

ANNEX No. 1: List of Designated Persons and their Roles *(to Article 5 of Internal Directive No. 1/2026 on Personal Data Protection and AML)*

The company **MATISTOTELES s.r.o.** hereby appoints the following persons who are **entrusted with specific activities** in the context of compliance with personal data protection and the fulfilment of anti-money laundering obligations (AML). Every employee is required, in the given situations, to turn to the relevant designated person according to the list below:

- **Company Director (Controller)** – *Mateusz Leon Jagoda*: The statutory body and the person with overall responsibility for personal data processing and for fulfilling AML obligations. Oversees and approves internal directives, decides on remedial measures and on reporting incidents to supervisory authorities.
- **Designated person for personal data protection agenda (GDPR)** – *Mateusz Leon Jagoda*: Responsible for monitoring compliance of processing with the GDPR, providing consultation to staff, receiving and handling data subjects' requests and complaints. Ensures the keeping of records of processing activities, updates the Privacy Policy and communicates with the Office for Personal Data Protection (ÚOOÚ). *(Note: A Data Protection Officer under Article 37 GDPR is **not** currently appointed; this role is performed by an internal appointed person.)*
- **Information Security Manager (IT Security)** – *Mateusz Leon Jagoda*: Responsible for technical and organisational measures to ensure the security of data. Manages and supervises IT systems (network security, passwords, encryption, backups, antivirus protection, etc.), addresses technical aspects of any incidents and proposes corrective measures.
- **Contact person for AML agenda** – *Mateusz Leon Jagoda*: Ensures fulfilment of obligations under the AML Act. Carries out client identification and due diligence under Sections 7 and 9 of the AML Act, evaluates potentially suspicious transactions and, if needed, submits notifications to the Financial Analytical Office (FAÚ). Oversees the keeping of records and archiving of client data in accordance with the AML Act.

ANNEX No. 2: “Client Identification Record” Form *(pursuant to Section 7 of the AML Act)*

Identifying employee (Name, position):

.....

Place and date of identification:

Identified client:

- **Natural person** – Name, surname:; **Date of birth:**; **Citizenship:**
Permanent residence (street, No., city, postcode):

.....
Type and number of identity document:; **Issued by:**; **Valid until:**

(If the client acts as a representative of another person, also provide the identification details of the represented person and the basis of representation.)

- **Legal entity – Business name:**; **Company ID (IČO):**

Registered office:

.....
.....

Statutory representative (identified natural person):

..... (name, surname, title)

Purpose and nature of the transaction/business relationship:

..... *(e.g. one-time cash purchase of goods, long-term supply services, etc.)*

Client's declaration: I have been informed that identification is carried out pursuant to Act No. 253/2008 Coll. for the purposes of preventing the legalisation of proceeds of crime and financing of terrorism. I have provided the above data truthfully.

Signature of identified person (client): **Employee's signature:**

Attachments: Copy of identity document [YES/NO]; Other documents:

.....

(This completed form is retained in accordance with Section 16 of the AML Act for a period of 10 years from the termination of the business relationship or the execution of the individual transaction.)

ANNEX No. 3: Records of Personal Data Processing and Training (GDPR/AML)

3A) Records of Processing Activities (per Article 30 GDPR)

The Controller, MATISTOTELES s.r.o., maintains an overview of all **registers of personal data** and processing activities it carries out. Each record contains information as required by Article 30 GDPR (purpose of processing, description of categories of data subjects and data, legal basis, recipients, retention periods, and security measures). Below is a summary table of the main registers:

Name of Register	Purpose of Processing	Categories of Data Subjects	Categories of Personal Data	Legal Basis	Data Recipients	Retention Period
------------------	-----------------------	-----------------------------	-----------------------------	-------------	-----------------	------------------

