IMF | **International Modeling Foundation (IMF)**
A Global Standard for Ethical Modeling

Privacy Policy

International Modeling Foundation (IMF)

Version 1.0 | Last updated: 01.12.2025] | Effective: 01.12.2025

1. INTRODUCTION

1.1 Who we are

The International Modeling Foundation ("IMF", "we", "us", "our") is a Dutch public benefit foundation (stichting) registered in the Netherlands. We operate the Model ID platform at model-id.com, providing certification and verification services for the modeling industry.

Contact details:

- Email: privacy@model-id.com
- Address: [registration pending], Rotterdam, Netherlands
- Website: model-id.com

1.2 What this policy covers

This Privacy Policy explains how we collect, use, store, and protect your personal data when you:

- Visit our website (model-id.com)
- Create an account
- Apply for certification
- Use the verification tool
- File or receive reports
- Contact us

1.3 Important documents

This Privacy Policy should be read alongside:

- Our Terms of Service
- Our Certification Visibility Agreement (for certified users)

- Our Ethical Charter and Code of Conduct

1.4 Updates to this policy

We may update this policy to reflect changes in our practices or legal requirements. Material changes will be communicated via email to registered users at least 30 days before taking effect. The "Last updated" date at the top indicates when changes were made.

2. DATA WE COLLECT

We collect different types of data depending on how you interact with Model ID.

2.1 When you visit our website (all visitors)

Data type	Examples	Purpose
Device information	Browser type, operating system, screen resolution	Website functionality and optimization
Usage data	Pages visited, time on site, clicks	Understanding how our site is used
IP address	Your internet protocol address	Security, fraud prevention, approximate location

We use privacy-focused analytics that do not require cookies or track you across websites.

2.2 When you create an account and apply for certification (Step 1)

During account creation and certification application, we collect the following information:

Identity and Contact Information

Data type	Required?	Purpose
Email address	Yes	Account access, notifications, communication
Password	Yes	Account security (stored as encrypted hash)
Legal name (first, middle, last)	Yes	Identity verification, certificate display

Data type	Required?	Purpose
Professional/stage name	Optional	Display name on certificate if different from legal name
Date of birth	Yes	Age verification, minor protection protocols
Gender	Yes	Profile information, industry matching
Nationality	Yes	Identity verification, regional compliance
Country of residence	Yes	Regional features, applicable regulations
City	Yes	Location-based features
Full address	Yes	Identity verification, correspondence
Phone number	Yes	Account security, urgent communications

Professional Information (Model user type)

Data type	Required?	Purpose
Years active in modeling	Yes	Professional profile, experience verification
Current agencies	Yes	Professional verification, industry connections
Previous agencies	Optional	Professional history
Notable campaigns or work	Optional	Professional portfolio
Special skills or training	Optional	Professional capabilities

Physical Characteristics (Model user type)

Data type	Required?	Purpose
Height	Yes	Industry standard professional data

Data type	Required?	Purpose
Measurements (bust/chest, waist, hips)	Optional	Industry standard professional data
Hair color	Yes	Professional profile
Eye color	Yes	Professional profile
Shoe size	Yes	Professional bookings
Clothing size	Yes	Professional bookings

Physical characteristics are standard industry data required for professional modeling work. This information is stored securely, used to match you with appropriate opportunities, and is not shared publicly without your consent. You may update this information at any time through your profile settings.

Social Media (Optional)

Data type	Required?	Purpose
Instagram handle	Optional	Professional profile, verification
TikTok handle	Optional	Professional profile, verification

Emergency Contact

Data type	Required?	Purpose
Emergency contact name	Yes	Safety during professional activities
Emergency contact phone	Yes	Safety during professional activities
Relationship to you	Yes	Context for emergency contact

By providing emergency contact information, you confirm that:

- You have the emergency contact's permission to share their details with us
- You have informed them that IMF may contact them in case of emergency
- The information is accurate and current

We only use emergency contact information for safety purposes and do not share it with third parties except in genuine emergencies.

2.3 During identity verification (Steps 3 and 5)

Identity verification varies based on your age. We use different processes to balance security with privacy:

For Adults (18 and over) - Automated Verification via Stripe Identity

Data type	Stored by	IMF receives
Government ID image	Stripe only	Verification result only (pass/fail)
Selfie photo	Stripe only	Verification result only (pass/fail)
Extracted ID data	Stripe only	Confirmation of name/DOB match

For adult verification, IMF does not receive or store copies of your identity documents. Stripe processes your ID securely and only confirms to us whether verification passed or failed. See Stripe's privacy policy at stripe.com/privacy for details on their data handling.

