

DIRECTIVE No. 1/2026, on the Protection of Personal Data and the Prevention of Money Laundering

Purpose of the Directive: The purpose of this directive is to **set basic rules and procedures** for the processing of personal data at MATISTOTELES s.r.o. (the “*Company*”) and to ensure compliance with the requirements of the GDPR and related laws (in particular **Act No. 110/2019 Coll., on the Processing of Personal Data**). At the same time, this directive defines **measures for the prevention of the legalisation of proceeds of crime and the financing of terrorism (AML)**, to ensure the Company’s fulfilment of its obligations under **Act No. 253/2008 Coll., on Certain Measures Against the Legalisation of Proceeds of Crime** (hereinafter the “*AML Act*”). This directive is one of the organisational measures for the protection of personal data within the meaning of Article 32 of the GDPR and simultaneously an internal regulation implementing the obligations under the AML Act.

Scope: This directive is **binding on all personnel** of MATISTOTELES s.r.o. (hereinafter the “*Company*”) who process personal data or perform other activities governed by the GDPR or the AML Act. Every employee or external collaborator of the Company is required to familiarise themselves with this directive and to comply with it. A breach of the obligations laid down in this directive may be considered a serious breach of work discipline or of contractual duties. The directive applies to all personal data processing carried out by the Company, whether by automated or non-automated means, as well as to all activities of the Company that fall under the scope of the AML Act.

Terms, Definitions and Abbreviations: For the purposes of this directive, the following terms are defined as follows:

- **GDPR** – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
- **Personal data** – any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier (such as a name, identification number, location data, online identifier) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Processing of personal data** – any operation or set of operations performed on personal data or sets of personal data, by automated or non-automated means (e.g. collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, sorting, combination, restriction, erasure or destruction of personal data).

- **Controller** – the entity that determines the purposes and means of personal data processing (for the purposes of this directive, this is our Company as the controller of data relating to its clients, employees, etc.).
- **Processor** – any party that processes personal data on behalf of the Controller based on the Controller’s instructions (typically an external service provider such as an accounting firm, IT storage provider, legal representative, etc., with whom the Company has concluded a data processing agreement).
- **Data subject** – any natural person about whom personal data are processed (e.g. a customer, website user, employee).
- **Staff member** – for the purposes of this directive, any person performing work for the Company, including but not limited to employees under an employment contract, persons working under agreements for work, external consultants or service providers, if their activities involve handling personal data or processes subject to GDPR/AML.
- **Supervisory Authority** – the Office for Personal Data Protection (*Úřad pro ochranu osobních údajů, ÚOOÚ*), which in the Czech Republic oversees compliance with the GDPR and the Act on the Processing of Personal Data. (Hereinafter also “*ÚOOÚ*” or “*Office*”).
- **DPO – Data Protection Officer**, as defined in Article 37 of the GDPR. (*Note: MATISTOTELES s.r.o. is not obligated to appoint a DPO, as it does not fall into the categories of controllers listed in Article 37 of the GDPR; however, it may voluntarily appoint one. As of the issuance of this directive, the Company has not appointed a DPO. If a DPO is appointed in the future, the DPO’s details and duties will be added to this directive.*)
- **Company** – the company MATISTOTELES s.r.o., Company ID No.: 245 92 269, having its registered office at Římská 1222/33, Vinohrady, 120 00 Prague 2, registered in the Commercial Register maintained by the Municipal Court in Prague, Section C, Insert 443776. The Company, represented by its statutory body (Managing Director **Mateusz Leon Jagoda**), is responsible for fulfilling the obligations under this directive.
- **Obligated entity (under AML)** – an entity obligated under the AML Act; in the context of this directive, this refers to MATISTOTELES s.r.o. when it engages in activities that trigger obligations under the AML Act (in particular when conducting a cash transaction valued at or above EUR 10,000, or when carrying out other activities listed in Section 2 of the AML Act).
- **Client** – a natural or legal person with whom the Company enters into a business relationship or carries out a one-off transaction falling under the AML Act (typically a customer purchasing goods in cash above the specified threshold, or another partner for whom identification and due diligence under AML are required).

