Terms and Conditions

Identity Verification Services – End User Terms and Conditions and Privacy Notice
Chmod LLC
Last updated: September 25, 2026

1. Introduction and Acceptance

1.1 These Terms and Conditions, which incorporate the privacy and data protection notice set out herein (collectively, these "**Terms**"), constitute a legally binding agreement between you and Chmod LLC, a limited liability company organized and existing under the laws of the State of Delaware, United States of America ("**Chmod**", "**we**", "**us**" or "**our**"). These Terms govern your access to and use of the Service and set out the terms upon which Chmod collects, uses, discloses, stores and otherwise Processes your Personal Data, including your Biometric Data, in connection with each Verification.

1.2 Chmod provides identity verification technology to businesses and other organizations. The Service is being made available to you because a Business has requested the verification of your identity and has engaged Chmod, directly or indirectly, for that purpose. The verification flow may display the name, trademarks, color schemes or other branding of the Business rather than those of Chmod; in all such cases, the Service remains provided by Chmod and these Terms continue to apply. Chmod does not charge you any fee for the Service.

1.3 By selecting the button or other interface element presented to you for the purpose of accepting these Terms, or by otherwise commencing, continuing or completing a Verification, you: (a) acknowledge that you have read and understood these Terms and agree to be bound by them; (b) give the consents and authorizations set out in Article 16; and (c) make the representations and warranties set out in Article 17. If you do not agree to these Terms, you must not proceed with the Verification, and you may contact the Business to inquire whether an alternative means of verifying your identity is available.

1.4 These Terms govern only the Service. Your underlying relationship with the Business — including, without limitation, the opening or maintenance of any account, the provision of any product or service, or your access to any platform — is governed exclusively by the Business's own terms and privacy policy, over which Chmod exercises no control. The Business may present you with additional notices or request additional consents of its own. In the event of any inconsistency, the Business's privacy policy shall govern the Business's Processing of your Personal Data, and these Terms shall govern Chmod's Processing of your Personal Data.

1.5 Nothing in these Terms excludes, limits or otherwise deprives you of any right or protection conferred upon you by any mandatory provision of Applicable Law, and these Terms shall be read subject to Article 26 in all respects.

2. Definitions and Interpretation

2.1 In these Terms, the following capitalized terms shall have the meanings set out below:

"**Applicable Law**" means all laws, statutes, regulations, regulatory requirements, codes and binding orders of any governmental, regulatory or judicial authority, in each case as applicable from time to time to a party, to the Service or to the Processing of Personal Data under these

Terms, including all Data Protection Laws.

"**Biometric Data**" means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, whether or not such data alone allows or confirms the unique identification of that person, including facial images and recordings insofar as so processed, facial-geometry templates and other mathematical representations of facial features, and liveness and facial-comparison measurements derived therefrom, however such data may be denominated under Applicable Law (including as "biometric identifiers", "biometric information", "faceprints" or "sensitive personal data").

"**Business**" means the company, organization or other legal entity that has requested the verification of your identity and in connection with whose products, services or platform the Verification is performed, together with any affiliate of that entity designated by it for the purposes of the Verification.

"**Controller**" means the person or entity that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, however such role may be denominated under applicable Data Protection Laws.

"**Data Protection Laws**" means all Applicable Law relating to privacy, data protection, data security, Biometric Data or the confidentiality of communications.

"**End User**", "**you**" or "**your**" means the natural person whose identity is the subject of a Verification.

"**Identity Document**" means a government-issued identity document presented by you in the course of a Verification, including, by way of example, a national identity card, passport, driver's license or residence permit.

"**Personal Data**" means any information relating to an identified or identifiable natural person, or that is otherwise defined or regulated as "personal data", "personal information" or an equivalent term under applicable Data Protection Laws.

"**Process**" and "**Processing**" mean any operation or set of operations performed upon Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, combination, restriction, erasure and destruction.

"**Processor**" means the person or entity that Processes Personal Data on behalf of a Controller, however such role may be denominated under applicable Data Protection Laws.

"**Result**" means the output generated by the Service in respect of a Verification, including any verification status, score, reason code, extracted data and supporting evidence.

"**SDK**" means the software development kit, application programming interfaces, and any associated software components of Chmod embedded in or made available through the application of the Business for the performance of Verifications.

"**Service**" means the identity verification services provided by Chmod, comprising the verification flow presented to you, the SDK, and the systems, infrastructure and processing operations used by Chmod to perform Verifications and to generate and deliver Results.

"**Service Provider**" means any subcontractor, sub-processor or other third-party provider engaged by Chmod to assist in the provision of the Service.

"**Verification**" means each identity verification process initiated in respect of you through the Service, whether or not completed.

"**Verification Data**" means all Personal Data collected, generated, derived or otherwise Processed in connection with a Verification, including the data described in Article 6, the Biometric Data described in Article 7 and the Result.

2.2 In these Terms: (a) headings are for convenience only and shall not affect interpretation; (b) the words "include", "including" and "by way of example" shall be construed without limitation; (c) words importing the singular include the plural and vice versa; (d) references to Articles are references to articles of these Terms; and (e) references to any law include that law as amended, replaced or re-enacted from time to time.

3. Relationship of the Parties; Allocation of Data Protection Roles

3.1 The Business determines why your identity is required to be verified, which verification components are performed, the criteria and thresholds applied to the Result, the use to which the Result and the Verification Data are put, and the period for which the Business retains its own records. Accordingly, as between the Business and Chmod, the Business acts as the Controller of your Personal Data in respect of the Verification.

3.2 Chmod Processes your Personal Data on behalf of, and in accordance with the documented instructions of, the Business, in the capacity of Processor, pursuant to written data protection terms binding upon Chmod in respect of the Business, whether agreed with the Business directly or with the entity through which the Business has engaged Chmod.

