Subject to change, sometimes significantly

SPECIAL TERMS OF USE FOR – CERTIFIO ID® (hereinafter the "Special Terms")

Between SOLUTIONS NOTARIUS INC., doing business as "Portage CyberTech," with a place of business at 465 McGill Street, Suite 300, Montreal, Quebec, Canada, H2Y 2H1 ("Portage"), and you (hereinafter "you," the "Client," the "Purchaser," or the "End User," as applicable) (individually referred to as a "Party" and collectively referred to as the "Parties").

Portage has developed and markets a web application for remote identity verification and certain related validations, including, in particular, document verification, biometric verification, banking verification, and AML screening features (the "Solution" or "CertifiO ID").

CertifiO ID is a technological tool designed to assist with identity verification, enabling, in particular, the generation of results, verification reports, and evidence associated with the verification process conducted via the Solution.

In exchange for payment of the applicable fees, Portage grants you a non-exclusive, non-transferable, and non-assignable license to use the CertifiO ID Solution, in whole or in part, in accordance with the terms and conditions set forth below.

By subscribing to CertifiO ID and/or using it, you acknowledge that you have read, understood, and accepted these Special Terms and Conditions.

1. GENERAL PROVISIONS

THESE SPECIAL TERMS AND CONDITIONS SUPPLEMENT THE GENERAL TERMS AND CONDITIONS, WHICH ARE DEEMED TO BE AN INTEGRAL PART OF THESE TERMS AND CONDITIONS AND JOINTLY GOVERN YOUR USE OF CERTIFIO ID.

1.1 The CertifiO ID Solution allows Buyers to verify the identity and/or perform certain related validations regarding End Users. The features offered may include, in particular:

- Identity verification using official documents and, where required, biometric data;
- Bank verification through a third-party technology provider integrated into the Solution;
- Screening related to the fight against money laundering and terrorist financing ("AML Screening");
- The collection, processing, transmission, and temporary operational storage of certain information, documents, or data necessary for the operation of the Solution and the verification process;
- The generation of results, Verification Reports, and evidence associated with the verification process;
- Certain features for the secure transmission of results or Verification Reports to third parties authorized by the Purchaser.

Certain features of the Solution may be provided directly or indirectly by third-party technology providers integrated into the Solution.

1.2 To be authorized to use the CertifiO ID Solution, your organization or professional must first have opened an account with Portage, which enables, among other things, the management of access, users, permissions, and applicable login credentials.

1.3 The Purchaser remains solely responsible for:

- determining the legal, regulatory, professional, or internal obligations applicable to its activities;
- retaining audit reports, results, consents, evidence, or other information it deems necessary;
- for implementing its own archiving, retention, and destruction policies.

Unless expressly stated otherwise in a separate written agreement, CertifiO ID does not act as a regulatory archiving system, legal deposit, or long-term retention service.

2. DEFINITIONS

Terms not defined in these Special Terms and Conditions have the meanings assigned to them in the General Terms and ConditionsHYPERLINK "https://www.portagecybertech.com/fr/conformite-gouvernance" \l "conditions_generales".

2.1 AML (Anti-Money Laundering) **Screening**: refers to the automated verification of certain information relating to an individual, in particular to determine whether that individual appears on sanctions lists, is identified as a politically exposed person (PEP), or is associated with high-risk media sources, in accordance with applicable legal and regulatory requirements.

2.2 Biometrics: Personal data resulting from technical processing of a natural person's physical, physiological, or behavioral characteristics, enabling or confirming the unique identification of a natural person (e.g., facial recognition based on a selfie).

2.3 Consent: As defined by applicable privacy laws, including notably Quebec's Bill 25, specific, express, informed, unambiguous, and freely given consent by an individual, through a clear and affirmative act, for specific purposes. In the context of remote identity verification, this specifically refers to the voluntary, informed, and specific expression by which the end user unequivocally accepts the processing of sensitive personal data, including biometric data.

2.4 Displayed Result: Information displayed on the screen for informational purposes in the Solution's user interface, which may include certain statuses, indicators, or verification results.

2.5 Evidence: Data, screenshots, logs, metadata, technical artifacts, or information collected or generated as part of a verification process.

2.6 End User: A natural person whose identity or bank account is verified via CertifiO ID, at the request of a Purchaser.

2.7 Purchaser: An organization, company, or professional authorized to use CertifiO ID to perform a Verification Process with respect to an End User.

