Data Processing Agreement

This data processing agreement and its appendices (**DPA**) are part of the Agreement between Juro and Customer. The DPA describes the parties' obligations when it comes to the processing and security of Customer Data. The DPA is effective on the DPA Effective Date.

1. Definitions

1.1. Capitalized terms used but not defined in the DPA have the meanings set out in the Agreement.

1.2. Capitalized terms used in the DPA but not defined elsewhere have the following meanings:

Additional Security Controls means security features which Customer may choose to use as it decides, including identity and access management and multi-factor authentication.

Agreement means the contract under which Juro has agreed to provide Services to Customer that refers to this DPA or a previous version of it.

Applicable Data Protection Law means any applicable European Data Protection Law or US Data Protection Law that applies to the processing of Customer Personal Data.

Audited Services means the then-current Hosted Services.

Customer Personal Data means any personal data contained within Customer Data.

Data Incident means a breach of Juro's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data on systems managed or otherwise controlled by Juro.

DPA Effective Date means the date on which the parties agreed to the DPA.

EU GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

European Data Protection Law means, as applicable: (a) the GDPR; or (b) the Swiss FADP.

European Law means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data); or (c) the law of Switzerland (if the Swiss FADP applies to the processing of Customer Personal Data).

GDPR means, as applicable: (a) the EU GDPR; or (b) the UK GDPR.

Juro's Third-Party Auditor means a Juro-appointed, qualified and independent third-party auditor.

Notification Email Address means the privacy contact email address designated by Customer in the Order Form.

Security Documentation means the Compliance Certification and the SOC Report.

Services means the Hosted Services under the MSA.

Subprocessor means a third party authorized as a processor under the DPA to process Customer Personal Data to provide parts of the Services.

Supervisory Authority means, as applicable: (a) a "supervisory authority" as defined in the EU GDPR; or (b) the "Commissioner" as defined in the UK GDPR or the Swiss FADP.

Swiss FADP means, as applicable, the Federal act on Data Protection of 19 June 1992 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 14 June 1993) or the revised Federal Act on Data Protection of 25 September 2020 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 31 August 2022).

UK GDPR is defined in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

US Data Protection Law means any state-level comprehensive privacy law in the United States (e.g. CCPA), but excluding sector-specific privacy laws (e.g. HIPAA).

1.3. The terms **personal data**, **data subject**, **processing**, **controller**, and **processor** as used in the DPA have the meanings given by Applicable Data Protection Law or, if not so defined, by the EU GDPR.

1.4. The terms **data subject**, **controller** and **processor** include **consumer**, **business**, and **service provider**, respectively, as required by Applicable Data Protection Law.

2. Duration

The DPA remains in effect from the DPA Effective Date until, and automatically expires when, Juro deletes all Customer Data (the **Term**).

3. Roles and compliance

3.1. **Roles.** Juro is a processor and Customer is a controller of Customer Personal Data.

3.2. **Processing summary.** The subject matter and details of the processing of Customer Personal Data are described in Appendix 1.

3.3. **Compliance with law.** Each party will comply with its obligations related to the processing of Customer Personal Data under Applicable Data Protection Law.

3.4. **Additional legal terms.** To the extent the processing of Customer Personal Data is subject to an Applicable Data Protection Law described in Appendix 3, the

corresponding terms in Appendix 3 will apply in addition to these General Terms and will prevail as described in paragraph 10.3(a)(ii).

4. Customer's instructions

4.1. Customer instructs Juro to process Customer Personal Data in accordance with the Agreement only as follows:

(a) to provide, secure, and monitor the Services; and

(b) as further specified by: (i) Customer's use of the Services; and (ii) any other written instructions given by Customer and acknowledged by Juro as instructions under the DPA,

(collectively, the **Instructions**).

4.2. Juro will comply with the Instructions unless required to do otherwise by European Law, where European Data Protection Law applies, or required to do otherwise by applicable law, where any other Applicable Data Protection Law applies, in which case Juro will inform Customer of that requirement before processing, unless that law prohibits Juro from doing so on important grounds of public interest.

5. Data deletion

5.1. **Deletion by Customer.** During the Term, Juro will enable Customer to delete Customer Data using functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, this is an Instruction to Juro to delete the relevant Customer Data from Juro's systems. Juro will comply with this Instruction as soon as reasonably practicable, unless European Law requires storage, where European Data Protection Law applies, or applicable law requires storage, where any other Applicable Data Protection Law applies.

