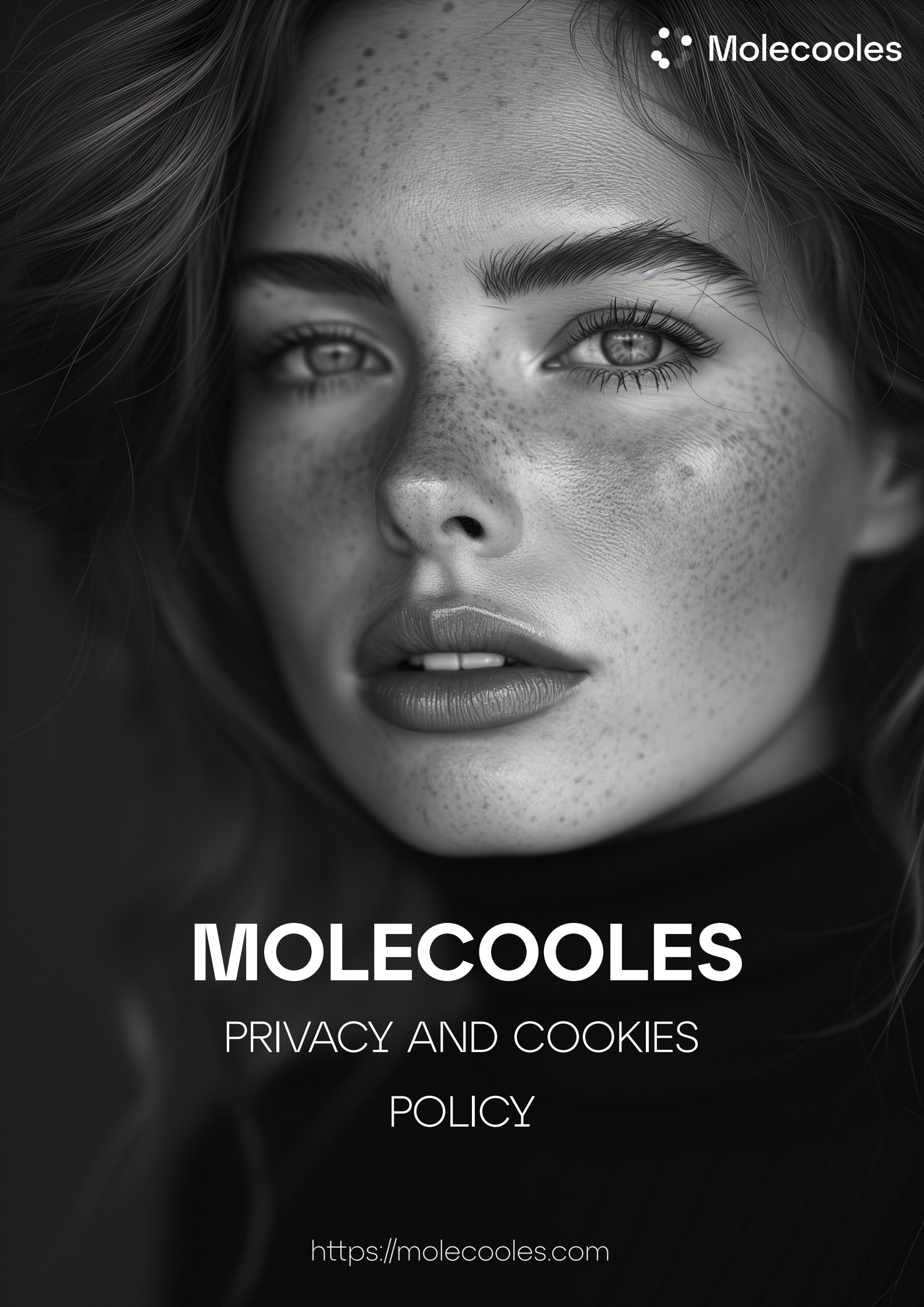

MOLECOOLES

PRIVACY AND COOKIES POLICY

https://molecooles.com

The online service operating at the address www.molecooles.com ("Service") is operated by: Molecooles OÜ, Harju maakond, Lasnamäe linnaosa, Narva mnt 13-27, 10151 Tallinn, Estonia, registration number 16871783, VAT number: EE102694369 (hereinafter: "Seller").

