VerifyMe Terms of Service

General Terms and Data Processing Terms for the VerifyMe self-service platform, in one document

Strike Business Builders B.V., trading as STRIKE Group | Zonnebaan 9, 3542 EA Utrecht, the Netherlands | Chamber of Commerce no. 74321293 | VAT no. NL859854218B01

Version 2.1 | Effective date: 13 November 2026 | These Terms apply to business customers only | Accepted by ticking one box at registration

Part A: General Terms

Articles 1 to 21. The contractual terms for the Account, Tokens, Subscriptions, payment, use of the Service, liability and termination.

Summary for the reader (not legally binding). VerifyMe is a self-service verification platform for businesses. You create an account, buy Tokens as a one-off Token Bundle or through a monthly Subscription, build your verification flows and run Checks on the people you need to verify. Each Check costs a number of Tokens. Tokens are valid for twelve months after they have been credited to your account. This single document is the whole agreement between your company and STRIKE: Part A contains the general terms and Part B contains the data processing terms that the GDPR requires between you (as controller) and STRIKE (as processor). By ticking the acceptance box you accept both parts on behalf of your company; no separate data processing agreement needs to be signed. You remain responsible for informing the people you verify and, where the law requires it, for obtaining their consent (Articles 4.9 and 28.1). The Service is available to businesses only; consumers cannot register.

1. Definitions

Capitalised terms have the following meaning in these Terms and in every document that forms part of the Agreement:

1.1 **Account**: the Customer's registered environment on the Platform, including all Authorised Users, flows, API keys, Tokens and Subscriptions linked to it.

1.2 **Account Administrator**: an Authorised User who holds the administrator role in the Account.

1.3 **Agreement**: the agreement between STRIKE and the Customer for the use of the Service, consisting of these Terms (Part A and Part B, including the Schedules), the Service Catalogue, the Documentation and each Order.

1.4 **Authorised User**: a natural person who is employed by or works under the authority of the Customer and whom the Customer has given access to the Account.

1.5 **Business Day**: a day other than a Saturday, Sunday or public holiday in the Netherlands.

1.6 **Check**: a verification, validation, screening, enrichment, monitoring or other function that the Platform offers as a step in a flow, as described in the Service Catalogue from time to time.

1.7 **Check Category**: a group of Checks with a comparable nature, data source and allocation of data protection roles, as set out in Schedule 1 to the Data Processing Terms.

1.8 **Customer**: the legal entity or business that accepts these Terms and holds the Account.

1.9 **Customer Data**: all data, including Personal Data, that the Customer or its Authorised Users submit to the Platform, that End Users submit through a Hosted Flow, that the Platform records about an End User's visit to a Hosted Flow, or that is generated for the Customer by the performance of a Check, including the Output.

1.10 **Data Processing Terms**: Part B of these Terms (Articles 22 to 36 and Schedules 1 to 3), which contains the terms required by Article 28(3) GDPR for the Processing of Personal Data by STRIKE on behalf of the Customer and constitutes the data processing agreement between the parties.

1.11 **Documentation**: the user guides, API specifications and integration instructions that STRIKE makes available for the Service.

1.12 **End User**: a natural person whose data the Customer submits to the Platform, or who is invited by the Customer to complete a Hosted Flow, in order to perform a Check.

1.13 **End User Notice**: the VerifyMe End User Verification Notice that STRIKE publishes on the Legal Page for End Users and that the Customer brings to the attention of End Users in accordance with Article 4.9.

1.14 **Fees**: all amounts payable to STRIKE under the Agreement, including the price of Token Bundles and Subscriptions.

1.15 **Hosted Flow**: a verification journey that the Customer configures in the Account and that STRIKE hosts, presented to the End User as a web page or as a frame embedded in the Customer's own website or application, in which the End User submits data, documents or images directly to the Platform at the Customer's request.

1.16 **Legal Page**: the page of the VerifyMe website on which STRIKE publishes these Terms, the End User Notice and the VerifyMe Privacy Statement.

1.17 **Order**: each purchase of a Token Bundle or a Subscription made through the Account, including through the payment pages operated by Stripe and through automatic top-up enabled by the Customer.

1.18 **Output**: the result that the Platform returns for a Check or for a verification as a whole, such as a match score, a status, a flag, extracted or completed data elements, or an overall outcome.

1.19 **Personal Data**, **Controller**, **Processor**, **Processing** and **Data Subject** have the meaning given to them in Regulation (EU) 2016/679 (GDPR).

1.20 **Platform**: the VerifyMe web application, API, Hosted Flows and related software made available by STRIKE.

1.21 **Service**: the Platform, the Checks, the Documentation and the support that STRIKE provides under the Agreement.

1.22 **Service Catalogue**: the overview of the available Checks with their description and Token Cost, as shown in the Account, together with the overview of the Token Bundles and Subscriptions on offer with their size and price, as shown in the Account and on the VerifyMe website, each as updated from time to time in accordance with Article 4.

1.23 **STRIKE**: Strike Business Builders B.V., trading as STRIKE Group, having its registered office at Zonnebaan 9, 3542 EA Utrecht, the Netherlands, registered with the Dutch Chamber of Commerce under number 74321293.

1.24 **Stripe**: Stripe Payments Europe, Limited and its affiliates, the payment service provider through which Fees are collected.

1.25 **Subscription**: an arrangement under which the Customer receives a fixed quantity of Tokens in each Subscription Period against a recurring Fee.

1.26 **Subscription Period**: the recurring period of a Subscription, being one (1) month unless a different period is stated at the Order.

1.27 **Terms**: these VerifyMe Terms of Service, consisting of Part A (General Terms) and Part B (Data Processing Terms), including the Schedules.

1.28 **Token**: a prepaid unit of consumption on the Platform. A Check debits the number of Tokens stated as its Token Cost. Tokens are an accounting unit of the Platform and not electronic money, a voucher or a financial instrument.

1.29 **Token Bundle**: a quantity of Tokens purchased in advance for a one-off price, including any bonus Tokens stated at the Order.

1.30 **Token Cost**: the number of Tokens that a Check debits, as stated in the Service Catalogue at the moment the Check is performed, including any surcharge for options that the Customer has selected for the step concerned and subject to any rate agreed individually under Article 6.11.

1.31 **Trial Tokens**: Tokens that STRIKE grants free of charge, for example upon registration, for the purpose of evaluating the Service.

1.32 **Validity Period**: the period during which Tokens can be consumed, as determined in Article 6.2.

2. Applicability and formation of the Agreement

2.1 These Terms apply to every registration for, Order placed on and use of the Service. The Agreement is concluded when the person who registers completes the registration form and ticks the box confirming acceptance of these Terms. The Account is available from that moment. The acceptance of these Terms covers Part A and Part B together: by accepting these Terms the Customer, as Controller, also enters into the Data Processing Terms with STRIKE, as Processor, and no separate signature or document is required for the data processing agreement to be concluded.

2.2 The Service is offered exclusively to parties acting in the course of a trade, business, craft or profession. By accepting these Terms the person who registers warrants that (a) the Customer is such a party, (b) the Customer is not a consumer and (c) that person is authorised to bind the Customer. Consumer protection rules, including the right of withdrawal, do not apply to the Agreement.

2.3 The Agreement is concluded electronically. STRIKE makes these Terms, including the Data Processing Terms, available before acceptance through a link at the acceptance box and on the Legal Page, in a format that allows the Customer to read, download, store and reproduce them. The Service Catalogue is available in the Account and on the VerifyMe website.

2.4 In the event of conflict, the following order of precedence applies: (a) a written agreement signed by both parties that expressly deviates from these Terms, (b) Part B (Data Processing Terms) with respect to the Processing of Personal Data, (c) Part A (General

Terms), (d) the Service Catalogue, (e) the Documentation. An Order never deviates from the documents listed above unless STRIKE confirms the deviation in writing.

2.5 The applicability of any purchasing or other general terms and conditions of the Customer is expressly rejected. Acceptance of a purchase order or similar document that refers to the Customer's terms does not amount to acceptance of those terms. The General Terms and Conditions of STRIKE Group do not apply to the Agreement; these Terms govern the Service exclusively.

2.6 STRIKE may have the Service performed in whole or in part by companies within its group and by subcontractors. STRIKE remains responsible for the performance of the Agreement.

2.7 Where the Platform asks an Authorised User to confirm these Terms, for example when that user first signs in or when a new version takes effect, that user gives the confirmation on behalf of the Customer. The Agreement binds the Customer for every Authorised User of the Account, whether or not that user has been asked for a confirmation.

3. Account, registration and verification of the Customer

3.1 Registration requires a business e-mail address, the name of the Customer's business, a password and the market and country in which the Customer operates. With its first Order the Customer provides the invoicing details requested at checkout, including its legal name, its address and, where it has one, its VAT identification number. The Customer warrants that all this information is accurate and complete and keeps it up to date.

3.2 The fact that an Account can be used directly after registration does not mean that STRIKE has verified or approved the Customer. STRIKE may verify the identity, legitimacy and intended use of the Customer at any time, before or after the first Order, and may request information or documents for that purpose, such as a trade register number, proof of authority of the person who registered and a description of the use case. The Customer provides what is requested within five (5) Business Days. STRIKE may refuse, limit, suspend or close an Account at its discretion, in particular where the identity, legitimacy, sector or intended use of the Customer cannot be established to STRIKE's satisfaction, or where the information provided does not match public registers.

3.3 STRIKE may make access to certain Checks or Check Categories conditional on additional verification of the Customer or on a written confirmation of the legal basis on which the Customer will perform those Checks. Some Checks can only be performed where the Customer itself holds the required licence, certificate or connection, such as Checks against the Dutch central register of exclusion from games of chance, which run on the connection details issued to the Customer by the Kansspelautoriteit.

3.4 The Customer is responsible for all activity under its Account, including activity of its Authorised Users and of any party that uses the Customer's credentials or API keys. Authorised Users sign in with the multi-factor authentication that the Platform requires. The Customer keeps credentials and API keys confidential and informs STRIKE without delay at security@trustbystrike.com if it suspects unauthorised access.

3.5 The Customer may only grant access to Authorised Users and ensures that each Authorised User complies with the Agreement. Shared or generic log-ins are not permitted. Automated access to the Platform takes place exclusively through API keys issued in the Account.