5.2. **Return or deletion at the end of the Term.** If Customer wishes to retain any Customer Data after the end of the Term, it may instruct Juro in accordance with the MSA to return that data. Customer instructs Juro to delete all remaining Customer Data (including existing copies) from Juro's systems at the end of the Term. After a recovery period of up to 60 days from the termination date, Juro will comply with this Instruction as soon as reasonably practicable, unless European Law requires storage, where European Data Protection Law applies, or applicable law requires storage, where any other Applicable Data Protection Law applies.

6. Data security

6.1. **Juro's security measures.**

(a) **Juro's security measures.** Juro will implement and maintain technical, organizational and physical measures designed to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the **Security Measures**). The Security Measures include measures to encrypt Customer Data; to help and ensure ongoing confidentiality,

integrity, availability and resilience of Juro's systems and services; to help restore timely access to Customer Data following an incident; and for regular testing of effectiveness. Juro may update the Security Measures from time to time, as long as the updates do not result in a material reduction to the security of the Services.

(b) **Access and compliance.** Juro will: (i) authorize its personnel and Subprocessors to access Customer Data only as necessary to comply with Instructions; (ii) take appropriate steps to ensure compliance with the Security Measures by its personnel and Subprocessors; and (iii) ensure that everyone who is authorized to access Customer Data is under an obligation of confidentiality.

(c) **Additional Security Controls.** Juro will make Additional Security Controls available to allow Customer to take steps to secure Customer Data.

(d) **Juro's security assistance.** Juro will (taking into account the nature of the processing of Customer Personal Data and the information available to Juro) assist Customer in ensuring compliance with its obligations relating to security and personal data breaches under Applicable Data Protection Law, by: (i) implementing and maintaining the Security Measures in accordance with paragraph 6.1(a); (ii) making Additional Security Controls available in accordance with paragraph 6.1(c); (iii) complying with paragraph 6.2; (iv) making the Security Documentation available in accordance with paragraph 6.5(a) and providing the information contained in Agreement; and (v) if (i) to (iv) above(inclusive) are insufficient for Customer to comply with such obligations, at Customer's request and expense, providing Customer with additional reasonable cooperation and assistance.

6.2. **Data Incidents.**

(a) **Notification.** Juro will notify Customer without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Personal Data.

(b) **Details of Data Incident.** Juro's notification of a Data Incident will describe: the nature of the Data Incident, including the Customer Personal Data impacted; the measures Juro has taken, or plans to take, to address the Data Incident and mitigate its potential risk; the measures, if any, Juro recommends that Customer take to address the Data Incident; and details of a contact point where more information can be sought. If it is not possible to provide all this information at the same time, Juro's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

(c) **No assessment of Customer Data by Juro.** Juro is not required to assess Customer Data in order to identify information subject to any specific legal requirements.

(d) **No acknowledgement of fault by Juro.** Juro's notification of or response to a Data Incident under this paragraph 6.2 is not an acknowledgement by Juro of any fault or liability with respect to the Data Incident.

6.3. **Customer's security responsibilities and assessment.**

(a) **Customer's security responsibilities.** Without prejudice to Juro's obligations under the Agreement, Customer is responsible for its use of the Services and its storage of any copies of Customer Data outside Juro's or Juro's Subprocessors' systems, including: (i) using the Services and Additional Security Controls to ensure a level of security appropriate to the risk to Customer Data; (ii) securing the account authentication credentials, systems and devices Customer uses to access the Services; and (iii) backing up or retaining copies of its Customer Data as appropriate.

(b) **Customer's security assessment.** Customer agrees that the Services, Security Measures, Additional Security Controls, and Juro's commitments under this paragraph 6 provide a level of security appropriate to the risk to Customer Data (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Data as well as the risks to individuals).

6.4. **Compliance Certification and SOC Report.** Juro will maintain at least the following for the Audited Services to verify the continued effectiveness of the Security Measures:

(a) a certificate for Cyber Essentials (the **Compliance Certification**); and

(b) a SOC 2 Type II report produced by Juro's Third-Party Auditor and updated annually based on an audit performed at least once every 12 months (the **SOC Report**).

Juro may add standards at any time. Juro may replace a Compliance Certification or SOC Report with an equivalent or enhanced alternative.

6.5. **Reviews and audits of compliance.**

(a) **Reviews of Security Documentation**. To demonstrate compliance by Juro with its obligations under the DPA, Customer may request (no more than once per year) a copy of the Security Documentation to review.