2.8 Set of identification information: refers to the username, online ID (or any other identifier), access code, password, security questions and answers, authentication token , or any other identity verification information necessary for the Customer and its members to directly access their Account(s) and End User Data on, via, or from the Solution.

2.9 Technology Provider: A third-party service provider or supplier integrated into the Solution to enable certain features or processes related to the Verification Process.

2.10 Verification Process: All operations performed via the Solution to validate the authenticity of an identity document, compare biometric data, or perform certain banking validations.

2.11 Verification Report: A structured document generated following an identity verification process via the Solution, which may include, in particular, verified information, verification results, evidence, technical metadata, audit logs, as well as certain mechanisms that may help ensure its integrity, traceability, timestamping, or digital signature.

3. RESPONSIBILITIES AND OBLIGATIONS OF THE BUYER

As a Buyer, you acknowledge, agree, and undertake, in particular, to:

3.1 Make the appropriate declarations to the Commission d'accès à l'information (CAI):

- submit, when required, any applicable declaration, analysis, assessment, or formality to the Commission d'accès à l'information ("CAI") or any other competent authority prior to the product's commissioning; and
- ensure that the use of biometrics complies with your legal and regulatory obligations.
- *Portage cannot be held liable for the Buyer's failure to fulfill these obligations*.

3.2 Use CertifiO ID in accordance with these Terms and not to:

- Access or attempt to access unauthorized accounts or data;
- Provide false information or falsify documents;
- Use the platform for fraudulent or illegal purposes;
- Use the Solution in a manner that could compromise its security, integrity, availability, or proper functioning;
- Conducting penetration tests without written authorization.

3.3 Manage end users' access, permissions, and authorizations regarding the Solution, for example by inviting them to use the tool for your purposes and revoking their rights at the appropriate time;

3.4 Establish and maintain policies and other internal administrative practices designed to prevent any unauthorized access, use, modification, or disclosure;

3.5 Assume sole responsibility for decisions, actions, or conclusions made based on the results, audit reports, or information generated by the Solution. The results generated via the Solution are intended as audit support tools and do not replace the Buyer's judgment, analysis, or decision-making obligations. The Purchaser remains solely responsible for the interpretation, use, and retention of the results obtained via CertifiO ID, as well as for any communication or decision made regarding an End User;

3.6 Ensure the retention, protection, and security of any information, Audit Report, result, or evidence extracted or obtained via the Solution;

3.7 Protect the confidentiality of your login credentials in accordance with applicable security best practices, and use them solely to access the Solution or its accessories, and never share them with third parties.

3.8 Contact Portage as soon as possible if you wish to upgrade your package or modify your subscription plan.

3.9 Comply with the API usage rules (if applicable):

3.9.1 Obtain API credentials (an API Key and an API Secret) from Portage in connection with CertifiO ID;

3.9.2 You are solely responsible for all activities associated with these API credentials, whether or not you were aware of such activities;

3.9.3 Keep your API credentials in a secure location, use them only as the sole means of accessing the CertifiO ID API, and never share your API Secret with third parties.

3.9.4 Ensure that all passwords and other access credentials are kept strictly confidential and are not shared with any unauthorized person.

3.9.5 Be solely responsible for the integration, use, and authentication of End Users via the CertifiO ID API, as well as for the security controls implemented in connection with such use.

3.9.6 Contact Portage as soon as possible if you wish to increase your transaction limit.

Any breach of these obligations may result, depending on the severity of the situation, in the temporary or permanent suspension of access to the Solution, as well as any other measures or remedies available under the Terms of Use or applicable laws.

4. RESPONSIBILITIES AND OBLIGATIONS OF THE END USER

As an End User, CertifiO ID allows you, in particular, to participate in a Remote Identity Verification Process and, where applicable, in certain related validations, including, in particular, banking validations or AML screening, at the request of a Buyer.

As part of this Verification Process, your active participation and the provision of certain information may be required. Consequently, you:

4.1 Confirm that the credentials used as part of the verification process, including your email address and/or phone number, are active, accurate, up-to-date, complete, and under your control. You agree to notify the Buyer of any relevant changes when required;

4.2 Confirm that the identification documents provided are valid, authentic, and issued by a recognized competent government authority;

4.3 Consent to the collection, use, and processing of your personal information, including certain biometric data when required, as part of the Verification Process and in accordance with these Terms of Use and applicable laws;

4.4 Notify the Buyer as soon as possible if you experience technical difficulties or find that you are unable to complete the Verification Process.