Contact with the Seller: hello@molecooles.com (the email address also constitutes an electronic point of contact within the meaning of the provisions on digital services). Written contact: as above (Seller's registered office address). Communication may take place in Polish or English.

§1. BASIC INFORMATION

1. This document ("Privacy and Cookies Policy", hereinafter: "Policy") defines the rules for processing personal data and the use of cookies and similar technologies in connection with using the online service available at www.molecooles.com ("Service").

2. The Policy applies to persons using the Service, in particular to:

a. persons browsing the Service,

b. persons placing orders in the online store operated in the Service ("Store"),

c. persons having an Account in the Service,

d. persons using the MQLS loyalty program ("MQLS Program"), including the panel presenting MQLS information and related functionalities,

e. persons using the skin analysis / face scan function ("AI face scan") available in the Service (if provided).

3. The Policy is informational in nature and is made available free of charge in the Service in a way that allows it to be saved, reproduced, and recorded.

4. Terms/concepts appearing in this Policy have the meaning assigned to them in this document, and in the absence of such a definition, in the Service Terms or MQLS Terms found in the Service.

5. The Policy is prepared in particular based on:

a. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter: "GDPR"),

b. provisions on privacy in electronic communications (so-called ePrivacy), in particular Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, and national provisions issued for its implementation – in the scope of using cookies and similar technologies,

c. other mandatory provisions of law applicable to the operation of the Service, including the provision of electronic services and distance sales – to the extent they apply to data operations or Service functionalities.

§2. WHAT DATA WE COLLECT AND WHERE WE GET IT FROM

1. Depending on how you use the Service, we may process the following categories of data:

a. Account / profile data (Account in the Service):

i. name and surname (or name), email address, password (in encrypted/hashed form), phone number (if required), delivery addresses, history of activity in the Service, Account settings.

ii. analysis results saved in the Account and materials sent by the user as part of this function (in accordance with its description in the Service).

b. Data related to orders in the Store:

i. information necessary to place and fulfill an order: ordered products, date and order number, price, currency, discounts, delivery costs, delivery method, fulfillment status, invoice data (if provided), history of returns and complaints.

c. Data related to payments:

i. We do not process full payment card data; payment processing is handled through the Payment Operator.

ii. We may process transaction identifiers, payment status information (e.g., "paid / rejected"), date and payment amount, general payment method, and data necessary for settlements and handling possible refunds.

d. Communication data:

i. content of correspondence and reports sent to us (e.g., email), contact details provided in the correspondence, contact dates, information provided during report handling.

e. Technical and operational data of the Service:

i. in particular: IP address, device and browser identifiers, operating system, approximate location derived from IP, visit dates and times, event logs, information about activity in the Service (e.g., entering subpages, actions in the Cart), error and performance data.

f. Cookies and online identifiers

i. identifiers stored in cookies or similar technologies (e.g., browser storage), which may be used for purposes necessary for the operation of the Service and, depending on your settings, for analytical and marketing purposes. Details are in the cookies section.

2. Where do we get the data from?

a. From you, when you provide it in the Service, e.g., you create an Account, place an order, contact us, or use the AI face scan function.

b. From the Service (automatically generated data) - when you use the Service, some data is generated automatically (e.g., logs, technical data, cookie identifiers, order history).

c. From our partners / service providers - to the extent necessary for the operation of the Service and provision of services:

d. Payment Operator - provides us with payment status information and transaction identifiers necessary for order settlement;

e. MQLS Program Provider - may process data related to MQLS Program functionalities, including wallet functionalities and (if applicable) KYC, in accordance with its terms and rules; we receive from the Program Provider information necessary for presenting and settling the MQLS Program in the Service.