(b) **Customer's audit rights.**

(i) **Customer audit.** Juro will, if required under Applicable Data Protection Law, allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Juro's compliance with its obligations under the DPA in accordance with paragraph 6.5(c) (a **Customer Audit)**. During a Customer Audit, Juro will cooperate reasonably with Customer or its auditor as described in this paragraph 6.5.

(ii) **Customer independent review**. Customer may conduct an audit to verify Juro's compliance with its obligations under the DPA by reviewing the Security Documentation (which reflects the outcome of audits conducted by Juro's Third-Party Auditor).

(c) **Additional terms for reviews and audits.**

(i) To request a Customer Audit, Customer must contact support@juro.com.

(ii) Following a Customer request under paragraph 6.5(c)(i), Juro and Customer will discuss and agree in advance on the reasonable start date, scope and duration of, and security and confidentiality controls applicable to, any Customer Audit.

(iii) Juro may charge a fee (based on Juro's reasonable costs) for any Customer Audit. Juro will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

(iv) Juro may object in writing to an auditor appointed by Customer to conduct any Customer Audit if the auditor is, in Juro's reasonable opinion, not suitably qualified or independent, a competitor of Juro, or otherwise manifestly unsuitable. Any such objection by Juro will require Customer to appoint another auditor or to conduct the audit itself.

(v) Any Customer requests under Appendix 3 for audits will also be subject to this paragraph 6.5(c).

7. Impact assessments and consultations

Juro will (taking into account the nature of the processing and the information available to Juro) assist Customer in ensuring compliance with its obligations relating to data protection assessments, risk assessments, prior regulatory consultations or equivalent procedures under Applicable Data Protection Law, by:

7.1. making Additional Security Controls available in accordance with paragraph 6.1(c) and the Security Documentation available in accordance with paragraph 6.5(a);

7.2. providing the information contained in the Agreement; and

7.3. if paragraphs 7.1 and 7.2 are insufficient for Customer to comply with such obligations, at Customer's request and expense, providing Customer with additional reasonable cooperation and assistance.

8. Access; data subject rights; data export

8.1. **Access; rectification; restricted processing; portability.** During the Term, Juro will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Juro as described in paragraph 5.1, and to export Customer Data. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for using such functionality to rectify or delete that data if required by Applicable Data Protection Law.

8.2. **Data subject requests.**

(a) **Responsibility for requests.** During the Term, if Juro receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Juro will: (i) tell the data subject to submit its request to Customer; (ii) promptly inform Customer; and (iii) not otherwise respond to that data subject's request without authorization

from Customer. Customer is responsible for responding to any such request including, where necessary, by using the functionality of the Services.

(b) **Juro's data subject request assistance.** Juro will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling its obligations under Applicable Data Protection Law to respond to requests for exercising the data subject's rights by: (i) making Additional Security Controls available in accordance with paragraph 6.1(c); (ii) complying with paragraphs 8.1 and 8.2(a); and if (i) and (ii) above are insufficient for Customer to comply with such obligations, at Customer's request and expense, providing Customer with additional reasonable cooperation and assistance.

9. Data processing locations

Customer Data may be processed in any country where Juro or its Subprocessors maintain facilities.

10. Subprocessors

10.1. **Consent to Subprocessors.** Customer specifically authorizes Juro to engage as Subprocessors those organisations described in paragraph 10.2 as of the Agreement effective date. In addition, without prejudice to paragraph 10.4, Customer generally authorizes Juro to engage other third parties as Subprocessors (**New Subprocessors**).

10.2. **Information about Subprocessors.** Names, locations and activities of Subprocessors are set out in Juro's privacy policy.

10.3. **Requirements for Subprocessor engagement.** When engaging any Subprocessor, Juro must:

(a) ensure using a written contract that: (i) the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement; and (ii) if required under Applicable Data Protection Law, the data protection obligations described in this DPA are imposed on the Subprocessor (as may be further described in Appendix 3); and

(b) remain fully liable for all obligations subcontracted to the Subprocessor.

10.4. **Opportunity to object to Subprocessors.**

(a) When Juro engages any New Subprocessor during the term of the Agreement, Juro will, at least 30 days before the New Subprocessor starts processing any Customer Data, notify Customer of the engagement (including the name, location and activities of the New Subprocessor).

(b) Customer may, within 14 days after being notified of the engagement of a New Subprocessor, object by notifying Juro.