3.6 The Customer may not use the Service on behalf of third parties, resell the Service or allow third parties to perform Checks through its Account, unless STRIKE has agreed to this in writing in a separate reseller or partner agreement.

3.7 STRIKE may close an Account that has not been used to sign in or to perform a Check for twelve (12) consecutive months, after giving thirty (30) days' notice by e-mail to the Account Administrators. Closure has the consequences of termination under Article 10.4; purchased Tokens that are still within their Validity Period at the time of closure are refunded in accordance with Article 10.6 as if STRIKE had terminated for convenience.

3.8 Where the Platform allows the Customer to connect its own contract with a data source or provider by entering its own credentials, the Customer is responsible for that contract, for the costs charged under it and for its compliance with the conditions of that source or provider. The source or provider then acts under the Customer's contract and not as a subcontractor or Sub-processor of STRIKE (Article 23.3).

4. The Service and the Service Catalogue

4.1 STRIKE makes the Platform available as a software-as-a-service solution with which the Customer builds verification flows and performs the Checks listed in the Service Catalogue. The Service Catalogue, and not these Terms, describes which Checks are available, how each Check works, what Output is returned and what each Check costs in Tokens. A Check, a source, a document type or a country that these Terms mention is only available if and for as long as the Service Catalogue offers it.

4.2 STRIKE develops the Service continuously. STRIKE may add new Checks, change the data sources, logic, Output format or Token Cost of existing Checks, and withdraw Checks. Changes become effective when they are published in the Service Catalogue. STRIKE gives at least thirty (30) days' notice by e-mail to the Account Administrators of (a) an increase of the Token Cost of an existing Check, (b) the withdrawal of a Check and (c) any other change that materially reduces the functionality of a Check that the Customer has used in the preceding three (3) months. A change that is required by law, by a data source or supplier of STRIKE, or by a security incident may be implemented immediately.

4.3 If a change referred to in Article 4.2 materially disadvantages the Customer, the Customer may cancel its Subscription with effect from the date on which the change becomes effective, by giving notice before that date. Unused Tokens remain available for other Checks for their remaining Validity Period. If the withdrawal of a Check leaves the Customer without any reasonable use for the Tokens it has purchased, the Customer may terminate the Agreement with effect from the date of the withdrawal, in which case Article 10.6 applies.

4.4 Each Check belongs to a Check Category. The Check Category determines the data protection roles of the parties as set out in the Data Processing Terms. STRIKE may add a new Check to an existing Check Category without amending the Data Processing Terms. STRIKE may only introduce a new Check Category by amending Schedule 1 to the Data Processing Terms in accordance with Article 18 of these Terms.

4.5 The Checks rely on data sources operated by STRIKE, by its group companies and by third parties, such as reference databases, public registers, banks, mobile network operators, document verification providers and sanctions and politically exposed persons lists. STRIKE selects and monitors its sources with care but has no control over their content. The Output is an indication based on the information available in those sources at the moment of the

Check; it is not a guarantee of the identity, integrity, creditworthiness or legal status of an End User.

4.6 The Platform combines the results of the Checks in a flow into an overall outcome on the basis of the rules that the Customer has configured for that flow, and makes that outcome available to the Customer. The Customer is solely responsible for those rules, for any decision that it takes on the basis of the Output and for complying with its own legal obligations, including its obligations under anti-money laundering, gambling, financial supervision and data protection law. The Output does not constitute legal, compliance or financial advice. The Platform does not inform the End User of the outcome; the Customer does so where appropriate. Where the law requires meaningful human involvement in a decision about an End User, the Customer ensures that such involvement takes place.

4.7 STRIKE may offer features labelled as beta, pilot or preview. Such features are provided for evaluation purposes only, may be changed or withdrawn at any time and are excluded from any service level or warranty.

4.8 STRIKE provides the Documentation and reasonable technical support through the support function in the Account, on Business Days between 09:00 and 17:00 Central European Time. STRIKE aims to give a first response within two (2) Business Days. STRIKE uses reasonable efforts to keep the Platform available around the clock and aims for a monthly availability of 99.5%, not counting maintenance, force majeure and unavailability of third-party sources. The response time and the availability stated in this Article are targets and not guarantees; they do not give rise to service credits or other compensation.

4.9 STRIKE publishes the End User Notice on the Legal Page. A Hosted Flow shows the name of the Customer and the steps that the Customer has configured. It does not by itself present the End User Notice or ask the End User for consent. The Customer therefore ensures that, before an End User starts a Hosted Flow, (a) the End User has received the information required by Articles 13 and 14 GDPR, including the content of the End User Notice or a link to it, in the Customer's own journey or in an information step that the Customer places at the start of the flow, and (b) any consent that the law requires for a Check has been obtained in accordance with Article 28.1. The End User Notice supplements, and does not replace, the Customer's own privacy information. If STRIKE adds the End User Notice, a link to it or a consent step to the Hosted Flow as a standard element, the Customer may not remove, hide or alter that element.

4.10 The Customer acknowledges that the Platform records technical data of the End User's visit (such as IP address, browser, operating system, device type, language, referring page and campaign parameters) as soon as a Hosted Flow is opened, that data which the Customer passes in when it starts a verification is stored with that verification, and that Checks which need no input from the End User may be performed as soon as the flow starts, depending on the configuration chosen by the Customer. The Customer passes in no more Personal Data than the flow requires. STRIKE may ask the Customer for evidence of the information given to End Users and of the consents obtained. Failure to inform End Users or to obtain a required consent is a material breach of the Agreement; STRIKE may suspend the affected Checks until the Customer has demonstrated compliance.

4.11 Where the Customer adds its own styling, scripts or tracking technologies to a Hosted Flow, the Customer does so at its own risk and responsibility. The Customer is the sole Controller for the data collected by those scripts and technologies, obtains any consent that the law requires for them, and does not use them to capture document images, live images, identification numbers or the content of the steps of the flow. STRIKE may remove or block

styling, scripts or technologies that endanger the security or proper functioning of the Platform or that infringe the Agreement.

4.12 STRIKE may offer additional plans, features or service levels against a separate Fee. The terms that apply to them, including any availability commitment, are published on the Legal Page or stated at the Order and then form part of the Agreement. As long as the Customer has not taken such a plan, no service level, service credit or guaranteed response time applies.

5. Permitted use and Customer obligations

5.1 The Customer uses the Service exclusively for its own lawful business purposes and in accordance with the Agreement, the Documentation and applicable law.

5.2 The Customer warrants that for every Check it performs it (a) has a valid legal basis under data protection law to submit the Personal Data of the End User and to obtain the Output, (b) has provided the End User with the information required by Articles 13 and 14 GDPR, including a reference to the use of a verification service provider, and (c) complies with any additional requirement that applies to the Check or Check Category concerned, such as obtaining explicit consent for the processing of biometric data and any consent that a bank, identity scheme or mobile network operator requires. The Service is not intended for the verification of persons under sixteen (16) years of age; where the Customer nevertheless submits data of such a person, the Customer warrants that it has a legal basis to do so and, where required, the consent of the holder of parental responsibility. Where the Customer performs Checks that include facial comparison on End Users who are residents of a jurisdiction with specific biometric privacy legislation (such as the Illinois Biometric Information Privacy Act, the Texas Capture or Use of Biometric Identifier Act or the Colorado Privacy Act), the Customer provides the notices and obtains the written release or consent required by that legislation before capture, and sets the retention period of its Account and erases individual verifications in such a way that every retention and destruction deadline of that legislation is met. Schedule 1, Part D, and Schedule 2, section 7, describe how long images and biometric data are kept on the Platform and how they are destroyed.

5.3 The Customer shall not, and shall not allow any third party to: (a) perform Checks on persons for private, journalistic, political, discriminatory, harassing or otherwise unlawful purposes; (b) use the Output, the Documentation or any part of the Platform to build, train, enrich or verify a database, machine learning or AI model, or product that competes with the Service or with any data source of STRIKE, or train any machine learning or AI model on the Output without STRIKE's prior written consent; (c) submit data that it is not entitled to submit, including citizen service numbers (BSN) where no statutory basis for their processing exists; (d) circumvent usage limits, rate limits or security measures; (e) reverse engineer, decompile or scrape the Platform except where mandatory law permits this; (f) introduce malicious code or test the security of the Platform without STRIKE's prior written permission; (g) use the Service in violation of sanctions or export control laws; (h) create multiple Accounts or organisations to obtain Trial Tokens more than once or to circumvent usage limits; (i) interfere with, bypass or test the liveness, anti-spoofing or fraud controls of a Hosted Flow; or (j) use the Output as the sole basis for an adverse decision about an End User where the law requires human involvement, or present the Output to third parties as a credit report, certificate or legal determination of identity.

5.4 STRIKE may set usage limits for the Platform and the API and may throttle or temporarily block traffic that exceeds those limits or that threatens the stability or security of the

Platform. The Customer integrates with the Platform in accordance with the Documentation, including the use of HTTPS, the verification of the signature of webhooks, the protection of API keys and the immediate revocation and replacement of an API key that may have been compromised.

5.5 The Customer provides STRIKE on first request with the information that STRIKE reasonably needs to verify compliance with this Article 5, including a description of the use case and the legal basis relied upon for a Check Category.

5.6 Where the Customer is an institution within the meaning of the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wwft) or comparable legislation, or a licence holder under the Dutch Betting and Gaming Act (Wet op de kansspelen) or comparable legislation, the Customer remains fully responsible towards its supervisory authority for the customer due diligence it performs with the help of the Service. STRIKE will, within the limits of the Agreement, cooperate with reasonable requests of the Customer or its supervisory authority for information about the Service.

5.7 The test environment of the Platform consults the same live sources as the production environment. The Customer therefore uses the test environment only with data of persons for whom it has a legal basis and who have been informed, such as its own staff who take part in the test; all obligations of the Customer under the Agreement, including Articles 4.9, 5.2 and 28, apply to the test environment in full.

6. Tokens and Token Bundles

6.1 Tokens are obtained by purchasing a Token Bundle, through a Subscription or as Trial Tokens. The price of Tokens, the Token Bundles and Subscriptions on offer and any bonus Tokens granted with a larger Token Bundle are stated in the Service Catalogue at the moment of the Order. Where the Platform offers the option to purchase an amount of the Customer's own choice, that purchase is a Token Bundle without bonus Tokens. Purchased Tokens are credited to the Account once Stripe has confirmed that the payment has succeeded. STRIKE may also credit Tokens manually, for example after payment of a separate invoice, as a correction or as a gesture of goodwill.