- **Identification and verification of client** – procedures under the AML Act (Sections 7 and 9 et seq. of the AML Act) including the ascertainment and verification of the client's identity (and, where applicable, that of their representative or beneficial owner), obtaining information on the purpose and nature of the transaction, and, if appropriate, determining the source of funds and evaluating whether the client is a politically exposed person or listed on sanction lists.
- **Unusual (suspicious) transaction** – a transaction or behaviour of a client that gives rise to a suspicion of money laundering or terrorist financing; as defined in Section 6 of the AML Act. Examples include transactions that do not correspond to the client's usual activity or volume, splitting payments into just below-threshold amounts, a client's reluctance to provide identification, etc.
- **FAÚ** – the Financial Analytical Office (*Finanční analytický úřad*), the government authority responsible for receiving reports of suspicious transactions and monitoring compliance with obligations under the AML Act.

Data Processing Principles in the Company: The Company carries out all processing of personal data in accordance with the principles set forth in Article 5 of the GDPR:

- **Lawfulness, fairness and transparency:** We always process personal data **on the basis of one of the legal grounds allowed by law** (especially those in Article 6 of the GDPR), and we act fairly and transparently towards data subjects. We fulfil our information duties towards customers, employees, and other data subjects under Articles 13 and 14 of the GDPR (data subjects are clearly informed of the purposes of processing, their rights, etc., usually via the document *Personal Data Processing Policy* available on our website, or via an individual notice).
- **Purpose limitation:** We collect and process personal data **only for specified, explicit and legitimate purposes**, and we do not further process it in a manner incompatible with those purposes. The specific purposes of processing within the Company are determined by members of the statutory body or by persons explicitly authorised by them. These persons also determine what personal data and for how long it will be processed for a given purpose, and ensure that these details are recorded (e.g. in the *records of processing activities* under Article 30 of the GDPR – see below).
- **Data minimisation:** We process personal data **only to the extent necessary** for the fulfilment of the given purpose. Staff members are allowed to process only those personal data that they genuinely need to perform their job duties. The Company has implemented access restrictions: employees have access only to those databases or folders that are relevant to their role.

- **Accuracy:** We keep personal data **accurate and up-to-date**. If we discover or receive information that certain personal data are inaccurate or outdated, we will ensure they are corrected or erased without undue delay. Every employee who finds an inaccuracy or incompleteness in personal data is obliged to report it to their superior or the designated responsible person (e.g. the relevant manager or the DPO if one is appointed) so that the issue can be resolved.
- **Storage limitation:** We store personal data **in an identifiable form only for as long as necessary** for the purposes for which they are processed. These retention periods are determined both by legal regulations (e.g. statutory retention periods for accounting documents, personnel records, etc.) and by the Company's internal policies (e.g. as set out in the records of processing activities). After the prescribed period expires, personal data are either securely deleted or anonymised.
- **Integrity and confidentiality:** We process personal data in a manner that **ensures appropriate security**, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. To this end, the Company has implemented suitable technical and organisational measures (see the section *Security of personal data* below). All staff members are obliged to maintain confidentiality regarding any personal data they access in the course of their duties.

Duties and Responsibilities of the Company as Controller: The statutory body of the Company (the Managing Director) is responsible for ensuring that personal data processing is in compliance with the GDPR. The Managing Director (or a person expressly authorised by him) in particular:

- **Determines** the specific purposes and means of processing for each personal data processing activity (record or system) within the Company.
- Ensures that each processing has an appropriate **legal basis** under Article 6 of the GDPR (or Article 9 of the GDPR for special categories of data). The typical legal bases in our Company are: performance of a contract with the data subject (e.g. processing customer data to deliver ordered goods), compliance with a legal obligation (e.g. keeping accounting records, mandatory reporting to authorities), the Company's legitimate interests (e.g. CCTV monitoring for security purposes), and consent of the data subject (particularly for marketing purposes involving individuals who are not yet our customers).
- Maintains and updates the **Records of processing activities** under Article 30 of the GDPR. These records provide an overview of each personal data processing operation (purpose, legal basis, categories of data subjects and data, recipients, retention periods, etc.). The records are maintained by

the Managing Director or a designated person and are available for potential inspection by the supervisory authority (ÚOOÚ).