4.5 Do not:

- Access or attempt to access unauthorized accounts or data;
- Provide false information or falsify documents;
- Use the Solution in a manner that could compromise its security, integrity, or proper functioning;
- Use the platform for fraudulent or illegal purposes.

5. PORTAGE'S RESPONSIBILITIES AND OBLIGATIONS

5.1 Provision of the Solution. Subject to payment of all applicable fees and compliance with all Terms of Use, including these Special Terms, Portage shall provide the Solution to the Purchaser and shall use commercially reasonable efforts to ensure that it is delivered substantially in accordance with its applicable Specifications. The Purchaser further acknowledges that certain features of the Solution may be provided directly or indirectly, in whole or in part, by third-party technology providers. Portage reserves the right to modify, replace, add, or remove certain features, technology providers, or components of the Solution as part of the normal evolution of the product, subject to applicable laws and applicable agreements with the Purchaser.

5.2 Security and Compliance. Portage implements security measures in accordance with applicable best practices to ensure the security, integrity, and confidentiality of the Solution and the data processed as part of the Verification Process. Certain features of the Solution may, in particular , include mechanisms for document verification, biometric verification, banking verification, or AML screening carried out directly or indirectly through third-party Technology Providers integrated into the Solution.

5.3 Limitations. Portage does not guarantee that every Verification Process will result in validation, a positive result, or the absence of fraud, error, identity theft, or attempts to circumvent the system. Certain automated validations, analyses, or comparisons performed via the Solution have limitations inherent to the technologies used and may, in particular, generate inaccurate, incomplete, false-positive, or false-negative results. The results generated by the Solution are verification support tools and do not replace the Buyer's judgment, analysis, or decision-making obligations. Portage cannot be held liable for any decisions, actions, or omissions taken by a Buyer, an End User, or a third party based on the results, Verification Reports, or information generated by the Solution.

5.4 Prevalence of the Verification Report. The results, statuses, indicators, or information displayed in the Solution's user interface are provided for informational and operational purposes only. In the event of a discrepancy between the information displayed in the Solution's user interface and the Verification Report generated by the Solution, the Verification Report shall prevail. The Purchaser acknowledges that the Verification Report constitutes the primary artifact reflecting the Verification Process performed via the Solution and may include, in particular, evidence, technical metadata, audit logs, as well as certain mechanisms designed to help ensure the integrity, traceability, timestamping, or digital signature of the Verification Report.

5.5 No Regulatory Warranty. CertifiO ID is a technological tool designed to assist with identity verification and certain related validations. Portage does not warrant that the use of the Solution alone will enable a Purchaser to satisfy its legal, regulatory, professional, or industry-specific obligations. Each Purchaser remains solely responsible for assessing the Solution's suitability for its needs and for determining any additional controls, validations, processes, or verifications it deems necessary.

5.6 No Guaranteed Service Level. At this time, no formal contractual service level agreement ("SLA") is offered with respect to the Solution. Portage will use commercially reasonable efforts to ensure the general availability and proper functioning of the Solution. Certain features of the Solution may depend on third-party technology providers and remain subject to their respective availability, limitations, or interruptions. As part of the Solution's ongoing evolution, Portage may eventually implement certain operational metrics, performance targets, or service monitoring mechanisms in connection with specific offerings or agreements.

6. CONSENT

6.1 Explicit Consent to Identity Verification. Prior to any use of the Solution, the End User must provide explicit consent regarding the Verification Process, including, where applicable, certain regulatory validations or AML Screening. The User expressly consents to Portage collecting, using, processing, and retaining certain personal information, including, in particular, the information appearing on their official identification documents, as part of the Verification Process and in accordance with these Terms of Use and applicable laws. This in al information will be retained only for as long as is reasonably necessary for the purposes of the Verification Process and to meet applicable legal, regulatory, security, audit, or retention obligations, and will then be deleted, anonymized, or destroyed in accordance with Portage's applicable policies.