(c) If the objection under paragraph 10.4(b) is due to an actual or likely breach of Applicable Data Protection Law as a result of the engagement of the New Subprocessor, then either (i) Juro may choose to accommodate the objection and

notify Customer when it has done so; or (ii) if Customer receives no such notice within 30 days after Customer's notice of objection under paragraph 10.4(b), then Customer may, within 14 days after such 30-day period, terminate the Agreement immediately by giving notice to Juro and Juro will refund to Customer pro rata any prepaid Fees that relate to the period after termination.

(d) If the objection under paragraph 10.4(b) is not due to an actual or likely breach of Applicable Data Protection Law as a result of the engagement of the New Subprocessor, then either (i) Juro may choose to accommodate the objection and notify Customer when it has done so; or (ii) Customer may immediately choose to cease processing Customer Data using Juro by itself deleting such Customer Data from the Juro Platform using the functionality of the Juro Platform and, conditional on providing the required notice, may terminate the Agreement on expiry of the Initial Term or then-current Renewal Term (as applicable) in accordance with the Agreement.

11. Processing records

11.1. **Juro's processing records.** Juro will keep appropriate records of its processing activities as required by Applicable Data Protection Law. To the extent any Applicable Data Protection Law requires Juro to collect and maintain records of certain information relating to Customer, Customer will supply such information to Juro and keep it accurate and up-to-date. Juro may make any such information available to competent regulators, including a Supervisory Authority, if required by Applicable Data Protection Law.

11.2. **Controller requests.** During the term of the Agreement, if Juro receives a request or instruction from a third party purporting to be a controller of Customer Personal Data, Juro will advise the third party to contact Customer.

Appendix 1: Subject matter and details of data processing

1. Subject matter of processing

Provision by Juro of the Services to the Customer under the Agreement.

2. Duration of the processing

Subject to paragraph 2 of the DPA, Juro will process Customer Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

3. Nature and purpose of the processing

Provision of the Services to the Customer under the Agreement, which include the Hosted Services, Implementation Services and Support Services.

4. Type of personal data

Customer may submit personal data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include the following categories of personal data:

→ Personal data contained in contracts processed by the Juro Platform, including contact details, signatures and personal data of contract counterparties.

→ IP addresses.

→ Geolocation information.

→ User device information.

→ Comments and activity within the Juro Platform.

5. Categories of data subjects

Customer may submit personal data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include personal data relating to the following categories of data subjects:

→ Juro Platform users.

→ Signatories and counterparties to contracts (including external signatories).

→ Anyone whose personal data is included in contracts or other documents processed via the Juro Platform.

Appendix 2: Security measures

Juro will implement and maintain the Security Measures described in this Appendix 2.

1. Data center and network security

1.1. Data centers

Infrastructure. Juro uses suppliers who maintain geographically distributed data centers. Juro stores product data in physically secure data centers.

Redundancy. Juro's infrastructure is provided by suppliers who design their services to eliminate single points of failure and minimize the impact of anticipated environmental risks. Services are designed to allow Juro to conduct maintenance without interruption.

Code quality. Juro's software development lifecycle process includes code review to increase the security of code used to provide the Services.

Business continuity. Juro has implemented and regularly plans and tests its business continuity and disaster recovery procedures.

1.2. Networks and transmission

Data transmission. Juro **transfers** data via Internet standard protocols.

External attack surface. Juro employs multiple layers of network devices and intrusion detection to protect its external attack surface. Juro considers potential attack vectors and incorporates appropriate technologies into external-facing systems.

Intrusion detection. Juro uses intrusion detection to identify ongoing attack activities and gather information to respond to incidents.

Incident response. Juro monitors a variety of channels for security incidents and its security team will react promptly to known incidents.

Encryption. All data transmission between the Juro application and customer endpoints is encrypted using industry-standard transport layer security (TLS) protocol. When data is at rest in Juro, it is encrypted using 256-bit advanced encryption standard (AES).

2. Access controls

2.1. Data center sites

Juro engages data center suppliers who implement rigorous on-site security measures 24 hours a day, 7 days a week, with formal access procedures for allowing physical access to data centers.

2.2. **Access controls**

Personnel. Juro has security policies for its personnel and they must complete security training. Juro's security team is responsible for the ongoing monitoring of Juro's security infrastructure and responding to security incidents.

Access control and management. Customer administrators and users must authenticate themselves using a username and password or via a single sign-on system to use the Services.

Internal data access. Juro's internal procedures are designed to prevent unauthorized access to systems used to process Customer Data. Personnel are granted access rights based on their job responsibilities and requirements on a principle of least privilege basis. Changes are managed using tools that maintain an audit record of all changes. Access to systems is logged to create an audit trail.

