Data Processing Addendum (DPA)

The terms of this data processing addendum (the "**Addendum**") form part of the main agreement (the "**Main Agreement**"), which consists of Validato Ltd.'s (including any company that is from time to time a subsidiary of Validato Ltd.; hereinafter collectively referred to as the "**Validato**") general terms and conditions, as published on its website from time to time, or any specific arrangement between the parties.

The Main Agreement is between the client (the "**Controller**") and Validato (the "**Processor**"; together the "**Parties**") and applies where the Processor processes personal data on behalf of the Controller under the Swiss Data Protection Act, EU General Data Protection Regulation, the United Kingdom General Data Protection Regulation or any other equivalent provision of the data protection laws applicable, unless the Parties have agreed a specific data processing agreement.

1. Purpose

This Addendum sets out the requirements that the Processor has to comply with when processing Personal Data on behalf of the Controller.

In the context of their contractual relationship, both Parties undertake to comply at all times with the Applicable Data Protection Rules.

The Processor shall process Personal Data only on documented instructions from the Controller, unless required to do so by applicable law. In such a case, the Processor shall (to the extent permitted by law) inform the Controller of that legal requirement before processing.

2. Definitions

In this Addendum, the following terms shall have the following meanings:

"**Applicable Data Protection Rules**" means (as applicable) the EU General Data Protection Regulation 2016/679 ("**GDPR**"), the Swiss Federal Act on Data Protection ("**Swiss DPA**"), the United Kingdom General Data Protection Regulation ("**UK GDPR**") and any other data protection laws expressly referenced in the Main Agreement;

"**Data Subject**" means the individual, whose Personal Data are processed pursuant to this Addendum;

"**Instructions**" means the Controller's documented instructions (including by email and in the tool of the Processor) to the Processor regarding the processing of Personal Data;

"**Personal Data**" means any information relating to an identified or identifiable natural person processed under this Addendum; and

"**Sub-processor**" means any third party engaged by the Processor to process Personal Data on behalf of the Controller.

3. Description of Processing Activities

The Processor processes Personal Data solely on behalf of and in accordance with the Controller's instructions for the purpose of providing the service(s) set forth in the Main Agreement (the "**Services**"). The Services include screening/background checks of a Data Subject as instructed by the Controller.

For the avoidance of doubt, this Addendum governs all processing of Personal Data by the Processor in the context of the Services, including any collection, verification, analysis and reporting activities performed as part of screening/background checks.

The Processor does not determine the purposes or essential means of the processing of Personal Data under this Addendum; the Controller remains the sole Controller of such Personal Data.

The Types of Personal Data that can be processed under this Addendum are set out in Appendix A.

Data Subjects include (i) Controller's employees, representatives and authorized users whose Personal Data is processed for account administration and support, and (ii) the individuals to whom the screening/background check relates (e.g., candidates, contractors, clients or other persons whose Personal Data is processed in relation to the rendering of the Services).

4. Duration

This Addendum takes effect on the date of entry into force of the Main Agreement and shall survive termination (for any reason) or expiry of the Main Agreement.

5. Obligations of the Processor (including indemnification of the Controller)

The Processor undertakes vis-à-vis the Controller to:

- process the Personal Data exclusively for the Purpose(s) defined in Section 1 and Section 3 of this Addendum;
- process the Personal Data exclusively in accordance with the Controller's documented (including by email and in the tool of the Processor) instructions;
- guarantee the confidentiality of the Personal Data subject to the instructions and subject to the disclosure of Personal Data to third parties (e.g. former employers, authorities, etc.) to provide the Services;
- ensure that each person authorised by the Processor to process Personal Data , including employees, contractors and other personnel acting under the Processor’s authority, is subject to appropriate confidentiality obligations and receives training appropriate to their role and access rights;
- inform immediately the Controller if the Processor can no longer comply with the terms of this Addendum or the Applicable Data Protection Rules; and
- provide, upon request, to the Controller:
    - documentary evidence of the Processor's continuous compliance with this Addendum and the Applicable Data Protection Rules; and
    - any other document reasonably required by the Controller to establish the Processor's compliance with this Addendum (e.g., copy of the Processor's relevant audit, ISO (International Organization for Standardization) or similar report(s) and/or written confirmations).

