# VerifyMe Privacy Statement

## How STRIKE Group processes personal data in connection with the VerifyMe platform

Controller: 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 | Privacy Officer: privacy@trustbystrike.com | Security and data breaches: security@trustbystrike.com

**Which section applies to you?** Section 2 is for people who use the VerifyMe platform on behalf of a business. Section 3 is for people whose data has been checked through VerifyMe by one of our customers. Section 4 is for people whose data is included in the reference databases we use to validate data. Sections 5 to 12 apply to everyone.

## 1. Who we are and what this statement covers

VerifyMe is a verification platform operated by Strike Business Builders B.V., trading as STRIKE Group ("STRIKE", "we", "us"), with its registered office at Zonnebaan 9, 3542 EA Utrecht, the Netherlands, registered with the Dutch Chamber of Commerce under number 74321293. Businesses use VerifyMe to validate, verify and screen the identity and contact data of the people they deal with, for example to meet their legal obligations to know their customers.

This statement explains how we process personal data in connection with VerifyMe, which rights you have and how to contact us. It does not cover processing by our customers. When a business uses VerifyMe to check your data, that business decides why and how your data is processed and is the controller for that processing; we act on its instructions as a processor. Section 3 explains what this means for you. How STRIKE processes personal data on its website, in its other services and in its reference data in general is described in the Privacy Statement STRIKE Group (EU), which applies alongside this statement.

You can reach our privacy team at privacy@trustbystrike.com or by post at the address above, marked "Privacy".

## 2. If you use the platform on behalf of a business

### 2.1 What data we process

When you register for or use a VerifyMe account as an employee or representative of a business, or when you contact us, we process: your business e-mail address, the name of the business you represent and the market and country in which it operates; your password (in protected form) and your multi-factor authentication settings; the version of our terms and of this statement that you accepted, with the date and time; your choice whether or not to receive marketing messages; your actions in the platform (such as the flows you build, the settings you change and the users you invite) with their time; the technical data that our systems log when you use the platform, such as IP address, browser and device information; the content of your support tickets and their attachments; and the invoicing details that your business provides at checkout. Payment card and bank details are processed by our payment service provider Stripe and are not stored by us; we keep the customer

number and payment references that Stripe gives us, and we can see the last four digits of a card when we look up a payment.

## 2.2 Why and on which legal basis

| Purpose | Legal basis (Article 6(1) GDPR) | Retention |
|---|---|---|
| Creating and managing the account, performing the agreement with your business, providing support | Performance of a contract (b), where you are the contracting party; otherwise our legitimate interest (f) in serving our business customers through their representatives | For as long as the account exists and two (2) years after it has been closed |
| Verifying, where we do so, that the business is a genuine business and that the person who registered is authorised; preventing misuse of the platform | Legitimate interest (f) in protecting the people whose data is checked, our customers and our platform; compliance with legal obligations (c) where applicable | For as long as the account exists and two (2) years after it has been closed |
| Securing the platform: authentication, logging, detecting and investigating abuse and incidents | Legitimate interest (f) in information security; legal obligation (c) under Article 32 GDPR | Technical logs: at most twelve (12) months. Activity log of an account: for as long as the account exists and two (2) years after. Incident files: five (5) years |
| Invoicing, collection and tax administration, including the records of tokens credited and consumed | Performance of a contract (b); legal obligation (c) under Dutch tax law | Seven (7) years (Article 52 General State Taxes Act) |
| Service communications about changes to the platform, terms, prices or security | Performance of a contract (b); legitimate interest (f) | For as long as the account exists |
| Marketing messages about our services | Your consent (a), which you give by ticking the separate box at registration or in another way; you can withdraw it at any time and every message contains an unsubscribe link | Until you withdraw your consent, and no longer than two (2) years after our last contact |
| Improving the platform using aggregated usage statistics | Legitimate interest (f) in developing our services; the statistics are aggregated and do not identify you | Aggregated data is retained indefinitely |

## 2.3 Who receives this data

We share this data with the group companies that develop, host and operate the platform for us, with the service providers that we use for hosting and for sending e-mail, with Stripe for payments, and with our professional advisers. We disclose data to authorities where the law requires it. We do not sell, rent, trade or otherwise commercialise personal data.