3. Data storage

Juro stores data in a multi-tenant environment on supplier servers. Juro replicates Customer Data between multiple geographically diverse data centers. Juro also logically isolates Customer Data.

4. Personnel security

Juro's personnel are required to behave in accordance with Juro's policies on confidentiality, appropriate usage, privacy and professional standards. To the extent permitted by law and consistent with local market practice, Juro conducts appropriate background checks on its personnel.

Juro's personnel are subject to binding confidentiality obligations and must read, and acknowledge receipt of, Juro's confidentiality and privacy policies. Juro provides its team with security and data protection training.

5. Subprocessor security

Before onboarding Subprocessors**,** Juro reviews information about their security and privacy practices to ensure they offer an appropriate level of security and privacy. If the Subprocessors risks are approved by Juro's security team, then subject to paragraph 10.3 of the DPA, the Subprocessor must enter contract terms with Juro that offer appropriate assurances about security, confidentiality and privacy.

Appendix 3: Specific privacy laws

The terms in each subparagraph of this Appendix 3 apply only where the corresponding law applies to the processing of Customer Personal Data.

European Data Protection Law

1. **Additional definitions**

Adequate Country means: (a) for Customer Personal Data processed subject to the EU GDPR: the European Economic Area, or a country or territory recognized as ensuring adequate protection under the EU GDPR; (b) for Customer Personal Data processed subject to the UK GDPR: the UK, or a country or territory recognized as ensuring adequate protection under the UK GDPR or Data Protection Act 2018; or (c) for Customer Personal Data processed subject to the Swiss FADP: Switzerland, a country or territory that is: (i) included in the list of states whose legislation ensures adequate protection as published by the Swiss Federal Data Protection and Information Commissioner, if applicable; or (ii) recognized as ensuring adequate protection by the Swiss Federal Council under the Swiss FADP, in each of (a), (b) and (c), other than on the basis of an optional data protection framework.

Alternative Transfer Solution means a solution, other than the SCCs, that enables the lawful transfer of personal data to a third country in accordance with European Data Protection Law.

C2P SCCs means SCCs sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor).

P2C SCCs means SCCs sections I, II, III and IV (as applicable) to the extent they reference Module Four (Controller-to-Processor).

P2P SCCs means SCCs sections I, II, III and IV (as applicable) to the extent they reference Module Three (Processor-to-Processor).

SCCs means the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

2. **Instruction notifications.** Without prejudice to Juro's obligations under paragraph 4.2 of the DPA or any other rights or obligations of either party under the Agreement, Juro will immediately notify Customer if, in Juro's opinion: (a) European Law prohibits Juro from complying with an Instruction; (b) an Instruction does not comply with European Data Protection Law; or (c) Juro is otherwise unable to comply with an Instruction, in each case, unless such notice is prohibited by European Law.

3. **Customer's audit rights.** Juro will allow Customer or an independent auditor appointed by Customer to conduct Customer Audits as described in paragraph 6.5(b) of the DPA. During such an audit, Juro will make available all information necessary to demonstrate compliance with its obligations under this DPA and contribute to the audit as described in paragraph 6.5 of the DPA and this paragraph 3.

4. **Data transfers.**

4.1. **Restricted transfers.** The parties acknowledge that European Data Protection Law does not require SCCs or an Alternative Transfer Solution in order for Customer Personal Data to be processed in or transferred to an Adequate Country. If Customer Personal Data is transferred to any other country and European Data Protection law applies to the transfers (as certified by Customer under paragraph 4.2 of this Appendix 3, if its billing address is outside the EEA or UK) (Restricted Transfers), then:

(a) if Juro has adopted an Alternative Transfer Solution for any Restricted Transfers, Juro will inform Customer of the relevant solution and ensure that such Restricted Transfers are made in accordance with it; or

(b) if Juro has not adopted an Alternative Transfer Solution for any Restricted Transfers, or informs Customer that Juro is no longer adopting, an Alternative Transfer Solution for any Restricted Transfers (without adopting a replacement Alternative Transfer Solution):

(i) if Juro's address is in an Adequate Country: (A) Juro must implement P2P SCCs with respect to such Restricted Transfers from Juro to Subprocessors; and (B) in addition, if Customer's billing address is not in an Adequate Country, the P2C SCCs will apply with respect to such Restricted Transfers between Juro and Customer; or

(ii) if Juro's address is not in an Adequate Country, the C2P SCCs will apply with respect to such Restricted Transfers between Juro and Customer.

