

Last updated: June 27, 2026

Personal Data Processing Policy

1. General information

For the purposes of this Policy, the data controller is:

Dilan Mirrors Technology Limited, 40 Holywell Green, Swords, Co. Dublin, K67 DF85, Ireland (hereinafter referred to as “DM”, “we”, “us” or “our”).

This Personal Data Processing Policy explains how **DM**, processes personal data in connection with its website, user accounts, products, services, customer support, contractual relationships, orders and communications.

For any questions regarding the processing of personal data, or to exercise your rights, you may contact us at:

- **Email:** privacy@dilan-mirrors.com
- **Postal address:** 40 Holywell Green, Swords, Co. Dublin, K67 DF85, Ireland

2. Definitions

For the purposes of this Policy:

- **Personal data** means any information relating to an identified or identifiable natural person.
- **User** means any person who accesses the DM website, creates an account, purchases or uses DM products or services, contacts DM, participates in promotions or otherwise interacts with DM.
- **Processing** means any operation performed on personal data, such as collection, recording, storage, use, disclosure, transfer, deletion or destruction.
- **Controller** means the entity that determines the purposes and means of processing personal data.
- **Processor** means a third party that processes personal data on behalf of the controller.

3. Categories of personal data we process

Depending on the specific interaction with DM, we may process the following categories of personal data:

- **Identity and contact data:** name, surname, postal address, email address, telephone number, fiscal code / personal identification number where required, date of birth where necessary, signature and similar identification data.
- **Account data:** username, account identifier, authentication data, account preferences, account activity and account status.
- **Order, payment and contractual data:** products or services purchased, order history, invoices, delivery details, payment confirmation, transaction identifiers, refund information, contractual documents and correspondence related to the contract.
- **Customer support and communication data:** messages, requests, complaints, notifications, responses, feedback and records of communication with DM.
- **Technical and device data:** IP address, browser type, operating system, device identifier, session data, error logs, diagnostic data, URL/referral data and similar technical data necessary for the website, applications and services to function securely.

- **Usage data:** information about how Users access and use DM products, services, website features and applications.
- **Location data:** approximate or precise location data only where it is necessary for the provision of a requested service, for fraud prevention, for technical operation of the service, or where the User has provided valid consent, depending on the case.
- **Image, voice and camera-related data:** only where such data is necessary for a feature requested or enabled by the User, for technical support, or for the provision of the relevant DM service. DM does not use such data for biometric identification or biometric authentication unless this is separately disclosed and a valid legal basis exists.
- **Fraud prevention and security data:** information necessary to detect, prevent or investigate misuse, fraud, security incidents, abusive use of DM products or services, or breach of contractual or legal obligations.
- **Marketing preference data:** consent status, communication preferences, opt-in / opt-out history and marketing interaction data.

We do not intentionally collect special categories of personal data, such as health data, political opinions, religious beliefs or biometric data for the purpose of uniquely identifying a person, unless such processing is expressly disclosed, legally permitted and necessary.

4. Sources of personal data

We may collect personal data:

- directly from the User, for example when the User creates an account, places an order, signs or accepts contractual documents, contacts DM, submits a complaint or participates in a promotion;
- automatically, for example when the User accesses the website, account, application or services;
- from payment, delivery, technical, hosting, customer support or other service providers acting in relation to the services requested by the User;
- from public sources, public registers, databases or authorities, where such processing is lawful and necessary;
- from social networks, online platforms or third parties, only where the User has made the data available, has authorized the disclosure, or where DM has another valid legal basis.

DM will not collect personal data from external sources in an excessive, hidden or incompatible manner.

5. Purposes and legal bases of processing

DM processes personal data only where there is a valid legal basis. The main purposes and legal bases are described below.

Where consent is used as the legal basis, the User may withdraw consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal.

Where processing is based on legitimate interest, the User has the right to object to the processing. DM will assess each objection and will stop the processing unless DM demonstrates compelling legitimate grounds or the processing is necessary for legal claims.

The mere use of DM services does not constitute consent for all processing activities. Consent will be requested separately where required by law.

PURPOSE OF PROCESSING	CATEGORIES OF DATA USUALLY INVOLVED	LEGAL BASIS
Creating and managing User accounts	identity, contact, account, technical data	performance of a contract; legitimate interest in account security and service administration
Concluding, performing, modifying and terminating contracts with Users	identity, contact, contractual, payment, order and delivery data	performance of a contract; legal obligation where invoices or statutory records are required
Handling orders, delivery, payments, refunds and service communications	identity, contact, order, payment, delivery and communication data	performance of a contract; legal obligation; legitimate interest in resolving operational issues