- Implements appropriate **technical and organisational measures to secure personal data** (see below) and regularly evaluates their effectiveness. In this context, the Managing Director conducts risk assessments concerning the rights and freedoms of data subjects and takes these into account when selecting security measures (the principle of **privacy by design and by default** is applied – e.g. new IT systems are chosen with regard to security and data minimisation requirements).
- Ensures that the Company **fulfils its duty to inform data subjects** at the time of data collection (in accordance with Articles 13/14 of the GDPR) and properly handles **requests from data subjects to exercise their rights** (under Articles 15–22 of the GDPR). Details of the procedures for data subject requests are provided later in this directive.
- If a certain planned personal data processing is likely to result in a high risk to the rights and freedoms of natural persons, ensures that a **Data Protection Impact Assessment (DPIA)** is carried out before commencing such processing, in accordance with Article 35 of the GDPR. This could apply, for example, to the deployment of a new large-scale monitoring system or customer profiling activities. If it appears that a high risk would remain even after measures are taken, the Managing Director will **consult the Office for Personal Data Protection (ÚOOÚ)** prior to starting the processing (Article 36 of the GDPR).
- In the event of a **personal data breach**, ensures that the notification obligations are met: specifically, that the breach is reported to the ÚOOÚ within 72 hours, and that affected data subjects are informed without undue delay if the breach is likely to result in a high risk to their rights (see the section *Procedure in case of a personal data breach* below).
- Monitors legal developments and guidance from supervisory authorities (e.g. opinions of the ÚOOÚ, guidelines from the European Data Protection Board) and updates this directive or other internal procedures in response to such developments.

Duties of Employees and Processors: Every staff member of the Company who processes personal data in the course of their work is obliged to:

- Process personal data **only in accordance with the Company's instructions** and within the scope of their job duties. Employees may only use personal data for the purposes for which they were collected and only to the extent necessary to perform their tasks.

- **Maintain confidentiality** regarding personal data and related security measures. This obligation continues even after the termination of their employment or other cooperation with the Company.
- **Protect access credentials** to IT systems and databases from misuse – employees must not disclose their login details (passwords) to anyone else, nor leave them unsecured. They are required to follow the Company's internal guidelines for strong passwords and to change their passwords regularly if required.
- **Report any observed or suspected issues:** If an employee discovers or suspects that any processing of personal data has resulted in a breach of this directive or of legal regulations (e.g. unauthorised access, data leak, loss of a document containing personal data, or any unauthorised or excessive processing), they must **immediately report** it to their supervisor or the designated responsible person (see Annex 1 – List of Designated Persons and their Roles). The same applies if they receive any request or complaint from a data subject concerning their personal data – the employee must promptly forward it to the designated person (typically the manager responsible for handling data subject requests, or the DPO if one has been appointed).
- Participate in **training and education** related to personal data protection and AML (see further below).

External suppliers who act as **processors** of personal data (e.g. an accounting firm, an IT cloud provider) are contractually obligated to process personal data only according to the Company's instructions, to maintain required security standards, and to assist the Company in fulfilling its obligations towards data subjects. A designated person within the Company (e.g. the Managing Director or legal department) keeps a record of all processors and the **data processing agreements** concluded with them. Employees responsible for liaising with contractors must ensure that no personal data are disclosed to any external party without appropriate contractual protection (except where the external entity is itself an independent controller, e.g. a public authority).

Data Protection Officer (DPO): Given the nature of MATISTOTELES s.r.o.'s activities (it is not a public authority and does not engage in large-scale processing of sensitive data or systematic monitoring of individuals), **the appointment of a Data Protection Officer is not mandatory** under Article 37 of the GDPR. As of the date of this directive, the Company has not appointed a DPO. If a DPO is appointed in the future (whether mandatorily or voluntarily), this directive will be updated to include the DPO's identification and contact details and a description of their tasks in accordance with Article 39 of the GDPR. In the meantime, certain tasks associated with overseeing personal data protection are performed directly by the Company's

statutory body (Managing Director) or by an administrative employee designated by him. This person primarily monitors compliance of processing activities with legal regulations and this directive, provides advice to employees on data protection issues, and may communicate with the ÚOOÚ (for instance, in case of an inspection).

Other Designated Persons (Data Protection Organisation): The Company's statutory body may, in writing, delegate specific employees to carry out certain tasks in the area of personal data protection or AML. Typically, the Company appoints: an **IT and Security Manager**, who is responsible for technical measures to secure data (password management, encryption, anti-virus protection, backups, etc.); a **Data Subject Request Manager**, who receives and handles requests from clients or other individuals regarding their personal data; and possibly an **AML Compliance Manager** (see below), who oversees the implementation of obligations under the AML Act. The current list of these designated persons and their specific roles is provided in **Annex 1 to this directive**. All employees must know whom to contact for particular issues (data breach, data subject request, suspicious transaction, etc.). If any of the above Managers are not appointed, their function and duties are carried out by the Managing Director of the Company.