4.2. **Certification by non-European Customers.** If Customer's billing address is outside the EEA or UK, and the processing of Customer Personal Data is subject to European Data Protection Law, then Customer must inform Juro and identify its competent Supervisory Authority by email to support@juro.com.

4.3. **Information about Restricted Transfers.** Juro will provide Customer with information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures: (a) as described in paragraph 6.5(a) of the DPA; and (b) in relation to Juro's adoption of an Alternative Transfer Solution (if any), in the materials at Juro's Trust Center.

4.4. **SCC operative provisions and additional terms.** If SCCs apply as described in paragraph 4.1 of this Appendix 3, this paragraph 4.4 of Appendix 3 and Appendix 4 apply. For the purposes of the C2P SCCs, Customer is the data exporter and Juro is the data importer. For the purposes of the P2C SCCs, Juro is the data exporter and Customer is the data importer. If any authorized affiliate Customer relies on the C2P SCCs or P2C SCCs for the transfer of Customer Personal Data, any references to Customer in paragraph 4 of this Appendix 3 include that authorized affiliate. Where paragraph 4.7 of this Appendix 3 does not explicitly mention the C2P SCCs or the P2C SCCs, it applies to all of them.

(a) **Reference to the SCCs.** Where SCCs apply to a Restricted Transfer, the relevant provisions of the SCCs are incorporated by reference and are an integral part of the DPA. The information required for the purposes of the Appendix to the SCCs are set out in Appendix 4 to the DPA.

(b) **Docking clause.** The option under clause 7 of the SCCs does not apply.

(c) **Instructions.** The Agreement is Customer's complete and final documented instructions at the time of signature. Any additional or alternative instructions must be consistent with the terms of the Agreement. For the purposes of clause 8.1(a) of the SCCs, the instructions by Customer to process Customer Personal Data are set out in paragraph 4 of the DPA and include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.

(d) **Certification of deletion.** Juro will only provide the certification of deletion of Customer Personal Data described in clauses 8.5 and 16(d) of the SCCs if requested by Customer in writing.

(e) **Security of processing.** For the purposes of clause 8.6(a), Customer is responsible for determining independently whether the technical and organisational measures set out in Appendix 2 and Juro's Trust Center meet Customer's requirements and Customer agrees (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals) that the security measures and policies implemented and maintained by Juro provide a level of security appropriate to the risk with respect to Customer Personal Data. For the purposes of clause 8.6(c) of the SCCs, personal data breaches will be handled in accordance with paragraph 6.2 of the DPA.

(f) **SCC audits.** Juro will allow Customer (or an independent auditor appointed by Customer) to conduct audits as described in clause 8.9 of the SCCs and, during an audit, make available all information required by the SCCs, both in accordance with paragraph 6.5(c) of the DPA.

(g) **General authorization to use Subprocessors.** Option 2 under clause 9 of the SCCs applies. For the purposes of clause 9(a) of the SCCs, Juro has Customer's general authorization to engage Subprocessors in accordance with paragraph 10.3 of the DPA.

(h) **Notification of New Subprocessors and objection right for New Subprocessors.** Under clause 9(a) of the SCCs, Customer acknowledges and agrees that Juro may engage New Subprocessors as described in paragraphs 10.3 and 10.4 of the DPA. Juro must inform Customer of any changes to Subprocessors using the procedure set out in paragraph 10.4 of the DPA.

(i) **Complaints - redress.** For the purposes of clause 11 of the SCCs, and subject to paragraph 8.2 of the DPA, Juro must inform data subjects on its website of a contact point authorized to handle complaints. Juro must inform Customer if it receives a complaint by, or dispute from, a data subject with respect to Customer Personal Data and must, without undue delay, communicate the complaint or dispute to Customer. Juro does not otherwise have any obligation to handle the request unless otherwise agreed with Customer. The option under clause 11 of the SCCs does not apply.

(j) **Supervision.** Clause 13 of the SCCs applies as follows:

(i) Where Customer is established in an EU Member State, the Supervisory Authority with responsibility for ensuring compliance by Customer with the EU GDPR as regards the data transfer shall act as competent supervisory authority.

(ii) Where Customer is not established in an EU Member State, but falls within the territorial scope of application of the EU GDPR in accordance with its Article 3(2) and has appointed a representative under Article 27(1) of the EU GDPR, the Supervisory Authority of the Member State in which the representative within the meaning of Article 27(1) of the EU GDPR is established shall act as competent supervisory authority.

