

VOLKSWAGEN

AKTIENGESELLSCHAFT

Group policy 27: Prevention of money laundering

Version: 2.0

Area of application: Volkswagen Group

Valid from: 28/04/2020

Review: 28/04/2021

Official Document Volkswagen Autoeuropa: SQ-ADF-F-0014; Emission date 16 July 2021

DISPOSE of Copies	7 anos
RETAIN Record Copy	06/ 2027
Schedule Number	VW-CSD- 2.1



Group Policy department: Group Compliance

Group Policy division manager: Group Compliance – K-IC
(Dr. K. Michels)

☐ +49 5361 9 28807

Issued by: Group Policy Management – K-IG/R
(J. Wrba)

☐ +49 5361 194527

Contents

- 1 Purpose**
- 2 Scope**
- 3. Central Money Laundering Prevention Office**
- 4. Money laundering prevention in Group companies**
 - 4.1. The responsibilities of management**
 - 4.2. Group companies subject to national anti-money laundering legislation**
- 5. Ban on cash transactions**
- 6 Indications ("Red Flags")**
- 7 Obligations in the event of suspected money laundering or terrorist financing**
- 8 Data Protection**
- 9 Protection of the employees**
- 10 Documentation and archiving**
- 11 Deveres Preventivos ao Abrigo da LBC (Sumário)**

1 Purpose

The purpose of this Policy is to prevent funds of a criminal origin or assets that have been illegally acquired from being brought into the economic cycle via Volkswagen Group companies (money laundering) and via Volkswagen Autoeuropa for the purpose of concealing their true origin.

Given the risk assessment, it is not plausible that there are situations of money laundering and terrorist financing at Volkswagen Autoeuropa. This assessment is based on the nature of Volkswagen Autoeuropa's activities and because cash payments is not allowed. In addition, bank transactions are carried out by banks and established controls, such as the principle of the four eyes, mitigate any risk.

The Policy also serves to prevent terrorist financing by adequately protecting the cash flows which terrorists may be able to access. Terrorist financing is defined as any situation in which cash or any other funds are provided or collected for terrorist acts or for supporting terrorist organizations¹.

Many countries around the world combat money laundering and terrorist financing and impose prison sentences and fines on companies as well as their employees. In addition to the money laundering legislation of other jurisdictions, the Act on Tracing Profits from Serious Criminal Offences (Money Laundering Act – European, German and Portuguese) imposes on German companies a duty to take the necessary precautions to prevent money laundering and terrorist financing.

All references to the prevention of money laundering in this document always also include the prevention of terrorist financing.

This Group policy defines binding Group-wide and Volkswagen Autoeuropa minimum standards, the basis for processes and main duties within the job description of the anti-money laundering contact person (AML contact person) for the effective prevention and combating of money laundering. In addition to implementing the legislative requirements, it also defines further requirements for the Group-wide Code of Conduct for the purpose of effective and sustainable prevention of money laundering.

The relevant national law takes precedence over or applies alongside this Policy where it contains different, additional or further-reaching requirements or provides for stricter measures.

In Portugal, law number 83/2017 of 18 August (amended by DL number 144/2019 of 23 September and Law number 58/2020 of 31 August). This law establishes measures to combat money laundering and terrorism financing and partially transposes Directives 2015/849/EU European Parliament and the Council of 20 May 2015 and 2016/2258/EU council of 5 December 2016 Money Laundering Act (LBC)

2 Scope

This Group Policy applies to all companies within the Volkswagen Group and to Volkswagen Autoeuropa. The binding standards must be implemented in individual regulations of the respective companies.

If any pre-existing rules adopted by a Group company contradict this Group Policy, these rules must be adjusted without delay to bring them into line with the following standards.

3. Central Money Laundering Prevention Office

A central money laundering prevention office has been established within Group Compliance. This office is known as the Centre of Competence for Anti-Money Laundering (“CoC AML”). CoC AML is responsible for ensuring uniform standards to prevent money laundering within the scope of this Group Policy. Reporting and regular communications within Volkswagen Group companies follows the line: CoC AML <-> Divisional Compliance Officer <-> Chief Compliance Officer <-> AML contact person.