6.2 Consent to the Use of Biometric Data. As part of the Verification Process, the User may be asked to provide a facial image or certain biometric information for the purpose of biometric comparison with the photo on an official ID. This data is considered biometric information within the meaning of applicable privacy laws, including notably Quebec's Bill 25. The User expressly consents to the collection, use, processing, and temporary storage of certain biometric data, including, in particular, the capture and analysis of images as part of liveness tests and facial comparisons, for the purposes of the Verification Process. This biometric data will be processed securely and will be retained only for as long as is reasonably necessary for the applicable purposes of the Verification Process, security, audit, or compliance, after which it will be deleted, anonymized, or destroyed in accordance with Portage's applicable policies and applicable laws.

6.3 Separate explicit consent will be requested from the User prior to any collection or use of biometric data.

6.4 If the User does not wish to provide consent regarding the Verification Process or the use of biometric data, they must contact the organization that requested the verification directly to determine whether an alternative method can be offered.

7. COLLECTION AND USE OF INFORMATION

7.1 The information and data collected as part of the Solution are limited to those reasonably necessary for the operation of the Solution, the Verification Process, security, fraud prevention, applicable legal or

regulatory obligations, as well as related support, compliance, and audit operations. This may include, in particular, certain technical logs, security logs, metadata, access logs, system events, or operational information necessary for the security, integrity, technical support, or audit of the Solution.

7.2 As part of the process of verifying a End User's identity, Portage may use the identification documents submitted via the Solution to, among other things, perform certain document validations, assess potential indicators of fraud, and enable the Purchaser to conduct the requested verifications. In this context, certain information contained in the submitted documents may be extracted, used, analyzed, processed, or transmitted to third-party technology providers integrated into the Solution, including, in particular: name, date of birth, document number, nationality, document type, gender, certain issuance or expiration dates, and the photograph appearing on the identity document. The results of the Verification Process may then be communicated to the Buyer in accordance with these Terms of Use. Certain validations, analyses, or comparisons performed as part of the Verification Process may be carried out automatically using algorithms, validation engines, or technologies operated by Portage or third-party technology providers.

7.3 A Verification Report may be generated upon completion of the Verification Process and transmitted to the Buyer in accordance with the applicable settings of the Solution.

7.4 As part of the Verification Process, certain biometric or liveness detection features ("liveness tests") may be used, in particular to confirm that an interaction is coming from a real person and to enable certain biometric comparisons with the identity documents provided. This processing may be carried out directly or indirectly through third-party technology providers integrated into the Solution, including notably Yoti. Your explicit and prior consent is required before any collection or use of biometric data. If you do not wish to provide this consent, you must contact the Purchaser who requested the verification to determine whether an alternative method can be offered. Certain processing related to biometric features may be performed on infrastructure or servers located outside of Quebec or Canada, including notably in the United Kingdom, in accordance with applicable laws and applicable contractual mechanisms for the protection of personal information. Processing performed by third-party technology providers also remains subject to their own terms of use, privacy policies, and applicable data processing practices. Portage implements reasonable measures to select Technology Providers that offer appropriate safeguards regarding security and the protection of personal information, but cannot be held liable for processing carried out independently by these third parties in accordance with their own applicable terms.

8. ACCESS AND USE

8.1 The End User must be legally authorized to consent to the Verification Process as well as to the collection, use, and processing of their personal information in accordance with applicable laws.

8.2 In the case of an End User who is a minor or otherwise unable to consent in accordance with applicable laws, the Buyer remains solely responsible for obtaining any required parental, legal, or regulatory authorization, consent, or approval prior to using the Solution.

9. PRICING, BILLING, AND PAYMENT

9.1 The fees applicable to the Solution may be indicated on Portage's website, in a commercial proposal, a purchase order, an account opening form, or any other applicable contractual agreement entered into with the Purchaser.

9.2 Billing may be based on usage, subscription, per transaction, purchase of credits or bundles, or any other terms set forth in an applicable agreement with the Purchaser.

9.3 Any verification attempt, transaction, API call, use of a feature, or consumption of a service performed via the Solution may be recorded for billing purposes in accordance with the terms applicable between Portage and the Purchaser, including, in particular, certain document, biometric, banking, or AML screening checks performed directly or indirectly by third-party technology providers, even when the Verification Process is not completed, fails, is interrupted, abandoned, or does not result in a positive outcome.

9.4 Unless otherwise specified in a specific agreement entered into with Portage, services are billed on a prepaid basis and may be paid by credit card or any other payment method accepted by Portage.

9.5 Any specific agreement providing for post-consumption billing or different payment terms shall prevail over these provisions. Unless otherwise specified in such an agreement, invoices are payable within thirty (30) days of their issuance date.