PURPOSE OF PROCESSING	CATEGORIES OF DATA USUALLY INVOLVED	LEGAL BASIS
Providing DM products and services, including requested voice, image or camera-related features	account, technical, usage, image, voice, camera-related and device data	performance of a contract; consent where legally required; legitimate interest for technical operation and security
Responding to questions, requests, complaints and notifications	identity, contact, communication and support data	performance of a contract; legitimate interest; legal obligation where applicable
Diagnosing errors, maintaining quality and ensuring the proper functioning of products and services	technical, device, session, error log and usage data	legitimate interest in maintaining secure and functional services; performance of a contract where necessary
Fraud prevention, abuse prevention, security and protection of rights	identity, account, transaction, technical, fraud prevention and security data	legitimate interest; legal obligation; establishment, exercise or defense of legal claims
Compliance with legal obligations and requests from authorities or courts	identity, contact, contractual, transaction and other relevant data	legal obligation; establishment, exercise or defense of legal claims
Managing disputes, claims and legal proceedings	contractual, transaction, communication and other relevant data	legitimate interest; legal obligation; establishment, exercise or defense of legal claims
Direct marketing by electronic means	identity, contact and marketing preference data	consent, unless applicable law allows a limited soft opt-in for similar products or services; User may opt out at any time
Service improvement, analytics and aggregated statistics	technical, usage and aggregated data	legitimate interest, provided that the processing is proportionate and does not override User rights; consent where required by law
Organizing events, campaigns, contests or promotions	identity, contact, participation and communication data	consent; performance of specific promotion terms; legitimate interest where appropriate

6. Fiscal code / personal identification number

DM may process the User's fiscal code / personal identification number only where necessary, for example for correct identification of the contracting party, invoicing, performance of legal obligations, fraud prevention, or the establishment, exercise or defense of legal claims.

DM applies appropriate safeguards, including restricted access, technical and organizational security measures, defined retention periods, confidentiality obligations and training of persons who process such data.

Where the fiscal code / personal identification number is legally or contractually required, refusal to provide it may make it impossible to conclude or perform the contract.

7. Image, voice, camera-related data and biometric data

Certain DM products or services may involve voice, image or camera-related functionalities. Such processing will be limited to what is necessary for the relevant feature, service, technical operation, support or security purpose.

Unless expressly stated otherwise in a separate notice, DM does not process image, voice or camera-related data for the purpose of uniquely identifying a person through biometric identification.

If DM introduces biometric identification, biometric authentication, facial recognition or similar functionality, DM will provide a separate notice and will rely on an appropriate legal basis, including explicit consent where required by applicable law.

8. Profiling, automated analysis and fraud prevention

DM may use limited profiling or automated analysis for fraud prevention, abuse prevention, service security, risk assessment, account protection and service improvement.

DM will not make decisions based solely on automated processing that produce legal effects concerning the User or similarly significantly affect the User, unless such processing is authorized by law, necessary for entering or performing a contract, or based on explicit consent, and appropriate safeguards are in place.

Where profiling is used for marketing or analytics, the User may object or withdraw consent, depending on the applicable legal basis.

9. Marketing communications

DM may send marketing communications only where legally permitted. In particular:

- DM may send marketing communications if the User has given consent;
- DM may send communications about similar products or services to existing customers where applicable law allows this and where the User is given a clear and simple opt-out option;
- the User may unsubscribe or opt out at any time by using the unsubscribe link or by contacting privacy@dilan-mirrors.com.

DM will not disclose personal data to third parties for their independent direct marketing purposes without the User's consent.

10. Cookies and similar technologies

DM may use cookies and similar technologies for the operation of the website, security, analytics, preferences and marketing, depending on the case.

Strictly necessary cookies may be used without consent where they are required for the website or service to function. Analytics, advertising or non-essential cookies will be used only in accordance with applicable law and, where required, based on the User's consent.

A separate cookie banner describes the categories of cookies used, their duration, providers and available choices.

11. Disclosure of personal data to third parties

Personal data may be disclosed to the following categories of recipients only where necessary and lawful:

- **Affiliated companies**, for internal administrative, operational or legitimate business purposes, subject to appropriate safeguards.
- **Service providers and processors**, including hosting providers, database providers, payment processors, delivery providers, customer support tools, IT maintenance providers, analytics providers and professional advisers. Such providers may process personal data only under contractual obligations and only for the purposes instructed by DM.
- **Business partners**, only where necessary for a joint promotion, event or service, and only where the User has been properly informed and, where required, has consented.
- **Authorities, courts, law enforcement bodies or regulators**, where disclosure is required by law, necessary to respond to lawful requests, or necessary for the establishment, exercise or defense of legal claims.
- **Professional advisers**, such as lawyers, auditors, accountants, insurers or consultants, where necessary for legitimate business, compliance or legal purposes.
- **Potential successors**, in the context of a merger, restructuring, acquisition, sale of assets or similar transaction, subject to confidentiality and data protection safeguards.

DM requires processors and service providers to comply with applicable data protection and information security requirements.

12. Hosting, database providers and international transfers

The DM website, related databases and related technical infrastructure may be hosted and maintained by third-party service providers.

- **Website hosting provider:** ROMARG SRL, a hosting provider established in Romania, within the European Economic Area.
- **Database / infrastructure provider:** ROMARG SRL, Romania, as part of the website hosting service, unless a separate provider is used for a specific service.