Records and Documentation: The Company maintains the required documentation concerning personal data processing, in particular:

- **Records of Processing Activities** (Article 30 GDPR) – as mentioned above, maintained by the Managing Director and updated regularly; available for inspection by the ÚOOÚ if needed.
- **Incident Log** – every breach of personal data security (e.g. loss of a device containing data, unauthorised access) is recorded in an internal incident log, including a description of the event, measures taken, and whether the ÚOOÚ was notified. This log is maintained by the executive office or a designated security officer.
- **Records and copies of communications with data subjects** – all requests from data subjects and our responses are archived in digital or paper form so that we can demonstrate compliance (kept for at least 3 years after the request is resolved). Any repeated requests from the same data subject may be subject to a fee if permitted by law (typically in the case of manifestly unfounded or excessive requests – in such cases, the Company may charge an administrative fee or refuse the request with justification).
- **Internal directives and methodologies** – in addition to this directive, the Company may have other internal regulations (e.g. a cyber security directive, code of ethics, etc.) which together form a comprehensive compliance framework. The statutory body is responsible for ensuring all such documents are reviewed regularly and kept in line with current legislation.

Procedure for Data Subject Rights: Every natural person whose personal data are processed by the Company (a data subject) has rights under Chapter III of the GDPR – notably the right of access to their data, the right to rectification, erasure, restriction of processing, data portability, and the right to object or to lodge a complaint with the ÚOOÚ. The Company is obligated to enable data subjects to exercise these rights.

- **Receiving requests:** If a data subject submits any request related to their personal data (for example, sends an email asking for information, delivers a letter raising an objection, or makes a request in person to an employee), the employee who receives the request must **immediately forward** it to the designated person (see Annex 1). Typically, such requests are handled by the Managing Director or by a **Data Subject Request Manager** designated for this purpose.
- **Verification of identity:** Before providing information or taking action, the Company will appropriately verify the **identity of the requester** to ensure that data is not disclosed to an unauthorised person. The method of verification depends on the type of request and communication channel – it may involve security questions, requiring a signature or electronic signature, or other security measures as appropriate.
- **Time limits for response:** The Company will handle requests **without undue delay, and at the latest within 1 month** of receiving the request. In exceptional cases (for example, if a request is complex or if multiple requests have been made by the same person), this period may be extended by an additional two months; in such a scenario, the Company will inform the requester of the extension in a timely manner and provide reasons for the delay. If the Company decides **not to act on a request** (e.g. if the data subject requests something to which they are not entitled under the GDPR, or if a request is manifestly unfounded or excessive), we will inform the requester of the reason for the refusal and of their right to lodge a complaint with the ÚOOÚ.
- **Form of response:** Information to the data subject is generally provided in the **same format as the request** was made, unless the data subject requests otherwise. Thus, if a request is received by email, we will reply to the same email address; if a letter is received, we will respond by letter. In justified cases we may choose another appropriate method (for example, a secure data box message).
- **Content of response:** When fulfilling the **right of access**, we will provide, in addition to copies of the personal data, the information required by Article 15 of the GDPR (purposes of processing, categories of personal data, recipients, planned retention period, data subject's rights, data source, whether any automated decision-making including profiling takes place, and whether data

were transferred to a third country). When fulfilling the **right to data portability**, we will provide the data in a structured, commonly used, machine-readable format (such as CSV or XML) either directly to the data subject, or to another controller at the data subject's request, if technically feasible. Upon a **request for erasure**, we will assess whether the conditions are met (Article 17 GDPR) – if they are, we will delete the data and confirm this to the data subject; if they are not (for instance, if we are required to continue processing the data due to a legal obligation or overriding legitimate interest), we will inform the data subject of the reason we cannot comply. For a **request for rectification or restriction**, we will make the necessary correction or mark the data as restricted and inform the data subject that this has been done. If a data subject lodges an **objection** to processing based on legitimate interests, we will evaluate whether we have compelling legitimate grounds that override the interests of the data subject – if not, we will cease the processing; if yes, we will inform the data subject of those compelling reasons. An **objection to processing for marketing purposes** will always be honoured – we will immediately cease using the data for direct marketing.

- **Fees:** The first time information is provided in response to a request, it is **free of charge**. For repeated or manifestly unfounded or excessive requests, the Company may charge a **reasonable fee** reflecting the administrative costs (for example, CZK 50 for each additional copy or excessive request), or we may refuse to act on the request if permitted by Article 12(5) of the GDPR. The decision to charge a fee or to refuse a request is made by the Managing Director (or by the DPO if one is appointed), and the requester will be informed of the reason for such decision in writing.

