GROUP POLICY

Group Anti-Money Laundering and Counter Terrorist Financing Policy

Draslovka a.s.

Draslovka

Document Information

Name:	Group Anti-Money Laundering and Counter Terrorist Financing Policy
Type:	Group Policy
Group Policy No.:	GP_006_v1
Area:	Business Governance
Key concepts:	Anti-Money Laundering, Terrorist Financing, Cash Payments, Know Your Customer, Beneficial Owner
Owner:	Group Head of Compliance
Applicable to:	All Employees and entities within Draslovka Group
Effective from:	1 August 2023
Frequency of review:	Annual

Document history

Version Number	Date of Issue	Reason for Change	Owner
GP_006_v1	5 May 2023	New document	Group Head of Compliance

Confidentiality Statement

This Policy shall not be disclosed or distributed outside Draslovka Group, unless for audit or other purposes required by law or regulation or upon written approval of the Group CEO or Group Head of Compliance.

Table of Contents

1 Purpose and Scope

1.1 Purpose

Commitment to ethical business behavior forms the basis of the Draslovka Code of Conduct. The purpose of this Policy is to affirm the position of Draslovka Group to prevent money laundering and terrorist financing through its operations, define roles and responsibilities of Group Companies and Employees and ensure a consistent approach to business practices throughout worldwide operations. This Policy also provides guidance for Employees how to recognize and deal with money laundering and terrorist financing risks.

Draslovka Group takes a zero-tolerance approach to money laundering and terrorist financing. All Employees must at all times act in accordance with this Policy and Applicable Anti-Money Laundering Laws and seek to avoid even the appearance of money laundering or terrorist financing, as participation in money laundering and terrorist financing or business relationship with entities involved in such illicit activities can expose Draslovka Group and/or Employees to civil and criminal penalties and reputational damage. An Employee that violates the requirements of this Policy will be subject to disciplinary actions which may lead up to termination. Also, under Applicable Anti-Money Laundering Laws, a requirement might exist to report suspected money laundering or terrorist financing to law enforcement authorities.

As appropriate and relevant, zero tolerance approach to money laundering and terrorist financing shall be communicated to all suppliers, contractors, business partners and other Third Parties.

1.2 Scope

This Policy is mandatory and applies to all Employees and all entities within Draslovka Group insofar as it does not contradict local legislation. The implementation of this Policy in Draslovka Group shall be proportionate and take into account size and internal organization of a Group Company and the nature, scale and complexity of its activities. It must also reflect country-specific risks and requirements of Applicable Anti-Money Laundering Laws (including when a Group Company becomes “obliged person” under EU law).

In line with Draslovka Group’s commitment to responsible business conduct and in order to manage money laundering and terrorist financing risk, this Policy applies even if the respective Group Company is not subject to any Applicable Anti-Money Laundering Laws.

1.3 Related Documents

This Policy represents an integral part of Draslovka Group compliance framework mainly laid down by the following documents:

(i) Draslovka Code of Conduct;

(ii) Group Anti-Bribery and Corruption Policy; and

(iii) Group Sanctions Policy.

2 Roles and Responsibilities

This clause defines roles and responsibilities related to matters covered by this Policy.

Group level

2.1 Board of Directors of Draslovka a.s.:

a) approves this Policy and ensures its regular review, at least annually, and

b) oversees implementation of this Policy.

2.2 Group CEO:

a) promotes transparency of Transactions and Third Parties and zero tolerance to money laundering and terrorist financing within Draslovka Group, and

b) approves exceptions for cash operations, together with Group CFO (clause 4.2.2).

2.3 Group CFO:

a) approves exceptions for cash operations, together with Group CEO (clause 4.2.2).

2.4 Group Head of Compliance:

a) monitors, oversees and controls the implementation of this Policy in Group Companies and regularly considers its suitability, adequacy, and effectiveness,

b) provides guidance to Employees in relation to any concern, suspicion, or uncertainty whether a particular act constitutes or might constitute money laundering or terrorist financing,

c) communicates, either directly or through Group Company Compliance Officer, with law enforcement authorities regarding suspicious Transactions and other related matters, and

d) approves Group Guidelines implementing this Policy.

