sale of your personal information. We do not “sell” personal information as such term is defined in the VCDPA.
- The right to opt out from profiling, defined as the automated processing of personal information to assess or forecast aspects of your behavior.
- The right to request us to correct errors in the personal information that we hold about you.
- The right to appeal if we decline a request that you have made.

Virginia residents can submit access and deletion requests by emailing us at support@codigo.ai. Virginia residents can also request that we delete your information through your account settings. You have the right not to receive discriminatory treatment for the exercise of your VCDPA privacy rights, subject to certain limitations.

An authorized agent may submit an access or deletion request on your behalf by sending a written authorization signed by you to support@codigo.ai. We may still require you to directly verify your identity and confirm that you provided the authorized agent permission to submit the request.

International Visitors

Our Services are primarily hosted in the United States and may also be hosted in locations abroad (for example, India). If you use the Services from regions of the world with laws governing data processing, you accept that you are transferring your information to the United States and other hosting locations for storage and processing. By providing information to Codigo, you agree to such transfer, storage, and processing.

Update Your Information or Pose a Question

You can update your account and profile information or close your account through your profile settings. If you have questions about your privacy on the Services or this privacy policy, please contact us at support@codigo.ai.

Changes to this Privacy Policy

We will post any adjustments to the Privacy Policy on this page, and the revised version will be effective when it is posted. If we materially change the ways in which we process information, we will provide you with notice in the application and via email in accordance with applicable legal requirements.

Contact Information

If you have any questions, comments, or concerns about our processing activities, please email us at support@codigo.ai.

Data Processing Agreement

This Data Processing Agreement ("**DPA**") amends and forms part of the Codigo Terms & Conditions (the "**Agreement**") between Codigo, Inc., a Delaware corporation ("**Company**") and you ("**Customer**"). This DPA prevails over any conflicting term of the Agreement.

1. Definitions
    1.1. In this DPA:

1.1.1. "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**", and "**Supervisory Authority**" have the meaning given to them in applicable Data Protection Law;

1.1.2. "**Customer Personal Data**" means any Customer Data that constitutes Personal Data, the Processing of which is subject to Data Protection Law, for which Customer or Customer's customers are the Controller, and which is Processed by Company to provide the Services;

1.1.3. "**Data Protection Law**" means all applicable laws and regulations in any jurisdiction relating to privacy, data protection, data security, breach notification, or the Processing of Customer Personal Data, including without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* ("**CCPA**"), the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"), and the United Kingdom Data Protection Act of 2018, as such laws may be amended from time to time. For the avoidance of doubt, if Company's Processing activities involving Customer Personal Data are not within the scope of a given Data Privacy Law, such law is not applicable for purposes of this Addendum.

1.1.4. "**Data Subject Rights**" means Data Subjects' rights to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision-making in accordance with Data Protection Law;

1.1.5. "**International Data Transfer**" means any transfer of Customer Personal Data from the EEA, Switzerland or the United Kingdom to an international organization or to a country outside of the EEA, Switzerland and the United Kingdom;

1.1.6. "**Services**" means the services provided by Company to Customer under the Agreement;

1.1.7. "**Subprocessor**" means a Processor engaged by Company to Process Customer Personal Data; and

1.1.8. "**Standard Contractual Clauses**" means, as applicable: (a) the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council; (b) the UK Addendum to the EEA SCCs adopted pursuant to or permitted under Article 46 of the UK GDPR; and/or (c) the UK International Data Transfer Agreement (IDTA) adopted pursuant to or permitted under Article 46 of the UK GDPR.

2. Scope and applicability

2.1. This DPA applies to Processing of Customer Personal Data by Company to provide the Services. The subject matter, nature and purpose of the Processing, the types of Customer Personal Data and categories of Data Subjects are set out in **Appendix 1**, below.

2.2. In the Standard Contractual Clauses, Module 2 (Controller to Processor) will apply where User is a Controller of Personal Data and Codigo is a Processor of Personal Data. Customer is a Controller and appoints Company as a Processor on behalf of Customer with respect to the Personal Data provided by Customer to Company to perform the

Services on Customer's behalf. Customer is responsible for compliance with the requirements of Data Protection Law applicable to Controllers.