Security of Personal Data: The Company maintains **appropriate technical and organisational measures** to ensure that personal data being processed are protected against unauthorised or unlawful processing, and against accidental loss, destruction, or damage (Article 32 GDPR). The main measures include:

- **Physical security:** Offices are kept locked, and access to the Company's premises is limited to authorised persons only. Documents containing personal data are stored securely in locked cabinets or files. Sensitive documents (such as contracts or personnel files) are kept in locked cabinets, accessible only to authorised staff.
- **Access control to IT systems:** Each employee is assigned a unique login account for the Company's information systems. These systems are protected by strong passwords that are changed regularly. Employee access rights are configured according to their role ("need-to-know" principle) – e.g. accounting personnel have access to accounting data but no access to HR folders. When

an employee leaves the Company, their accounts are immediately deactivated.

- **Encryption and pseudonymisation:** Sensitive electronic databases (containing, for example, customer passwords or employees' health data) are encrypted. Transfers of personal data outside our internal network are protected by encryption (e.g. SSL/TLS for websites, encrypted email attachments with the password sent separately). Where feasible, we apply pseudonymisation (separating identifying information from other data).
- **Anti-virus and security protection:** All Company computers have up-to-date antivirus software and firewalls installed. Operating systems and other software are regularly updated to incorporate security patches.
- **Data backups:** We regularly back up important databases (customer system, accounting, etc.) to secure storage. Backups are encrypted and stored off-site. We periodically test data restoration from backups to ensure that data can be successfully recovered in case of a failure.
- **CCTV system:** A security camera system is installed on the Company's premises (monitoring the entrance and office areas) for the purpose of protecting property and ensuring personal safety. Cameras record video in designated zones, and recordings are retained for no more than 7 days (depending on storage capacity), after which they are automatically deleted (unless an incident requiring longer retention is identified).
- **Organisational policies:** Employees receive regular training on safe data handling practices (e.g. not sending sensitive data without encryption, not taking documents off-site without proper safeguarding, locking their computer when leaving their desk, not installing unapproved software, being vigilant about phishing emails, etc.). There are rules governing the use of personal devices for work purposes (if such use is allowed, the device must be approved and secured by the IT department).
- **Assessment of service providers:** Before transferring personal data to an external provider (processor), we verify that they provide sufficient guarantees of data security (for example, holding certifications such as ISO 27001, using encryption, having internal data protection policies). Our contracts with processors include obligations regarding data protection and the Company's right to audit their compliance.
- The Company continuously **evaluates risks** and adapts its security measures to address current threats. Every staff member must comply with the established rules – any breach (such as using an unauthorised cloud service for company data, or copying data onto an unsecured USB drive) may lead to disciplinary action.

Procedure in Case of a Personal Data Breach: A “personal data breach” is any security incident that results in accidental or unlawful destruction, loss, alteration,

unauthorised disclosure of, or access to, personal data (Article 4(12) GDPR). If such a security incident occurs, the procedure is as follows:

- **Immediate response and internal reporting:** Every employee who becomes aware of or suspects a security breach (e.g. loss of a laptop containing data, a hacker attack, an email with personal data sent to the wrong recipients, etc.) must **immediately inform their supervisor and the designated incident-response person** (see Annex 1). This designated person (e.g. the IT Security Manager) will promptly investigate the incident, take initial measures to prevent further damage (such as disconnecting a compromised system, changing passwords, convening a crisis team), and document the facts ascertained.
- **Incident analysis:** The designated person, in cooperation with the Managing Director, will as soon as possible evaluate the nature of the incident and **assess the risk** to data subjects. If it is determined that the incident is **unlikely to result in a risk to the rights and freedoms** of the affected individuals (for example, if data was lost but was encrypted and backed up), then **notification to the authorities is not required**. However, if a **risk cannot be excluded** (for example, unencrypted client data has been compromised), a report must be **submitted to the Office (ÚOOÚ) within 72 hours** after discovery of the incident.
- **Notification to the Supervisory Authority:** The responsible person (Managing Director or designated manager) will **notify the ÚOOÚ** of the breach **without undue delay**, via the data box or the Office's online form. If the notification is made more than 72 hours after becoming aware of the breach, it must include the reasons for the delay. The notification shall include: a description of the incident (what happened, categories and approximate number of data subjects and records affected), the likely consequences, measures taken or proposed to address the breach (including mitigation of its adverse effects), and contact details of a person able to provide further information. Prior to submission, the Company may consult the notification with the DPO (if one is appointed). A copy of the submitted notification is kept on file.
- **Informing data subjects:** If it is **likely that the incident will result in a high risk** to the rights and freedoms of the affected individuals (e.g. sensitive data were leaked that could be misused for fraud or significantly impact privacy), the Company will **without undue delay also inform the affected data subjects** about the breach. This notification will be provided individually (e.g. by email or letter) and must clearly describe the nature of the breach, the measures taken, and recommendations on how the affected persons should protect themselves (for example, changing passwords, being alert to suspicious communications, etc.). If direct notification of each individual would