Group Company level

2.5 Group Company Approving Body:

a) approves local implementation of this Policy and ensures regular review of its implementation, at least annually, and

b) has overall responsibility for ensuring that local implementation of this Policy complies with Group Company's legal obligations.

2.6 Business Unit CEO:

a) promotes transparency of Transactions and Third Parties and zero tolerance to money laundering and terrorist financing within a Group Company, and

b) requests exceptions for cash operations exceeding the limit (clause 4.2.2).

2.7 Group Company Compliance Officer:

a) is responsible for local implementation of this Policy in a Group Company and for ensuring that local implementation complies with the Applicable Anti-Money Laundering Laws,

b) reports implementation status of this Policy and substantial changes to the Applicable Anti-Money Laundering Laws to Group Compliance Department,

c) provides support to Group Head of Compliance in communication with local law enforcement authorities, if relevant (clause 4.1.3), and

d) provides guidance to Employees in relation to any concern, suspicion or uncertainty whether a particular act constitutes or might constitute money laundering or terrorist financing.

In case any of the above function does not exist in a Group Company, Business Unit CEO shall be responsible for ensuring that the requirements set out by this Policy are properly implemented in a Group Company.

3 Anti-Money Laundering and Anti-Terrorist Financing

3.1 What is Money laundering and Terrorist Financing

Money Laundering is a process through which illegally obtained funds are transformed to appear legitimate. The process usually consists of a long chain of Transactions, with the goal of hiding the link to the illicit origin of money. Illegal arms or drugs, prostitution, but also bribery, computer frauds, tax avoidance, embezzlements and many other schemes generate large sums of money and such activities are heavily fined in vast majority of jurisdictions. Effectively fighting against money laundering is of critical importance in preventing and uncovering these crimes.

Terrorist financing is similar in the sense that the aim is to hide the link between the source of money and the final destination. In this case, however, the source may be legal, but it is provided, collected, or further transferred with the intention to finance terrorism or similar criminal acts.

Both in case of Money Laundering and Terrorist Financing, the funds may change forms many times. Bank transfers, cash operations, buying and selling things of value, or financing companies which further generate profit are among the forms which Money Laundering or Terrorist Financing can take.

3.2 Prohibition of Money Laundering and Terrorist Financing

Employees must not engage (organize, facilitate, condone, or otherwise) in Money Laundering or Terrorist Financing and in any Transaction or other activity that might lead to, or suggest, a breach of this Policy or which is prohibited under Applicable Anti-Money Laundering Laws.

Money Laundering and Terrorist Financing are deliberate actions of the organizers. Reasonable effort must be made to protect Draslovka Group's operations from being misused for such unlawful conduct. Business relationships with Third Parties suspected of taking part in Money Laundering or Terrorist Financing, as well as accepting money of suspicious origin, are strictly prohibited.

3.3 Compliance with this Policy and Applicable Laws

Employees must at all times comply with all provisions of this Policy, as well as with all Applicable Anti-Money Laundering Laws. Applicable Anti-Money Laundering Laws might, among others, impose restrictions on cash operations and set more detailed rules for identification of Third Parties and their Beneficial Owners, risk assessment and communications with law enforcing authorities.

Each Employee is responsible for knowing and understanding this Policy, the Draslovka Code of Conduct and other relevant policies and procedures. Group Company might require specified Employees to complete anti-money laundering training and/or certification.

4 Key Principles Against Money Laundering and Terrorist Financing

4.1 Transparency of Business Relationships

4.1.1 Reputable and Transparent Third Parties

Group Company shall only deal with reputable and transparent Third Parties that are operating within the law and are committed to ethical business practices. Group Companies shall always provide correct and full information about themselves in business relationships.

Transactions are performed based on written contractual documents that include identification data of the Third Party and allow such information to be stored and easily

accessible. Exceptions from this rule must be carefully considered, including an alternative way of keeping record of the Third Parties and their identification data.