4. Money laundering prevention in Group companies

4.1. The responsibilities of management

The management of each Group company is responsible for observing the statutory and internal standards. To this end, it must ensure that within its own area of responsibility the applicable national money laundering legislation, the internal rules, the regulatory requirements and this Policy are duly complied with. Management is responsible for defining the processes required for this, issuing the corresponding work instructions and ensuring that they are observed, enforced and regularly monitored. This also includes documenting in writing the requirements, instructions and measures that have been taken and archiving this documentation. Management may delegate the performance of these duties to the contact persons referred to in Sections 4.2 and 4.3.

4.2. Group companies subject to national anti-money laundering legislation

Group companies located in jurisdictions with national anti-money laundering legislation must nominate an anti-money laundering contact person (AML contact person) immediately after this policy takes effect. In the course of selection and nomination, it must be ensured that there are no conflicts of interest or self-controls. In particular, employees who perform a purchasing or sales function are not permitted to exercise the function as AML contact person.

The AML contact person function must be assigned to the Compliance Officer at all companies in which at least 50% of the responsible Compliance Officer’s duties entail compliance tasks (“full-time Compliance Officer”). Any deviations from this

requirement necessitate the prior unanimous consent of CoC AML and the Chief Compliance Officer responsible for the brand.

Group companies that do not have a full-time Compliance Officer must immediately notify the CoC AML and the next higher compliance function (Chief Compliance Officer and Divisional Compliance Officer) in written form of any planned appointment of an AML contact person. A nomination may only be made after prior unanimous consent by the CoC AML and the Chief Compliance Officer responsible for the brand

Any change of AML contact person must be reported in written form to the CoC AML and to the next higher compliance functions (Chief Compliance Officer and Divisional Compliance Officer) immediately. The CoC AML and the Chief Compliance Officer responsible for the brand must agree unanimously to the changes.

The AML contact person may exercise this function for multiple Group companies regardless of whether he or she is simultaneously the Compliance Officer as far as this is appropriate and legally permissible. This requires the unanimous approval of the next higher compliance functions (Chief Compliance Officer and Divisional Compliance Officer) as well as CoC AML.

This function must be included in the job description of the AML contact person. The main duties particularly include:

- a) Acting as contact person for CoC AML and the next higher compliance functions to execute any individual and general reporting requests,
- b) Identifying and ensuring compliance with local, European and national statutory requirements governing the prevention of money laundering,
- c) Establishing clear reporting processes for suspicious transactions including transaction stops in the event of suspected money laundering in the light of the local, European and national statutory requirements,
- d) Supporting management in ensuring compliance with national law and this Policy,
- e) Monitoring the national legal situation with respect to money laundering prevention on a continuous basis, however, no less than once a year, as well as ensuring the implementation of the local European and national statutory AML requirements,
- f) Ensuring compliance with the reporting duties under money laundering legislation to local public authorities Central Department of Investigation and Criminal Action (DCIAP) - (reports of suspected money laundering) in consultation with other departments where required by law,
- g) Arranging for all relevant employees to receive the necessary training,
- h) Designing and implementing appropriate and necessary information and communication activities as required under local law and internal guidelines,

- i) Reporting regularly to management on the current status of anti-money laundering measures,
- j) Reporting regularly to management on matters and incidents pertaining to money laundering.

In jurisdictions in which national anti-money laundering legislation is enacted for the first time after this Policy takes effect, the local Group companies must immediately appoint an AML contact person and inform CoC AML as well as the next highest compliance functions (Chief Compliance Officer and Divisional Compliance) in writing of the new national anti-money laundering legislation and the name of the AML contact person.

5. Ban on cash transactions

The following applies to all Group companies with the exception of the Financial Services companies:

Cash transactions in the form of making or receiving either by oneself or by third parties, with a value equaling or exceeding EUR 10,000 are not permitted.

At Volkswagen Autoeuropa, cash transactions, of any value, are not authorized.

Cash transactions of high-value goods according to the Section 1 (10) sentence 2 number 1 GWG (precious metals such as gold, silver and platinum), from a threshold of EUR 2,000 or more and which are made or received either by oneself or by third parties, are not permitted.