3.3 Notwithstanding Article 3.2, Chmod Processes certain Verification Data for its own purposes, and in respect of such Processing acts as an independent Controller, solely to: (a) develop, train, test, validate and improve its technology, and generate aggregated or de-identified statistics, in accordance with Article 9; (b) protect the security, integrity and proper functioning of the Service and detect, prevent and investigate fraud, misuse and unlawful activity; (c) comply with its legal and regulatory obligations; and (d) establish, exercise or defend legal claims.

3.4 Inquiries concerning the outcome of a Verification, the Business's use of your Personal Data, or your relationship with the Business should be directed to the Business in the first instance. Inquiries concerning Chmod's Processing under Article 3.3, and any other privacy inquiry, may be directed to Chmod in accordance with Articles 15 and 28.

4. Description of the Service

4.1 Depending on the configuration selected by the Business, a Verification may comprise some or all of the following components, the availability of which may further vary according to the jurisdiction concerned and the type of Identity Document presented:

(a) **Document capture.** You photograph the front and, where applicable, the reverse of your Identity Document. Software executing on your device assesses framing, focus, glare, stability and illumination in real time in order to permit automatic capture of an image of sufficient quality.

(b) **Facial capture and liveness detection.** You record a short video of your face in accordance with on-screen instructions while your screen displays a sequence of colored lights. This component is designed to establish that a live natural person is physically

present before the camera, and to detect presentation attacks (including photographs, screens, printed reproductions and masks) and manipulated, synthetic or injected content (including so-called “deepfakes”).

(c) **Document analysis.** The Service identifies the type, issuing country and side of the Identity Document; extracts the information appearing on it, including the machine-readable zone and any barcodes; assesses the document for indicia of forgery, alteration, tampering, digital manipulation, synthetic generation, screen recapture or printed reproduction; and validates the internal consistency and validity of the extracted information, including expiry dates and check digits.

(d) **Facial comparison (one-to-one).** The Service compares the facial images captured during the Verification against the portrait appearing on the Identity Document and, where applicable, against a reference image of you previously collected or provided in connection with the same Business, in order to assess whether they correspond to the same person. The Service also assesses the quality and attributes of the facial images (including whether the eyes are open or the face is occluded) and estimates facial attributes, such as age range and sex, in order to assess their consistency with the Identity Document and with the criteria configured by the Business.

(e) **Facial search (one-to-many), where enabled by the Business.** The Service may compare your facial data against facial data derived from prior Verifications performed for the same Business, and against facial data that the Business has associated with fraudulent or prohibited activity, in order to detect duplicate enrollments, impersonation and repeated fraud attempts. Chmod does not search your facial data against facial data collected in connection with any other business.

(f) **External source verification and screening, where enabled by the Business.** The Service may validate the information and, where available, the portrait contained in your Identity Document against the records of the issuing authority or other authoritative or official sources, directly or through authorized providers (in certain cases by means of access credentials or arrangements held by the Business itself); and may screen your name, date of birth, nationality and comparable identifiers against sanctions lists, lists of politically exposed persons, other watchlists and adverse media sources, on a one-time basis or, where the Business so requests, on a recurring basis.

(g) **Device, network and location signals.** The Service collects and analyzes information concerning your device, your network connection and, subject to your device-level permission, your location, in order to detect risk indicators, including the use of emulators, compromised (rooted or jailbroken) devices, VPNs, proxies or anonymization networks, simulated location data, and inconsistencies between your reported location and your network location.

(h) **Generation and delivery of the Result.** The Service generates the Result by applying the rules, criteria and thresholds configured by the Business, and delivers the Result, together with the associated Verification Data, to the Business.

4.2 The components described in Article 4.1 are performed principally by automated means, including through artificial-intelligence and machine-learning systems, certain of which are operated by Service Providers. Article 14 sets out further information concerning automated Processing.

4.3 Where a Verification is not successful, the Business may permit you to make further attempts. Each attempt, whether or not completed, is recorded and constitutes part of the Verification Data.

5. Health and Safety Notice

5.1 Photosensitivity warning. The liveness detection component displays a sequence of flashing colored lights on your screen. A small percentage of individuals may experience epileptic seizures or other adverse reactions when exposed to flashing lights or patterns, including individuals with no previous history of such reactions.

5.2 If you, or any member of your family, have an epileptic condition or are otherwise sensitive to flashing lights, you should not commence the liveness detection component and should contact the Business to inquire about an alternative. You should discontinue use of the Service immediately and seek medical attention if you experience dizziness, altered vision, eye or muscle twitching, disorientation, loss of awareness or any involuntary movement.

5.3 You should not use the Service while driving, operating machinery or engaged in any other activity requiring your attention.

6. Personal Data Collected

6.1 Data provided by you in the course of the Verification. Chmod collects:

(a) images of your Identity Document (front and, where applicable, reverse);

(b) the information appearing on or encoded in your Identity Document, which may include, depending on the document: your full name; date and place of birth; sex or gender as recorded on the document; nationality; document type, subtype and number; dates of issue and expiry; issuing country and authority; personal or national identification numbers; residential address; marital status; the contents of the machine-readable zone and of any barcode; the portrait photograph; your signature; and any further information the document contains, which on certain documents may include physical characteristics (such as height or eye color) or conditions and restrictions (such as a requirement for corrective lenses); and

(c) the images and video of your face captured during the facial capture and liveness detection component.

6.2 Biometric Data. From the facial images and video referred to in Article 6.1 and from the portrait appearing on your Identity Document, the Service generates Biometric Data, including facial-geometry templates, liveness and similarity scores, and estimated facial attributes. Article 7 sets out the specific undertakings applicable to Biometric Data.