involve disproportionate effort (for example, if a very large number of people are affected), the Company may issue a public announcement (e.g. on its website) with similar effect. Notification to data subjects is not required if the Company subsequently implements measures that **ensure that the high risk is no longer likely to materialise** (for example, by rendering the compromised data unintelligible through additional encryption), or if such notification would require disproportionate effort – in the latter case, a public announcement will be used instead. The decision whether to notify data subjects is made by the Managing Director after consultation with the DPO/designated person.

- **Recording and remedial actions:** All personal data breaches are recorded in an internal **Incident Register** (see above under Records and documentation). The Managing Director, together with the designated persons, analyses the causes of the incident and implements **measures to prevent** similar occurrences in the future (for example, adjusting procedures, providing additional training to employees, investing in security technologies). The incident record also includes a description of these measures taken.

Training and Awareness-Raising: MATISTOTELES s.r.o. ensures that all staff members who handle personal data or engage in activities under the AML regime are **adequately informed of their obligations**. To this end:

- **Induction training:** Every new employee undergoes training on personal data protection (GDPR) rules and, if relevant to their position, on obligations under the AML Act. This includes familiarisation with this directive, with internal procedures, and with the consequences of non-compliance. The employee confirms by signature that they have been instructed and that they understand the directive.
- **Regular training:** All relevant staff receive **training at least once a year** – either through an in-person seminar or e-learning – on up-to-date GDPR and AML rules. The training also covers any changes in law, new internal procedures, a reminder of security principles, and the review of any incidents with lessons learned.
- **Training records:** A record is made of each training session (date, content, trainer, participants). These records are maintained by the HR department or another designated person and are kept for a minimum of 5 years. The designated person ensures that every relevant employee completes training within the required time frame.
- **Knowledge testing:** The Company may use knowledge tests or quizzes to verify that employees have understood their duties. If an employee repeatedly fails to demonstrate sufficient knowledge, they will receive additional individual training.

- **Updating training content:** The training content is regularly updated to reflect changes in legislation and guidance from supervisory authorities (e.g. new guidelines from the ÚOOÚ, FAÚ, etc.). The training includes practical examples and case studies (e.g. how to respond to a data subject's request, how to identify a suspicious transaction).

Oversight and Compliance Monitoring: The responsibility for ensuring compliance with this directive lies with the Company's statutory body (Managing Director). The Managing Director also serves as a point of contact for employees regarding data security, personal data protection, and AML obligations. If any employee is unsure about the correct procedure or interpretation of this directive, they should consult the Managing Director (or the DPO if one is appointed, or another designated person listed in Annex 1). The interpretation provided by the statutory body is binding.

The Managing Director is also responsible for the regular **updating of this directive** to reflect current legal requirements and the Company's organisational structure. At least once a year, the Managing Director (potentially in cooperation with a DPO or legal advisor) will review the directive and, if necessary, issue revisions or propose a new consolidated version for approval.

PART II – Prevention of Money Laundering and Terrorist Financing (AML)

MATISTOTELES s.r.o. becomes an **obliged entity under the AML Act** (Act No. 253/2008 Coll.) in cases where it conducts or intermediates cash transactions worth **€10,000 or more**, or engages in any other activities listed in Section 2 of the AML Act. Although the Company's primary activity is operating an e-commerce platform (most payments being non-cash) and a community platform, the Company is committed to **preventing its services from being used for money laundering or terrorist financing**. This part of the directive establishes the internal policies and procedures to meet AML requirements.

Client Identification and Due Diligence: In situations where the Company enters into a business relationship or carries out a one-off transaction that is subject to AML obligations, it must first perform **client identification** and the relevant **basic or enhanced client due diligence** (CDD) as per Sections 7 and 9 of the AML Act.