For Minors (under 18) - Manual Verification

Data type	Stored by	Purpose
Government ID image	IMF (via Cloudinary)	Age and identity verification by admin
ID document details	IMF database	Verification record

For minors, identity documents are uploaded directly to our secure storage for manual review by IMF administrators. This additional oversight helps protect young people in the industry. Documents are stored securely with encryption and access is strictly limited to authorized personnel.

For Parents/Guardians of Minors - Consent Verification

Data type	Stored by	Purpose
Parent/guardian government ID	IMF (via Cloudinary)	Verify authority to consent
Signed consent form	IMF (via Cloudinary)	Legal record of parental consent
Parent/guardian contact details	IMF database	Communication about minor's account

Parents or guardians receive a secure email link to upload their identification and signed consent form. This ensures we have verified parental consent before certifying any minor. These documents are stored securely with the same protections as other identity documents.

Documents uploaded directly to IMF (all users):

Data type	Purpose	Storage
Proof of address (utility bill, bank statement)	Address verification	Cloudinary (encrypted)
Professional documents, portfolio images	Professional verification	Cloudinary (encrypted)

2.4 When you complete payment

Data type	Purpose	Processed by
Payment card details	Process certification fee	Stripe
Billing name and address	Payment processing, receipts	Stripe

What IMF receives from Stripe:

- Confirmation of successful payment
- Transaction ID and timestamp
- Last 4 digits of card (for your reference)

- Payment amount and currency

What IMF does NOT receive or store:

- Your full card number
- Your CVV
- Your full billing address

2.5 When you are certified

Data type	Purpose	Visibility
Certificate number	Unique identifier	Public (verification tool)
Certification status	Current standing	Public (verification tool)
Issue and expiry dates	Validity period	Public (verification tool)
User type	Category of certification	Public (verification tool)
Blockchain hash	Tamper-proof verification	Public (blockchain)

2.6 When you update your profile after certification

After certification, you can add additional information to enhance your professional profile:

Data type	Required?	Purpose
Profile photo	Optional	Visual identification on your profile
Portfolio photos	Optional	Showcase your professional work
Experience entries (campaigns, brands, years)	Optional	Professional history and portfolio
Languages and proficiency levels	Optional	Professional capabilities for bookings
Additional skills (dancing, acting, etc.)	Optional	Professional capabilities for bookings

This information is stored securely and currently visible only to you and IMF administrators.

If we introduce public profile features in the future, you will have full control over what information is displayed publicly. We will update this policy and notify you before any such features are launched.

2.7 When you file a report

Data type	Purpose	Retention
Reporter identity	Investigation, follow-up	Confidential (IMF staff only)
Report content	Investigation	Per retention schedule (1-3 years or permanent)
Evidence/attachments	Investigation	Per retention schedule
Reported party details	Investigation	Per retention schedule

2.8 When someone files a report about you

Data type	Purpose	Your access
Report existence	Notification (named reports only)	Yes (named), No (anonymous)
Report details	Your response	Yes (named), No (anonymous)
Warning points	Track certification standing	Yes (your account only)
Outcomes	Enforcement	Yes

2.9 Minors (under 18)

For users under 18, we also collect:

- Parent/guardian name and contact information

- Parent/guardian consent documentation
- Relationship to minor

2.10 Data we do NOT intentionally collect

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Genetic data
- Health data
- Sexual orientation

We may receive information about criminal conduct through reports filed on our platform.

3. HOW WE USE YOUR DATA

3.1 Purposes and legal bases

Purpose	Legal basis (GDPR)
Provide account services	Contract (Art. 6(1)(b))
Process certification	Contract (Art. 6(1)(b))
Process payments	Contract (Art. 6(1)(b))
Public verification	Contract + Legitimate interest (Art. 6(1)(b), (f))
Investigate reports	Legitimate interest (Art. 6(1)(f))
Enforce certification standards	Legitimate interest (Art. 6(1)(f))
Maintain safety records	Public interest (Art. 6(1)(e))