3. Instructions
   3.1. Company will Process Customer Personal Data to provide the Services and in accordance with Customer's documented instructions. The Controller's instructions are documented in this DPA, the Agreement, and any applicable statement of work.

   3.2. Unless prohibited by applicable law, Company will inform Customer if Company is subject to a legal obligation that requires Company to Process Customer Personal Data in contravention of Customer's documented instructions.

   3.3. Company will not sell Customer Personal Data or otherwise Process Customer Personal Data for any purpose other than for the specific purposes set forth herein. For purposes of this paragraph, "sell" shall have the meaning set forth in the CCPA.

4. Personnel
   4.1. Company will ensure that all personnel authorized to Process Customer Personal Data are subject to an obligation of confidentiality.

5. Security and Personal Data Breaches
   5.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Company will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the measures listed in **Appendix 2**.

   5.2. Company will notify Customer without undue delay after becoming aware of a Personal Data Breach involving Customer Personal Data. If Company's notification is delayed, it will be accompanied by reasons for the delay.

6. Subprocessing
   6.1. Customer hereby authorizes Company to engage Subprocessors. Company's current Subprocessors are Google and Stripe.

   6.2. Company will enter into a written agreement with Subprocessors which imposes the same obligations as required by Data Protection Law. If Company processes Customer Personal Data of residents in the European Economic Area (EEA), United Kingdom, or Switzerland on Customer's behalf, Company will notify Customer prior to any intended change to Subprocessors. In such circumstances, Customer may object to the addition of a Subprocessor based on reasonable grounds relating to a potential or actual violation of Data Protection Law by providing written notice detailing the grounds of such objection within thirty (30) days following Company's notification of the intended change. Customer and Company will work together in good faith to address Customer's objection.

7. Assistance
   7.1. Taking into account the nature of the Processing, and the information available to Company, Company will assist Customer, including, as appropriate, by implementing technical and organizational measures, with the fulfilment of Customer's own obligations under applicable Data Protection Law to: comply with requests to exercise Data Subject Rights; conduct data protection impact assessments, and prior consultations with Supervisory Authorities; and notify a Personal Data Breach.

8. Audit
   8.1. Company will make available to Customer required information necessary to demonstrate compliance with the obligations of this DPA and allow for and contribute to audits, including inspections, as mandated by a Supervisory Authority or reasonably requested by Customer by at least sixty (60) days' notice, and no more than once per calendar year, and performed by an independent auditor as agreed upon by Customer and Company. Any such audit must be conducted during Company's business hours, without disruption to Company's operations, and in compliance with Company's confidentiality obligations.

   8.2. Company will inform Customer if Company believes that Customer's instruction under **Section 8.1** infringes Data Protection Law. Company may suspend the audit or inspection, or withhold requested information until Customer has modified or confirmed the lawfulness of the instructions in writing.

9. International Data Transfers
   9.1. This section 9 on "International Data Transfers" and its subparts applies only to the extent that Company processes Customer Personal Data of residents in the European Economic Area (EEA), United Kingdom, or Switzerland on Customer's behalf.

   9.2. Customer hereby authorizes Company to perform International Data Transfers to any country deemed adequate by the EU Commission; on the basis of appropriate safeguards in accordance with Data Protection Law; or pursuant to the Standard Contractual Clauses referred to in **Section 9.3**.

   9.3. By executing this DPA, Customer and Company conclude the Standard Contractual Clauses, which are hereby incorporated into this DPA and completed as follows: the "data exporter" is Customer; the "data importer" is Company; in Clause 7 of the Standard Contractual Clauses, the option docking clause will not apply; in Clause 9 of the Standard Contractual Clauses, Option 2 will apply; in Clause 11 of the Standard Contractual Clauses, the option will apply; and Appendix 1 and Appendix 2 to the Standard Contractual Clauses are provided at Appendix 1 and 2 to this DPA, respectively.