# 3. If your data has been checked by one of our customers

## 3.1 Our role

A business that uses VerifyMe (our customer) may check your data or ask you to verify yourself on a VerifyMe verification page: for example to confirm that your name and address are correct, that you are the holder of a bank account, that your identity document is genuine, or that you do not appear on a sanctions list. The customer decides to perform the check, chooses the steps and determines the purpose. For that processing the customer is the controller and we are its processor. We process your data only on the customer's instructions and under the Data Processing Terms (Part B of the VerifyMe Terms of Service), which meet Article 28 GDPR.

The customer is responsible for telling you why it verifies you and what happens with your data and, where the law requires your consent (for example for comparing your face with the photograph on your document), for asking that consent before the step concerned. The name of the customer is shown on the verification page. The VerifyMe End User Verification Notice, which is published on our legal page, explains in plain language how a verification works; our customers are required to bring it to your attention.

Because the customer is the controller, questions about why your data was checked, and requests to access, correct or delete it, should be addressed to the customer. If you contact us, we will forward your request to the customer where we can identify it, and we will help the customer respond.

## 3.2 What data we process on the customer's behalf

Depending on the checks selected by the customer, this includes: your name, date of birth, gender, address and contact details; your bank account number and the result of a name-to-account comparison; the identity data that your bank confirms through a bank identity scheme such as iDIN; your mobile number and the result of a comparison of your details with the records of mobile network operators; images of your identity document, the portrait on it and the data read from it; where the customer has enabled this, a live image of your face that is compared once with the photograph on your document; the result of a comparison with politically exposed persons lists, sanctions lists and adverse media, with insolvency and guardianship registers and with sources on deceased persons; for gambling operators in the Netherlands, the answer of the central register of exclusion from games of chance (CRUKS), for which you enter your citizen service number (BSN) yourself; your e-mail address and the one-time code used to verify it; the answers you give in forms of the customer and the confirmations you give, with their time; and the overall outcome of the verification.

When you open a verification page we also record technical data about your visit on the customer's behalf: IP address, browser, operating system, type of device, language, the page you came from and campaign parameters in the link you followed. This data is used to secure the verification, to prevent fraud and to let the customer see how its verification flow is used. Where the customer has enabled this, values derived from your verified data are kept to recognise a repeated verification of the same person within that customer's own account.

Where a check involves facial comparison, biometric data is derived by our document verification provider for that single comparison only; it is not stored on the platform. The live image itself is kept with your verification. When we read an identity document, the field with the Dutch citizen service number (BSN) is masked on the stored image and the number is not stored. The BSN that you enter for a check against CRUKS is passed to the register and is not stored on the platform.

## 3.3 How long we keep it

Your verification as a whole, including the data you entered, the images of your document, the live image, the results and the technical data, is kept for the period that the customer has set for its account. That period is at least thirty (30) days and at most one thousand eight hundred and twenty-five (1,825) days after the verification was completed, and is three hundred and sixty-five (365) days if the customer has made no choice. At the end of the period the verification is deleted automatically. The customer can delete a verification earlier, and you can ask the customer to do so. After deletion, copies may remain in back-ups for up to thirteen (13) weeks; these are only used to restore the platform after an incident and expire automatically. The video used to check that a live person is present and the machine-readable lines of your document are not stored.

This retention schedule, together with Schedule 1, Part D, and Schedule 2, section 7, of the VerifyMe Terms of Service, is our published retention and destruction policy for images and biometric data. If you live in a US state with specific biometric privacy legislation (such as Illinois, Texas or Colorado), the business that asked you to verify is responsible for the written consent those laws require and for setting a retention period that meets the deadlines of those laws.

We do not use the data of your verification to train or improve models, and we do not add it to our reference databases, unless the customer has enabled a check for which this is expressly stated.

## 3.4 Sources we consult

To perform a check we may consult the reference databases of our group (see Section 4), licensed data suppliers, public registers, banks and bank-operated identity schemes, mobile network operators, document verification technology, providers of politically exposed persons and sanctions lists and, for gambling operators, the exclusion register kept by the Dutch gambling authority (Kansspelautoriteit). The providers that process data on our behalf are listed, by name or by function, in Schedule 3 of the VerifyMe Terms of Service. The customer that verified you can tell you which providers were involved in your verification.