HR – employees	Management of the employment relationship, payroll calculation, and fulfilment of employer obligations.	Employees (and job applicants).	Identification and contact details, birth number, qualification data, salary data, health insurance company, etc.	Performance of contract and legal obligation (Labour Code, Social Security Act).	Accounting firm; public authorities (Social Security Administration, health insurance companies, Tax Office), etc.	50 years from end of employment (personnel files); payroll records 30 years; others 10 years.
Customers – e-shop orders	Processing orders, delivering goods/services, and customer account maintenance.	Customers – natural persons (consumers); and contact persons of customer businesses.	Identification and contact details, order information (purchased products, prices), payment details.	Performance of contract (purchase contract) and legal obligation (accounting regulations).	External carriers (shipping companies); payment gateway; e-shop IT service provider.	10 years from end of the year in which the order was completed (per Accounting Act).
Marketing – newsletter	Sending commercial communications to subscribed recipients and customers.	Customers and individuals subscribed to the newsletter.	Contact details (email, name), records of interactions (email opens, clicks).	Data subject's consent (for new subscribers); legitimate interest (for existing customers).	Email platform provider (processor) – e.g. mailing service; no other external disclosure.	For the duration of consent (until withdrawn); for customers until objection, max. 3 years from last purchase.
Suppliers – contracts	Record and management of contracts with	Suppliers (self-employed individuals);	Identification and contact details, Company	Performance of contract and legal obligation	External accounting (processor); banking	10 years from end of contractual

	suppliers, communications and payments.	representatives of legal entities).	ID/VAT No., details of goods/services provided, bank details.	n (contract archiving, accounting).	institutions (payments); legal advisors if applicable.	relationship (per Commercial Code archiving duties and VAT Act).
--	---	-------------------------------------	---	-------------------------------------	--	--

3B) Training Plan and Records of Training (GDPR/AML)

The Company ensures regular **employee training** in the area of personal data protection and anti-money laundering prevention (AML) – see the “Training and Awareness” section of the Directive. Every new employee undergoes initial training, followed by refresher training **at least once a year** or in the event of legislative changes. Below is an overview of planned and completed training sessions:

Date	Type of Training	Target Group / Participants	Trainer	Confirmation of Attendance
<i>plan 2027</i>	<i>Recurring GDPR/AML training</i>	<i>All employees</i>	<i>As needed (ČIIK course)</i>	<i>(planned – to be added)</i>

Each training session is documented (program, date, list of participants, instructor) and records are archived by HR. All employees also continuously receive significant updates and guidance (e.g. information on new security risks such as **phishing** attacks, updates to directives, etc.).

3C) Record of Security Incidents and Notifications to Authorities

The Company maintains an internal **Incident Register** relating to personal data protection and AML, in which every case of a personal data security breach (data breach) or suspicious transaction is recorded, including measures taken and any notifications to supervisory authorities (ÚOOÚ, FAÚ). This register is managed by the Managing Director or a designated person, is kept confidential, and is available for inspection in the event of an audit.

For each incident, at least the following information is recorded:

- **Date and time of detection of incident:**

- **Description of incident:** (e.g. loss of a flash drive containing customer data / unauthorised access to system / suspicious cash transaction of EUR 15,000 ...)
- **Measures taken to remedy:** (e.g. access blocked, passwords changed, customers notified, temporary suspension of transaction, etc.)
- **Reported to supervisory authority:** (ÚOOÚ – YES/NO; FAÚ – YES/NO; if yes, date and reference number of report sent)
- **Outcome and closure of incident:** (summary of how the matter was resolved, lessons learned, date of closure)
- **Person responsible for resolution:** (name of employee who handled it and prepared the record)

ANNEX No. 4: Templates of Consents and Notices for Data Subjects

4a) Sample Consent Text for Personal Data Processing (Marketing Purpose)

Purpose: Consent of a customer to the use of their personal data for marketing purposes (sending commercial communications, targeted advertising). This consent is required especially from individuals who are not existing customers (e.g. when signing up for a newsletter).