6.3 Data collected automatically from your device. Chmod collects:

(a) **device information:** device model and manufacturer; operating system and version; an application-level device identifier made available by your operating system, which is not your advertising identifier; screen resolution, density and orientation; memory and storage capacity; language and time zone settings; and SDK version;

(b) **device integrity signals:** indicators of whether the device is an emulator, has been rooted or jailbroken, has developer mode enabled, or has a debugger attached;

(c) **network information:** IP address; connection type; mobile carrier name, country and network codes; and information derived from your IP address, including approximate location at the level of country and city, the identity of your internet service provider, and indicators of the use of a VPN, proxy or anonymization network; and

(d) **precise location data**, solely where you have granted the corresponding permission at the level of your device: satellite-based coordinates, their reported accuracy, and indicators that the location may be simulated. Where you decline the permission, that fact is recorded, and the Business determines whether the Verification may nonetheless proceed.

6.4 Data received from the Business. The Business may provide Chmod with the identifier by which it refers to you and, depending on its configuration, your name, contact details, identity information previously verified or held by it, or a reference image of you, for the purposes of associating the Verification with your record and performing the comparisons described in Article 4.

6.5 Data received from third-party sources. Where the corresponding components are enabled, Chmod receives responses from official or authoritative registries and authorized data providers; the results of sanctions, politically-exposed-person, watchlist and adverse-media screening; and IP-address intelligence.

6.6 Records generated by the Service. Chmod generates and retains Results, decisions, scores, reason codes, timestamps, technical logs and records evidencing the presentation of, and your acceptance of, these Terms.

6.7 Device permissions. The Service requires access to your camera. The Service may additionally request access to your location, which you may grant or decline, and may revoke at any time, through your device settings. The Service does not request access to your contacts, photograph library or files, and is not designed to record audio.

7. Biometric Data

7.1 Chmod collects, uses and stores Biometric Data solely to: (a) establish that a live natural person is present during the Verification; (b) perform the facial comparisons described in Article 4.1(d) and, where enabled by the Business, the facial search described in Article 4.1(e); (c) detect, prevent and investigate fraud, impersonation and presentation or injection attacks; and (d) develop, train, test, validate and improve its technology in accordance with Article 9.

7.2 Chmod does not sell, lease, trade or otherwise derive commercial profit from your Biometric Data, other than through the provision of the Service itself. Chmod discloses Biometric Data only to the Business, to Service Providers acting on Chmod's behalf and subject to obligations of confidentiality and data protection, and otherwise only as described in Article 10 or as required by Applicable Law or legal process.

7.3 Chmod permanently destroys Biometric Data upon the earliest of: (a) the fulfillment of the purpose for which it was collected, where no other purpose set out in Article 7.1 subsists; (b) the expiry of the retention period set out in Article 12.1; and (c) the expiry of any shorter maximum retention or destruction period prescribed by Applicable Law; in each case unless and to the extent that retention is required by Applicable Law or by a valid order of a court or other competent authority, or is permitted under Article 12.1, 12.2 or 18.4.

7.4 Chmod stores, transmits and protects Biometric Data using a standard of care at least equal to the standard it applies to other confidential and sensitive information, and in no event less than the reasonable standard of care applicable within Chmod's industry, as further described in Article 13.

7.5 This Article 7, together with Articles 12 and 13, constitutes Chmod's written policy and retention schedule governing the collection, retention and destruction of Biometric Data. That policy is made available to each End User through the Service before any Biometric Data is collected, is published and kept permanently available at a publicly accessible location maintained by Chmod, and is additionally available at any time upon request in accordance with Article 27.7, in satisfaction of any requirement of Applicable Law for a publicly available written policy or retention schedule.

8. Purposes and Bases of Processing

8.1 Chmod Processes Verification Data exclusively for the following purposes:

(a) **provision of the Service:** performing the components described in Article 4, verifying and authenticating your identity, and generating and delivering the Result to the Business;

(b) **fraud prevention and security:** detecting, preventing and investigating identity fraud, impersonation, presentation and injection attacks, and other unlawful or prohibited activity, and protecting you, the Business, Chmod and the Service;

(c) **support of the Business's compliance functions:** assisting the Business in discharging its customer due diligence, anti-money-laundering, counter-terrorist-financing, age-verification and other regulatory obligations under Applicable Law;

(d) **improvement of the technology:** the purposes described in Article 9;

(e) **operation and support:** operating, maintaining, securing and supporting the Service, diagnosing and remedying defects, performing quality assurance (which may include review of Verification Data by authorized and trained personnel bound by obligations of confidentiality), and responding to requests and inquiries;

(f) **legal compliance and claims:** complying with Applicable Law and with lawful requests of competent authorities, enforcing these Terms, and establishing, exercising or defending legal claims;

(g) **statistics:** producing aggregated or de-identified information that does not identify you; and

(h) **corporate transactions and governance:** the disclosures described in Articles 10.5 and 10.6.

8.2 Chmod does not sell your Personal Data, does not share it for cross-context behavioral or targeted advertising, and does not use it for advertising or marketing of any kind.

8.3 Chmod Processes Verification Data on one or more of the following bases, where and as recognized by Applicable Law: the consent you give under Article 16; the necessity of the Processing for the performance of the Verification initiated in respect of you; compliance with legal obligations to which Chmod is subject; and the legitimate interests of Chmod and the Business in providing and securing the Service, preventing and investigating fraud, and

establishing, exercising or defending legal claims. The Processing described in Articles 3.3(b) through (d) rests on the latter two bases and may accordingly continue notwithstanding a withdrawal of consent, as described in Article 16.5.

9. Improvement of the Service; Training of Models

9.1 In order to maintain and improve the accuracy, security, reliability and fraud-resistance of the Service, Chmod uses Verification Data — including images of Identity Documents, facial images and video, Biometric Data, extracted document information, Results and device, network and location signals — to develop, train, test, validate and improve its algorithms, models and systems. Such activity includes, by way of example, the improvement of models that detect and classify identity documents, extract textual information, detect forged, altered or synthetically generated documents, detect presentation and injection attacks, and perform facial comparison, as well as the measurement and mitigation of error rates and demographic bias.

9.2 Improvements resulting from such activity are incorporated into the Service as made available to Chmod's customers generally.