## 3.5 Automated processing and decisions

VerifyMe uses automated technology, including artificial intelligence, to read identity documents, assess their authenticity, compare your face with the photograph on your document, detect whether a live person is present and match names against lists. The facial comparison only confirms that you are the person shown on your own document (a one-to-one verification); it does not search for you in a database of faces and is therefore not a remote biometric identification system under the EU AI Act. STRIKE does not review your documents or images manually.

VerifyMe returns results per check, such as a match score, a status or a flag, and combines them into an overall outcome according to rules that the customer has set. That outcome goes to the customer; we do not show it to you and we do not take any decision about you. Whether and how a decision is taken on the basis of the outcome is determined by the customer, which must comply with Article 22 GDPR where a decision is based solely on automated processing and has legal or similarly significant effects for you. In that case you can ask the customer for human intervention, give your point of view and contest the decision.

# 4. If your data is included in our reference databases

## 4.1 What the reference databases are

To validate the data that customers submit, STRIKE and its group companies maintain reference databases of name, address and contact data of persons in the Netherlands and related address-level attributes. For these databases STRIKE and the group companies concerned are independent controllers. The data is compiled from public registers, from data suppliers that are entitled to license it to us, and from our own data operations. Where we obtain data from a source other than you, Article 14 GDPR applies and this Section provides the information required by that Article.

## 4.2 What data, why and on which legal basis

The reference databases contain: name, initials, gender, date of birth or age category, postal address, relocation history, telephone number and e-mail address where available, indicators of deceased status and, at the level of an address or neighbourhood rather than a person, socio-demographic attributes such as property value category, owner or tenant status and household composition. We process this data to allow our customers to validate the correctness and currency of the data they hold about their customers and relations, to prevent fraud and errors, and to help them meet their legal obligations. The legal basis is our legitimate interest and that of our customers (Article 6(1)(f) GDPR) in accurate, up-to-date and verified customer data. We have assessed this interest against your interests and rights and have concluded that, given the nature of the data (ordinary contact data), the purpose (validation rather than profiling of individuals) and the safeguards we apply (no sale of data, no use for direct marketing by STRIKE, strict access control, retention limits and your right to object), the processing is proportionate. A VerifyMe check returns only the result of the comparison and, for an address, the corrected or completed address; it does not return socio-demographic attributes.

## 4.3 Retention and recipients

Reference data is kept as long as it is current and for at most five (5) years after our source indicates that it is no longer valid, so that we can recognise outdated data and prevent its re-use. Reference data is used to answer checks for our customers; the customer receives only the result of the comparison for the person it submitted, not our database. Our data suppliers and our hosting provider may have access as needed to deliver or host the data.

## 4.4 Your right to object and to be excluded

You may object at any time to the inclusion of your data in our reference databases on grounds relating to your particular situation (Article 21 GDPR). If you object, we will stop processing your data in the reference databases unless we demonstrate compelling legitimate grounds that override your interests, and we will place your data on an internal exclusion list so that it is not re-added from our sources. You can also ask us which data we hold about you and have it corrected. Contact details are in Section 11.

# 5. Children

The VerifyMe platform is aimed at businesses and is not intended for children. Our customers use VerifyMe, among other things, to keep minors out of services that are not meant for them, such as online gambling; an age check processes only the data needed to establish whether the age requirement is met. VerifyMe is not intended for the verification of persons under sixteen (16); where

a customer nevertheless verifies such a person, the customer is responsible for a valid legal basis and, where required, for the consent of a parent or guardian.

## 6. Requests from authorities

We disclose personal data to public authorities, courts or law enforcement only where we are legally obliged to do so, or where this is necessary to establish, exercise or defend legal claims. We verify the legal basis of every request, disclose no more than is required and, where the law allows, inform the customer concerned before we disclose data processed on its behalf.