Subject to the limitation of liability set forth in the Main Agreement, the Processor shall indemnify and hold harmless the Controller from and against all claims, losses, costs (including reasonable attorney's fees), fines and other financial prejudice incurred by the Controller as a result of any breach, by the Processor, of this Addendum or the Applicable Data Protection Rules. The Processor's indemnification obligation under this Addendum applies only to damages resulting from the Processor's proven intentional or grossly negligent breach of this Addendum. The Processor shall not indemnify the Controller for (i) processing activities carried out under the Processor's independent controller role, (ii) damages caused by inaccurate, incomplete or unlawful data provided by the Controller, its users or a Data Subject, or (iii) damages resulting from the Controller's instructions or failure to comply with applicable data protection laws.

To the extent permitted by applicable law, the Processor shall not be liable to the Controller for damages, losses, claims, costs or regulatory consequences arising from the Controller's breach of its obligations as controller, including where such damages arise from the absence of a valid legal basis, insufficient transparency towards Data Subjects, inaccurate or unlawful Personal Data provided by or on behalf of the Controller, or unlawful instructions issued by the Controller. Nothing in this Addendum limits any liability that cannot be limited under Applicable Data Protection Rules or affects the statutory rights of Data Subjects.

6. Obligations of the Controller

The Controller undertakes vis-à-vis the Processor to:

- ensure that it has a valid legal basis for all Personal Data submitted or made available to the Processor for the Services;
- ensure that any processing of special categories of Personal Data, criminal-offence or criminal-conviction data, background-check data or other sensitive information is lawful, necessary, proportionate and permitted under the Applicable Data Protection Rules and any applicable employment, labour, regulatory or sector-specific laws;
- provide Data Subjects with all required privacy notices and transparency information before instructing the Processor to perform the Services, unless an exemption under applicable law applies;
- provide clear, lawful and documented instructions to the Processor and ensure that such instructions remain compliant with Applicable Data Protection Rules;
- ensure that Personal Data provided to the Processor is accurate, relevant, limited to what is necessary and lawfully obtained;
- promptly inform the Processor of any change in law, instruction, scope, retention requirement or Data Subject request that may affect the Processor's processing of Personal Data;
- ensure that its authorised users use the Processor's platform and Services in compliance with Applicable Data Protection Rules; and
- carry out any necessary export, download or preservation of Customer Data before expiry or termination of the Services, unless otherwise agreed in writing.

7. Sub-processors

The Controller agrees that the Processor may engage Sub-processors to carry out specific processing activities on behalf of the Controller. The Processor maintains a publicly accessible and up-to-date list of Sub-processors at validato.com/sub-processors (the "**Sub-processor List**"), including any wholly owned entity of the Processor within the EEA or Switzerland. In the event

the Sub-processor List is temporarily unavailable online, the current list is available upon request.

Prior to engaging any new Sub-processor not already on the Sub-processor List, the Processor shall provide the Controller with at least 30 days' advance written notice by email. The Controller has the right to object to the engagement of such Sub-processor within that period. No Personal Data shall be transferred to that Sub-processor until the notice period has expired without objection, or until any objection raised has been resolved.

In connection with the Processor's Services relating to screening and background checks, the Processor maintains a separate list of Sub-processors engaged for specific checks (the "**Screening Sub-processor List**"). This list may vary on the time and scope of the Controller's order.

Given the commercially sensitive nature of the Processor's sourcing relationships, the Screening Sub-processor List is treated as confidential information and is made available to the Controller upon request, subject to confidentiality obligations no greater than those already applicable under the Main Agreement.

Sub-processors on the Screening Sub-processor List are engaged solely where the relevant source of information is unable to provide data directly to the Processor, or where no direct source exists. The Processor's standard practice is to verify information directly at source including official registers, public authorities, and issuing institutions, wherever this is technically and operationally feasible. Therefore, the engagement of Sub-processors for verification purposes is the exception rather than the standard mode of service delivery.

The Processor shall ensure that each Sub-processor is bound by data protection obligations that are no less protective than those set out in this Addendum, to the extent applicable to the services provided by that Sub-processor. The Processor remains responsible to the Controller for the performance of each Sub-processor's data protection obligations.

8. Cross-border Transfer

8.1. Cross-border transfer to Processor

If the Processor is located in a country in respect of which no finding of adequacy by the Swiss Data Protection and Information Commissioner or no EU adequacy exists, the Parties agree to incorporate into this Addendum the standard contractual clauses for the transfer of personal data to processors established in third countries (Commission Implementing Decision (EU) 2021/914), in the form adopted by the European Commission, as these standard contractual clauses may be amended or replaced from time to time (the "**Model Clauses**").