Purpose	Legal basis (GDPR)
Send service notifications	Contract (Art. 6(1)(b))
Improve our services	Legitimate interest (Art. 6(1)(f))
Prevent fraud	Legitimate interest (Art. 6(1)(f))
Comply with law	Legal obligation (Art. 6(1)(c))
Protect minors	Legal obligation + Legitimate interest

3.2 Identity verification (biometric data)

When you verify your identity through Stripe Identity:

- Your ID document and selfie are processed using automated facial comparison technology
- This constitutes processing of biometric data under GDPR
- Legal basis: Your explicit consent (Art. 9(2)(a)) obtained during certification process
- You may withdraw consent, but this will prevent certification completion

3.3 Automated decision-making

We use automated processing in the following ways:

Process	Automation level	Human review available?
Stripe Identity verification	Automated initial check	Yes - IMF admin reviews flagged cases
Warning point calculation	Automated (7 points = suspension)	Yes - admin reviews before suspension
Report tier classification	Admin-assigned, not automated	N/A

You have the right to request human review of any automated decision that significantly affects you.

3.4 What we do NOT do with your data

We do NOT:

- Sell your personal data to third parties
- Use your data for advertising or marketing by third parties
- Share your documents with the public
- Make certification decisions using fully automated processing without human oversight

4. HOW WE SHARE YOUR DATA

4.1 Public information

The following is intentionally public through our verification tool:

- Your name (as certified)
- Certificate number
- Certification status
- Issue and expiry dates
- User type
- Profile photo (in verification results)

This public visibility is core to the certification service and cannot be opted out of. See our Certification Visibility Agreement for full details.

4.2 Third-party service providers

We share data with the following service providers who process data on our behalf:

Provider	Purpose	Location
Stripe	Payment processing	USA
Stripe Identity	Identity verification	USA
Cloudinary	Document storage	USA
Railway	Database hosting	USA/EU

Provider	Purpose	Location
Vercel	Website hosting	USA
SendGrid	Email delivery	USA

All providers are bound by data processing agreements requiring GDPR-compliant handling.

4.3 Blockchain records

Certificate verification data is recorded on blockchain:

- Certificate hash (digital fingerprint)
- Certificate number
- Status changes
- Timestamps

Blockchain records are distributed globally. This is inherent to blockchain technology. Only certificate hashes and status are recorded - not personal details like your name or documents.

4.4 When we may disclose your data

We may disclose your personal data:

- To comply with legal obligations or valid legal requests
- To protect our rights, privacy, safety, or property
- To law enforcement if we believe disclosure is necessary to prevent harm
- In response to court orders or legal process
- If required for safeguarding concerns involving minors
- During merger, acquisition, or asset sale (with notice to you)

4.5 Reporter identity

For named reports, reporter identity may be shared with the reported party as part of investigation or resolution. See the Certification Visibility Agreement Section 9.7 for details. Anonymous reporter identity is never shared with reported parties.

5. INTERNATIONAL DATA TRANSFERS

5.1 Where your data goes

IMF is based in the Netherlands (EU). Your data may be transferred to and processed in countries outside the European Economic Area (EEA), particularly the United States, where several of our service providers are located.

5.2 Safeguards for transfers

We protect international transfers through:

- **Standard Contractual Clauses (SCCs):** Approved EU contract terms with service providers
- **Adequacy decisions:** Where the EU has determined a country provides adequate protection
- **Supplementary measures:** Additional technical and organizational safeguards where needed

5.3 Blockchain data

Certificate verification data recorded on blockchain is distributed globally. This is inherent to blockchain technology and cannot be restricted to specific jurisdictions. Only certificate hashes and status are recorded - not personal details.

6. DATA RETENTION

6.1 General retention periods

Data type	Retention period
Account data	Duration of account + 30 days
Certification records	See Certification Visibility Agreement
Identity documents (proof of address)	Duration of certification + 1 year, or per revocation schedule
Payment records	7 years
Report data (Administrative tier)	1 year from resolution
Report data (Professional tier)	2 years from resolution

Data type	Retention period
Report data (Safety tier)	3 years from resolution
Report data (Severe tier)	Permanent
Audit logs	7 years
Website analytics	26 months
Verification tool query logs	90 days

6.2 Special retention rules

- **Blockchain records:** Permanent (cannot be deleted due to blockchain technology)
- **Revoked certifications:** See Certification Visibility Agreement Section 5.4 for visibility periods
- **Data subject to legal hold:** Retained until legal matter resolved

6.3 Stripe Identity data

Stripe retains identity verification data according to their own retention policy. You may contact Stripe directly regarding their data practices. IMF cannot delete data held by Stripe.