(iii) Where Customer is not established in an EU Member State, but falls within the territorial scope of application of the EU GDPR in accordance with its Article 3(2) without however having to appoint a representative under Article 27(2) of the EU GDPR, the Irish Data Protection Commission shall act as competent supervisory authority.

(iv) Where Customer is established in the UK or falls within the territorial scope of application of the Applicable Data Protection Laws of the UK (**UK Data Protection Law**), the Information Commissioner's Office (**ICO**) shall act as competent supervisory authority.

(v) Where Customer is established in Switzerland or falls within the territorial scope of application of the Applicable Data Protection Laws of Switzerland (**Swiss Data**

Protection Law), the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Law.

(k) **Notification of government access requests.** For the purposes of clause 15(1)(a) of the SCCs, Juro must notify Customer (only) and not the data subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the relevant data subject(s) as necessary.

(l) **Governing law.** The governing law for the purposes of clause 17 of the SCCs shall be the law that is designated in the governing law section of the Agreement. If the Agreement is not governed by an EU Member State law, the SCCs will be governed by either (i) Irish law; or (ii) where the Agreement is governed by the law of any part of the UK, the laws of England and Wales.

(m) **Choice of forum and jurisdiction.** The courts under clause 18 of the SCCs shall be those designated in the jurisdiction section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with the Agreement, the parties agree that the courts of either (i) Ireland; or (ii) where the Agreement designates any part of the UK as having exclusive jurisdiction, the courts of England and Wales shall have exclusive jurisdiction to resolve any dispute arising from the SCCs. For data subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

(n) **Appendix.** The Appendix to the SCCs shall be completed as follows: The contents of the applicable part of paragraph 1 of Appendix 4 to the DPA shall form Annex I.A to the SCCs. The contents of paragraphs 2 to 9 of Appendix 4 to the DPA shall form Annex I.B to the SCCs. The contents of paragraph 10 of Appendix 4 to the DPA shall form Annex I.C to the SCCs. The contents of paragraph 11 of Appendix 4 to the DPA shall form Annex II to the SCCs.

(o) **Data exports from the UK under the SCCs.** For data transfers governed by UK Data Protection Law, the Mandatory Clauses of the Approved Addendum, being the template addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as revised under Section 18 of those Mandatory Clauses (**Approved Addendum**) shall apply. The information required for Tables 1 to 3 of Part One of the Approved Addendum is set out in Appendix 4 to this DPA (as applicable). For the purpose of Table 4 of Part One of the Approved Addendum, neither party may end the Approved Addendum when it changes.

(p) **Data exports from Switzerland under the SCCs.** For data transfers governed by Swiss Data Protection Law, the SCCs also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as personal data under Swiss Data Protection Law until such laws are amended to no longer apply to a legal entity. In such circumstances, general and specific references in the SCCs to EU GDPR or Member State law shall have the same meaning as the equivalent reference in Swiss Data Protection Law.

(q) **No modification of SCCs.** Nothing in the Agreement is intended to modify or contradict any SCCs or prejudice the fundamental rights or freedoms of data subjects under European Data Protection Law.

(r) **Conflicts.** The SCCs are subject to the DPA and the additional safeguards set out under it. The rights and obligations afforded by the SCCs will be exercised in accordance with the DPA, unless stated otherwise. If there is any conflict or inconsistency between the SCCs and any other part of the DPA, the SCCs take priority.

5. **Requirements for Subprocessor engagement.** European Data Protection Law requires Juro to ensure via a written contract that the data protection obligations described in this DPA, as referred to in Article 28(3) of the EU GDPR, if applicable, are imposed on any Subprocessor engaged by Juro.

CCPA

1. **Additional definitions.**

   CCPA means the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020, together with all implementing regulations.

   Customer Personal Data includes personal information.

   The terms **business**, **business purpose**, **consumer**, **personal information**, **processing**, **sale**, **sell**, **service provider**, and **share** have the meanings given in the CCPA.

2. **Prohibitions.** Without prejudice to Juro's obligations under paragraph 5.2 of the DPA, with respect to the processing of Customer Personal Data in accordance with the CCPA, Juro must not, unless otherwise permitted under the CCPA:

2.1. sell or share Customer Personal Data;

2.2. retain, use or disclose Customer Personal Data: (a) other than for a business purpose under the CCPA on behalf of Customer and for the specific purpose of performing the Services; or (b) outside of the direct business relationship between Juro and Customer; or

2.3. combine or update Customer Personal Data with personal information that Juro receives from or on behalf of a third party or collects from its own interactions with the consumer.