8.2. Cross-border transfer to Sub-processors

The Processor may, with the prior written consent (including by email and in the tool of the Processor) of the Controller in conformity with Section 6 above, transfer Personal Data to a Sub-processor located in a country outside of the European Economic Area (EEA), UK or Switzerland in the following situations:

- transfer to a country, territory or sector in respect of which there is a current European Community and Swiss finding of adequacy of protection in data protection matters;
- where no finding of adequacy exists, and to the extent necessary, the Controller hereby expressly authorizes and instructs the Processor to sign, with the Sub-processor located

in a country outside of the EEA, UK or Switzerland, in the Controller's name and on its behalf, the Model Clauses, and taking into account any additional requirement which may be imposed by a competent data protection supervisory authority and/or a competent court (it being understood that the Processor warrants to the Controller that any such transfer of Personal Data is made in accordance with the Applicable Data Protection Rules, as interpreted from time to time by the competent data protection supervisory authorities and the competent courts);

- equivalent means of compliance implemented by the Processor are in place to ensure that the transfer of Personal Data is made in full compliance with the Applicable Data Protection Rules (as interpreted by the competent data protection supervisory authorities and the competent courts); and
- if such transfer is mandatorily required by European Union, Swiss, UK or national law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before such transfer, unless the applicable European Union, Swiss, UK or national law prohibits such information on important grounds of public interest.

If any of the mechanisms for cross-border transfers of Personal Data referred to above is found by a competent authority and/or under Applicable Data Protection Rules to be an invalid means of complying with the restrictions on transferring Personal Data outside of the EEA, UK or Switzerland as set out in the Applicable Data Protection Rules, the Parties shall negotiate in good faith the implementation of an alternative solution to enable the Party transferring the Personal Data to comply with the provisions of the Applicable Data Protection Rules in respect of any such transfer.

9. Provision of Information to the Data Subjects

The Controller shall provide the Data Subjects with the information required pursuant to the Applicable Data Protection Rules.

If a Data Subject contacts the Processor to exercise one of his/her rights, the Processor shall immediately forward such request (and all other relevant information) to the Controller. Unless instructed in writing by the Controller, the Processor shall not respond directly to a request received from a Data Subject. The Processor shall assist the Controller, upon request, in handling Data Subject requests in accordance with the Applicable Data Protection Rules.

10. Notification of a Personal Data Breach

The Processor shall notify the Controller without undue delay and in any event within 48 hours after becoming aware of a Personal Data Breach.

The notification shall include, to the extent available at the time:

- a description of the nature of the breach (including categories and approximate number of affected data subjects and records, where feasible);
- likely consequences of the breach;
- measures taken or proposed to address the breach and mitigate possible adverse effects; and
- contact details for the Processor's incident response point of contact.

The Processor shall keep the Controller informed of material developments and shall cooperate in good faith to enable the Controller to comply with its breach notification and communication obligations.

Notices under this Section shall be sent to: gdpr@validato.com and info@validato.com.

11. Assistance by the Processor to the Controller

The Processor undertakes to assist the Controller (i) regarding investigations initiated by, or prior consultations with, the competent data protection supervisory authorities, (ii) with respect to the notification of a data breach to the supervisory authorities and the communication to the Data Subjects and (iii) with the establishment of a data protection impact assessment.

The Processor undertakes to make available to the Controller all information and documentation necessary to allow the Controller to demonstrate its compliance with its obligations under the Applicable Data Protection Rules.

The Processor shall allow the Controller, or a third party retained by the Controller, to audit and inspect the Processor. Except in case of emergency (such as in relation to a request of a competent supervisory authority or in case of Personal Data breach), an audit may be carried out only during normal working hours, with no less than 10 (ten) days' prior written notice. The scope of the audit shall be limited to matters relevant to this Addendum. The Controller shall bear the costs of any audit. If an audit determines that the Processor has breached any of its obligations under this Addendum, the Processor will promptly remedy the breach at its own cost.

12. Return / Destruction of the Personal Data

Upon expiry of the Main Agreement, the Processor shall securely delete the Personal Data in a demonstrable manner and in accordance with the Applicable Data Protection Rules within 120 days, unless a mandatory statutory obligation applicable to the Processor requires storage of the Personal Data.