6.2 All Tokens, however obtained, have a Validity Period of twelve (12) months from the date on which they are credited to the Account, unless a different Validity Period is stated at the Order or, for Tokens credited free of charge, at the grant. The Validity Period of purchased Tokens is never shorter than three (3) months. The Validity Period that applies at the moment of the Order is binding for the Tokens of that Order.

6.3 Tokens that have not been consumed at the end of their Validity Period lapse without compensation. The purchase of further Tokens does not extend the Validity Period of Tokens already in the Account. The Account shows one Token balance; the records of STRIKE determine on which date Tokens were credited and on which date they lapse. STRIKE may remind the Customer before Tokens lapse but is not obliged to do so. If STRIKE removes lapsed Tokens from the balance later than the end of their Validity Period, this is not a waiver of the lapse of those or of other Tokens; Checks performed with those Tokens in the meantime remain paid for.

6.4 Tokens are deemed to be consumed in the order in which they were credited to the Account, the oldest first, so that the Tokens that lapse first are consumed first.

6.5 Tokens are not refundable, not transferable to another Account or legal entity, cannot be exchanged for money and have no monetary value outside the Platform, except where Article 10.6 provides otherwise. Tokens may only be consumed for Checks performed through the Account to which they were credited.

6.6 A Check is debited when it has been completed with a final result, whatever that result is. A Check that returns a negative, inconclusive or "no match" result is a completed Check and is debited, because the result reflects the information available in the source. A Check that ends in a technical error on the side of STRIKE or its sources, or that is still waiting for a result, is not debited. A session that the End User abandons before a Check has been completed is not debited for that Check. Repeated attempts within the same step of a flow, for example because an image is unreadable, are debited once. Where the flow configured by the Customer leads the End User back to a step that has already been completed, that step is performed again and debited again. Checks performed in the test environment consult live sources and are debited in the same way as Checks in the production environment. The Service Catalogue may provide for specific debiting rules per Check.

6.7 The Customer may enable automatic top-up in the Account. The Customer then selects the balance below which a top-up takes place, the quantity of Tokens to be purchased and a maximum amount per calendar month. Whenever the Token balance falls below the selected threshold, STRIKE places an Order for the selected quantity on the Customer's behalf and charges the payment method linked to the Account, up to the selected monthly maximum. Automatic top-up pauses when a payment fails, until the Customer enables it again. The Customer may change or disable automatic top-up at any time; Orders already placed are not affected.

6.8 Trial Tokens are granted at STRIKE's discretion, are limited in number and validity, may be withdrawn at any time, and may only be used to evaluate the Service with End Users for whom the Customer has a legal basis. A Customer may not obtain Trial Tokens more than once, including by registering multiple Accounts or organisations. Trial Tokens are never refunded or converted.

6.9 The Account shows the current Token balance and the consumption history. The records of STRIKE constitute full evidence of the Tokens credited, consumed and lapsed, subject to proof to the contrary by the Customer.

6.10 A verification that has been started is completed even if the Token balance is not sufficient for all its Checks; the balance may then become negative. A negative balance is a debt of the Customer that is settled with the next Tokens credited to the Account and that STRIKE may invoice at the price per Token that applies to the smallest Token Bundle on offer. STRIKE may refuse the start of new verifications for as long as the balance is not sufficient.

6.11 STRIKE and the Customer may agree individual Token Costs, surcharges or discounts. STRIKE applies them in the Account, where they prevail over the Service Catalogue for the period agreed.

7. Subscriptions

7.1 A Subscription starts on the date of the Order and runs for successive Subscription Periods. It renews automatically for a further Subscription Period of the same length until the Customer cancels it through the subscription management page that is reached from the Account and operated by Stripe. Cancellation takes effect at the end of the current Subscription Period. No refund is made for a Subscription Period that has started.

7.2 In each Subscription Period the Customer receives the quantity of Tokens stated at the Order. The Tokens are credited to the Account once the payment for that Subscription Period has succeeded. Tokens credited under a Subscription have the Validity Period of Article 6.2 and remain available for the rest of that period after the Subscription has ended, for as long as the Agreement continues.

7.3 The Customer can hold one Subscription at a time. To change to a different Subscription the Customer cancels the current Subscription and places a new Order; additional Tokens can be purchased at any time as a Token Bundle. STRIKE may offer the possibility to upgrade or downgrade a Subscription; the conditions are then stated at the Order.

7.4 Where STRIKE offers Subscriptions with a longer Subscription Period or with a minimum term, for example against a lower price, the period, the minimum term and the conditions are stated at the Order. Such a Subscription cannot be cancelled with effect before the end of its minimum term.

7.5 STRIKE may change the price of a Subscription with at least thirty (30) days' notice by e-mail to the Account Administrators. The new price applies from the first renewal after the notice period. The Customer may cancel the Subscription with effect from that renewal if it does not accept the new price.

7.6 If the payment for a Subscription Period fails, no Tokens are credited for that period. STRIKE may end the Subscription if the payment has not succeeded within fourteen (14) days after the renewal date.

8. Fees, payment and Stripe

8.1 All Fees are stated in euro and exclusive of VAT and other levies. The Customer owes the Fees stated in the Service Catalogue at the moment of the Order, subject to Article 6.11.

8.2 Payment is made through the payment pages operated by Stripe. By placing an Order the Customer accepts that Stripe processes the payment and that the terms of Stripe applicable to the chosen payment method apply to that payment. STRIKE does not receive or store full payment card details; these are processed by Stripe as an independent payment service provider.

8.3 By taking out a Subscription or enabling automatic top-up the Customer authorises STRIKE and Stripe to charge the selected payment method for each renewal and each top-up until the Subscription is cancelled or the automatic top-up is disabled. The Customer keeps a valid payment method linked to the Account for the duration of each Subscription.

8.4 Invoices and receipts are issued electronically. The Customer agrees to electronic invoicing. The Customer is responsible for providing correct invoicing details, including a valid VAT identification number where it has one. VAT is calculated at checkout on the basis of those details and in accordance with applicable VAT law. Where the Customer is established in another EU member state and has provided a valid VAT identification number, VAT is reverse charged in accordance with Articles 44 and 196 of Council Directive 2006/112/EC; otherwise STRIKE charges the VAT that is due. The Customer indemnifies STRIKE against any VAT, interest and penalties resulting from incorrect information provided by the Customer.

8.5 If a payment fails, is reversed or is charged back, STRIKE may immediately withdraw the Tokens that have not been paid for, suspend the affected Subscription and the Account, and recover the amount due together with the reasonable costs of recovery. From the due date

the Customer owes the statutory commercial interest under Article 6:119a of the Dutch Civil Code without further notice of default.

8.6 The Customer is not entitled to suspend payment or to set off amounts owed to STRIKE against any claim it has or alleges to have against STRIKE.

8.7 STRIKE may adjust the prices in the Service Catalogue annually in line with the consumer price index (CPI, all households) as published by Statistics Netherlands (CBS) for the month of October of the preceding year, and may at any time pass on increases imposed by its data or infrastructure suppliers, in each case with the notice stated in Article 4.2. A price change does not affect Tokens that have already been credited.

9. Suspension

9.1 STRIKE may suspend or restrict the Account, individual Authorised Users, API keys, Checks or Check Categories, in whole or in part, if (a) the Customer is in breach of Article 3, 4.9, 5 or 8, (b) STRIKE reasonably suspects fraud, misuse or unlawful processing of Personal Data, (c) a competent authority, court or data source requires it, (d) the security or integrity of the Platform or of the Personal Data of End Users is at risk, or (e) the Customer's verification under Article 3.2 or 3.3 cannot be completed.

9.2 Where reasonably possible STRIKE will inform the Customer in advance and give it the opportunity to remedy the situation. Suspension does not relieve the Customer of its payment obligations and does not extend the Validity Period of Tokens or the term of a Subscription. STRIKE is not liable for damage resulting from a suspension made in accordance with this Article.

10. Term, termination and consequences

10.1 The Agreement is entered into for an indefinite period. The Customer may terminate the Agreement at any time by giving notice to STRIKE through the support function in the Account or by e-mail to info@trustbystrike.com, sent by an Account Administrator. STRIKE then closes the Account within ten (10) Business Days after the notice, or on the later date that the Customer requests. The Customer cancels any running Subscription itself in accordance with Article 7.1; if it has not done so, STRIKE may cancel the Subscription on the Customer's behalf when it closes the Account.

10.2 STRIKE may terminate the Agreement for convenience with two (2) months' notice by e-mail.

10.3 Either party may terminate the Agreement with immediate effect by written notice if the other party (a) commits a material breach that is not remedied within fourteen (14) days of a written notice specifying the breach, or that cannot be remedied, (b) is declared bankrupt, applies for a suspension of payments or is wound up, or (c) ceases its business activities. STRIKE may also terminate with immediate effect if the Customer breaches Article 4.9, 5.2 or 5.3, or if a verification under Article 3 reveals that the Customer has provided false information.

10.4 Upon termination for whatever reason (a) the right to use the Service ends, (b) all Subscriptions end, (c) unused Tokens lapse subject to Article 10.6, (d) all Fees due become immediately payable, and (e) STRIKE provides the Customer, on a request made no later than thirty (30) days after the effective date of termination, with an export of the Customer Data that is stored on the Platform at that time, in a structured, commonly used and

machine-readable format. STRIKE provides this export free of charge and without switching charges, in accordance with Chapter VI of Regulation (EU) 2023/2854 (Data Act). During the term of the Agreement the Customer can retrieve the data of individual verifications through the Account and the API.

10.5 After the period referred to in Article 10.4(e), or earlier if the Customer requests this in writing, STRIKE deletes the Customer Data in accordance with the Data Processing Terms, unless and to the extent that STRIKE is required by law to retain it or Customer Data is contained in routine back-ups that are deleted in the ordinary course within the period stated in the Data Processing Terms.

10.6 If STRIKE terminates the Agreement for convenience under Article 10.2, or if the Customer terminates under Article 4.3 because the withdrawal of a Check left it without any reasonable use for its purchased Tokens, STRIKE refunds the price paid for the purchased Tokens that are unused and within their Validity Period on the effective date of termination. The refund is calculated on the price per Token actually paid in the Order concerned, applying the order of consumption of Article 6.4. Bonus Tokens, Trial Tokens and other Tokens credited free of charge are never refunded. In all other cases no refund is made.