Third parties within the meaning of this Group Policy are in particular persons acting on the initiative and on the instructions of Volkswagen AG, such as intermediaries who hold funds on the trust basis for Volkswagen AG and Volkswagen Autoeuropa, messengers including money couriers (cash transport), agents, representatives on the initiative and on the instructions of Volkswagen Group and of Volkswagen Autoeuropa, such as intermediaries who hold funds on the trust basis for Volkswagen Group, messengers including money couriers (cash transport), agents, representatives. In addition, the prohibition on cash transactions includes cash deposit transactions and transactions via money remittance agencies.

Financial Information Unit of the Judicial Police (FIU) is the central authority of investigations into financial transactions

Central Department of Investigation and Criminal Action (DCIAP) is an organ of the Public Prosecutor's Office of Portugal that has its own competence in the field of the prevention of money laundering and terrorist financing receiving and analyzing the communications of suspicious operations that may configure the practice of the crime of laundering or terrorist financing.

Direction in the meaning of this Policy refers to VW AG and Volkswagen Autoeuropa employees at the management level (MK) and at higher levels, or at equivalent hierarchy levels.

Money laundering is the act of introducing illegally earned money into the legal financial

or economic system, with the aim of concealing its true origin.

PEP (politically exposed persons) is a natural person who has held or held a high-level public office, important at international, European or national level, or a public office at national level of comparable political importance, a family member of that person or someone known to be close to that person.

Examples of politically exposed people include:

Heads of State or Government; ministers (deputy ministers); members of the Commission European Union; secretaries of state; members of similar legislative bodies; members of the governing bodies of political parties; members of supreme courts, constitutional courts or other high-level courts whose decisions are not by rule subject to appeal; members of the governing bodies of the courts of auditors; members of central bank management bodies; ambassadors, business officers and defense attachés; members of the administrative, management or supervisory bodies of public undertakings; directors, deputy directors, members of the management body or other managers with similar functions in an international or European intergovernmental organization

Potential Business Partner are those natural/legal persons and partnerships, with whom a current contractual relationship does not yet exist, however, entering into a contractual relationship appears possible or is intended by at least one party.

Red Flags are indications that may substantiate a money laundering or terrorist finance suspicion.

Smurfing is the repeated and/or regular execution of multiple related cash transactions in order to create the impression that the transaction volume is below the threshold.

Terrorist financing is the provision or collection of assets with the knowledge or with the intention to be used entirely or in part for terrorist activities.

Transaction is one (or multiple) act causing a money transaction or any other transfer of assets.

Beneficial owner is the natural person who ultimately has ownership or control of the contracting party or the natural person at whose instruction a transaction is ultimately carried out or a business relationship is ultimately established. In the case of companies, any natural person is assumed to be a beneficial owner who directly or indirectly holds more than 25% of its capital, or voting rights or who is able to exercise control in a comparable manner.

Cash deposit transaction is the deposit of an amount of cash for the credit of a beneficiary's account.

A cash transaction can consist of a single transaction or a series of transactions that appear to be associated.

Where the applicable national legislation provides for a lower limit in the form of a reduction or prohibition in respect of cash transactions, that limit shall prevail.

6. Indications („Red Flags“)

Among other things, the following “red flags” may substantiate the suspicion of money laundering or terrorist financing and give rise to further obligations on the part of

employees:

- The customer withdraws their offer after learning that further information must first be collected
- The transaction is not typical or does not make sense economically
- It is apparent from the conclusion of the contract that the customer intends to cancel the contract at a later date
- Constantly changing bank accounts
- Unclear payments from third-parties

However, not all of these “red flags” automatically substantiate the suspicion of money laundering or terrorist financing.

7. Obligations in the event of suspected money laundering or terrorist financing

As a company that trades high-value goods, precautions have to be taken at an organisational level as well as with regard to the employees’ day-to-day activities in order to minimise the risk of money laundering or terror financing. In the centre of prevention of money laundering are the general and enhanced due diligence obligations, which vary depending on the individual case and must be fulfilled.