When implementing this Policy, Group Company shall determine the list of minimal information to be required from the Third Party, considering the requirements of local law and taking into account the instances when the Group Sanctions Policy requires an analysis of the Transaction and Third Party. As a guidance, the Group Company shall record at least:

- For **individuals**: their first and last name, date of birth, current address, nationality, and if applicable, tax identification number.
- For **companies**: their name and legal form, registered seat, identification number and/or tax identification number, other names and addresses they might be associated with, and the information pertaining to the members of the board and/or to the person dealing on behalf of the company.
- For **trusts**: the name and identification of the trustee to the extent applicable for individuals.

Group Company shall refrain from dealing with Third Parties where suspicion exists as to the source of their funds and all reasonable effort shall made in the pursuit of transparency, including examining the Third Party's background, qualifications and reputation. Business relationship or any Transaction with a Third Party contradicting this Policy shall be terminated.

4.1.2 Risk Assessment and Red Flags

Group Company shall never knowingly accept funds acquired through illicit means. Actions of Third parties, including even long-term business partners and other well-known Third Parties, must be reasonably monitored. Due to numerous reasons, such as changes to Third Party's ownership structure, their scope of business or location, Third Parties with active contracts should be re-evaluated at least **annually**. The approach to post contractual diligence should be risk based, considering the information gathered about the Third Party in the past, as well as changes of external factors.

Money Laundering and Terrorist Financing might be more probable using goods that can be easily resold, but this is not an absolute rule. Sometimes whole companies with a seemingly legitimate business are used for Money Laundering and Terrorist Financing. Persons holding influential public positions (politically exposed persons) are usually assumed to be at greater risk of corruption, bribery, or Money Laundering.

Perpetrators of Money Laundering or Terrorist Financing are in constant search for innovative ways that would allow them to break the link. With that in mind, these are some of the common **money-laundering red flags**:

- Anonymous payments: Third Party pays or requests paying using cash, cashier checks, money orders or similar instruments allowing anonymity (as opposed to checks or bank transfers), where it is not common practice, especially if repeatedly in a short period of time (see prohibition of cash payments in clause 4.2).
- Using different entity: Money is requested to be given to or received from a different entity than the products or services were received from or provided to.
- Identification issues or Inconsistency: Third Party and/or the person dealing on their behalf takes steps in order not to be identified or there is a suspicion as to the authenticity of the identity or the documents provided, or the Third Party provides

inconsistent information (e.g. different taxpayer numbers, a person acting on behalf of multiple legal entities, a person obviously avoiding personal contact).

- Uncertainty: Uncertainty exists as to the actual location or nature of business of the Third Party.
- Unrelated Transaction: The Transaction is unrelated to the business of the Third Party, or the size/volume/extent of the Transaction is unproportionally big compared to the business operation of the Third Party, including sudden unexplained changes.
- Non-transparent Transaction: Third Party is enquiring or makes request for the Transaction not being recorded in the books.
- Non-transparent Payment: Third Party requires payments made from one account (e.g. by mistake or as a deposit) to be returned to a different account, or the payment structure is otherwise unnecessarily complex or is using an account which is clearly personal for company purposes.
- High Risk Jurisdiction: Third Party operates in or is shipping goods through a region where anti-money laundering or counter-terrorist financing laws and regulations are not adequately enforced or which has a high level of corruption and other criminal activities, or which is known for supporting terrorist organizations or where such organizations operate.
- Off-market Pricing: Third Party is expressing willingness to provide or accept obviously under- or overpriced goods or services.
- Hidden Beneficial Owners: Third Party is using ownership structures to hide real Beneficial Owners.
- Sanctions: refer to the Group Sanctions Policy (risks or prohibitions may be associated directly with the Third Party, territories, and certain products and services).