10.7 Articles 1, 2.5, 5.2, 5.3, 6.5, 8, 10, 12, 13, 14, 15, 16, 17 and 21 and any other provision that by its nature is intended to survive, remain in force after termination.

11. Changes to the Platform and maintenance

11.1 STRIKE may update, patch, migrate or otherwise change the Platform. STRIKE will use reasonable efforts to maintain backward compatibility of the API for at least six (6) months after announcing a change that is not backward compatible, except where a shorter period is required for security or legal reasons.

11.2 Maintenance that is expected to make the Platform unavailable for more than thirty (30) minutes is announced by e-mail to the Account Administrators at least forty-eight (48) hours in advance where reasonably possible, and is performed outside Dutch business hours where reasonably possible. Short interruptions for the release of new versions and urgent maintenance for security reasons may take place without prior announcement.

12. Data protection

12.1 The parties' roles in the Processing of Personal Data are set out in the Data Processing Terms (Part B). In summary: for the Personal Data of End Users that the Customer submits, or has End Users submit, to perform a Check, the Customer is the Controller and STRIKE is the Processor. For the reference data that STRIKE and its group companies maintain and use to perform validation Checks, STRIKE and those group companies are independent Controllers. Third parties such as banks, bank-based identity schemes, mobile network operators, public registers and Stripe act as independent Controllers for their own processing. Schedule 1 sets out the roles per Check Category.

12.2 The Customer instructs STRIKE to Process End User Personal Data to perform the Checks that the Customer has included in its flows and to return the Output. The Customer acknowledges that configuring a flow and starting a verification constitute documented instructions within the meaning of Article 28(3)(a) GDPR.

12.3 STRIKE processes Personal Data of Authorised Users and of the Customer's contact persons as a Controller for account management, security, invoicing and communication, as

described in the VerifyMe Privacy Statement. The Customer ensures that its Authorised Users have been informed of that Privacy Statement.

12.4 STRIKE may use data about the use of the Service, such as the number and type of Checks performed, response times, error rates and results at aggregated level, for the purpose of operating, monitoring, securing, supporting and invoicing the Service; for that purpose the data may be linked to an Account and to the number of a verification. For the purpose of improving and benchmarking the Service STRIKE uses such data only in aggregated form that cannot be related to an identifiable End User. STRIKE will not use End User Personal Data to enrich or train its reference databases unless the Service Catalogue states so for a specific Check and the Customer has enabled that Check.

12.5 STRIKE does not sell, rent, trade or otherwise commercialise Personal Data of End Users or of Authorised Users, and does not use End User Personal Data for its own purposes to train or improve machine learning models or to build profiles of End Users. Functions that the Customer enables for its own purposes, such as the detection of duplicate verifications within its own Account and the analysis of the use of its own flows, are performed on the Customer's instruction and on its behalf.

13. Confidentiality

13.1 Each party keeps confidential all information of the other party that is marked as confidential or that it should reasonably understand to be confidential, including the terms of any individual arrangement, non-public information about the Platform, its security measures, the identity of its data sources and Sub-processors as provided under Article 30.1, and Customer Data. Confidential information may only be used for the performance of the Agreement.

13.2 The obligation does not apply to information that is or becomes public without breach of this Article, was already lawfully known to the receiving party, is independently developed, or must be disclosed under a legal or regulatory obligation, provided that the receiving party, where permitted, informs the other party in advance.

13.3 Each party imposes equivalent obligations on its employees, group companies and subcontractors who have access to confidential information. This Article remains in force for five (5) years after the end of the Agreement, and indefinitely for trade secrets and Personal Data.

14. Intellectual property

14.1 All intellectual property rights in the Platform, the Documentation, the Service Catalogue, the reference databases, the algorithms, scoring models and the structure of the Output belong exclusively to STRIKE, its group companies or its licensors. The Customer only obtains a non-exclusive, non-transferable and non-sublicensable right to use the Service during the term of the Agreement for the purposes described in Article 5.

14.2 The Customer retains all rights in the Customer Data. The Customer grants STRIKE a non-exclusive licence to Process Customer Data to the extent necessary to perform the Agreement and as permitted by Article 12.4.

14.3 The Customer may use the Output for its own internal business purposes, including compliance with its legal obligations, and may store it in its own records. The Customer shall

not disclose, sell or license the Output to third parties, except to its own advisers, auditors and supervisory authorities, or as required by law.

14.4 If the Customer provides feedback or suggestions about the Service, STRIKE may use them without restriction or compensation.

14.5 STRIKE indemnifies the Customer against third-party claims that the Platform, as provided by STRIKE and used in accordance with the Agreement, infringes an intellectual property right valid in the European Union, provided that the Customer notifies STRIKE promptly, leaves the defence to STRIKE and provides reasonable assistance. STRIKE may, at its option, procure the right for the Customer to continue using the Platform, modify or replace the infringing part, or terminate the Agreement and refund the price of unused purchased Tokens in accordance with Article 10.6. This Article states STRIKE's entire liability for infringement.

15. Warranties and disclaimers

15.1 STRIKE warrants that it provides the Service with reasonable skill and care and substantially in accordance with the Documentation and the Service Catalogue.

15.2 The Service is otherwise provided "as is". STRIKE does not warrant that the Service is uninterrupted or error-free, that the Output is accurate, complete or up to date, or that the Service meets the specific requirements of the Customer or of any supervisory authority. STRIKE does not warrant the identity, integrity or legal status of any End User; the Output is an indication for the Customer's own assessment. The Customer acknowledges that the accuracy of the Output depends on the quality of the data submitted by the Customer or the End User and on the content of third-party sources, for which STRIKE accepts no responsibility.

15.3 The Customer must notify STRIKE in writing of any defect in the Service within thirty (30) days after it discovered or should reasonably have discovered the defect, stating the defect in sufficient detail, failing which the Customer's rights in respect of that defect lapse.

16. Liability

16.1 STRIKE's total aggregate liability towards the Customer under or in connection with the Agreement, whether in contract, tort (including negligence), breach of statutory duty or otherwise, is limited per contract year to the total Fees paid by the Customer in the twelve (12) months preceding the event giving rise to the claim, up to a maximum of EUR 25,000 (twenty-five thousand euro) per contract year. A series of connected events counts as one event.

16.2 STRIKE is not liable for indirect or consequential damage, including loss of profit, loss of revenue, loss of business, loss of goodwill, loss or corruption of data, damage resulting from decisions taken on the basis of the Output, administrative fines or penalties imposed on the Customer, and claims of End Users or other third parties against the Customer, except to the extent such damage results directly from an attributable breach by STRIKE of the Data Processing Terms.

16.3 The limitations in this Article do not apply to liability for damage caused by intent or deliberate recklessness of STRIKE's management, to death or personal injury, or to any other liability that cannot be limited under mandatory law.

16.4 Any claim for damages lapses twelve (12) months after the Customer became aware or should reasonably have become aware of the damage and of STRIKE as the liable party.

16.5 The liability regime in the Data Processing Terms applies to the Processing of Personal Data and is subject to the same cap as this Article 16, unless the Data Processing Terms expressly provide otherwise.

17. Indemnification by the Customer

17.1 The Customer indemnifies STRIKE, its group companies and their directors, employees and subcontractors against all claims, damages, fines, costs and expenses (including reasonable legal fees) arising from (a) a breach by the Customer of Article 3, 4.9, 4.11, 5 or 12, (b) the absence of a valid legal basis or consent for a Check or of adequate information to End Users, (c) decisions taken by the Customer on the basis of the Output, (d) claims of End Users or supervisory authorities relating to the Customer's use of the Service, and (e) inaccurate registration or invoicing data.

18. Changes to the Terms, the Data Processing Terms and the Service Catalogue

18.1 STRIKE may amend these Terms, including the Data Processing Terms. STRIKE notifies the Customer of an amendment at least thirty (30) days before it takes effect, by e-mail to the Account Administrators and by publishing the new version on the Legal Page. The notice identifies the changes.

18.2 If the Customer does not accept an amendment that materially disadvantages it, the Customer may terminate the Agreement with effect from the date on which the amendment takes effect. Continued use of the Service after that date constitutes acceptance of the amended Terms; the Platform may in addition ask Authorised Users to confirm the new version. Amendments that are required by law or by a supervisory authority, that concern a new Check Category under Article 4.4 and are favourable or neutral to the Customer, or that are merely clarifying, may take effect immediately upon notice.

18.3 Changes to the Service Catalogue are governed by Article 4.2 and do not require the procedure in this Article.

18.4 STRIKE publishes the current version of these Terms, with its version number and effective date, on the Legal Page and provides earlier versions on request.

19. Force majeure

19.1 Neither party is liable for a failure to perform its obligations, other than payment obligations, if the failure results from circumstances beyond its reasonable control (force majeure, Article 6:75 of the Dutch Civil Code). For STRIKE, force majeure in any event includes: failure, unavailability or changes of third-party data sources, registers, banks, identity schemes, mobile network operators or payment providers; internet, hosting or telecommunications failures not caused by STRIKE; distributed denial-of-service and other cyber attacks despite reasonable security measures; government measures; strikes; and pandemics.

19.2 If force majeure lasts longer than sixty (60) consecutive days, either party may terminate the Agreement with immediate effect without liability. STRIKE then refunds the price of unused purchased Tokens in accordance with Article 10.6.

20. Miscellaneous

20.1 The Customer may not assign or transfer the Agreement or any right under it without STRIKE's prior written consent. STRIKE may assign the Agreement to a group company or to a successor of its business upon notice to the Customer.

20.2 Notices under the Agreement are given in writing by e-mail: to the Customer at the e-mail addresses of the Account Administrators, and to STRIKE at info@trustbystrike.com or through the support function in the Account. Privacy matters are addressed to privacy@trustbystrike.com and security incidents to security@trustbystrike.com. A notice is deemed received on the next Business Day after sending. The Customer ensures that at least one Account Administrator with a working e-mail address is linked to the Account at all times.

20.3 STRIKE may refer to the Customer as a user of the Service in its customer lists, unless the Customer objects by e-mail.

20.4 If a provision of the Agreement is void or unenforceable, the remaining provisions remain in force and the parties replace the provision with a valid one that approximates its purpose as closely as possible.