7.1 In case of a money laundering or terrorist financing suspicion, employees are obliged to comply with the following procedures. This applies in particular to employees that are in contact with contractual partners or overview payment flows on a daily basis. In such cases, it is important to be vigilant so that any suspicious circumstances can be identified and caution can be exercised as soon as possible.

a) Obligation to report internal suspicious cases

In case of a money laundering or terrorist financing suspicion employees must contact their superior as well as the AML contact person in writing/by telephone to report the suspected case. The obligation of Inhouse lawyers to report suspicions pursuant to § 2 Abs. 1 Nr. 10 i.V.m. § 43 I GwG, remains unaffected thereof.

b) Transaction stop

In the event of a suspicion of money laundering or terrorist financing, no services shall be requested, accepted, offered or provided. The transaction shall not be executed until it has been approved by the AML contact person. Especially incoming payments must be transferred on a separate clarification account.

c) No disclosure of information on suspected cases

In the event of any suspicion of money laundering or terrorist financing this information or any other details, respectively in the form of a warning, shall not be disclosed to the principal of the transaction (e.g. the business partner) or to any other third parties (no “tipping-off”).

7.2 The AML contact person examines the circumstances of the case and decides on the further steps. After evaluating the case he immediately reports, if necessary, the suspicion to the FIU.

If the AML contact person concludes that the suspicion of money laundering or terrorist financing has substantive grounds, additional due diligence obligations will be defined in consultation and cooperation with the AML contact person and must be fulfilled by the responsible business unit. These legally required general and/or enhanced due diligence obligations, are to be defined on a case by case basis and can, depending on the evaluation of the case, trigger inter alia the following additional obligations:

a) Identification of the contractual partner and, where applicable, the person representing them

If employees have direct contact with the contractual partner, they are obliged to identify the contractual partner as well as any persons representing them (e.g. agent or messenger). The contractual partners of Volkswagen Autoeuropa's partners have the same status as the latter if they enter into any commercial transaction with us. Where necessary and subject to consultation with the AML contact person, the identification of such third parties must be established by the contractual partner. It should be noted that a distinction is drawn depending on whether the contractual partner is a natural person (see a)) or a legal person (see b)). The following information of the contractual partner must be requested to establish the identity.

aa) The contractual partner is a natural person

If the contractual partner is a natural person the following information must be obtained:

- First and last name
- Place of birth
- Date of birth
- Nationality
- Residential address

The natural person's identity must be verified based on the following original documents:

- Valid official ID card or
- Valid passport

A copy of these documents must be made and attached to the identification form.

bb) The contractual partner is a legal person

If the contractual partner is a legal person the following information must be obtained:

- Company, name or designation
- Legal form
- Registration number (if any)
- Address of registered office or principal place of business
- The names of the members of the executive bodies or statutory representatives and, if the member of the executive body or the statutory representative is a legal person, the information set out under letters a. to d.

The information can also be obtained from public sources (website or self-disclosure). The identity of the legal person of the contractual partner must be verified based on to the following original documents:

- Extract from the commercial or cooperative register or comparable official register or directory, or
- certificate of incorporation or other equivalent documents (e.g. information from credit agencies), or
- own documented inspection of the data held in a register or directory (in particular electronic ones).

A copy of these documents must be made and attached to the identification form.

b) Identification and verification of the beneficial owner

In addition, each employee is obliged to establish and verify the identity of the beneficial owner using the identification forms in the event of a suspicion. The following information on the beneficial owner must be obtained:

- First and last name
- Place of birth
- Date of birth
- Nationality
- Residential address

The information on the beneficial owner must be duly verified, e.g. in the form of self-disclosures or research on the Internet.

c) Identification of the purpose of the transaction

If the purpose of the business relation is not self-evident beyond any doubt (e.g. as indicated in the preamble of the contract or other documents or invoices), information indicating the purpose of the business relationship must be obtained and the results documented in case of a suspicion of money laundering or terrorist financing.

d) Special constellations

In certain cases, further precautions must be taken in addition to the measures outlined above. This is in particular necessary, if:

- aa) the contracting party or the beneficial owner is a PEP, a family member of a PEP (the spouse or civil partner, a child and the child's spouse or civil partner and both parents) or a person known to be a close associate. In the course of the above mentioned identification process, each employee must determine whether the contractual partner or the beneficial owner is considered as a PEP (politically exposed person). It is necessary that the employee expressly ask the business partner for their "PEP status".
 - bb) the business or contractual partner or their beneficial owner is identified as a high-risk third party according to the respective applicable EU. Negative list or is a natural or legal person domiciled in such a high-risk third country
 - cc) the transaction, in relation to comparable cases, is particularly complex or large, follows an unusual pattern or has no apparent economic or lawful purpose,
- e) Under the above mentioned special constellations (7.2 d)) a transaction or establishment of a business relationship is only permitted if the following conditions are met:

aa) Requirement of approval

The establishment or continuation of the business relationship requires the approval of a responsible member of the management of Group Compliance.