## 7. Recipients, group companies and international transfers

VerifyMe is developed, hosted and operated for us by companies of the STRIKE Group in the Netherlands: Communicatie Data Diensten Nederland (CDDN) B.V., Smart Data Services B.V., EDM DQ B.V. and Hummingbird Data Group B.V. They are bound by the same obligations as we are. The platform is hosted with Microsoft Azure in the region West Europe (the Netherlands). We use further service providers to send e-mails and to perform specific checks, such as a document verification provider, a provider that verifies the name on a bank account, providers of screening lists and a provider that connects to mobile network operators. These providers process data only on our instructions under written agreements. Stripe Payments Europe, Limited processes payment data as an independent controller under its own privacy policy. Banks, mobile network operators and the keepers of public registers are responsible for their own processing.

We store personal data within the European Economic Area, and our providers process it there, with the exception of providers established in the United Kingdom, such as the provider that connects to mobile network operators. For the United Kingdom the European Commission has adopted an adequacy decision. Where a provider belongs to a group with companies outside the EEA, or where any other provider processes data outside the EEA, we rely on an adequacy decision or on the standard contractual clauses, supplemented where necessary with additional measures following a transfer impact assessment. You can obtain information about the safeguards used by contacting us.

## 8. How we protect your data

The STRIKE Group companies that develop, host and operate the platform are certified against ISO/IEC 27001. Our measures include encryption of data in transit and of stored files and databases, mandatory multi-factor authentication for the users of our customers, access for our own staff on a need-to-know basis, logical separation of the data of each customer, monitoring of the platform, security reviews of the software, an independent penetration test at least once a year from 2027, automated deletion of verifications at the end of their retention period and contractual obligations for all staff and suppliers. Our measures are described in Schedule 2 of the VerifyMe Terms of Service, which applies to all our customers. If a personal data breach occurs at STRIKE that affects data we process on behalf of a customer, we inform that customer without undue delay and in any event within forty-eight (48) hours after becoming aware of it, so that the customer can meet its own obligations under Articles 33 and 34 GDPR.

## 9. Your rights

You have the right to access the personal data we hold about you, to have it rectified or erased, to restrict its processing, to receive it in a portable format where the processing is based on a contract or

consent, and to object to processing based on legitimate interests. Where processing is based on your consent you may withdraw it at any time, without affecting the lawfulness of processing before the withdrawal.

To exercise your rights, contact us at privacy@trustbystrike.com. We may ask you to verify your identity in a proportionate way; we will not ask for a copy of your identity document unless no other way exists. We respond within one month, which may be extended by two further months for complex requests, in which case we will inform you. If your request concerns a check performed by one of our customers, we will forward it to the customer as explained in Section 3.

You have the right to lodge a complaint with a supervisory authority, in particular in the EU member state of your habitual residence, place of work or place of the alleged infringement. In the Netherlands this is the Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl). We would appreciate the opportunity to address your concerns first.

## 10. Cookies and similar technologies

The VerifyMe platform and its verification pages use only cookies that are strictly necessary for them to work: session, authentication and security cookies, and a cookie that remembers your language choice for one (1) year. No consent is needed for these cookies. We place no advertising cookies and no analytics cookies. Where we measure how the platform is used, we do so without cookies and without following you across other websites.

A business that uses VerifyMe can add its own styling, scripts or measurement tools to its verification pages. That business is responsible for those tools and for asking your consent for them where the law requires it. As described in Section 3.2, a verification page records technical data about your visit, including the page you came from and the campaign parameters in the link you followed, so that the business can see how its verification flow is used. Cookies on the STRIKE Group website are described in the Privacy Statement STRIKE Group (EU).

## 11. Contact and Privacy Officer

Questions, requests and complaints about this statement can be sent to privacy@trustbystrike.com (Privacy Officer) or to Strike Business Builders B.V., attn. Privacy Officer, Zonnebaan 9, 3542 EA Utrecht, the Netherlands, telephone +31 (0)88 835 70 70. Security incidents and suspected data breaches: security@trustbystrike.com.

## 12. Changes to this statement

We may update this statement when our services, the law or our processing change. The version and effective date are shown at the top of this statement. Where a change materially affects how we process personal data, we inform the administrators of each account by e-mail before the change takes effect. Previous versions are available on request.

Document control: Version 2.1, effective 13 November 2026. Versions before 2.1 were not published. Published on the VerifyMe legal page.