20.5 A failure to enforce a provision does not constitute a waiver. The Agreement contains the entire understanding between the parties regarding its subject matter and supersedes all earlier arrangements, including any trial or pilot arrangement, unless a signed written agreement provides otherwise.

20.6 The Customer complies with applicable anti-bribery, sanctions and export control laws in connection with its use of the Service and warrants that neither it nor its ultimate beneficial owners are the subject of EU, UN, UK or US sanctions.

20.7 These Terms are drawn up in English. Translations are provided for convenience only; the English version prevails.

20.8 Article 7:404, 7:407(2) and 7:409 of the Dutch Civil Code do not apply. Article 6:227b(1) and 6:227c of the Dutch Civil Code do not apply between the parties.

21. Governing law and jurisdiction

21.1 The Agreement and any non-contractual obligation arising out of or in connection with it are governed by the laws of the Netherlands. The United Nations Convention on Contracts for the International Sale of Goods does not apply.

21.2 All disputes arising out of or in connection with the Agreement are submitted exclusively to the competent court of the District Court of Midden-Nederland, location Utrecht, the Netherlands, without prejudice to STRIKE's right to bring proceedings before the court of the Customer's domicile. The parties agree that this clause constitutes an agreement conferring jurisdiction within the meaning of Article 25 of Regulation (EU) No 1215/2012 and that the electronic acceptance of these Terms provides a durable record of that agreement.

21.3 Before starting proceedings, the parties first make a good-faith attempt to resolve the dispute through consultation between representatives who are authorised to settle it.

Part B: Data Processing Terms

Articles 22 to 36 and Schedules 1 to 3. The processor terms required by Article 28 GDPR between the Customer (Controller) and STRIKE (Processor). Accepted together with Part A; no separate signature is needed.

22. Purpose and scope

22.1 This Part B (the "Data Processing Terms") sets out the arrangements between the Customer, as Controller, and STRIKE, as Processor, for the Processing of Personal Data of End Users that STRIKE performs on behalf of the Customer when the Customer uses the Service. It is intended to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 (GDPR) and constitutes the data processing agreement between the parties. It is modelled on the standard contractual clauses between controllers and processors adopted by the European Commission in Implementing Decision (EU) 2021/915 under Article 28(7) GDPR, adapted to a self-service platform.

22.2 These Data Processing Terms form an integral part of the Agreement and are accepted together with Part A by the single acceptance described in Article 2.1. Capitalised terms that are not defined in this Part B have the meaning given to them in Part A. Where these Data Processing Terms and Part A conflict with respect to the Processing of Personal Data, these Data Processing Terms prevail.

22.3 Schedule 1 (Description of the Processing and allocation of roles), Schedule 2 (Technical and organisational measures) and Schedule 3 (Sub-processors) form part of these Data Processing Terms.

22.4 These Data Processing Terms do not apply to Processing for which STRIKE is itself a Controller. That Processing is described in Schedule 1, Part C, and in the VerifyMe Privacy Statement.

23. Roles of the parties

23.1 For the Personal Data that the Customer submits to the Platform, or has End Users submit through a Hosted Flow, in order to perform a Check, for the technical data that the Platform records about an End User's visit to a Hosted Flow, and for the Output, the Customer is the Controller and STRIKE is the Processor. The Customer determines whether, when and for which End Users a Check is performed, which Checks and options its flows contain, how long the data is kept and for which purpose it uses the Output.

23.2 STRIKE and the group companies named in Schedule 3 are independent Controllers for the reference databases that they maintain and against which data submitted for a Check is validated (Schedule 1, Part C). Personal Data submitted for a Check is not added to those reference databases, except where the Service Catalogue states this for a specific Check and the Customer has enabled that Check.

23.3 Third parties that provide a result on the basis of their own data and under their own responsibility act as independent Controllers for their part of the Processing. This applies to banks and the operator of a bank-based identity scheme, to mobile network operators, to the Kansspelautoriteit as the authority that keeps the Dutch central register of exclusion from games of chance, to the keepers of public registers and to payment service providers. A third party that Processes Personal Data on STRIKE's instructions in order to perform a Check, including a provider through which a scheme, an operator or a source is reached, is

a Sub-processor and falls under Article 30 and Schedule 3. Where the Customer connects its own contract with a source or provider to the Platform (Article 3.8), that source or provider acts under the Customer's contract, as the Customer's own processor or as an independent Controller, and is not a Sub-processor of STRIKE. Schedule 1 states the roles per Check Category.

23.4 The parties are not joint controllers. Each party is separately responsible for its own compliance with the GDPR in respect of the Processing for which it is Controller.

23.5 The Customer warrants that it is entitled to act as Controller for the Personal Data it submits and, where it submits data on behalf of a group company or client, that it has the authority to accept these Data Processing Terms on that party's behalf and that these Data Processing Terms extend to that party's Personal Data.

24. Instructions

24.1 STRIKE Processes Personal Data only on documented instructions from the Customer, unless required to do so by Union or Member State law to which STRIKE is subject. In that case STRIKE informs the Customer of that legal requirement before Processing, unless the law prohibits this on important grounds of public interest.

24.2 The Customer's documented instructions consist of (a) these Terms, including these Data Processing Terms, (b) the configuration of the Account, including the flows that the Customer has built, the Checks and options enabled in them, the retention period, the Hosted Flow settings and the Authorised Users, (c) each start of a verification, through the Account, a link or the API, and each erasure of a verification, and (d) any further written instruction agreed between the parties. By including a Check in a flow the Customer instructs STRIKE to perform the Processing described for that Check in the Service Catalogue and in Schedule 1, including the consultation of the sources and the use of the Sub-processors that belong to that Check.

24.3 STRIKE informs the Customer without delay if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection law. STRIKE may suspend the execution of such an instruction until the Customer has confirmed or amended it.

24.4 Instructions that go beyond the functionality of the Platform may result in additional costs. STRIKE informs the Customer in advance and does not perform such instructions before the Customer has agreed to the costs.

25. Purpose limitation

25.1 STRIKE Processes Personal Data only for the specific purpose of performing the Checks that the Customer has included in its flows, returning the Output, operating, securing and supporting the Platform, and complying with its legal obligations, as further described in Schedule 1.

25.2 STRIKE does not Process Personal Data of End Users for its own purposes, does not sell Personal Data and does not use End User Personal Data for marketing, profiling or the training of models. Article 12.4 describes the limited use that STRIKE makes of data about the use of the Service.

26. Duration, return and deletion

26.1 The Processing lasts for the term of the Agreement and, per verification, for the retention period described in this Article and in Schedule 1, Part D.

26.2 The Customer sets one retention period for its Account, of at least thirty (30) and at most one thousand eight hundred and twenty-five (1,825) days. If the Customer makes no choice, the period is three hundred and sixty-five (365) days. The period runs from the completion of a verification or, if a verification is never completed, from its start. At the end of the period the Platform automatically deletes the whole verification: the data entered by the End User, the data passed in by the Customer, the document images, the portrait taken from the document, the live image, the extracted data, the results of the Checks, the overall outcome, the technical data of the visit and the values derived for search and duplicate detection. The retention period applies to the verification as a whole; there is no separate, shorter period for images.

26.3 The Customer can erase an individual verification at any time through the Account or the API. The Platform then keeps only a record that the verification took place (its number, its overall outcome and its dates) and the related entries of Tokens consumed. The Customer chooses a retention period that is no longer than necessary for the purpose for which it performs the Checks (Article 5(1)(e) GDPR) and that fits the statutory retention obligations and destruction deadlines that apply to it, and erases individual verifications where the law requires earlier deletion.

26.4 Upon termination of the Agreement STRIKE provides the export described in Article 10.4 on request. After the period referred to there, or earlier at the Customer's written request, STRIKE deletes all Personal Data Processed on behalf of the Customer within thirty (30) days, unless Union or Member State law requires storage.

26.5 After a deletion under this Article, copies may remain for a limited time for technical reasons: deleted files can be recovered from storage for up to thirty (30) days and database back-ups are kept for up to thirteen (13) weeks. These copies are not used for any purpose other than recovery after an incident and expire automatically.

26.6 STRIKE confirms deletion in writing on request. STRIKE retains, as Controller, the records that are necessary to evidence the Checks performed and the Tokens credited and consumed, for invoicing, tax and dispute purposes. Those records consist of the Account, the type of entry, the number of Tokens or the amount, the time, a description, the payment reference, the verification number, the step and Check type and the balance after the entry. They contain no input data and no Output.

27. Security of processing

27.1 STRIKE implements the technical and organisational measures described in Schedule 2 to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing, in accordance with Article 32 GDPR. The STRIKE Group companies that develop, host and operate the Platform are certified against ISO/IEC 27001; the certificates are available on request.

27.2 STRIKE may update Schedule 2 from time to time, provided that the overall level of security is not reduced. The current Schedule 2 is part of the version of these Terms that is published on the Legal Page.

27.3 STRIKE grants access to Personal Data only to persons who need that access to perform the Agreement and who are bound by confidentiality under contract or by statutory obligation, and ensures that those persons have received appropriate instruction.

27.4 The Customer is responsible for the security of its own systems, credentials and API keys, for configuring the Account and its flows appropriately, for the accuracy of the data it submits and for the lawful onward use of the Output.

28. Special categories of data, national identification numbers and automated outcomes

28.1 Where a Check involves facial comparison (Schedule 1, Check Category C), biometric data within the meaning of Article 9 GDPR is Processed on behalf of the Customer. Facial comparison and liveness detection are switched off by default and are only performed where the Customer has enabled them for a step in its flow. The Customer warrants that it has a valid condition under Article 9(2) GDPR and, where applicable, under national law (in the Netherlands, Article 29 of the GDPR Implementation Act (UAVG)) for that Processing, and that it has informed the End User accordingly. Where that condition is the explicit consent of the End User, the Customer obtains and records the consent before the capture starts, in one of the following ways: (a) by placing, directly before each step for which facial comparison is enabled, a confirmation step in the flow in which the End User actively confirms the consent text that STRIKE makes available in the Documentation or on the Legal Page, or a text that gives the End User at least the same information, which confirmation the Platform records with the time; or (b) by obtaining the consent in its own journey before the End User starts the Hosted Flow and keeping its own record of it. In both cases the Customer keeps a record of the text that was presented to the End User. The Customer offers an End User who does not give consent another way to be verified where the law requires that consent can be refused without detriment. If STRIKE adds a standard consent step to the Hosted Flow, the Customer uses that step from the moment it is available. The recording of a confirmation by the Platform is a measure taken on behalf of the Customer and does not make STRIKE the Controller for that consent. STRIKE applies the additional measures in Schedule 2, section 7, for these Checks.