- **When to identify:** The obligation to identify a client arises in particular when receiving or making a cash payment **exceeding €10,000** (or equivalent in another currency) in a single transaction or in a series of related transactions. Identification is also required whenever a **suspicious transaction** is detected (see below), even if the amount is below this threshold. Furthermore, identification is performed upon establishing a long-term business relationship (e.g. concluding a framework agreement) if required by law, regardless of transaction value.

- **How identification is done:** An individual client (natural person) must present a valid proof of identity (national ID card or passport; for foreign nationals, a travel document and visa if required). A Company employee compares the person's appearance with the photo on the document and records the necessary details from the document: name and surname, national identification number (or date of birth), permanent address (or other residence address), nationality, type and number of the document, issuing authority, and its validity. These details are entered into an internal **Client Identification Record** (see Annex 2 – template form), and the client confirms their accuracy by signing the form. For a **legal entity**, the employee will identify the representative (natural person) in the same way, and obtain details about the legal entity being represented (business name, company ID number, registered office, names and birth data of the persons acting on its behalf and of its beneficial owner). Sources such as an extract from the Commercial Register or the Register of Beneficial Owners are used; in the case of a foreign company, equivalent documents are requested.
- **Scope of due diligence:** In addition to verifying the client's identity, the responsible employee conducts a **client due diligence** – i.e., obtains information about the **purpose and intended nature** of the transaction or business relationship (for example, by asking what the requested service will be used for, or why the client is making a large cash payment), and if relevant, inquires about the **source of funds** for any unusually high amount. The employee also assesses whether the client is a **Politically Exposed Person (PEP)** – they ask the client and check the client's name against available databases (such as PEP lists or international sanctions lists). If the client is identified as a PEP, **enhanced due diligence** is applied (e.g. approval of the transaction by senior management, obtaining information on the origin of the client's assets, etc.). Similarly, for clients from higher-risk countries (according to FATF/EU lists), additional measures are implemented (such as requesting additional documentation, obtaining management approval to establish the business relationship).
- **Refusal of transaction:** If a client refuses to provide the required information or cooperation for identification, or if due diligence reveals that proceeding with the transaction could breach sanctions or legal requirements, the Company will **not execute the transaction**, and will consider filing a report with the Financial Analytical Office (see below).
- **Record-keeping and retention (AML):** For each identification carried out, the responsible employee completes a **Client Identification Record** (Annex 2). This record, including any copies of ID documents, is retained by the Company for **10 years** from the execution of the transaction or the end of the business relationship, whichever occurs later (Section 16 of the AML Act).

Likewise, all documents and information obtained as part of client due diligence (e.g. correspondence, records on determining the source of funds, results of checks against PEP/sanction lists) are archived for 10 years. These materials are secured similarly to sensitive personal data – paper documents in locked files and electronic records in encrypted storage – accessible only to the Managing Director and persons he authorises. After the ten-year period, the documents are shredded or securely deleted.

The Company maintains an internal **Register of Suspicious Transactions and FAÚ Reports** (Annex 3), in which it logs all assessed suspicious transactions and whether or not they were reported to the Financial Analytical Office. This register assists in internal reviews and checking the effectiveness of our AML procedures; it is treated as highly confidential.

Reporting Suspicious Transactions: If an employee of the Company, during interactions with a client or in processing transactions, detects facts suggesting a **suspicious transaction** (for example, a client clearly attempts to circumvent threshold limits by structuring payments, provides obviously false information, conducts a transaction that lacks economic rationale, or proposes an unusually large cash deal with no clear justification), that employee must **immediately notify** the designated **AML responsible person** (see Annex 1). This responsible person is typically the Managing Director, or an explicitly appointed employee (e.g. a compliance officer). The responsible person evaluates the situation and may request additional information from the client or the employee. If the **suspicion is confirmed or cannot be ruled out**, the responsible person will **without undue delay submit a suspicious transaction report** to the **Financial Analytical Office (FAÚ)**, pursuant to Section 18 of the AML Act. The report is submitted electronically via a secure channel (usually through the FAÚ's data box or designated reporting system). The report includes all relevant details of the transaction and the client, including identification information, a description of the transaction, and the reasons why it is considered suspicious.