The Processor shall confirm in writing to the Controller that the Processor has not kept any copy of the Personal Data, except if the Processor is under a mandatory statutory obligation to retain a copy of the Personal Data. In this latter case, the Processor undertakes that:

- the confidentiality of all such Personal Data is ensured; and
- such Personal Data is only processed as long as necessary for the purpose(s) specified in the mandatory statutory obligation requiring its storage.

13. Record of Data Processing Activities

The Processor shall maintain a record of data processing activities carried out on behalf of the Controller, in accordance with Article 30 (2) GDPR and Article 12 of the Swiss Data Protection Act.

14. Security measures to be implemented by the Processor

The Processor undertakes to take all appropriate technical and organizational security measures, required pursuant to Article 32 GDPR and Article 8 of the Swiss Data Protection Act (as applicable), as set out in Appendix B (the "**Security Measures**") in order to ensure a level of security appropriate to the risks, including, if so required:

- a process to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and Services;
- a process to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
- measures to guarantee that any person under the authority of the Processor, who has access to Personal Data, processes the Personal Data only in accordance with the Controller's instructions; and
- any other measure set forth in this Addendum or in the Controller's instructions.

The Processor shall maintain and regularly review the Security Measures, as necessary to keep such measures up-to-date, effective and adequate with respect to the sensitivity of the Personal Data.

The Processor takes part in a certification mechanism (as defined in Article 13 of the Swiss Data Protection Act or Article 42 GDPR (if applicable)). The certification mechanism relied upon by the Processor is ISO 27001.

For the duration of the Main Agreement, the Processor undertakes to continuously fulfil the relevant requirements of its ISO 27001 certification and to renew such certification prior to its expiration. Upon request, the Processor shall provide the Controller with evidence of the valid ISO 27001 certification. The Processor shall inform the Controller without undue delay if the ISO 27001 certification is not renewed, expires without renewal, is suspended or is withdrawn.

15. Controller and Processor Roles

For all Personal Data processed under this Addendum in connection with the Services (including screening/background checks), the Controller is the controller, and the Processor is the processor.

The Processor may process limited business contact data of the Controller's authorised users and representatives (e.g., name, business email, phone number, role, billing and support communications) as an independent controller for account administration, billing, fraud prevention and compliance purposes. Such processing is governed by the Processor's privacy notice and applicable law.

16. Jurisdiction and Applicable Law

The forum selection clause set out in the Main Agreement shall apply to this Addendum.

The choice of law clause set out in the Main Agreement shall apply to this Addendum.

APPENDIX A – Categories of Personal Data

Identification data

- first name
- last name
- date and place of birth
- nationalities
- residence
- legal guardianship
- civil status
- first and last name of parents
- identity card
- passport
- email address
- phone number
- age
- gender
- work permits
- national identification number

KYC data

- professional activity
- public functions (local and international PEP, international and sport organisations etc.)
- criminal record extract
- debt collection register/financial integrity
- personal credit rating

Habits and relationships data

- leisure time activities
- particular behaviour or social contacts
- family and registered partnership
- memberships in associations (other than related to politics, religion, trade union)

Career related data

- CV
- working certificates
- degrees
- references
- external mandates
- representation powers

Personal characteristics data

- political opinions

Biometric data

A facial scan of the individual (live capture from multiple angles)

APPENDIX B – Security Measures

1. Governance & Policies

- Information security policies, risk management, and periodic review.
- Confidentiality obligations for staff and contractors.

2. Access control

- Role-based access control (least privilege), MFA for administrative access.
- Strong authentication, secure password policies, periodic access reviews.

3. Encryption

- Encryption in transit (TLS) and encryption at rest for stored Personal Data, where applicable.
- Key management controls and restricted access to keys.

4. Logging & monitoring

- Security logging for access and administrative actions.
- Monitoring/alerting for suspicious activity.

5. Vulnerability & patch management

- Regular vulnerability scanning and timely security patching.
- Secure configuration baselines.

6. Secure development & change management (if applicable)

- Change control, peer review, separation of environments.
- Security testing proportionate to risk.

7. Backup & recovery

- Regular backups where applicable; recovery testing.
- Disaster recovery and business continuity measures proportionate to risk.

8. Incident response

- Documented incident response process, breach escalation paths.
- Post-incident review and corrective actions.

9. Sub-processor security

- Due diligence and contractual security obligations; monitoring of compliance.

10. Data minimisation & retention

- Logical separation between customers; retention controls per Section 11.