Consent to Personal Data Processing for Marketing:

I hereby give my consent to **MATISTOTELES s.r.o.**, Company ID: 24592269, as controller, to process my personal data in the scope of **email address and name** for the purposes of sending commercial communications (product offers, newsletters and information about events) and possible personalisation of these offers. This consent is granted for a period of **5 years** from its submission, or until it is withdrawn. I acknowledge that providing this consent is **voluntary** and that I may **withdraw it** at any time, for example by sending a message to reklamace@matistoteles.cz or complaints@matistoteles.cz. Withdrawal of consent does not affect the lawfulness of processing carried out before its withdrawal. I also confirm that I have acquainted myself with the personal data processing conditions stated in the *Privacy Protection* section on the company's website.

In Prague on DD. MM. YYYY

Name and surname: _____ **Signature:**

4b) Sample Information for Clients on Personal Data Processing (pursuant to Article 13 GDPR)

Information on Personal Data Processing

Controller: MATISTOTELES s.r.o., Company ID: 24592269, registered office at Římská 1222/33, Praha 2, 120 00, registered with the Municipal Court in Prague, Section C, File 443776. Contact: email info@matistoteles.cz, tel. (+420) ...

Purpose and legal basis of processing: Your personal data in the scope of **name, surname, address, contact details (telephone, e-mail)** and possibly other data provided in the order (e.g. delivery address) will be processed for the purpose of **concluding and performing the purchase contract** – delivering the ordered goods/services (legal basis is performance of a contract under Article 6(1)(b) GDPR). Furthermore, we may retain some of this data to fulfil **legal obligations** (especially accounting and tax obligations, legal basis is Article 6(1)(c) GDPR) and possibly use it to **protect our legitimate interests** (e.g. for establishing, exercise or defence of legal claims, Article 6(1)(f) GDPR).

Recipients of data: Your personal data may, for the above purposes, be transferred to the **shipping company** that delivers the goods (your name, address, telephone) and to the **payment gateway provider** (in case of an online payment). These entities process personal data as independent controllers. Your data are also processed by our external **accounting firm** (as a processor) to meet accounting obligations.

Retention period: Personal data will be stored for the duration of the contractual relationship and subsequently **10 years after its termination** (in accordance with statutory archiving periods in accounting and taxation), unless it is necessary to retain the data longer for the protection of our rights (in which case, no longer than until the expiry of limitation periods or the conclusion of any dispute).

Rights of data subjects: You have the right to request from us **access** to your personal data, their **rectification or erasure**, or **restriction of processing**. You may also object to the processing and, for data processed automatically on the basis of a contract or consent, you have the right to **data portability**. If you believe that the processing is unlawful, you have the right to lodge a **complaint with the Office for Personal Data Protection**. Detailed information about your rights and how to exercise them can be found on our website in the *Privacy Protection* section, or we will provide them to you upon request.

Additional information: Providing personal data for the above purposes is a **contractual requirement** – without it we would not be able to process your order. Our website may store cookies, about which we inform you separately in the Cookies Policy. Your data are not transferred to any countries outside the EU/EEA. We do not perform any automated decision-making that would produce legal effects for you. If you have any questions regarding the processing of personal data, please contact us via the above-mentioned contact details.

In Prague on DD. MM. YYYY

4c) Sample Response to a Data Subject's Request *(pursuant to Articles 15–22 GDPR)*

Subject: Handling of your request for ...

Dear ...,

On ... we received your request in which you exercised the right to In accordance with the GDPR, we hereby provide you with the following information and resolution of your request:

Our company processes the following personal data about you: (details in the attachment). The purpose of processing is ..., the legal basis is ..., the data are intended for ... and are stored for *(Attached to this response is a copy of your personal data from our system.)*

We have complied with your requests – as of ... we have deleted/irreversibly anonymised all personal data we hold about you that we no longer need. However, some data cannot be deleted immediately due to the fulfilment of legal obligations (e.g. we are required by law to archive invoices for a certain period). These data have been segregated and will be securely erased after the statutory periods expire.

We have carried out the requested correction/update of your personal data (specifically ...).