- **Suspending the transaction:** If feasible and appropriate, alongside filing the report, the Company will **delay the execution of the suspicious transaction** until instructions are received from the FAÚ, but for no longer than 48 hours from the moment the report was delivered (Section 20 of the AML Act). The FAÚ may within that period order a further suspension (up to 5 working days) or the seizure of assets. If the specified time passes without the FAÚ taking further action or informing us that it has taken over the case (e.g. handed it to law enforcement), the transaction may be carried out. Decisions on such steps are made by the Managing Director in consultation with legal counsel.
- **Confidentiality and non-disclosure (tipping-off ban):** All employees acknowledge that they are legally obliged to maintain **confidentiality about**

having submitted a report to the FAÚ or about any ongoing investigation of a suspicious transaction (Section 38 of the AML Act). They **must not inform the client** or any other third party that their transaction has been flagged as suspicious or reported to the FAÚ. Breach of this obligation (*“tipping-off”*) is a serious offence and may result in penalties for the individual as well.

Internally, information about suspicious transactions is only shared with employees who need to know in order to investigate and report the matter.

- **Internal control and cooperation with authorities:** The statutory body is responsible for implementing and maintaining an **internal AML control system**. At least once a year, the Managing Director conducts an evaluation of whether the implemented processes (client identification, record-keeping, reporting) are functioning effectively and whether they are appropriate for the current risk environment. External advisors may be involved in this evaluation. The Company closely **cooperates with the FAÚ and other authorities**, responding promptly to requests for explanations, providing required documents, and allowing inspections (by the FAÚ or other supervisory bodies). All employees are obliged to submit to any such inspection and provide full cooperation (e.g. explaining our procedures or presenting records).
- **Risk profile and measures:** The Company has prepared an **internal risk assessment** in the area of money laundering and terrorist financing, which identifies types of transactions and clients by risk level. In general, the risk is assessed as relatively low (the main line of business is retail trade with low unit values, mostly cashless); however, there are potentially risky scenarios – e.g. sudden large cash purchases of high-value goods, unusual payment requests, or deliveries to high-risk countries. Based on this assessment, the Company has adopted appropriate measures (as described above: identification for transactions over €10,000, transaction monitoring, etc.). The risk assessment will be reviewed at least annually and updated in the event of changes to the Company’s activities (for example, if the Company starts offering new financial services or enters markets with higher risk). The internal risk assessment report is available to the FAÚ upon request.
- **Training in AML:** The training programme described above (*Training and Awareness-Raising*) **also covers AML** – employees are trained to **identify and report suspicious transactions**, and in customer identification procedures. Employees are acquainted with current methods of “money laundering” observed in practice and with guidance from the FAÚ, the Czech National Bank, or relevant professional bodies (e.g. for attorneys, guidelines from the Czech Bar Association) as applicable to our operations. At least once a year, a specialised AML training under Section 23 of the AML Act is conducted for relevant staff. This includes a verifiable knowledge test. A

separate record of completed AML training is kept (as part of Annex 3 – Training Schedule and Records).

Final Provisions: This directive enters into effect on **1 May 2026** and supersedes any previous internal regulations in this area. Employees were acquainted with the content of the directive on ... (each confirmed by signing an attendance sheet). The annexes listed below form an integral part of this directive. This directive was approved and issued by the Company's Managing Director; it is kept in paper form at the Company's registered office and in electronic form on the intranet. All personnel are required to comply with this directive.

This directive will be reviewed and updated regularly to reflect changes in legislation or in the Company's activities. Updates are issued by the statutory body in the form of numbered amendments or revised full versions of the directive. The Managing Director (in cooperation with any DPO and legal advisors) is responsible for ensuring updates.

Annexes:

- **List of Designated Persons and their Roles** (e.g. Data Protection Manager, IT Security Manager, AML contact person, including names and positions).
- **Client Identification Record Form** (template form pursuant to Section 7 of the AML Act, containing fields for client ID/passport details, signatures of client and employee, etc.).
- **Processing and Training Records** – (a) a consolidated table of records of personal data processing activities under Article 30 GDPR; (b) a schedule and logs of GDPR/AML training (dates, participants); (c) a log of any incidents and notifications to ÚOOÚ/FAÚ.
- **Templates of Consents and Notices to Data Subjects** – sample text of consent for personal data processing (e.g. for marketing), a sample information notice for clients under Article 13 GDPR, a sample response to a data subject request, a sample internal record of request handling.
- **Internal Procedure for Handling a Suspicious Transaction** – a schematic diagram or brief description for employees on how to proceed when an unusual transaction is detected (e.g. notify the responsible person, do not complete the transaction, fill out an internal report, etc.).

In Prague, 1 May 2026

Mateusz Leon Jagoda

Managing Director, MATISTOTELES s.r.o.