§3. FOR WHAT PURPOSES WE PROCESS DATA AND ON WHAT LEGAL BASIS

1. In paragraph 4 below, we present a summary of data processing purposes ("purpose → data → legal basis → recipients → retention period").

2. The scope of data and recipients may vary depending on which Service functions you use.

3. Legal bases (GDPR):

a. Art. 6(1)(b) - performance of a contract / taking steps at the request of the data subject prior to entering into a contract,

b. Art. 6(1)(c) - legal obligation,

c. Art. 6(1)(f) - legitimate interests pursued by the controller,

d. Art. 6(1)(a) - consent (e.g., marketing/analytical or marketing cookies, if used).

4. Table: processing purposes.

COOKIE	PROVIDER	PURPOSE	RETENTION	CATEGORY	BASIS	LINK
Essential cookies (session) - e.g. session_id / csrf_token	Molecooles	Ensuring proper operation of the Service (session handling, security, login, cart)	Session / up to X days	Essential	Essential (no consent required)	—
Preference cookies - e.g. lang	Molecooles	Remembering user settings (e.g. language)	Up to X days	Functional	Consent or essential (depending on implementation)	—
CMP / banner cookies - e.g. cookie_consent	CMP provider/ Molecooles	Storing your cookie preferences	Up to X days / months	Essential / Functional	Essential (no consent required)	(CMP policy link)
Google Analytics (if used) - ga, _ga_*	Google	Statistics and analytics of Service usage	Usually up to 2 years (depending on configuration)	Analytical	Consent	(Google policy link)
Meta Pixel (if used) - fbp	Meta (Facebook)	Marketing/remarketing, ad performance measurement	Usually up to 3 months (depending on configuration)	Marketing	Consent	(Meta policy link)
Google Ads / Floodlight (if used)	Google	Remarketing and campaign measurement	Depends on the tool	Marketing	Consent	(Google policy link)
Hotjar/Clarity (if used)	Hotjar/Microsoft	User behavior analysis (e.g. click maps, session recordings)	Depends on configuration	Analytical	Consent	(Provider policy link)
YouTube/Vimeo embeds (if used)	Google/Vimeo	Video playback, potential tracking cookies	Depends on provider	Functional / Marketing	Consent (for optional cookies)	(Provider policy link)
Stripe (payment elements, if cookies are set)	Stripe	Payment processing and transaction security	Depends on Stripe	Essential / Functional	Essential or consent (depending on scope)	(Stripe policy link)

§ 4. MQLS PROGRAM - DATA AND ROLE OF THIRD PARTIES

1. The MQLS loyalty program ("MQLS Program") is available in the Service. Below, we explain what data is processed in connection with the MQLS Program and what role third parties play in its operation.

2. In connection with the MQLS Program, we may process in particular:

a. Account identifiers in the Service (e.g., Account ID, email as login), to assign awards to the correct user;

b. Data regarding orders necessary for awarding benefits in MQLS, in particular: order identifier, date, order value (e.g., net/gross, depending on Program rules), discount information, return/chargeback information (to the extent necessary for settlements);

c. Data regarding MQLS awards and settlements, e.g., number of MQLS awarded under Cashback or Affiliation, balance presented in the panel, history of MQLS Program events in the scope presented in the Service;

d. Affiliation data – in particular, Affiliate Link identifier, information about assigning a purchase to a referral, data necessary for awarding MQLS bonus.