   9.4. Company hereby represents and warrants that (a) it is not and will not be in breach of any provision of the Standard Contractual Clauses as referred to in Section 9.3 above; and (b) it has not been declared by a court of competent jurisdiction to be subject to the U.S. Foreign Intelligence Surveillance Act ("FISA") or Executive Order 12333 ("EO"), and nor has it received any requests under Section 702 or, to the best of its knowledge, been subject to any action under the EO. If Company receives any future requests discussed in this paragraph during the terms of this DPA, Company commits to taking reasonable steps to challenge such requests and/or seek judicial redress. If following such steps Company is still ordered to comply with such a request, and where Company is prohibited by applicable law from disclosing the receipt of such a request, Company shall inform Customer that Company can no longer comply with Customer's processing instructions without providing details as to why, so that Customer can terminate the Processing.

   9.5. All authorizations of International Data Transfers in this Section 9 are expressly conditioned upon Company's ongoing compliance with the requirements of Data Protection Law applicable to International Data Transfers, and any applicable legal

instrument for International Data Transfers. If such compliance is affected by circumstances outside of Company's control, including circumstances affecting the validity of an applicable legal instrument, Company and Customer will work together in good faith to reasonably resolve such non-compliance.

10. Notifications
    10.1. All notices made under this DPA shall be made to Customer via email at the email Customer has used to sign up.

11. Termination and return or deletion
    11.1. This DPA is terminated upon the termination of the Agreement. Customer may request return of Customer Personal Data up to ninety (90) days after termination of the Agreement. Unless required or permitted by applicable law, Company will delete all remaining copies of Customer Personal Data within one hundred eighty (180) days after returning Customer Personal Data to Customer.

APPENDIX 1

Description of the Processing

6 Data Subjects

The Customer Personal Data Processed concern the following categories of Data Subjects (please specify): Paid customers of Codigo and Codigo users.

7 Categories of Customer Personal Data

The Customer Personal Data Processed concerns the following categories of data (please specify): Any Personal Data processed by Codigo on behalf of Customer in connection with providing the Services, including contact information, usage information, profile information, and user-generated content.

8 Sensitive data

The Customer Personal Data Processed concern the following special categories of data (please specify): N/A

9 Processing operations

The Customer Personal Data will be subject to the following basic Processing activities (please specify): Codigo will Process the Customer Personal Data for purposes of providing Services pursuant to the Agreement and this DPA.

APPENDIX 2

Security Measures

Company will implement and maintain the following administrative, technical, physical, and organizational security measures for the Processing of Personal Data:

Company's Information Security Program includes specific security requirements for its personnel and all subcontractors or agents who have access to Personal Data ("**Data Personnel**"). Company's security requirements cover the following areas:

a. Information Security Policies and Standards. Company will maintain information security policies, standards and procedures addressing administrative, technical, and physical security controls and procedures. These policies, standards, and procedures shall be kept up to date, and revised whenever relevant changes are made to the information systems that use or store Personal Data.
b. Physical Security. Company will maintain commercially reasonable security systems at all Company sites at which an information system that uses or stores Personal Data is located ("**Processing Locations**") that include reasonably restricting access to such Processing Locations, and implementing measures to detect, prevent, and respond to intrusions.
c. Organizational Security. Company will maintain information security policies and procedures addressing acceptable data use standards, data classification, and incident response protocols.
d. Network Security. Company maintains commercially reasonable information security policies and procedures addressing network security.
e. Access Control. Company agrees that: (1) only authorized Company staff can grant, modify or revoke access to an information system that Processes Personal Data; and (2) it will implement commercially reasonable physical and technical safeguards to create and protect passwords.
f. Virus and Malware Controls. Company protects Personal Data from malicious code and will install and maintain anti-virus and malware protection software on any system that handles Personal Data.
g. Personnel. Company has implemented and maintains a security awareness program to train employees about their security obligations. Data Personnel follow established security policies and procedures. Disciplinary process is applied if Data Personnel fail to adhere to relevant policies and procedures.
h. Subcontractor security. Company shall only select and contract with subcontractors that are capable of maintaining appropriate security safeguards that are no less onerous than those contained in the Addendum and this Appendix.
i. Business Continuity. Company implements disaster recovery and business resumption plans that are kept up to date and revised on a regular basis. Company also adjusts its Information Security Program in light of new laws and circumstances, including as Company's business and Processing change.