28.2 The Dutch citizen service number (BSN) and comparable national identification numbers may only be Processed where the Customer has a statutory basis (in the Netherlands, Article 46 UAVG). When the Platform reads an identity document, it masks the BSN field on the stored image and does not store the BSN or the data of the machine-readable zone. The Platform offers an option, switched off by default, to store with a verification a coded value derived from part of the BSN in order to detect duplicate verifications. The Customer only enables that option, and only passes a BSN to the Platform when it starts a verification or in a form, where it has a statutory basis for Processing the BSN; by enabling the option or passing the number the Customer confirms to STRIKE that it has such a basis. For Checks against the Dutch central register of exclusion from games of chance, the BSN entered by the End User is passed to the register through the Customer's own connection and is not stored on the Platform.

28.3 Output of screening and register Checks (Schedule 1, Check Categories D and F) may reveal that an End User appears on a sanctions or politically exposed persons list or in adverse media, is subject to insolvency or guardianship, is deceased or is registered in an exclusion register. The Customer uses such Output only for the compliance purpose for which the Check was performed. The overall outcome that the Platform derives from the

Checks in a flow follows from rules set by the Customer (Article 4.6). The Customer ensures that a decision with legal or similarly significant effects for an End User is not based solely on that outcome or on other automated Processing unless an exception of Article 22(2) GDPR applies, and that the End User can obtain human intervention, express his or her point of view and contest the decision where Article 22(3) GDPR requires this.

29. Documentation, compliance and audits

29.1 STRIKE makes available to the Customer all information necessary to demonstrate compliance with Article 28 GDPR and with these Data Processing Terms. STRIKE does so primarily through (a) the current ISO/IEC 27001 certificates referred to in Article 27.1, (b) a summary of the most recent security review of the Platform and, once it is available, of the most recent independent penetration test, (c) these Data Processing Terms and their Schedules, and (d) answers to a reasonable written security and privacy questionnaire, at most once per year. STRIKE has an independent penetration test of the Platform performed within six (6) months after 13 November 2026 and at least once a year after that.

29.2 If the information under Article 29.1 is not sufficient to demonstrate compliance, the Customer, or an independent auditor mandated by it and bound by confidentiality, may audit the Processing. An audit takes place at most once per contract year, unless a supervisory authority requires otherwise or a Personal Data Breach affecting the Customer has occurred. The Customer gives at least thirty (30) days' written notice, the parties agree the scope and timing in good faith, the audit is conducted during Business Days without disrupting STRIKE's operations, and the Customer bears its own costs and STRIKE's reasonable costs of cooperation. STRIKE may refuse an auditor that is a competitor of STRIKE.

29.3 STRIKE provides supervisory authorities competent for the Customer, including authorities supervising compliance with anti-money laundering or gambling legislation, with the information and access to which they are entitled by law, and informs the Customer of such requests where permitted. If STRIKE receives a request from a public authority, court or law enforcement body for Personal Data Processed on behalf of the Customer, STRIKE verifies the legal basis of the request, discloses no more than is legally required, and, unless prohibited by law, informs the Customer before disclosure so that the Customer can seek a protective order or other remedy.

29.4 STRIKE maintains a record of Processing activities carried out on behalf of the Customer in accordance with Article 30(2) GDPR.

30. Sub-processors

30.1 The Customer grants STRIKE a general written authorisation to engage Sub-processors. Schedule 3 lists the Sub-processors engaged at the effective date of this version, with their Processing activity, their location and the transfer mechanism. STRIKE's group companies and its hosting provider are listed by name. The other Sub-processors are listed by a code and by their function, because the identity of the data sources and providers that STRIKE has contracted is a trade secret of STRIKE. On request of the Customer STRIKE provides, within five (5) Business Days, the name, address and contact details of every Sub-processor that Processes Personal Data on the Customer's behalf. That information is confidential information of STRIKE under Article 13. The Customer may use it, and pass it on, only to the extent necessary to meet its own obligations under data protection law, such as its

records of processing activities, a data protection impact assessment, an audit, a request of a Data Subject who is entitled to the information or a request of a supervisory authority.

30.2 STRIKE informs the Customer of any intended addition or replacement of a Sub-processor at least thirty (30) days before the Sub-processor starts Processing Personal Data, by e-mail to the Account Administrators, stating the Processing activity, the location and the transfer mechanism of the new Sub-processor; its identity is provided on request in accordance with Article 30.1. The Customer may object on reasonable, documented grounds relating to data protection within that period; if no objection is received within that period, the Sub-processor is deemed accepted. The parties discuss an objection in good faith. If no solution is found, the Customer may stop using the affected Checks or terminate the Agreement with effect from the date the Sub-processor starts, in which case STRIKE refunds the price of unused purchased Tokens in accordance with Article 10.6.

30.3 STRIKE imposes on each Sub-processor, by way of a written contract, data protection obligations that are substantially the same as those in these Data Processing Terms, in particular sufficient guarantees to implement appropriate technical and organisational measures. STRIKE remains fully liable to the Customer for the performance of the Sub-processor's obligations.

30.4 STRIKE provides, on request, a copy of the data protection terms agreed with a Sub-processor, redacted for commercial information.

30.5 Companies within STRIKE's group that are involved in operating the Service or performing Checks are Sub-processors and are listed in Schedule 3.

31. International transfers

31.1 STRIKE hosts the Platform and stores the Personal Data that it Processes on behalf of the Customer within the European Economic Area. Sub-processors Process Personal Data within the European Economic Area, except where Schedule 3 states another location for a specific Sub-processor. STRIKE does not otherwise transfer Personal Data to a third country or international organisation except on the Customer's documented instruction or where required by Union or Member State law. By including in a flow a Check or function for which Schedule 3 states a location outside the European Economic Area, the Customer instructs STRIKE to make the transfer that belongs to it.

31.2 Where a Sub-processor Processes Personal Data outside the European Economic Area, STRIKE ensures that the transfer is covered by an adequacy decision under Article 45 GDPR or by appropriate safeguards under Article 46 GDPR, such as the standard contractual clauses adopted by the European Commission in Implementing Decision (EU) 2021/914, together with supplementary measures where a transfer impact assessment shows these to be necessary. Where STRIKE relies on the EU-US Data Privacy Framework, STRIKE also puts the standard contractual clauses in place as a fallback. The transfer mechanism per Sub-processor is stated in Schedule 3.

31.3 If the Customer itself is established outside the European Economic Area, or submits Personal Data from outside it, the Customer is responsible for the lawfulness of the transfer of Personal Data to STRIKE under the law applicable to it.

32. Assistance to the Controller

32.1 STRIKE promptly, and in any event within five (5) Business Days, forwards to the Customer any request it receives directly from a Data Subject relating to Personal Data Processed on behalf of the Customer. STRIKE does not respond to the request itself, other than to confirm receipt and to refer the Data Subject to the Customer, unless the Customer authorises it to do so.

32.2 Taking into account the nature of the Processing, STRIKE assists the Customer by appropriate technical and organisational measures in fulfilling the Customer's obligation to respond to requests for exercising Data Subject rights under Chapter III GDPR. The Platform allows the Customer to search for, retrieve and erase the verifications of individual End Users. Assistance beyond that functionality is provided at STRIKE's then current hourly rates.

32.3 Taking into account the nature of the Processing and the information available to STRIKE, STRIKE assists the Customer in ensuring compliance with Articles 32 to 36 GDPR, including by providing the information in Schedule 1 and Schedule 2 for the Customer's data protection impact assessment and by cooperating with a prior consultation of the supervisory authority.

33. Personal Data Breach

33.1 STRIKE notifies the Customer without undue delay, and in any event within forty-eight (48) hours, after becoming aware of a Personal Data Breach affecting Personal Data Processed on behalf of the Customer. The notification is sent by e-mail to the Account Administrators.

33.2 The notification contains, to the extent available, the information listed in Article 33(3) GDPR: the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, the measures taken or proposed and a contact point. Information that is not yet available is provided in phases without undue further delay.

33.3 STRIKE takes reasonable measures to contain the breach and to mitigate its effects, documents the breach in accordance with Article 33(5) GDPR and cooperates with the Customer in its notification to the supervisory authority and, where applicable, to Data Subjects. STRIKE does not notify the supervisory authority or Data Subjects on the Customer's behalf unless the Customer instructs it to do so in writing.

33.4 The Customer notifies STRIKE at security@trustbystrike.com without undue delay, and in any event within twenty-four (24) hours after discovery, of any Personal Data Breach or security incident on its side that affects the Platform, the Output or End User Personal Data, including compromised credentials or API keys.

34. Non-compliance and termination

34.1 Without prejudice to the GDPR, if STRIKE is in breach of its obligations under these Data Processing Terms, the Customer may instruct STRIKE to suspend the Processing until the breach is remedied or the Agreement is terminated. STRIKE informs the Customer without delay if it is unable to comply with these Data Processing Terms for whatever reason.

34.2 The Customer may terminate the Agreement, insofar as it concerns the Processing of Personal Data, if (a) the Processing has been suspended under Article 34.1 for more than

thirty (30) days, (b) STRIKE is in substantial or persistent breach of these Data Processing Terms or of its obligations under the GDPR, or (c) STRIKE fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Data Processing Terms or the GDPR.

34.3 STRIKE may terminate the Agreement, insofar as it concerns the Processing of Personal Data, if the Customer insists on an instruction that STRIKE has notified as infringing the GDPR, or if the Customer fails to remedy a breach of Article 23.5, 27.4 or 28 within fourteen (14) days of written notice.

34.4 Termination under this Article has the consequences stated in Article 26 and in Article 10.

35. Liability

35.1 Each party is liable towards the other for damage caused by its breach of these Data Processing Terms. The limitations and exclusions of liability in Article 16 apply to these Data Processing Terms, with the exception that the exclusion of liability for administrative fines and third-party claims in Article 16.2 does not apply to the extent such fines or claims result directly from STRIKE's attributable breach of these Data Processing Terms. The aggregate cap in Article 16.1 applies in all cases.

35.2 Where both parties are involved in the same Processing and are responsible under Article 82 GDPR for damage caused by that Processing, each party is liable towards the other for the part of the damage that corresponds to its responsibility, after any compensation paid to the Data Subject.