3. Division of roles – Seller vs. Program Provider:

a. Seller:

i. The Seller is responsible for the operation of the Service and the organization of the MQLS Program in the Service, in particular for:

ii. defining the rules of the MQLS Program (e.g., awarding Cashback, Affiliation, and rules for using MQLS in the Service),

iii. presenting information about the MQLS Program in the Service (e.g., panel/ balance/events),

iv. handling inquiries and complaints regarding the operation of the MQLS Program in the Service (to the extent they concern the Seller).

b. Program Provider:

i. Functionalities related to handling the MQLS wallet, performing token operations, and possible KYC verification are carried out by the external provider, the Program Provider, based on its own conditions and rules.

c. In particular, the Seller:

i. does not provide CASP/custody services,

ii. does not control private keys and does not perform wallet actions on the user's side,

iii. does not conduct the KYC process in connection with wallet operations; if required, it is conducted by the Program Provider.

4. In connection with using the MQLS Program, data may be transferred to the Program Provider to the extent necessary to ensure the operation of the MQLS Program functionalities, in particular for the purpose of:

a. launching and maintaining MQLS wallet functions (e.g., assigning/handling MQLS Wallet address in custodial model),

b. performing token operations (e.g., awards, transfers, withdrawals/deposits, if such functions are available),

c. handling KYC/access restrictions (if KYC is required for a given function),

d. ensuring security and preventing abuses within functionalities provided by the Program Provider.

5. The scope of data transferred to the Program Provider may include in particular: Account identifiers, order and MQLS Program event identifiers, information necessary for awards and settlements, and if the Customer uses functions requiring KYC, data required by the Program Provider as part of its verification process.

6. Information about possible data transfers outside the EEA, including to the

USA, is in the Policy section on data transfers.

§5. AI / FACE SCAN - PRIVACY RULES FOR THIS FUNCTION

1. The skin analysis / face scan function ("AI face scan") is available in the Service. Below, we explain what data is processed in connection with this function and on what principles.

2. Using the AI face scan function is optional. Using or not using this function does not affect the ability to browse the Service or make purchases in the Store (in the scope of standard Service functions).

3. In the AI face scan, the following data may be processed in particular:

a. face image (photo or image material taken via the user's device camera);

b. analysis results generated based on the submitted image (e.g., information about skin features, matched recommendations, or assessment result);

c. technical data related to performing and displaying the result (e.g., session dentifier, date and time, device/browser information).

4. The analysis results may refer to skin features or information that may be interpreted as health-related data. For this reason, to ensure a higher level of protection, data processed in the AI face scan may be treated as special category data within the meaning of Art. 9 GDPR (in particular, if the analysis results indicate features that may be related to health status).

5. Note: AI face scan is not intended to provide medical services or make diagnoses. The results are informational in nature.

6. In the scope of processing data in the AI face scan (including face image and analysis results), the legal basis is the user's consent - Art. 6(1)(a) GDPR.

7. If special category data is processed in the AI face scan (e.g., health-related data), the legal basis is additionally the user's explicit consent - Art. 9(2)(a) GDPR.

8. The user may withdraw consent at any time, which does not affect the lawfulness of processing carried out before its withdrawal.

9. AI face scan results and saved materials (if the Service provides for their saving) are available only in the user's Account in the Service. The Seller does not publish these data in the Service nor make them available to other users.

10. The user may delete saved AI face scan results (if the Service provides such a function) via the Account in the Service or by contacting the Seller.

11. If the user does not delete these data earlier, they will be stored as a rule until the Account in the Service is deleted, and then deleted or anonymized, unless there is a legal obligation for further storage (as a rule, this does not apply to AI face scan data).

12. The AI face scan functionality may be implemented using external technology providers (e.g., AI tools or hosting). In such a case, the Seller:

a. selects providers in a way that ensures an appropriate level of data protection,

b. transfers data only to the extent necessary for the operation of the AI face scan function (data minimization principle),

c. ensures an appropriate legal basis for data sharing (e.g., data processing agreement), and describes issues of transfers outside the EEA in the section on data transfers.

13. Information about the provider/providers used for AI face scan may be indicated in the Service or provided at the user's request, to the extent required by provisions.

§6. DATA RECIPIENTS (CATEGORIES) AND PROCESSORS

1. In connection with operating the Service and providing services, your personal data may be shared with recipients only to the extent necessary to achieve the specific purposes mentioned in this Policy.