bb) Identification of the source of the funds

Furthermore the obligation to apply suitable methods (e.g. consultation with the business partner, examination of annual financial statements) to identify the source of the funds which are used for a transaction or in connection with the business relationship, must be complied with.

cc) Enhanced ongoing monitoring

If the AML contact person concludes that a higher risk of money laundering or terrorist financing may arise, the respective business relationship including the relevant transactions are subject to continuous monitoring. For this purpose, all available information held on the business partner must be updated in appropriate regular intervals.

The AML contact person, in coordination with the responsible business unit, defines appropriate measures, which shall then be fulfilled by the responsible business unit. A feedback regarding the implementation of the defined measures to the AML contact person follows the upfront specified scope.

The ongoing monitoring also includes an enhanced monitoring of incoming payments taking place within the business relationship. Therefore the AML contact person, in consultation and cooperation with the business unit accounts receivable, which is involved in the downstream support process of

handling the financial flows based on the underlying legal transactions, defines appropriate monitoring measures. The defined monitoring measures must be conducted as required and must be reported back to the AML contact person accordingly.

8. Data Protection

Volkswagen Autoeuropa ensures compliance with the applicable legislation on the processing of personal data, without prejudice to the powers legally conferred on Volkswagen Autoeuropa, as a obliged entity, in the context of the fulfilment of its preventive duties, in accordance with articles 57.º e (ss). of LBC.

The processing of personal data carried out pursuant to LBC is intended solely to prevent money laundering, and such data may not be further processed for any other purposes, including commercial purposes.

9. Protection of employees

Volkswagen Autoeuropa ensures the protection of any worker or collaborator who, under this Policy or the compliance with legal or regulatory duties imposed in the prevention and combating of money laundering, complies with the duty of communication required to DCIAP or the FIU. Any worker or employee who reports a suspicious fact to these entities may not be subject to any reprisal, penalty, and discriminatory treatment.

10. Documentation and archiving

The applicable national statutory and regulatory requirements governing the documentation of the measures taken to combat money laundering and for addressing any matters found to be related to money laundering must also be observed over and above the stipulations contained in this Policy. This also applies to any duties stipulated by national law with respect to reporting to the competent authorities. In this connection, the internal data protection guidelines as well as national data protection legislation and statutory archiving periods must be duly observed.

Documents obtained and prepared in the context of a report on suspected money laundering or terrorist financing shall be archived for seven years, unless other mandatory legal provisions provide for a longer retention period. This period shall start at the end of the calendar year in which the information in question is obtained.

11. Preventive Duties under the LBC (Summary) (Sumário)

PREVENTIVE DUTIES	
Control duty	Adoption of internal mechanisms and models of control and risk management
Duty of Identification and Diligence	Customer Identification (required after verification of assumptions) Identification of your representative (if applicable) Identification or knowledge of the Beneficial Owner (if applicable) Knowledge of ownership or control structure (if applicable) Adequate knowledge of the origin and destination of the funds (if applicable) Possibility of adopting simplified measures Possibility of adopting enhanced measures
Duty of Communication	Mandatory and timely communication to DCIAP and FIU where money laundering is suspected
Duty of Abstention	Suspension of the execution of material or legal acts arising from commercial relations where money laundering is suspected
Duty of Refusal	Refusal to start commercial relations when money laundering is suspected Cessation of commercial relations when money laundering is suspected
Conservation Duty	Retention on long-term support and for a period of 7 years of all relevant information relating to the Customer Record, execution of operations, communications with the competent authorities, as well as information relating to the performance of other preventive duties
Duty of Examination	Careful and prudent examination and follow-up of the business relationship when money laundering is suspected
Duty of Collaboration	Prompt and full cooperation with the DCIAP, FIU, Tax and Customs Authority or any judicial or police authority
Duty of Non-Disclosure	Abstention of communication with the Client or any third party of which there has been or is ongoing an investigation that has as its object the crime of money laundering

The Board of Directors of Volkswagen Autoeuropa