4.1.3 Suspicious Transactions

In some instances, a red flag might be easily explained as a misunderstanding. In other instances, a red flag is a clear stop sign, meaning that it is without a doubt that Group Company should not enter in business relationship with certain entity. In between those two possibilities, the **red flags require further assessment**, investigation, decision, and reaction, to dispel suspicion of attempts of money laundering, terrorist financing, or other unlawful or unethical behavior.

Employees should seek guidance from their Manager or Group Company Compliance Officer if they have any concerns regarding Third Parties. Any red flag or other suspicious behavior of a Third Party must be reported to Manager and to the Group Company Compliance Officer, who will assess the case without undue delay, while seeking advice from other departments or functions such as finance or legal on a needed basis, and informing the Group Head of Compliance in matters requiring such attention, especially if having a potential impact on the Group level.

While asking the respective Third Party for explanation is generally considered as a reasonable step to resolve the unclarities, Employees must be aware that confidentiality might be required by Applicable Anti-money Laundering Laws under specific circumstances.

In this respect, Group Company Compliance Officer, or Group Head of Compliance, if involved:

(i) coordinates further course of action, including reporting the suspicious Transaction to law enforcing authorities, if appropriate, and

(ii) in consultation with other competent functions finally approves whether the Transaction can be completed or continued with.

4.1.4 Verification of Third Parties

In the following instances, the Third Party's identification data should be verified (i.e. compared with a reliable source, such as an ID, public register, or related documents):

(i) when required by local law,

(ii) when it is necessary to resolve a red flag, and

(iii) under conditions identified as risky by Group Company while applying this Policy (e.g. exceeding certain threshold, with certain regions).

4.1.5 Beneficial Owners

Group Companies shall respect laws and regulations requiring them to report their Beneficial Owners. If required by law, Group Company shall collect and/or verify the details about Beneficial Owners from Third Parties.

4.2 Cash operations

4.2.1 Prohibition of Cash Payments

In Draslovka Group, the generally preferred forms of payment are those that do not allow anonymous transfer of money. To minimize the risk of money laundering, Draslovka Group strictly **prohibits cash payments** to be accepted and/or provided, subject to the following exceptions:

(i) cash payments up to **100 USD** (or its equivalent in other currencies) are allowed, though non-cash payments are still highly preferred; or

(ii) if permitted under clause 4.2.2.

4.2.2 Cash Payments Approval Form

If the Group Company needs to accept and/or provide cash payments, the Business Unit CEO is entitled to request exception to cash payments prohibition up to (i) 10,000 EUR in the European Union, (ii) 10,000 USD in the USA, and (iii) equivalent of 10,000 USD in other currencies in other countries, unless the Applicable Anti-Money Laundering Laws determine lower limits for cash transactions.[1] Approval may be granted for cash payments only up to limits allowed by Applicable Anti-Money Laundering Laws.

The request for cash payments exception must be submitted by using the Cash Payments Approval Form attached below. The cash payments exception is subject to mutual approval of the Group CEO and Group CFO. Both Group CEO and CFO's approval can be revoked at any time by email notification. If any of the approvals is revoked, the cash payments are prohibited with immediate effect.

GP_006_v1_Cash Payments Approval Fc

[1] As an example, lower limits for cash transaction are currently applicable in Belgium (3,000 EUR), Slovenia (5,000 EUR), or Australia (10,000 AUD). As another example, in Canada, cash payments exceeding 10,000 CAD need to be reported.

Group Companies must be also aware of reporting requirements that may be imposed by Applicable Anti-Money Laundering Law on cash transactions exceeding defined limits. Reporting usually goes hand in hand with the requirement to verify the identity of the Third Party.

4.2.3 Cross-border transports of cash

Group Company and each Employee shall be aware of, and respect, local requirements related to cross-border transport of cash or other things of value, including limits and reporting requirements.