2. Main categories of recipients:

a. Payment Operator - In the scope of payment handling, refunds, and settlements, data may be transferred to the payment operator Stripe (or entities from its capital group) - to the extent necessary for transaction handling and payment security.

b. MQLS Program Provider - In the scope of MQLS Program functionalities, including those related to the MQLS wallet, token operations, and possible KYC, data may be shared with the Program Provider - to the extent necessary for providing these functionalities.

c. IT and Service maintenance providers - In particular, these may be:

i. hosting and server infrastructure,

ii. CDN providers (content delivery),

iii. IT security, monitoring, and backup service providers,

iv. cookie consent management tool providers (CMP) – if used.

d. Communication and customer service providers - In particular:

i. email service providers,

ii. SMS service providers (if used),

iii. helpdesk/CRM system providers (if used).

e. Analytical and marketing tool providers (if used) - In particular, entities providing analytical, statistical, or advertising/remarketing tools, in the scope depending on your cookie settings and consents granted.

f. Entities handling order fulfillment - In particular, carriers and logistics operators (couriers), as well as entities supporting warehousing and return handling - if used.

g. Accounting and settlement support entities - Entities providing accounting, tax, or settlement and audit support services.

h. Legal advisors and auditors - If necessary (e.g., dispute, debt collection, pursuit or defense of claims), data may be shared with legal advisors, law firms, and auditors.

i. Public authorities and other authorized entities - Data may be shared with public authorities or other entities entitled to receive them under legal provisions (e.g., courts, law enforcement authorities, tax authorities) - only to the extent required by law.

3. In many cases, the above recipients act as processors on our behalf (e.g., hosting, email, helpdesk). In such situations, we ensure the legally required safeguards, in particular, we conclude data processing agreements (Art. 28 GDPR), if required.

§7. DATA TRANSFERS OUTSIDE THE EEA

1. In connection with using the Service and our providers' services, your personal data may be transferred to countries outside the European Economic Area (EEA), in particular to the United States (USA).

2. Data transfer outside the EEA may occur in particular when:

a. you use MQLS Program functionalities that are implemented by an external provider (e.g., Enzo) and require data processing on infrastructure located outside the EEA;

b. we use IT service providers (e.g., hosting, cloud infrastructure, CDN, monitoring and security systems) that have servers outside the EEA or use subcontractors outside the EEA;

c. we use analytical or marketing tools whose providers are based outside the EEA or process data on servers outside the EEA (if such tools are used).

3. In the case of data transfer outside the EEA, we ensure the legal basis required by GDPR. Depending on the provider and transfer direction, this may include in particular:

a. a decision establishing an adequate level of protection issued by the European Commission (if applicable);

b. standard contractual clauses (SCC) adopted by the European Commission;

c. other mechanisms provided in GDPR (e.g., additional safeguards or, in exceptional cases, specific derogations), if required and appropriate in a given case.

4. Detailed information on the transfer mechanism used for a given provider may result from its documentation or agreements concluded with the Seller.

5. You can obtain a copy of the safeguards applied for data transfer outside the EEA (e.g., a copy of standard contractual clauses, to the extent permissible) or additional information regarding the transfer by contacting us at: hello@molecooles.com

§8. DATA RETENTION PERIODS

1. We store personal data for a period no longer than necessary to achieve the purposes for which the data is processed, taking into account legal obligations and limitation periods for claims.

2. Data related to the Account in the Service is stored:

a. for the duration of having the Account, and then

b. after deleting the Account, for the period necessary for:

c. settlements (if transactions occurred),

d. handling possible complaints and disputes,

e. establishment, pursuit, or defense of claims (until the expiry of limitation periods),

f. fulfillment of legal obligations (e.g., archiving of certain documents).

3. Data related to order fulfillment, as well as accounting and tax documents (e.g., invoices), is stored for the period required by legal provisions applicable to settlements and accounting, and for the period necessary for defense of claims.