36. Acceptance, evidence and versions

36.1 The Customer accepts these Data Processing Terms as part of these Terms by ticking the single acceptance box during registration (Article 2.1). The person who accepts warrants that he or she is authorised to bind the Customer. This electronic acceptance constitutes a contract in writing in electronic form within the meaning of Article 28(9) GDPR and Article 6:227a of the Dutch Civil Code; no separate signature of the Data Processing Terms is required.

36.2 STRIKE records the version of these Terms that was accepted, the user who accepted and the date and time of acceptance. On request STRIKE provides the Customer with that record and with a copy of the accepted version, and countersigns that copy, so that the Customer can file it as evidence of its data processing agreement.

36.3 Amendments to these Data Processing Terms follow the procedure in Article 18. STRIKE may update Schedule 2 in accordance with Article 27.2 and Schedule 3 in accordance with Article 30, and may add Checks to an existing Check Category in Schedule 1 without following that procedure.

36.4 If the Customer requires a separately negotiated data processing agreement, for example because it is bound by sector-specific requirements, it may contact STRIKE. A separately signed data processing agreement replaces this Part B from its effective date; Part A continues to apply.

36.5 These Data Processing Terms are governed by the laws of the Netherlands and Article 21 applies to them.

Schedule 1: Description of the Processing and allocation of roles

Part A: Parties

Party	Details
Controller (Customer)	The legal entity or business that holds the Account, identified by the business name, market and country registered in the Account and by the invoicing details provided at checkout. Contact persons: the Account Administrators. The Customer may inform STRIKE at privacy@trustbystrike.com of its data protection officer or privacy contact if it wants notices to be sent to that person as well.
Processor (STRIKE)	Strike Business Builders B.V., trading as STRIKE Group, Zonnebaan 9, 3542 EA Utrecht, the Netherlands, Chamber of Commerce no. 74321293. Privacy contact: privacy@trustbystrike.com. Security and data breaches: security@trustbystrike.com, +31 (0)88 835 70 70.

Part B: Processing on behalf of the Customer, per Check Category

The Service Catalogue lists every available Check. The table below states the Check Category to which each kind of Check belongs. STRIKE may add Checks to a Check Category without amending this Schedule. A new Check Category requires an amendment of this Schedule in accordance with Article 18. The labels under which Checks are grouped in the Account (such as Identity, Financial, Legal, KYC, AML, Payment, System, Actions and Other) are for navigation only; the Check Category follows from this Schedule. A Check or function described below is only performed if the Service Catalogue offers it and the Customer has included it in a flow.

Check Category	Nature and purpose	Categories of data and Data Subjects	Roles and sources
A. Reference data validation	Comparison of the name, address, date of birth and contact details of the End User with reference databases, and validation and completion of an address on the basis of postal code and house number. Where the Service Catalogue offers it: enrichment with further attributes. Purpose: validating the identity and address data of End Users and improving data quality for the Customer's customer due diligence or data management.	Data Subjects: End Users (customers, prospects or relations of the Customer). Data: name, initials, gender, date of birth, postal address, e-mail address, telephone number; Output such as match status, match score and corrected or completed address elements (street, city, municipality, province, coordinates).	Customer: Controller for the input data and the Output. STRIKE: Processor for the input data and the Output. STRIKE and its group companies: independent Controllers for their reference databases (see Part C). Sources: reference databases of STRIKE's group companies and licensed data of third-party data suppliers acting as independent Controllers for their own databases.
B. Bank-based	Verification of identity data	Data Subjects: End Users.	Customer: Controller.

Check Category	Nature and purpose	Categories of data and Data Subjects	Roles and sources
checks	through a bank-operated identity scheme (such as iDIN) and verification of the name of the holder of a bank account (IBAN-name check). Purpose: confirming the identity or age of the End User on the basis of the data held by his or her bank, or confirming that the End User is the holder of the stated bank account.	Data: name, address, date of birth, confirmation of age (18 or older) and, where the Customer requests them, the telephone number and e-mail address registered at the bank; IBAN, bank identifier, scheme transaction identifiers; Output such as match, no match or near match with a suggested name.	STRIKE: Processor. Banks and the operator of the identity scheme: independent Controllers for their own processing. The provider through which the scheme is reached and the account-name verification provider: Sub-processors (Schedule 3).
C. Document and biometric checks	Capture and verification of the authenticity of identity documents (such as passport, identity card, driving licence or residence permit), extraction of the data on the document and, only where the Customer has enabled this for a step, comparison of the document photograph with a live image of the End User (facial comparison together with liveness detection). Purpose: identification and identity verification of the End User. STRIKE performs no manual review of documents or images; if STRIKE introduces a Check that includes manual review, the Service Catalogue states this.	Data Subjects: End Users. Data: document images, the portrait taken from the document, document type and number, issuing country, validity dates, name, date and place of birth, nationality, gender and other data shown on the document (such as address, marital status or academic title); live image; Output such as document authenticity result, extracted data, liveness result and facial comparison score. The video used for liveness detection and the data of the machine-readable zone are not stored. Special categories: biometric data, derived for the facial comparison. National identification number: the BSN field is masked on the stored image and the number is not stored (Article 28.2).	Customer: Controller, responsible for the Article 9(2) GDPR condition, for the consent where required and for information to the End User. STRIKE: Processor. Document verification provider: Sub-processor (Schedule 3). The End User submits the images directly to the capture component of that provider, which is embedded in the Hosted Flow.
D. Screening and register checks	Screening of End Users against politically exposed	Data Subjects: End Users and, for list matches, their	Customer: Controller. STRIKE: Processor.

Check Category	Nature and purpose	Categories of data and Data Subjects	Roles and sources
	persons lists, sanctions lists and adverse media, and consultation of insolvency and guardianship registers and of sources on deceased persons. Checks are performed once per verification. Where the Service Catalogue offers it: continuous monitoring for the period selected by the Customer. Purpose: supporting the Customer's compliance with anti-money laundering, sanctions and gambling legislation and keeping its customer records accurate.	relatives and close associates as recorded on the lists. Data: name, date of birth, nationality, address, identifiers; Output such as potential matches with list entries, match score, list source and register status. Data of a sensitive nature: possible indications of political exposure, sanctions, adverse media, insolvency, guardianship or death.	List and register providers: independent Controllers for their lists and registers, or Sub-processors where they Process the Customer's input data on STRIKE's behalf (Schedule 3).
E. Mobile-operator checks	Verification, through a service connected to mobile network operators, that a mobile telephone number belongs to the person whose details are submitted. Purpose: confirming that the End User is the user of the stated mobile number and preventing fraud.	Data Subjects: End Users. Data: mobile telephone number, initials, family name, house number, postal code, date of birth; Output such as match indications per data element.	Customer: Controller, responsible for any consent that the operators require. STRIKE: Processor. Mobile network operators: independent Controllers for their subscriber data. The provider through which the operators are reached: Sub-processor (Schedule 3).
F. Statutory exclusion registers	Consultation of the Dutch central register of exclusion from games of chance (CRUKS), kept by the Kansspelautoriteit under Article 33h of the Dutch Betting and Gaming Act (Wet op de kansspelen), through the Customer's own connection to that register. Purpose: enabling a licence holder to meet its statutory obligation to check whether a player is registered before admitting that player.	Data Subjects: End Users (players). Data: citizen service number (BSN), date of birth and family name, or, for persons without a BSN, names, place and date of birth, or the register code; Output: registered or not registered. The BSN is entered by the End User and is not stored on the Platform.	Customer: Controller and holder of the connection to the register. STRIKE: Processor, passing the request and the answer through the Customer's connection. Kansspelautoriteit: independent Controller for the register.
G. Platform	Functions that support a	Data Subjects: End Users.	Customer: Controller.

Check Category	Nature and purpose	Categories of data and Data Subjects	Roles and sources
functions	flow: verification of an e-mail address with a one-time code, forms and questions defined by the Customer, information and confirmation screens (including the recording of the End User's confirmation with the time), detection of duplicate verifications within the Customer's own Account, automated actions such as sending an e-mail on the Customer's behalf or splitting a name into its parts, recording of the technical data of the visit, analysis of the use of the Customer's flows and delivery of results to the Customer's systems.	Data: e-mail address, answers given in forms, confirmations with their time, technical data of the visit (IP address, browser, operating system, device type, language, referring page, campaign parameters and advertising click identifiers), and values derived from verified data for duplicate detection, partly in coded form.	STRIKE: Processor. E-mail delivery provider: Sub-processor (Schedule 3).

Part C: Processing for which STRIKE is an independent Controller

STRIKE, together with the group companies that maintain them, is an independent Controller for (a) the reference databases used for validation Checks, which are compiled from public registers, licensed data suppliers and the group's own data operations, (b) the Personal Data of Authorised Users and contact persons of the Customer, for account management, authentication, security logging, support, invoicing and communication, (c) the records of Tokens credited and consumed described in Article 26.6, and (d) aggregated usage data. This Processing is described in the VerifyMe Privacy Statement. Personal Data submitted for a Check is not added to the reference databases unless the Service Catalogue states this for a specific Check that the Customer has enabled.