5 Books and Records

Group Company must maintain a system of internal controls to facilitate compliance with this Policy and keep its books and records in a manner providing reasonable details that accurately and fairly reflect Transactions and dispositions or transfer of assets. Group Company must ensure that, among others:

- all Transactions must be executed in accordance with management's general or specific authorization.
- all payments and other entries must be prepared and maintained by a Group Company with strict accuracy, completeness, and reasonable detail and properly recorded in a Group Company's books and records.
- false, misleading or incomplete entries in a Group Company's books, records and other business documents are prohibited. No Transaction should ever be entered into that requires or contemplates the making of false or fictitious records, in whole or in part.
- no accounts must be kept "off book" to facilitate or conceal improper payments.
- circumventing or evading Group Company's internal accounting controls, or any attempt to do so, is prohibited.
- all payments on behalf of a Group Company must be approved and supported with appropriate documentation.
- no payments shall be made with the intention or understanding that the payment or its part is to be used for a purpose other than described by the supporting documents.

The requirements set out in this clause shall apply to all Transactions regardless of financial value or materiality.

6 Use of Third Parties

Transactions that a Group Company, or its Employees, should either deny or treat as suspicious under this Policy, cannot be made, promised, or accepted indirectly through a Third Party.

7 Speaking Up and Non-Retaliation

7.1 Seeking Guidance and Speaking Up

The process of dealing with a suspicious Transaction is described in clause 4.1.3. Besides that, if Employee has any query or doubt as to potential Money Laundering or Terrorist Financing risks, or any question related to anti-money laundering or counter-terrorist financing processes, Employee should seek further guidance. Similarly, every Employee who suspects that violations of law or this Policy may be occurring or are about to occur or becomes aware of suspicious, risky, or evidently unlawful conduct of any person is required to report it.

Employee's immediate Manager or supervisor is usually the first and best resource, since this person is familiar with individual roles and duties. If the Manager or supervisor is not available, or if Employee is not comfortable discussing the matter with a direct supervisor, the following resources are also available:

- Management of a business unit, department or workplace of Employee
- Compliance, Legal, HR or Finance department
- Compliance confidential mailbox ethics@draslovka.com
- Draslovka Group Ethics Hotline

7.2 Non-Retaliation

No Employee will suffer negative consequences for refusing to engage in or permit Money Laundering, Terrorist Financing or other activities prohibited by this Policy, or for raising honest concerns in a good faith, even if it may result in Draslovka Group losing business or otherwise suffering a disadvantage.

It is prohibited to threaten or retaliate against Employee who has refused to take part in Money Laundering or Terrorist Financing or who has raised concerns under this Policy. Such retaliations might include dismissal, disciplinary action, threats, or other unfavourable treatment connected with raising a concern. If Employee believes that he/she suffered threatening or retaliation, Employee should report it to Group Head of Compliance or use any of reporting channels listed in clause 7.1, including Draslovka Group Ethics Hotline.

8 Compliance Control

8.1 Group Company Internal Control

Group Company shall conduct periodic controls or audits of its relevant units to help ensure compliance with this Policy and Applicable Anti-Money Laundering Laws.

8.2 Group Compliance Control

Group Compliance Department may conduct control/audit focused, without limitations, on:

a) compliance with this Policy,

b) awareness and training management, and

c) effectiveness of reporting system.

Employees shall fully cooperate during such controls or audits and promptly provide all requested information, documents and records. Unless required otherwise, result of each control or audit shall be recorded in a protocol signed by responsible Manager. Material findings shall be escalated to Business Unit CEO or Group CEO, as appropriate.

9 Local Implementation

9.1 Local Implementation of the Policy

Group Company is required to implement this Policy into local internal documents by approval of its Approving Body. Group Company is obliged to follow the full scope application of this Policy unless exception was approved under clause 9.2.

Group Company may apply additional or stricter rules at local level, taking into account country and industry specific risks and Applicable Anti-Money Laundering Laws.

Group Company Compliance Officer (or other responsible function, as applicable) shall continuously monitor changes in laws and regulations, together with the possible change in the scope of Group Company's operations, and reports material changes to the Group Head of Compliance.

9.2 Exceptions

Group Company Compliance Officer (or other responsible function, as applicable) has the right to ask Group Head of Compliance for exceptions from this Policy only if this exception is necessary to meet the local regulatory requirements. All exceptions approved under this Policy shall be documented by Group Compliance Department and must be available upon request. Form of Exceptions Evidence is attached below.