9.3 In carrying out the activities described in this Article 9, Chmod shall: (a) restrict access to authorized personnel and systems subject to obligations of confidentiality; (b) remove or pseudonymize direct identifiers wherever compatible with the purpose pursued; (c) not sell the data, not authorize any third party to use it for the development, training or improvement of that third party's own products, services or models, and contractually require each Service Provider that Processes the data to do so solely for the purpose of providing services to Chmod; and (d) not retain the data beyond the period set out in Article 12. Trained models consist of numerical parameters; they are not used to identify you, and are not designed to reproduce your images or your Personal Data.

9.4 For the sole purpose of measuring and mitigating error rates and demographic bias, Chmod may estimate demographic characteristics, such as age range and sex, from facial images. Such estimates are used exclusively for that measurement and mitigation, are not used to make any decision concerning you, and are not disclosed to the Business. Beyond the foregoing and the attribute estimation described in Article 4.1(d), Chmod does not use Verification Data to infer race, ethnicity, religious belief, state of health or any other special characteristic that your Identity Document or facial images may incidentally reveal.

9.5 The Processing described in this Article 9 is undertaken on the basis of the consent you give upon accepting these Terms, as set out in Article 16. You may withdraw that consent at any time in accordance with Article 16.5, in which case Chmod shall exclude your Verification Data from future training and improvement activities; where Applicable Law permits the Processing described in this Article 9 on a basis other than consent, Chmod shall nonetheless give effect to any such withdrawal in the same manner. Withdrawal does not affect models already trained, Processing already performed, or the Processing necessary for the performance of Verifications requested by the Business, and does not, of itself, prevent the performance of future Verifications.

10. Disclosure of Personal Data

10.1 Disclosure to the Business. Chmod discloses to the Business the Result and the Verification Data pertaining to your Verification, including the images of and information extracted from your Identity Document, the facial images and video, Biometric Data and associated scores and attributes, device, network and location information, and the results of any external source verification or screening. The Business Processes such data as Controller under its own privacy policy and may retain its own records for the period it determines in accordance with the Applicable Law to which it is subject.

10.2 Disclosure to Service Providers. Chmod discloses Personal Data to Service Providers that Process it on Chmod's behalf, on the basis of written agreements imposing obligations of confidentiality, security and data protection, and solely to the extent necessary for the provision of the Service. Such Service Providers comprise, by category: (a) providers of cloud infrastructure, computing and storage services; (b) providers of artificial-intelligence, computer-vision and document- and biometric-analysis services, including liveness detection, facial comparison and text extraction; and (c) where the corresponding components are enabled, providers of official-source validation, sanctions and watchlist screening, and IP-address intelligence. An up-to-date list of Chmod's material Service Providers is available upon written request addressed to privacy@chmod.com.

10.3 Disclosure to official sources. Where the Business enables external source verification, Chmod transmits to the competent authority or authorized provider the data necessary to perform the check (which may include your document number, name, date of birth and portrait) and receives in return the corresponding response, which may be limited to a confirmation of whether the submitted data corresponds to the records held by that source.

10.4 Disclosure required by law. Chmod may disclose Personal Data to courts, law enforcement agencies, regulators and other competent authorities where required to do so by Applicable Law, subpoena, court order or other valid legal process, or where Chmod reasonably believes that disclosure is necessary to prevent fraud or other unlawful activity or to protect the rights, property or safety of any person. Where legally permitted, Chmod will inform the Business of any such disclosure.

10.5 Corporate transactions. In the event of any merger, acquisition, financing, reorganization, sale of assets, insolvency proceeding or comparable transaction involving Chmod, or the preparation or negotiation thereof, Personal Data may be disclosed to and transferred to the parties to such transaction and their advisers, subject to obligations of confidentiality, and any successor shall remain bound by these Terms or by terms no less protective.

10.6 Professional advisers. Chmod may disclose Personal Data to its professional advisers and auditors, subject to obligations of confidentiality.

10.7 Segregation between businesses. Chmod does not disclose your Verification Data to any business other than the Business, and does not use Verification Data collected in connection with one business in the performance of Verifications for any other business, except through the general improvement of its technology described in Article 9.

11. International Transfers of Personal Data

11.1 Your Personal Data may be stored and Processed in, and transferred to, jurisdictions other than the jurisdiction in which you reside, including jurisdictions in which Chmod or its Service Providers maintain processing facilities. Such jurisdictions may not afford a level of protection for Personal Data equivalent to that afforded in your jurisdiction of residence.

11.2 Where Personal Data is transferred as described in Article 11.1, Chmod implements safeguards designed to ensure that the data continues to receive an adequate level of protection, including contractual commitments binding upon the recipients, the security measures described in Article 13 and, where required by Applicable Law, transfer mechanisms recognized under the Data Protection Laws of the exporting jurisdiction. Information concerning the safeguards applied is available upon written request addressed to privacy@chmod.com.

11.3 To the extent that your consent constitutes a lawful basis or condition for such transfers under Applicable Law, you give that consent upon accepting these Terms, as set out in Article 16.

12. Data Retention and Destruction

12.1 Chmod retains Verification Data for a maximum period of five (5) years from the date of the Verification to which it relates. Upon expiry of that period, Chmod deletes the data or irreversibly anonymizes it, unless and to the extent that continued retention is required by Applicable Law or by a valid order of a court or other competent authority, save that Chmod may retain, to the minimum extent and for the minimum duration necessary: (a) records evidencing the presentation and acceptance of these Terms and the consents given under Article 16; and (b) Verification Data whose retention is necessary for the establishment, exercise or defense of legal claims or in connection with pending or reasonably anticipated proceedings, investigations or disputes.

12.2 Chmod deletes Verification Data before the expiry of the period set out in Article 12.1 where the Business so instructs or where Applicable Law so requires, save that Chmod may retain such data, to the minimum extent and for the minimum duration necessary, in order to comply with a legal obligation, to prevent or investigate fraud in accordance with Article 18.4, or to establish, exercise or defend legal claims.