Part D: Duration and retention

Data	Retention	Notes
A verification: data entered by the End User, data passed in by the Customer, document images, portrait, live image, extracted data, results of the Checks, overall outcome, technical data of the visit, values for search and duplicate detection	The period set by the Customer for its Account: 30 to 1,825 days from the completion of the verification (or from its start if it is never completed). Default: 365 days	Deleted automatically by a daily job at the end of the period. One period applies to the whole verification, including the images. The Customer can erase any verification earlier (Article 26.3). The maximum allows Customers with a statutory record-keeping obligation, such as Article 33 of the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act, to

Data	Retention	Notes
		keep verifications on the Platform for almost five years; those Customers remain responsible for keeping their own records for the full statutory period.
Video used for liveness detection; data of the machine-readable zone; BSN read from a document; BSN entered for a Check against the exclusion register	Not stored on the Platform	Used only to perform the Check. Where the Customer has enabled the option to store a coded value derived from the BSN for duplicate detection (Article 28.2), that value is kept with the verification.
Biometric data derived for a facial comparison	Not stored on the Platform	Derived by the document verification provider for the single comparison and kept by that provider no longer than is needed to perform the Check and return the result. The Platform keeps the live image and the comparison score with the verification.
Record of an erased verification (number, overall outcome, dates)	Until the Account is closed	Contains no input data, no images and no results of individual Checks.
Residual copies after deletion	Deleted files: recoverable for up to 30 days. Database back-ups: up to 13 weeks. E-mails to End Users that could not be delivered: up to 30 days	Expire automatically and are used only for recovery after an incident (Article 26.5).
Delivery log of results sent to the Customer's systems; invitations sent to End Users, after they have been used or have expired	90 days	Deleted automatically.
Customer Data after termination of the Agreement	Deleted within 30 days after the period in Article 10.4(e), or earlier at the Customer's written request	Residual copies as stated above.
Records of Tokens credited and consumed (Article 26.6)	Seven (7) years	Retained by STRIKE as Controller under Dutch tax law (Article 52 General State Taxes Act). Contain no input data and no Output.
Activity log of the Account (user, action, time, e-mail addresses of invited users)	Term of the Agreement plus two (2) years	Retained by STRIKE as Controller for security and evidence.
Support tickets and their attachments	Term of the Agreement plus two (2) years	The Customer does not put more End User Personal Data in a ticket than is needed to describe its question.
Technical and monitoring logs of	At most twelve (12) months	Retained by STRIKE as Controller for security,

Data	Retention	Notes
the Platform		monitoring and incident investigation. May contain the Account and verification number, not the content of a verification.

Schedule 2: Technical and organisational measures

STRIKE implements at least the following measures. They are reviewed at least once a year and after every significant incident. The STRIKE Group companies that develop, host and operate the Platform are certified against ISO/IEC 27001.

1. Governance

- Information security and privacy policies approved by management, with assigned ownership and periodic review.
- A security contact (security@trustbystrike.com) and a privacy contact (privacy@trustbystrike.com); a documented incident response and breach notification procedure with a target of notifying affected Customers within forty-eight (48) hours.
- Risk assessments and audits within the ISO/IEC 27001 management systems of the group companies concerned.
- A record of the Processing activities carried out on behalf of Customers (Article 30(2) GDPR).

2. Personnel

- Confidentiality obligations in employment and contractor agreements.
- Security and privacy awareness instruction for staff, and specific instruction for developers and support staff.
- Access to production systems only for named members of the development and operations team who need it to operate and support the Platform; access rights are reviewed periodically and withdrawn when a person leaves or changes role.

3. Access control and authentication

- Multi-factor authentication with an authenticator app is mandatory for every Customer user of the Platform.
- STRIKE staff sign in with individual company accounts in a central identity service, protected by multi-factor authentication; operators reach the database only through a secured connection with their company account.
- API access through keys per Account, each bound to either the test or the production environment, stored in hashed form only and revocable by the Customer at any time; results sent to the Customer's systems are signed.
- Sign-in, registration and public start pages are protected against automated attempts by rate limiting.
- Logical separation of Customer Data: every record carries the identifier of the Account to which it belongs and the application enforces that separation on every request.
- Support access by STRIKE staff to a Customer's environment takes place in a session that is limited in time, gives access to the configuration of flows only and not to verifications, is logged and is visible to the Customer.
- For operating and supporting the Service a limited number of authorised STRIKE staff can view the results of verifications in text form in an internal administration environment; document images and live images are not shown there.

4. Encryption and data handling

- Encryption in transit with TLS; HTTP Strict Transport Security is enforced.
- Stored files, including document images and live images, are encrypted at rest with a key that STRIKE manages in a dedicated key vault and that is rotated automatically; databases and back-ups are encrypted at rest by the hosting provider.
- Credentials that Customers enter for their own contracts with sources or providers are additionally encrypted by the application.
- The BSN field on a stored document image is masked; the BSN, the data of the machine-readable zone and the video used for liveness detection are not stored.
- A daily automated job deletes verifications at the end of the retention period set by the Customer (Schedule 1, Part D).

5. Infrastructure and operations

- Hosting in data centres of Microsoft Azure in the region West Europe (the Netherlands), a provider that holds ISO/IEC 27001 certification and independent assurance reports; physical security is managed by the hosting provider.
- The databases, the file storage and the key vault cannot be reached from the public internet.
- Central logging and monitoring of the availability and performance of the Platform, with alerts to the operations team.
- Changes to the Platform are built, tested and released through an automated release process. Security reviews of the code against the OWASP Top 10 are performed internally, most recently in September 2026. An independent penetration test is performed within six (6) months after 13 November 2026 and at least once a year after that; a summary is available to Customers on request once the first test has been completed.
- Separate test and production environments for Customers, each with its own API keys; the test environment consults live sources (Article 5.7).
- Daily back-ups of the databases with the possibility to restore to a point in time, and continuity and recovery procedures within the management systems referred to above.

6. Suppliers and Sub-processors

- Assessment of Sub-processors before engagement, including their security certifications and data protection terms.
- Written data processing agreements with every Sub-processor that meet Article 28 GDPR; an adequacy decision or standard contractual clauses with a transfer impact assessment where Processing takes place outside the European Economic Area.
- Periodic review of Sub-processors and maintenance of Schedule 3.

7. Additional measures for document and biometric checks

- Document images and live images are submitted by the End User directly to the capture component of the document verification provider and are Processed by that provider within the European Economic Area.
- Facial comparison and liveness detection are switched off by default, are only performed where the Customer has enabled them for a step and are always performed together.
- Facial comparison is performed as a one-to-one verification against the photograph on the End User's own document only. There is no one-to-many identification and no use of images

or biometric data for training. The threshold for a positive comparison is set by STRIKE and is the same for all Customers.

- The verification components use automated technology, including machine learning, to read documents, assess their authenticity, compare faces and detect liveness and presentation attacks. The facial comparison is a verification system whose sole purpose is to confirm that a person is who he or she claims to be and is therefore not a remote biometric identification system within the meaning of Annex III, point 1(a), of Regulation (EU) 2024/1689 (AI Act). The End User Notice informs End Users that automated technology including artificial intelligence is used. STRIKE provides Customers on request with the information available to it about the functioning and limitations of these components, for their own assessments.
- STRIKE performs no manual review of documents or images. If STRIKE introduces a Check that includes manual review, it takes place only by trained reviewers bound by confidentiality, within the European Economic Area and with logging of every review.
- Retention and destruction: the retention period and the deletion described in Schedule 1, Part D, apply to document images, portraits and live images; biometric data derived for the comparison is not stored on the Platform. Together with this section, Schedule 1, Part D, is STRIKE's published retention and destruction policy for images and biometric data.

Schedule 3: Sub-processors

The table below lists the Sub-processors engaged at the effective date of this version, in accordance with Article 30. STRIKE's group companies and its hosting provider are listed by name. The other Sub-processors are listed by a code and by their function; STRIKE provides their name, address and contact details to the Customer on request and in confidence (Article 30.1). A Sub-processor only Processes Personal Data for a Customer that uses the Checks or functions for which that Sub-processor is engaged.

Sub-processor	Processing activity	Location	Transfer mechanism
Communicatie Data Diensten Nederland (CDDN) B.V., Zonnebaan 9, 3542 EA Utrecht, the Netherlands (group company of STRIKE)	Development, operation and support of the Platform; performance of Checks of Check Categories A, D and E against group reference data, registers and connected sources	Netherlands (EEA)	Not applicable (EEA)
Smart Data Services B.V., the Netherlands (group company of STRIKE)	Management of the hosting environment of the Platform; performance of Checks of Check Category A	Netherlands (EEA)	Not applicable (EEA)
EDM DQ B.V., Zonnebaan 9, 3542 EA Utrecht, the Netherlands (group company of STRIKE)	Data quality services and reference data used for Checks of Check Category A; support of the Platform	Netherlands (EEA)	Not applicable (EEA)
Hummingbird Data Group B.V., Zonnebaan 9, 3542 EA Utrecht, the Netherlands (group company of STRIKE)	Group services that support the operation of the Platform, including staff, IT and security management	Netherlands (EEA)	Not applicable (EEA)
Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland	Hosting of the Platform (Microsoft Azure, region West Europe): application, databases, file storage, key management, logging and back-ups; identity service for STRIKE staff	Netherlands (EEA)	Not applicable (EEA). For any access from outside the EEA by the provider's group: adequacy decision for the EU-US Data Privacy Framework and standard contractual clauses (Decision (EU) 2021/914)
VM-SP-01: document verification and identity-scheme provider	Check Category C: capture and authenticity verification of identity documents, data extraction, facial comparison and liveness detection. Check Category B: connection to the bank-based identity scheme	Netherlands (EEA)	Not applicable (EEA)
VM-SP-02: account-name	Check Category B: verification of	EEA	Not applicable (EEA)

Sub-processor	Processing activity	Location	Transfer mechanism
verification provider	the name belonging to a bank account		
VM-SP-03: screening data provider	Check Category D: matching of End User data against politically exposed persons lists, sanctions lists and adverse media	EEA or United Kingdom	EEA: not applicable. United Kingdom: adequacy decision of the European Commission (Article 45 GDPR)
VM-SP-04: mobile-operator verification provider	Check Category E: verification of a mobile number and the related personal details with mobile network operators	United Kingdom	Adequacy decision of the European Commission for the United Kingdom (Article 45 GDPR)
VM-SP-05: e-mail delivery provider	Sending of e-mails of the Platform to Authorised Users and, on the Customer's behalf, to End Users (verification codes and e-mails that are part of a flow)	European Union	Not applicable (EEA). For any access from outside the EEA by the provider's group: adequacy decision for the EU-US Data Privacy Framework and standard contractual clauses (Decision (EU) 2021/914)

For transparency: Stripe Payments Europe, Limited (1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Ireland) processes payment data as an independent Controller and is therefore not a Sub-processor under these Data Processing Terms. Banks and the operator of the bank-based identity scheme (Check Category B), mobile network operators (Check Category E), the Kansspelautoriteit (Check Category F) and the keepers of public registers (Check Category D) act as independent Controllers for their own processing. A source or provider that the Customer connects under its own contract (Article 3.8) is not a Sub-processor of STRIKE.

Document control: Version 2.1, effective 13 November 2026. Versions before 2.1 were not published. Published on the VerifyMe Legal Page. This document contains the VerifyMe Data Processing Terms (Part B); no separate data processing agreement is needed. Questions: info@trustbystrike.com. Privacy: privacy@trustbystrike.com. Security: security@trustbystrike.com.