3. **Compliance.** Without prejudice to Juro's obligations under paragraph 5.2 of the DPA or any other rights or obligations of either party under the Agreement, Juro will notify Customer if, in Juro's opinion, Juro is unable to meet its obligations under the CCPA, unless such notice is prohibited by applicable law.

Appendix 4: Description of processing / transfer

1. **List of parties**

A - C2P SCCs

Data exporter: Customer and its authorized affiliates

Address: Set out in the Order Form

Contact person's name, position and contact details: Set out in the Order Form.

Activities relevant to the data transferred under these SCCs: The data importer provides Services to the data exporter under the Agreement. Those Services include the Hosted Services, the Implementation Services and the Support Services (all as defined in the Agreement).

Signature and date: The parties agree that execution of the Agreement constitutes execution of these SCCs by both parties

Role: Controller

Data importer: Juro (as defined in the Agreement)

Address: Set out in the Agreement

Contact person's name, position and contact details: Michael Haynes, Data Protection Officer, support@juro.com

Activities relevant to the data transferred under these SCCs: The data importer provides Services to the data exporter under the Agreement. Those Services include the Hosted Services, the Implementation Services and the Support Services (all as defined in the Agreement).

Signature and date: The parties agree that execution of the Agreement constitutes execution of these SCCs by both parties

Role: Processor

B - P2C SCCs

Data exporter: Juro (as defined in the Agreement)

Address: Set out in the Agreement

Contact person's name, position and contact details: Michael Haynes, Data Protection Officer, support@juro.com

Activities relevant to the data transferred under these SCCs: The data importer provides Services to the data exporter under the Agreement. Those Services include the Hosted Services, the Implementation Services and the Support Services (all as defined in the Agreement).

Signature and date: The parties agree that execution of the Agreement constitutes execution of these SCCs by both parties

Role: Processor

Data importer: Customer and its authorized affiliates

Address: Set out in the Order Form

Contact person's name, position and contact details: Set out in the Order Form.

Activities relevant to the data transferred under these SCCs: The data importer provides Services to the data exporter under the Agreement. Those Services include the Hosted Services, the Implementation Services and the Support Services (all as defined in the Agreement).

Signature and date: The parties agree that execution of the Agreement constitutes execution of these SCCs by both parties

Role: Controller

2. Categories of data subjects whose personal data is transferred

Customer may submit personal data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include personal data relating to the following categories of data subjects:

→ Juro Platform users.

→ Signatories and counterparties to contracts (including external signatories).

→ Anyone whose personal data is included in contracts or other documents processed via the Juro Platform.

3. Categories of personal data transferred

Customer may submit personal data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include the following categories of personal data:

→ Personal data contained in contracts processed by the Juro Platform, including contact details, signatures and personal data of contract counterparties.

→ IP addresses.

→ Geolocation information.

→ User device information.

→ Comments and activity within the Juro Platform.

4. **Sensitive data transferred (if applicable)**

   Customer may submit special categories of data to the Services, the extent of which is determined and controlled by Customer in its sole discretion. Special categories of data are personal data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life of sexual orientation.

   The applicable security measures are described in Appendix 2 to the DPA and in Juro's Trust Center from time to time, or as otherwise made reasonably available by Juro.

5. **Frequency of the transfer**

   Continuous, depending on the use of the Services by Customer.

6. **Nature of the processing**

   Provision of the Services under the Agreement.

7. **Purpose of processing, the data transfer and further processing**

   Juro will process Customer Personal Data as necessary to perform the Services under the Agreement, and as further specified by Customer in its Instructions.

8. **Duration of processing**

   Subject to paragraph 2 of the DPA, Juro will process Customer Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

9. **Subprocessor transfers**

   Subprocessors will process Customer Personal Data as necessary to perform the Services under the Agreement. Subject to paragraph 2 of the DPA, Subprocessors will process Customer Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

   Identities of Subprocessors used to provide the Services and their country or region of location are set out in Juro's privacy policy.

10. **Competent supervisory authority**

    The Supervisory Authority specified in paragraph 4.4(j) of Appendix 3 to the DPA will act as the competent supervisory authority.

11. **Technical and organisational measures**

    Juro will maintain administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Customer Personal Data uploaded to the Services, as described in Appendix 2 to the DPA and in Juro's Trust Center from

time to time. Juro will not materially decrease the overall security of the Services during the term of the Agreement.

Last updated: 7 March 2025