12.3 Where Applicable Law prescribes a maximum retention or destruction period for Biometric Data or any other category of Verification Data shorter than the period set out in Article 12.1, the shorter period shall apply to the data concerned, in accordance with Articles 7.3 and 26.

12.4 The Business retains its own copy of the Result and the Verification Data delivered to it for the period the Business determines, under its own policies and the Applicable Law to which it is subject. Deletion of data by Chmod does not effect deletion of the Business's records; inquiries concerning the Business's retention practices should be directed to the Business.

12.5 Chmod may retain aggregated or de-identified information that does not identify you without limitation in time. Chmod maintains such information in aggregated or de-identified form, does not attempt to re-identify it, and does not permit any third party to attempt to do so.

12.6 Where Verification Data resides in backup or disaster-recovery systems from which immediate deletion is not technically practicable, Chmod shall isolate such data from active Processing and shall delete or overwrite it in the ordinary rotation cycle of those systems; such

data shall not be restored to active systems except for the purposes permitted by these Terms.

13. Information Security

13.1 Chmod implements and maintains technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure and unauthorized access, appropriate to the nature of the data and the risks presented by the Processing, which include, as appropriate to the systems and data concerned: encryption of data in transit; encryption of stored images and data at rest; logical segregation of the data of each business; access controls founded on the principle of least privilege; scoped, time-limited access credentials; recording and monitoring of relevant system activity; confidentiality undertakings binding upon personnel; and due diligence upon, and contractual security obligations binding upon, Service Providers.

13.2 No system can be guaranteed to be secure in all circumstances. In the event of a personal data breach affecting your Personal Data, Chmod shall notify the Business without undue delay and shall, where required by Applicable Law, notify you and the competent authorities.

14. Automated Processing; Human Review

14.1 The components described in Article 4 are performed principally by automated means, and the Result is generated by the application of the rules, criteria and thresholds configured by the Business. The Business determines the consequences attached to the Result — including approval, rejection, escalation to manual review or an invitation to reattempt — and the Business may act upon the Result by automated means.

14.2 Automated systems are subject to error. Factors including poor illumination, a damaged, worn or non-standard Identity Document, low image quality, occlusion of the face and connectivity failures may produce an inaccurate or inconclusive Result.

14.3 If you disagree with a decision made in reliance upon a Result, you may contact the Business in order to contest the decision, provide additional information or request a further attempt. Where Applicable Law confers upon you the right not to be subject to a decision based solely on automated Processing which produces legal or similarly significant effects, you may exercise that right by addressing a request to the Business; the manner in which such requests are handled is determined by the Business in accordance with Applicable Law. Chmod shall provide the Business with the assistance and information reasonably necessary for a meaningful human review.

14.4 A successful Verification does not constitute a certification of your identity for any purpose beyond the Verification concerned, and does not oblige the Business to accept you or to provide you with any product or service. The Service is provided for identity verification and fraud-prevention purposes only; Results are not provided for use, and are not intended to be used, as a factor in establishing eligibility for credit, insurance, employment, housing or any similar purpose, and Chmod assumes no responsibility for any such use.

15. Rights of the End User

15.1 Subject to and in accordance with Applicable Law, you may have the right to: (a) obtain confirmation as to whether your Personal Data is Processed, and access to and a copy of that data; (b) obtain the rectification of inaccurate or incomplete data; (c) obtain the erasure of your data; (d) obtain the restriction of, or object to, certain Processing; (e) receive certain data in a structured, commonly used and machine-readable format, and have it transmitted to another Controller; (f) withdraw any consent you have given, in accordance with Article 16.5; (g) not be subject to certain decisions based solely on automated Processing, in accordance with Article 14.3; and (h) lodge a complaint with the supervisory or data protection authority competent for your jurisdiction.

15.2 Exercise of rights. Because the Business is the Controller of your Personal Data in respect of the Verification, requests should be addressed to the Business in the first instance. You may also address requests to Chmod at privacy@chmod.com, identifying the Business that requested the Verification and, where possible, its approximate date. Where Chmod Processes the relevant data on behalf of the Business, Chmod shall transmit the request to the Business without undue delay and shall provide the Business with reasonable assistance in responding to it. Where the request concerns Processing carried out by Chmod as an independent Controller under Article 3.3, Chmod shall respond directly.

15.3 Chmod may require you to provide information reasonably necessary to verify your identity before giving effect to a request. Such information shall be used solely for that purpose and shall not be retained longer than necessary.

15.4 Requests addressed to Chmod shall be answered by Chmod within the periods prescribed by Applicable Law. The exercise of rights is free of charge, save where Applicable Law permits a reasonable fee in respect of requests that are manifestly unfounded or excessive. Chmod shall not discriminate against you or subject you to detriment for exercising your rights; the consequences that the Business attaches to the outcome or non-completion of a Verification are determined by the Business, as described in Article 14.1.

16. Consent; Withdrawal of Consent

16.1 By accepting these Terms in the manner described in Article 1.3, you freely, specifically, expressly and on an informed basis consent to:

(a) the collection, use, storage and other Processing of your Personal Data — including the images of your Identity Document, the images and video of your face, and your Biometric Data — for the purposes set out in Article 8;

(b) the use of your Verification Data, including your Biometric Data, for the development, training, testing, validation and improvement of Chmod's technology, as described in Article 9;

(c) the disclosure of your Personal Data to the Business and to the other categories of recipients identified in Article 10;

(d) where enabled by the Business, the facial search described in Article 4.1(e) and the external source verification and screening described in Article 4.1(f);

(e) the storage and Processing of your Personal Data in, and its transfer to, jurisdictions other than your jurisdiction of residence, as described in Article 11; and

(f) where you grant the corresponding device permission, the collection of your precise location data.