9.6 Certain features of the Solution may depend on third-party technology providers and be subject to fees, usage limits, transaction quotas, or specific terms that may change over time. Portage reserves the right to adjust the commercial terms applicable to these features in accordance with the Terms of Use or any applicable agreement with the Purchaser.

10.DATA PROCESSING AND RETENTION

10.1 The information and data processed in connection with the Solution may be hosted, processed, or accessed in Canada or in other jurisdictions in accordance with applicable privacy laws, as well as the applicable contractual mechanisms and safeguards implemented by Portage and its Technology Providers.

10.2 Portage implements reasonable security measures that comply with applicable best practices to protect the information and data processed in connection with the Solution, including, in particular, certain measures for encrypting data in transit and at rest, where applicable. Portage also seeks to limit the retention of information and data to the minimum reasonably necessary for the applicable purposes of the Verification Process, security, compliance, auditing, or operation of the Solution.

10.3 Unless otherwise specified in a specific agreement entered into with the Purchaser or where a different period is required by applicable laws, certain operational data related to the Verification Process may be retained for a maximum period of approximately thirty (30) days following the applicable processing. The Buyer remains solely responsible for the archiving, long-term retention, and protection of any Audit Reports, results, or evidence that it wishes to retain.

11.SUSPENSION OR TERMINATION

11.1 Portage may, at its discretion and in accordance with the applicable Terms of Use, suspend, limit, or terminate access to the Solution or certain features thereof in the event of, among other things:

- failure to comply with these Terms of Use;
- fraudulent, abusive, or unlawful use of the Solution;
- a security risk, a breach of the Solution's integrity, or a regulatory risk;
- in the event of a default;
- or to comply with a legal or regulatory obligation or a request from a competent authority.

Where reasonably possible under the circumstances, Portage will provide prior notice to the Buyer before such suspension or termination.

11.2 Subject to applicable laws, security, audit, compliance, or retention obligations, as well as reasonable operational limitations of the Solution and third-party technology providers, the Purchaser may request the closure of their account as well as the deletion or anonymization of certain data associated with it in accordance with Portage's applicable policies.

11.3 The End User must direct any request regarding their personal information, including, without limitation, any request for access, correction, or deletion, directly to the Purchaser who requested the Verification Process, unless otherwise required by applicable laws.

12.CONFIDENTIALITY AND SECURITY

12.1 Portage does not sell personal information processed in connection with the Solution. Personal information may, however, be disclosed, processed, used, or made accessible:

- when required for the purposes of the Verification Process or the operation of the Solution;
- to third-party technology providers integrated into the Solution;
- when required by applicable laws;
- or with the applicable consent of the User concerned.

12.2 To the extent permitted by applicable laws, Portage may notify the Purchaser of any request, order, or requirement from a competent authority regarding the information or data processed in connection with the Solution, except where such disclosure is prohibited by law or an applicable order.

13.INTEGRATION OF THIRD-PARTY PROVIDERS

The Solution may integrate certain technologies, services, or features provided directly or indirectly by third-party technology providers, including, notably, Yoti for certain biometric features and Flinks for certain banking validations.

As part of the Verification Process, certain information or data may be transmitted, processed, used, or made available to these third-party technology providers to enable the execution of the applicable features of the Solution.

Subject to change, sometimes significantly

These third-party technology providers may also use their own suppliers, subcontractors, or technological infrastructure in accordance with their operational practices and applicable terms and conditions.

The processing carried out by these third-party technology providers remains subject to their own terms of use, privacy policies, data processing practices, and applicable legal obligations. Certain features of the Solution may also depend on technologies, interfaces, APIs, software components, or services operated by these third-party technology providers.

Portage makes reasonable efforts to select Technology Providers that offer appropriate safeguards regarding security and the protection of personal information, but cannot be held liable for processing carried out independently by these third parties in accordance with their own applicable terms.

When required for the use of certain features of the Solution, the End User may be asked to review and accept the applicable terms of use or privacy policies of certain third-party technology providers.

Additional information regarding certain third-party Technology Providers can be found at the following addresses:

- Yoti: https://www.yoti.com/terms/organisations and https://www.yoti.com/privacy/
- Flinks: https://www.flinks.com/terms-and-conditions and https://www.flinks.com/privacy-policy#services-privacy-statement-2

Effective Date: May 22, 2026