We have received your objection to the processing of personal data for ... purposes. After consideration, we have decided to uphold your objection – as of today, we no longer process your data for that purpose. *(Alternatively: We did not uphold your objection, because our legitimate grounds outweigh your rights and interests – see the reasoning below.)*

If you have any further questions regarding the information provided, please do not hesitate to contact us. You also have the right to lodge a complaint with the Office for Personal Data Protection, if you believe that our processing of your data is in violation of legal regulations.

Sincerely,

Mateusz Leon Jagoda, Managing Director
MATISTOTELES s.r.o.

4d) Sample Internal Record of Handling a Data Subject's Request

Identification of request: Reference number/ID of request: _____; date received: _____; method received: (by post/email/in person).

Requester (data subject): Name and surname:

_____; contact:

_____.

Data subject's request: (description of the right exercised – e.g. request for erasure of personal data related to the customer account).

Handling of request:

- Date of response to data subject: _____ (sent on _____ via _____).
- Outcome: (fulfilled – data erased/provided/address corrected; or refused – with explanation).

Actions taken in system: (brief description, e.g. customer account anonymised, email removed from marketing list, archive folder marked for deletion on DD.MM.YYYY).

Person responsible for handling: Name Surname; signature:

Review and approval: (checked by supervisor/another person – if not applicable, leave blank).

(Note: A copy of the original request and a copy of the response sent to the data subject are attached to this record. These documents are retained for at least 5 years after the request is handled.)

ANNEX No. 5: Internal Procedure for Suspicious Transactions (AML)

Procedure for Employees (Step-by-Step):

- **Recognising a suspicious transaction:** Pay attention to warning signs such as unusually large cash transactions (or their deliberate splitting just below the EUR 10,000 limit), unusual behaviour by the client during identification (refusing to provide information, presenting suspicious documents), transactions that do not match the client's profile or economic purpose, involvement of a client from a high-risk country or on a sanctions list, etc. If you notice such factors, consider the transaction potentially suspicious.
- **Immediate notification of designated person (AML):** As soon as you become suspicious, **immediately inform** the company's **AML designee** or directly the Managing Director (contact them in person or by phone; do not cause unnecessary delay with email communication). Provide all available information and documentation regarding the observed circumstances.
- **Suspending the transaction: Do not execute the suspicious transaction, if possible, until directed by management.** In accordance with Section 15 of the AML Act, execution of the transaction can be postponed for up to 48

hours from the moment the suspicion arose. During this time, wait for instructions from the Managing Director/designee, or for the FAÚ's guidance. Explain any delay to the customer tactfully, citing technical or administrative reasons – **you must not alert them to the suspicion** (the tipping-off ban).

- **Internal record:** Without delay, fill out an **Internal Suspicious Transaction Report** and submit it to the Managing Director/designee. Include the client's identifying details, a detailed description of the transaction, the reasons why you consider it suspicious, and attach related documents (copies of contracts, IDs, correspondence, etc.). A report form is available on the internal network and contains the particulars per FAÚ guidelines.
- **Notification to FAÚ:** If the responsible person determines that the transaction is suspicious, they will prepare and **send a notification to the Financial Analytical Office (FAÚ)**. The notification is sent via the FAÚ's data box or other secure channel within 5 working days of detecting the suspicious transaction (though usually sooner, typically within 24–48 hours). Until the FAÚ provides further directions, the Company will not execute the transaction (and will act according to any FAÚ instructions, e.g. further postponement or securing of funds).
- **Further steps:** After submitting the notification, await any instructions from the FAÚ. Provide full cooperation to all authorities (FAÚ, police) during their investigation. Once the incident is closed, add final information to the internal records (e.g. that the FAÚ found no wrongdoing / the transaction was blocked and funds were seized by the police, etc.).
- **Maintaining confidentiality:** A reminder that **employees are obliged to maintain confidentiality** about the fact that a transaction was flagged as suspicious or that a report was submitted to the FAÚ. The client and any unauthorised persons must not be informed, so as not to thwart the purpose of the investigation. Breaching confidentiality could result in criminal liability.