16.2 You are under no obligation to give the consents set out in Article 16.1; however, they are a condition of the performance of the Verification, which cannot be carried out without them, save that the subsequent withdrawal of the consent described in Article 16.1(b) does not, of itself, prevent the performance of future Verifications, as described in Article 9.5. Whether an alternative means of verification is available to you is determined by the Business.

16.3 Where Applicable Law requires that any consent or release relating to Personal Data or Biometric Data be given in writing, your acceptance of these Terms by electronic means constitutes, to the maximum extent permitted by Applicable Law, your written consent and release, given to Chmod, to the Service Providers acting on Chmod's behalf and, in respect of the Verification Data delivered to the Business under Article 10.1 and the components enabled by the Business, to the Business; and the record generated by the Service of that acceptance constitutes a written record thereof. Chmod retains records evidencing the presentation and acceptance of these Terms in respect of each Verification. You agree that such records constitute admissible evidence of your acceptance and consents, and you agree not to contest the validity, enforceability or admissibility of these Terms, or of such records, solely on the ground that they were concluded or are maintained in electronic form. Where Applicable Law requires a separate, specific or differently formalized consent or release, Articles 16.4 and 26.1(a) apply.

16.4 Where Applicable Law or the Business requires any separate, specific or additional notice, consent, authorization or formality, these Terms do not dispense with that requirement, and any such notice or consent supplements, and does not replace, these Terms. Chmod shall give any such notice, and obtain any such consent, as Applicable Law requires of Chmod.

16.5 Withdrawal. You may withdraw any consent given under these Terms at any time, in whole or in part, by contacting the Business or by writing to privacy@chmod.com. Withdrawal takes effect for the future and does not affect the lawfulness of Processing carried out prior to withdrawal. Withdrawal of the consent described in Article 16.1(b) takes effect upon receipt by Chmod, and may be communicated directly to privacy@chmod.com; a withdrawal of that consent communicated to the Business takes effect upon its transmission to Chmod. If you withdraw a consent other than that described in Article 16.1(b) before or during a Verification, the Verification cannot be completed. Following withdrawal, Chmod and the Business may continue to retain and Process Personal Data where and to the extent that Applicable Law requires or permits, including for the prevention and investigation of fraud, compliance with legal obligations and the establishment, exercise or defense of legal claims.

16.6 The consents set out in this Article 16 are sought and relied upon to the extent that Applicable Law requires consent for the relevant Processing. Where Applicable Law permits or requires the relevant Processing to be conducted on another lawful basis — including the performance of a contract or of steps taken at your request, compliance with a legal obligation, the prevention and detection of fraud, or legitimate interests — such Processing may be conducted on that basis, and the invalidity, absence or withdrawal of a consent does not affect Processing lawfully conducted on such other basis, subject, in the case of the Processing described in Article 9, to Article 9.5.

17. Eligibility; Representations and Warranties of the End User

17.1 Save where the Business permits the verification of minors in accordance with this Article 17.1, you must be at least eighteen (18) years of age, or such higher age of majority as applies in your jurisdiction of residence, in order to use the Service. Where the Business permits the verification of minors, a minor may use the Service only with the authorization and under the supervision of a parent or legal guardian, who accepts these Terms on the minor's behalf. The parent or legal guardian who so accepts represents and warrants to Chmod and to the Business that they have authority to do so and that every consent, authorization or formality required by Applicable Law for the minor's verification has been obtained or observed. Verification Data relating to an End User whom Chmod knows to be under eighteen (18) years of age is not used for the purposes described in Article 9. Where Chmod becomes aware that Verification Data has been collected from a person below the age required by this Article 17.1 without the authorization it requires, Chmod shall delete such data without undue delay, subject only to Article 12.2, and shall inform the Business.

17.2 You represent and warrant to Chmod and to the Business, on each occasion on which you use the Service, that:

(a) you present only your own Identity Document, and that such document is genuine, valid and lawfully held by you;

(b) all information you provide is true, accurate, complete and current;

(c) you complete the Verification personally, in real time, and in your own physical presence, in accordance with the instructions presented to you;

(d) you have the legal capacity to accept these Terms, or these Terms have been accepted on your behalf in accordance with Article 17.1;

(e) your use of the Service complies with these Terms and with Applicable Law;

(f) you have read the health and safety notice set out in Article 5 and, by commencing the facial capture and liveness detection component, you confirm that you are not aware of any condition described therein affecting you or that you have chosen to proceed notwithstanding, assuming the risks described in Article 5 to the extent permitted by Applicable Law; and

(g) you do not access or use the Service from a jurisdiction in which the Service, or your use of it, is prohibited by Applicable Law.

18. Prohibited Conduct

18.1 You shall not, and shall not attempt to, directly or indirectly:

(a) impersonate any person, or present the Identity Document, facial features, likeness or Personal Data of any person other than yourself, whether or not with that person's permission;

(b) present any forged, counterfeit, altered, stolen or unlawfully obtained document;

(c) present photographs, screens, printed reproductions, masks, prostheses, synthetic or manipulated media (including deepfakes) or any other artifact in place of a live capture of your face or of a genuine document;

(d) employ virtual cameras, emulators, injection tools, instrumentation frameworks, bots or scripts, or otherwise introduce manipulated data into the capture process;

(e) circumvent, disable, probe or interfere with the liveness detection, fraud prevention or security controls of the Service;

(f) copy, modify, adapt, translate, decompile, disassemble or reverse engineer the Service or the SDK, or create derivative works thereof, save to the extent such restriction is prohibited by Applicable Law;

(g) interfere with, disrupt or impose disproportionate load upon the Service or any related infrastructure; or

(h) use the Service for any unlawful or fraudulent purpose.