4. Data related to complaints, returns, withdrawals from contracts, and disputes is stored for the time necessary to handle the matter, and then for the period enabling establishment, pursuit, or defense of claims, i.e., as a rule, until the expiry of limitation periods for claims.

5. Technical data, system logs, and information related to Service security is stored for a limited time, appropriate to security and accountability purposes (e.g., incident detection, prevention of abuses, event reconstruction). The storage period depends on the type of logs and may be shortened when the data is no longer needed for these purposes.

6. Data processed in the AI face scan function (in particular, face image and analysis results) is stored:

a. until deleted by the user (if the Service provides such a possibility) or

b. until the Account in the Service is closed/deleted, if the user has not deleted them earlier.

7. After closing/deleting the Account, these data are deleted or anonymized, unless there is an exceptional case requiring their retention (e.g., for dispute resolution purposes, if the data is necessary and proportionate).

8. In cases where data processing is based on consent (e.g., marketing or certain cookies), data is stored until consent is withdrawn, unless it is no longer needed earlier.

§9. USER RIGHTS

1. In connection with the processing of your personal data, you have rights arising from GDPR. You can exercise them by contacting us at: hello@molecooles.com.

2. Depending on the legal basis and processing circumstances, you have the right to:

a. access to data (Art. 15 GDPR), you can obtain information whether we process your data, and if so - receive a copy and information about the processing;

b. rectification of data (Art. 16 GDPR) - if the data is incorrect or incomplete;

c. erasure of data (Art. 17 GDPR) - in cases provided in GDPR (e.g., when data is no longer needed, and there is no other basis for processing);

d. restriction of processing (Art. 18 GDPR) - e.g., when you contest the accuracy of data or need the data for establishing claims;

e. data portability (Art. 20 GDPR) - when processing is based on consent or contract and carried out by automated means;

f. objection (Art. 21 GDPR) - when we process data based on legitimate interests; in such a case, we will stop processing the data unless we demonstrate compelling legitimate grounds overriding your interests, rights, and freedoms or grounds for establishment, pursuit, or defense of claims.

3. If we process data based on your consent, you have the right to withdraw it at any time, without affecting the lawfulness of processing carried out before withdrawal. This applies in particular to:

a. consent to use the AI face scan function (including - if applicable - explicit consent for special category data),

b. consents regarding cookies (analytical/marketing - if used),

c. marketing consent (e.g., newsletter - if conducted in this form).

4. If you believe that the processing of your data violates provisions, you have the right to lodge a complaint with a supervisory authority. Due to the Seller's seat in Estonia, the competent supervisory authority is the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon).

5. Regardless of the above, as a person residing in another EU country, you also have the possibility to lodge a complaint with the local supervisory authority in your place of habitual residence, place of work, or place of alleged infringement. In Poland, the supervisory authority is the President of the Personal Data Protection Office (PUODO): ul. Stanisława Moniuszki 1A, 00-014 Warsaw, email: kancelaria@uodo.gov.pl, website: UODO (contact).

§10. DATA SECURITY

1. We make efforts to protect personal data processed in the Service from unauthorized access, loss, destruction, alteration, or disclosure. We apply organizational and technical measures appropriate to the risk and nature of processing.

2. In particular, we apply (to the extent appropriate to the systems and processes of the Service):

a. access control to systems and data, access is granted only to authorized persons, to the extent necessary for performing their duties;

b. limitation of authorizations and registration and verification of access (to the extent justified by security needs);

c. encryption of data transmission (e.g., HTTPS/TLS connections), to limit the risk of data interception during transmission;

d. infrastructure and IT environment safeguards, including monitoring of Service operation and responding to incidents to the extent appropriate to the conducted activity;

e. selection of service providers (e.g., hosting, payments, IT tools) taking into account security requirements and, if required, concluding appropriate agreements and arrangements regarding data protection.