The website and related databases are hosted by ROMARG SRL, a hosting provider established in Romania, within the European Economic Area. When ROMARG SRL or any other service provider processes personal data on behalf of DM, DM will ensure that appropriate data processing agreements, security obligations and confidentiality obligations are in place.

Personal data may be processed in the European Economic Area, in countries recognized as providing an adequate level of protection, or in other countries where appropriate safeguards are implemented.

Where any personal data is transferred outside the EEA by DM or its service providers, DM will rely on appropriate safeguards, such as an adequacy decision, Standard Contractual Clauses, binding corporate rules, or another lawful transfer mechanism, where required by applicable law. Where required, DM will also assess whether supplementary measures are necessary.

Consent will be used for international transfers only where permitted by applicable law and only after the User has been informed of the possible risks of such transfer.

13. Retention of personal data

DM retains personal data only for as long as necessary for the purposes for which it was collected, including for the performance of contracts, provision of services, compliance with legal obligations, resolution of disputes, fraud prevention, security, accounting and the establishment, exercise or defense of legal claims.

As a general rule:

- The previous general retention statement of six years should be applied only where it corresponds to a legal obligation or applicable limitation period. If a different statutory period applies, the statutory period prevails.
- Upon expiry of the applicable retention period, DM will delete, anonymize or securely destroy personal data, unless continued retention is required by law or for legal claims.

CATEGORY OF DATA	RETENTION PERIOD
Account data	for the duration of the account and a reasonable period after closure, unless a longer period is required for legal claims, security or statutory obligations
Contract, order, invoice and payment-related data	for the statutory accounting/tax retention period and, where relevant, for the limitation period applicable to legal claims
Customer support and complaint data	for the time necessary to resolve the request and, where relevant, for the limitation period applicable to legal claims
Technical logs and security data	for a limited period, necessary for security, diagnostics and fraud prevention, unless a longer period is required for investigation or legal purposes
Marketing consent and preference data	until withdrawal of consent or opt-out, plus a reasonable period necessary to keep evidence of the opt-out or consent status
Data processed based on consent	until withdrawal of consent, unless another legal basis requires continued retention

14. Information security

DM implements appropriate technical and organizational measures to protect personal data against unauthorized access, disclosure, alteration, loss, misuse, accidental destruction or unlawful processing.

These measures may include, depending on the case:

- access control and authentication measures;
- confidentiality obligations for personnel and contractors;
- encryption or pseudonymization where appropriate;
- secure hosting and backup procedures;
- monitoring and logging of security-relevant events;
- regular review of security measures;
- incident response procedures;
- staff training and internal policies.

No electronic service can be guaranteed to be completely secure. However, DM will take reasonable and proportionate steps to protect personal data according to the risks presented by the processing.

15. Rights of the User

Subject to the conditions and limits provided by applicable law, the User has the following rights:

- **Right of access** – to obtain confirmation whether DM processes personal data and to receive information about such processing.
- **Right to rectification** – to request correction of inaccurate or incomplete personal data.
- **Right to erasure** – to request deletion of personal data where the legal conditions are met.
- **Right to restriction of processing** – to request limitation of processing in certain cases.
- **Right to data portability** – to receive certain personal data in a structured, commonly used and machine-readable format, where applicable.
- **Right to object** – to object to processing based on legitimate interest, including profiling based on legitimate interest.
- **Right to withdraw consent** – where processing is based on consent, to withdraw consent at any time.
- **Right not to be subject to certain automated decisions** – where applicable, to object to decisions based solely on automated processing that produce legal effects or similarly significant effects.
- **Right to lodge a complaint** – to lodge a complaint with the competent supervisory authority.

Requests may be submitted to privacy@dilan-mirrors.com. DM may need to verify the identity of the requester before responding. DM will respond within the period required by applicable law.

Competent supervisory authority: The Data Protection Commission (DPC): 6 Pembroke Row, Dublin, 2 D02 X963 Ireland.

16. Exercising choices and controls

The User may, where applicable:

- update account information;
- withdraw consent;
- opt out of marketing communications;
- change cookie preferences;
- disable certain device permissions, such as camera, microphone or location permissions, through the settings of the device or browser;
- object to processing based on legitimate interest;
- request deletion, restriction or correction of personal data.

Some choices may affect the availability or functionality of certain services.

17. Children's data

DM products and services are not intended for children unless expressly stated otherwise. DM does not knowingly collect personal data from children without the consent or authorization required by applicable law.

If DM becomes aware that it has collected personal data from a child without the required legal basis, it will take appropriate steps to delete or otherwise lawfully process such data.

The minimum age for using DM website is 18 years and parental consent process if the products/services are offered to children.

18. Changes to this Policy

DM may update this Policy from time to time. The latest version will be published on the DM website:

<https://dilan-mirrors.com/>

Where changes are material, DM will take reasonable steps to inform Users, for example by publishing a notice on the website, sending an email, or requesting renewed consent where required by law.