18.2 Chmod and the Business may employ automated and manual means to detect conduct prohibited by this Article 18.

18.3 Where Chmod or the Business has reasonable grounds to believe that you have engaged in conduct prohibited by this Article 18, the Verification may be rejected or flagged, your access to the Service may be suspended or terminated, and the matter may be reported to the Business and, where Applicable Law permits or requires, to competent authorities. Where a Verification is so determined to involve fraudulent or prohibited activity, the facial data and associated Verification Data concerned may be designated by or on behalf of the Business for use in the facial search described in Article 4.1(e) in respect of future Verifications performed for that Business; such data is retained in accordance with Articles 12 and 18.4, and you may contest any such designation, and request its review or removal, through the channels described in Articles 14.3 and 15.2.

18.4 Notwithstanding Articles 7.3 and 12, Chmod may retain Verification Data and other records constituting evidence of conduct prohibited by this Article 18, to the extent and for the duration necessary for the prevention, detection and investigation of fraud and the establishment, exercise or defense of legal claims, in each case in accordance with Applicable Law.

18.5 To the extent permitted by Applicable Law, you shall be liable for loss or damage caused by your fraudulent use of the Service or your intentional breach of these Terms.

19. Intellectual Property; Limited License

19.1 The Service, the SDK and all software, models, algorithms, databases, documentation, interfaces, designs, trademarks and other materials comprised therein or related thereto, and all intellectual property rights subsisting in any of the foregoing, are and remain the exclusive property of Chmod and its licensors. No right or license is granted to you other than as expressly set out in Article 19.2.

19.2 Chmod grants you a limited, personal, revocable, non-exclusive, non-transferable and non-sublicensable license to use the SDK, in object code form only, and to access and use the Service, solely for the purpose of completing Verifications requested by the Business, subject to and in accordance with these Terms.

19.3 As between you and Chmod, you retain all rights you hold in your Personal Data. You grant to Chmod the authorizations necessary for Chmod to Process your Personal Data as described in these Terms; these Terms do not grant Chmod any license or right in respect of your Personal Data beyond that Processing.

20. Availability, Suspension and Modification of the Service

20.1 Chmod does not warrant that the Service will be available at any particular time or without interruption. The Business controls your access to the verification flow and may withdraw, restrict or condition that access at any time.

20.2 Chmod may suspend, restrict or discontinue the Service, in whole or in part, where reasonably necessary for security, legal, regulatory or technical reasons, or upon the instruction of the Business.

20.3 Chmod may modify the Service from time to time, including by adding, altering or removing components, provided that any modification materially affecting the Processing of your Personal Data shall be reflected in an amendment to these Terms in accordance with Article 25.

21. Disclaimers

21.1 To the maximum extent permitted by Applicable Law, the Service is provided "as is" and "as available", and Chmod disclaims all warranties, conditions and representations of any kind, whether express, implied, statutory or otherwise, including any implied warranties of merchantability, satisfactory quality, fitness for a particular purpose, accuracy and non-infringement.

21.2 Without limiting Article 21.1, Chmod does not warrant that the Service will be uninterrupted, timely, secure or error-free, that any Verification will be completed or will produce any particular Result, or that any Result will be free from error, and Article 14.2 applies to all Results. Chmod does not warrant the accuracy, completeness or currency of information contained in Identity Documents or obtained from official or authoritative sources, screening or media providers or other third-party sources, which the Service Processes as received.

21.3 Chmod is not responsible for the products, services, acts, omissions, decisions, terms or privacy practices of the Business, including the Business's decision to accept or reject you, the Business's use of the Result or of the Verification Data, or the Business's compliance with Applicable Law.

21.4 Nothing in these Terms excludes any warranty, guarantee or condition which cannot lawfully be excluded, or limits your rights under any mandatory provision of Applicable Law, including consumer protection and Data Protection Laws.

22. Limitation of Liability

22.1 To the maximum extent permitted by Applicable Law, in no event shall Chmod, its affiliates, or their respective officers, directors, employees, agents or Service Providers, nor the Business in its capacity as recipient of the Service, be liable to you for any indirect, incidental, special, consequential, exemplary or punitive damages, or for any loss of profits, revenue, business, goodwill, data or opportunity, arising out of or in connection with the Service or these Terms, whether in contract, tort (including negligence), breach of statutory duty or otherwise, and whether or not such damages were foreseeable.

22.2 To the maximum extent permitted by Applicable Law, the aggregate liability of Chmod, its affiliates and their respective officers, directors, employees, agents and Service Providers, and of the Business in its capacity as recipient of the Service, to you for all claims arising out of or in

connection with the Service or these Terms shall not exceed one hundred United States dollars (US$100).

22.3 The exclusions and limitations set out in Articles 22.1 and 22.2 do not apply to: (a) liability arising from Chmod's gross negligence, willful misconduct or fraud; (b) liability for death or personal injury caused by negligence, to the extent such liability cannot be excluded or limited; or (c) any other liability which cannot be excluded or limited under Applicable Law. Nothing in these Terms limits the rights conferred upon you by mandatory consumer protection or Data Protection Laws.

22.4 The Business and its affiliates, and Chmod's affiliates and the respective officers, directors, employees, agents and Service Providers of Chmod and its affiliates, are intended beneficiaries of, and may rely upon and enforce, Articles 5, 16, 17, 18, 21, 22, 23 and 24 as if named therein. Save as expressly provided in this Article 22.4, these Terms confer no rights upon any third party.

23. Indemnification

23.1 To the extent permitted by Applicable Law, you shall indemnify and hold harmless Chmod, its affiliates, and their respective officers, directors, employees and agents, and the Business and its affiliates, from and against all losses, damages, liabilities, costs and expenses (including reasonable legal fees), whether or not arising out of a third-party claim, demand, proceeding or governmental investigation, to the extent attributable to: (a) your fraudulent or unlawful use of the Service; (b) your breach of the representations and warranties set out in Article 17; (c) your breach of Article 18; or (d) your violation of the rights of any person, including through the presentation of another person's Identity Document, likeness or Personal Data.

23.2 The indemnity in Article 23.1 shall not apply to the extent that the relevant loss is attributable to the gross negligence or willful misconduct of the party seeking indemnification.