3. The security of the Account in the Service also depends on you. In particular:

a. use a strong password and do not share it with third parties;

b. do not save the password in a way that enables easy access by unauthorized persons;

c. use trusted devices and up-to-date software;

d. if you suspect unauthorized access to the Account, change the password immediately and contact us.

4. We may take actions to protect the Account and the Service (e.g., temporary access restriction or verification of selected actions), if justified by security or suspicion of abuses.

§11. COOKIES AND SIMILAR TECHNOLOGIES

1. In the Service, we use cookies and similar technologies (e.g., local storage, online identifiers) ("Cookies") to ensure proper operation of the Service, enhance its functionality, and depending on your settings, conduct analytics and marketing activities.

2. Cookies are small text files saved on your device (computer, phone, tablet) while using the Service. They enable, among others:

a. maintaining sessions and proper operation of basic functions (e.g., login, Cart, session retention),

b. remembering selected settings,

c. analyzing the use of the Service (statistics),

d. tailoring content and ads.

3. Cookies may be set:

a. by Molecooles (own cookies), to ensure the operation of the Service;

b. by third parties (external cookies), if the Service uses providers of tools (e.g., analytical, marketing, video tools, maps, chats, etc.). The scope and types of cookies depend on the tools actually used.

4. The Service may use the following categories of Cookies:

a. Essential (necessary): They are needed for the proper operation of the Service and its basic functions (e.g., security, login, Cart, session retention). Your consent is not required for these cookies.

b. Functional: They enable remembering your settings and preferences (e.g., language, display settings) to facilitate using the Service. They may require consent, depending on their nature and national provisions.

c. Analytical (statistical): They help us understand how users use the Service (e.g., which subpages are visited, how navigation works) to improve it. These cookies are used based on your consent (if used).

d. Marketing: They may serve to display tailored content and ads and measure campaign effectiveness (e.g., remarketing). These cookies are used based on your consent (if used).

5. During your first visit to the Service, we display a consent management tool (e.g., banner) that enables:

a. accepting selected cookie categories,

b. rejecting optional cookies,

c. changing settings at any time.

6. You can change your cookie settings at any time (including withdrawing consent) via the mechanism available in the Service (e.g., "Cookie settings" link/icon or similar function).

7. You can also manage cookies through your web browser settings (e.g., blocking cookies, deleting saved cookies). Remember that disabling essential cookies may affect the operation of the Service.

8. Some browsers offer a "Do Not Track" (DNT) setting. Currently, different services and tools may interpret DNT differently, so the Service may not automatically respond to this signal. You can always manage consents in the cookie settings described above.

§ 12. CHANGES TO THE POLICY

1. We may update this Privacy and Cookies Policy, in particular when:

a. legal provisions or supervisory authority guidelines change,

b. the way the Service operates changes, the scope of services provided (e.g., MQLS Program, AI face scan functions),

c. tools or providers used change (e.g., hosting, analytics, payment operator, Program Provider),

d. it is necessary due to security or improving information transparency.

2. We may inform about selected changes via the Service (e.g., message) or by email, if we have your address and such channel is appropriate for the type of change.

3. The updated version of the Policy is effective from the date indicated in its content. In the case of changes that significantly affect data processing (e.g., introduction of new purposes or new recipient categories), we may apply additional information measures or – if required – ask for re-consent (e.g., in the scope of cookies or AI face scan function).

§13. FINAL PROVISIONS

1. This Privacy and Cookies Policy is informational in nature and describes the rules for processing personal data in the Service and the rules for using cookies and similar technologies.

2. In matters not regulated by this Policy, the appropriate legal provisions apply, in particular GDPR and national provisions on personal data protection and electronic communications (in the scope of cookies).

3. If any provision of this Policy proves invalid or ineffective, this does not affect the validity of the remaining provisions. In place of the invalid provision, a solution as close as possible to the economic and legal purpose is applied, while maintaining legal requirements.

4. The current version of the Policy is always available in the Service.