GP_Exceptions Evidence.xlsx

10 Final Provisions

10.1 Assumption

This Policy applies insofar as it does not contradict local legislation. If implementation of some rules under this Policy is not permitted under local legislation, Group Company shall proceed according to clause 9.2.

10.2 Implementing Group Guidelines

Group Guidelines, which describe in more detail selected matters covered by this Policy, may be developed only if there is an explicit authorization (reference) stated in this Policy and approved by Group Head of Compliance. Group Guidelines do not build part of this Policy, however they shall be consistent with it.

10.3 Definitions

The meaning of capitalized terms used in this Policy is set out in Annex 1.

10.4 Owner of the Policy

Owner of this Policy is Group Head of Compliance.

10.5 Implementation

This Policy was issued on 5 May 2023 and shall be effective from 1 August 2023 (i.e. this is the target date from which the Policy shall be locally implemented and followed in Group Companies).

10.6 Amendments

This Policy does not form part of Employee's contract of employment and may be amended at any time.

Annex 1

Definitions

In this Policy:

"**Applicable Anti-Money Laundering Laws**" means any applicable law or regulation addressing Money Laundering, Terrorist Financing, cash operations and/or Beneficial Owners, applicable to Employee, Group Company and/or the Group, as well as any applicable international convention.

"**Approving Body**" means a body entitled to and responsible for approval and implementation of this Policy based on Group Company's corporate processes, including but not limited to Board of Directors.

"**Beneficial Owner**" means a person who, directly or indirectly, exercises substantial control over a company, or owns or controls at least a certain percentage of a company. Exact definition, such as the criteria to determine substantial control, should be applied in accordance with applicable local laws and regulations.

"**Draslovka a.s.**" means Draslovka a.s., with its registered office at Evropská 2758/11, Dejvice, 160 00 Prague 6, Czech Republic, identification number 11786728 registered in Commercial Registry maintained by Municipal court of Prague, under file B section 26599.

"**Draslovka Group**" or "**Group**" means all Group Companies; when this term is used in connection with specific position/function it refers to managers/officers/functions with specific "Group-wide" responsibility, reporting (directly or indirectly) to Group CEO.

"**Employee(s)**" means each person working at any level of the Group or a Group Company, including, without limitations, all full-time and part-time employees, family members, members of a Group Company's board of directors or supervisory board, officers, directors, senior managers, consultants, contractors or any other third parties acting on behalf of the Group or a Group Company.

"**Group Company**" means Draslovka a.s. and any entity controlled by Draslovka a.s. by means of direct or indirect majority participation or a control agreement respectively.

"**Group Compliance Department**" means organization unit managed by Group Head of Compliance; in case there is no other staff in Group Compliance Department than Group Head of Compliance, Group Compliance Department shall refer to Group Head of Compliance.

"**Manager**" means a person that is entitled to define and impose on subordinate Employee(s) working tasks and binding instructions and organize, manage, and supervise their work.

"**Money Laundering**" has the meaning ascribed to in in clause 3.1.

"**Owner**" means function/department responsible for administration of this Policy or its amendment (draft, coordination, approval process, waivers and exceptions).

"**Policy**" means this Group Anti-Money Laundering and Counter Terrorist Financing Policy.

"**Sanction**" means a ban of trade, embargo or similar restrictive measure imposed by, for example, the European Union or the United Nations against a certain country, entity or individual, as applicable.

"**Terrorist Financing**" has the meaning ascribed to in in clause 3.1.

"**Third Party**" means any individual or entity, with which Employee comes into contact during the course of work for the Group, including but not limited to actual and potential customers, contractors, suppliers, distributors, intermediaries, business partners, agents, advisers, public officials, and their advisors.

"**Transaction**" means any exchange of goods, services, and/or money, including but not limited to products being purchased or sold, services being rendered or ordered and money being lent from or to a Third Party.