6.4 Deletion requests

When you request account deletion:

- We delete most personal data within 30 days
- Certain data is retained per the schedules above
- We will inform you of any data we cannot delete and why

7. DATA SECURITY

7.1 Technical measures

We protect your data through:

- Encryption in transit (TLS/HTTPS for all connections)

- Encryption at rest for sensitive data
- Secure password hashing using bcrypt (passwords never stored in plain text)
- JWT token-based authentication with secure session management
- Access controls limiting who can view data
- Login attempt tracking to detect suspicious activity
- Regular security assessments
- Secure cloud infrastructure with reputable providers

7.2 Organizational measures

- Staff training on data protection
- Access on need-to-know basis only
- Confidentiality obligations for all staff
- Incident response procedures
- Regular policy reviews

7.3 What you can do

- Use a strong, unique password
- Keep your login details confidential
- Log out when using shared devices
- Report any suspicious activity to security@model-id.com

7.4 Data breaches

If we experience a data breach that poses a risk to your rights:

- We will notify the Dutch Data Protection Authority within 72 hours
- We will notify affected individuals without undue delay
- We will explain what happened, what data was affected, and what we're doing about it

8. YOUR RIGHTS

Under GDPR, you have the following rights regarding your personal data:

8.1 Right to access (Art. 15)

You can request a copy of the personal data we hold about you. We will respond within 30 days.

8.2 Right to rectification (Art. 16)

You can ask us to correct inaccurate data or complete incomplete data.

8.3 Right to erasure / "Right to be forgotten" (Art. 17)

You can request deletion of your data. However, this right does not apply where we need to retain data for:

- Compliance with legal obligations
- Public interest purposes (safety-related revocations)
- Establishment, exercise, or defense of legal claims
- Certification integrity (see Certification Visibility Agreement)

8.4 Right to restriction (Art. 18)

You can ask us to limit how we use your data while we address a concern you've raised.

8.5 Right to data portability (Art. 20)

You can request your data in a structured, machine-readable format to transfer to another service.

8.6 Right to object (Art. 21)

You can object to processing based on legitimate interests. We will stop unless we have compelling grounds that override your interests.

8.7 Rights related to automated decisions (Art. 22)

You can request human review of significant automated decisions. Our identity verification includes automated elements but always has human review available.

8.8 Right to withdraw consent

Where processing is based on consent (e.g., biometric verification), you can withdraw consent at any time. This doesn't affect processing that occurred before withdrawal.

8.9 How to exercise your rights

Contact us at: privacy@model-id.com

We will:

- Respond within 30 days (extendable by 60 days for complex requests)
- Verify your identity before acting
- Provide information free of charge (excessive or repetitive requests may incur a reasonable fee)

8.10 Right to complain

If you're unsatisfied with how we handle your data, you can complain to:

Dutch Data Protection Authority (Autoriteit Persoonsgegevens)

- Website: autoriteitpersoonsgegevens.nl
- Address: Postbus 93374, 2509 AJ Den Haag, Netherlands

You may also complain to the supervisory authority in your country of residence.

9. SPECIFIC SITUATIONS

9.1 Using the verification tool (without an account)

When you verify someone's certificate:

- We log the query for security and abuse prevention purposes
- We collect your IP address and timestamp
- We do not require an account or personal details to verify certificates
- Query logs are retained for 90 days and then deleted

9.2 Filing a report without an account (guest reports)

You can file reports without a Model ID account:

- We collect information you provide in the report
- We collect your email address for follow-up
- Guest reports have limited enforcement capabilities (see reporting form for details)
- Data retention follows standard report retention schedules

9.3 Founding Members

If you become a Founding Member:

- Additional profile information you provide may be displayed in our public Founding Member Directory
- Directory visibility is optional and controlled in your account settings
- See Certification Visibility Agreement Section 2 for full details

9.4 Newsletter and marketing (when available)

If you subscribe to our newsletter:

- We use your email to send updates about IMF and the modeling industry
- You can unsubscribe at any time via the link in each email
- Legal basis: Consent (Art. 6(1)(a))
- We do not send marketing emails to users who have not explicitly opted in
- We do not share your email with third parties for marketing

10. COOKIES AND TRACKING

10.1 Our approach

We take a privacy-first approach to cookies and tracking. We use only essential cookies required for the platform to function, and privacy-focused analytics that do not use cookies or track you across websites.