24. Governing Law; Dispute Resolution

24.1 These Terms, and any dispute or claim (whether contractual or non-contractual) arising out of or in connection with them or their subject matter, shall be governed by and construed in accordance with the laws of the State of Delaware, United States of America, without regard to its conflict-of-laws rules.

24.2 Before commencing any proceeding, you agree first to contact Chmod at privacy@chmod.com, describing the dispute, so that the parties may attempt to resolve it amicably within thirty (30) days.

24.3 Subject to Article 24.4, the courts sitting in the State of Delaware shall have exclusive jurisdiction over any dispute or claim arising out of or in connection with these Terms, and each party submits to the jurisdiction of such courts.

24.4 Where you are a consumer and any mandatory provision of the Applicable Law of your jurisdiction of habitual residence confers upon you the protection of that law, or the right to bring or defend proceedings before the courts of that jurisdiction, nothing in this Article 24 deprives you of that protection or that right.

24.5 To the maximum extent permitted by Applicable Law: (a) any claim arising out of or in connection with the Service or these Terms shall be brought in an individual capacity only, and not as a plaintiff or member of a class in any class, collective, consolidated or representative

proceeding; and (b) each party irrevocably waives any right to a trial by jury. Where Applicable Law does not permit any part of the foregoing waivers, that part shall not apply to you, without affecting the remainder of these Terms.

24.6 To the maximum extent permitted by Applicable Law, any claim arising out of or in connection with the Service or these Terms must be commenced within one (1) year after the date on which the claim accrued, failing which it is permanently barred; where Applicable Law prescribes a longer minimum period that cannot be shortened by agreement, that longer period shall apply.

25. Amendments to these Terms

25.1 Chmod may amend these Terms from time to time, including to reflect changes in the Service, in Applicable Law or in Chmod's Processing practices. The date of the most recent amendment is indicated at the head of these Terms.

25.2 The version of these Terms presented to you at the commencement of a Verification governs that Verification.

25.3 Where an amendment materially affects the Processing of your Personal Data or otherwise materially diminishes your rights, Chmod shall make the amended Terms available through the Service before they take effect and shall, where required by Applicable Law, obtain your renewed consent.

26. Mandatory Provisions of Local Law

26.1 These Terms are intended to apply to End Users in all jurisdictions in which the Service is made available, and shall in each case be read and applied in conjunction with the Applicable Law of the relevant jurisdiction. Accordingly:

(a) where Applicable Law requires any notice, disclosure, consent, authorization or formality additional to, or different from, those set out in these Terms, that requirement is not dispensed with by these Terms; the notice shall be given, and the consent, authorization or formality shall be obtained or observed, by Chmod or by the Business, according to which of them Applicable Law places the relevant obligation upon, before the relevant Processing takes place, and the requirement shall prevail over these Terms to the extent of any inconsistency;

(b) where Applicable Law confers upon you rights additional to those set out in Article 15, Article 15 shall be deemed supplemented accordingly, and such rights may be exercised through the channels described in Article 15.2;

(c) where Applicable Law prescribes shorter retention, blocking or destruction periods than those set out in these Terms, the shorter periods shall apply in accordance with Articles 7.3 and 12.3;

(d) where Applicable Law designates a particular authority competent to supervise the Processing of Personal Data or to receive complaints, you may address complaints to that authority, without prejudice to any other remedy available to you; and

(e) where any provision of these Terms is inconsistent with a mandatory provision of Applicable Law, that provision shall apply to the maximum extent permitted, and the mandatory provision shall prevail to the extent of the inconsistency, without affecting the

remainder of these Terms.

26.2 This Article 26 prevails over every other provision of these Terms.

27. General Provisions

27.1 Entire agreement. These Terms constitute the entire agreement between you and Chmod with respect to the Service and supersede all prior or contemporaneous understandings with respect thereto. This Article 27.1 does not affect the agreements existing between Chmod and the Business, nor between you and the Business.

27.2 Severability. If any provision of these Terms is held to be invalid, illegal or unenforceable, that provision shall be enforced to the maximum extent permissible, and the remaining provisions shall continue in full force and effect.

27.3 No waiver. No failure or delay by Chmod in exercising any right under these Terms operates as a waiver of that right, and no single or partial exercise of any right precludes any further exercise thereof.

27.4 Assignment. You may not assign or transfer these Terms or any rights or obligations hereunder. Chmod may assign these Terms to an affiliate or in connection with a transaction described in Article 10.5.

27.5 Survival. Provisions which by their nature are intended to survive the completion of a Verification or the termination of your use of the Service — including Articles 7 through 19 and 21 through 28 — shall so survive, and Articles 14 and 15 shall continue to apply for so long as Chmod retains your Personal Data.

27.6 Language. These Terms are drawn up in the English language. Where a translation is made available, it is provided for convenience only, and the English version shall prevail to the extent permitted by Applicable Law.

27.7 Electronic form; availability. These Terms are concluded in electronic form. A copy of these Terms is published and kept available at a publicly accessible location maintained by Chmod, and is available at any time upon request addressed to privacy@chmod.com.

27.8 No agency. Nothing in these Terms creates any agency, partnership, employment or fiduciary relationship between you and Chmod.

27.9 Force majeure. Chmod shall not be liable for any failure or delay in performance to the extent caused by circumstances beyond its reasonable control, including acts of God, acts of governmental or regulatory authorities, failures of telecommunications, utilities or third-party infrastructure, and malicious attacks, provided that Chmod resumes performance as soon as reasonably practicable. Nothing in this Article 27.9 relieves Chmod of any obligation imposed by Applicable Law.

28. Contact

28.1 All notices, requests and inquiries under these Terms may be addressed to:

Chmod LLC
A limited liability company organized under the laws of the State of Delaware, United States of America

Email: privacy@chmod.com

28.2 When contacting Chmod in connection with a Verification, please identify the Business that requested the Verification and, where possible, its approximate date, in order to enable Chmod to locate the relevant records.