We do NOT use:

- Advertising or marketing cookies
- Cross-site tracking cookies
- Social media tracking pixels
- Third-party analytics that profile users

10.2 Cookies we use

The following cookies are set by Model ID:

Cookie name	Purpose	Type	Duration
accessToken	Keeps you logged in and authenticates your requests	Essential	15 minutes
refreshToken	Allows automatic renewal of your session without re-entering password	Essential	7 days

These cookies are:

- HttpOnly: Cannot be accessed by JavaScript, protecting against XSS attacks
- Secure: Only transmitted over encrypted HTTPS connections
- SameSite Strict: Only sent to our domain, protecting against CSRF attacks

These are essential cookies required for the platform to function. Under GDPR, essential cookies do not require consent as they are strictly necessary to provide the service you have requested.

10.3 Analytics

We use Plausible Analytics to understand how visitors use our website. Plausible is a privacy-focused analytics service that:

- Does not use cookies
- Does not collect personal data
- Does not track you across websites
- Does not create user profiles
- Is fully GDPR compliant without requiring consent
- Is hosted in the EU

Plausible collects only aggregate, anonymous data such as page views, referral sources, browser type, and country. This data cannot be used to identify you personally.

For more information, see Plausible's privacy policy at plausible.io/privacy.

10.4 Third-party cookies

When you interact with certain features, third-party services may set their own cookies:

Service	When used	Their cookie policy
Stripe	During payment or identity verification	stripe.com/privacy
Cloudinary	When uploading documents	cloudinary.com/privacy

These services only set cookies when you directly interact with them (e.g., making a payment). We do not control their cookies; please refer to their privacy policies for details.

10.5 How to control cookies

You can control cookies through your browser settings:

- Block all cookies: Most browsers allow you to block all cookies, but this will prevent you from logging in to Model ID
- Delete cookies: You can delete cookies at any time, but you will be logged out and need to sign in again
- Browser settings: Check your browser's help documentation for instructions on managing cookies

Since we only use essential cookies for authentication, blocking them will prevent you from using the platform's logged-in features. The public verification tool works without cookies.

10.6 Do Not Track

Some browsers send a "Do Not Track" (DNT) signal. Since we do not track users across websites and do not use advertising cookies, our practices already align with DNT preferences. We do not change our behaviour based on DNT signals because our default behaviour is already privacy-respecting.

10.7 Cookie consent

Under GDPR and ePrivacy regulations, strictly necessary cookies (like our authentication cookies) do not require consent. Since we do not use any non-essential cookies, we do not display a cookie consent banner.

If we ever add non-essential cookies in the future, we will update this policy and implement appropriate consent mechanisms before doing so.

11. CHILDREN'S PRIVACY

11.1 Age requirements

- You must be at least 16 years old to create an account without parental consent
- Users aged 16-17 may create accounts but require parental consent for certification
- Users under 16 require parental consent for both account creation and certification

11.2 Parental consent for certification

For users under 18 seeking certification:

- Parent/guardian must provide consent during the certification process (Step 5)
- Parent/guardian receives copies of important notifications
- Parent/guardian may manage the account and request deletion on the minor's behalf
- Parent/guardian must upload their government ID and signed consent form via secure email link (Step 5)

11.3 Children under 13

We do not knowingly collect data from children under 13. If we learn we have collected data from a child under 13 without verified parental consent, we will delete it promptly. Contact us at privacy@model-id.com if you believe we have data from a child under 13.

11.4 Enhanced protections for minors

We take additional care with minor data:

- Reports involving minors are escalated for senior review
- We may involve appropriate authorities for safeguarding concerns
- Minor status (age, date of birth) is never publicly displayed

12. CONTACT US

For privacy questions or to exercise your rights:

Email: privacy@model-id.com

For general support:

Email: support@model-id.com

For security concerns:

Email: security@model-id.com

Postal address:

International Modeling Foundation

[Registration pending]

Rotterdam, Netherlands

Response times:

- Data subject requests: Within 30 days
- General privacy inquiries: Within 14 days

13. DOCUMENT INFORMATION

Field	Value
Document	Privacy Policy
Version	1.0
Last updated	01.12.2025
Effective date	01.12.2025
Approved by	IMF Board
Next review	01.01.2027

This Privacy Policy was last updated on 01.12.2025.