Anti-Money Laundering

Issued by: Group Head of Shared Services
Issue 1 / October 2022

1. INTRODUCTION

1.1 As a company, we are committed to carrying on business in accordance with the highest ethical standards. This includes complying with all applicable laws and regulations aimed at combating money laundering and terrorist financing. This Policy has been developed by the Bodycote Group to reduce the risk of money laundering and terrorist financing associated with its business and the sale of its service and products. This Policy explains our individual responsibility in complying with anti-money laundering and counterterrorist financing laws ("AML Laws") around the world and ensuring that any third parties that we engage to act on our behalf do the same.

1.2 The management of the Bodycote Group is committed to complying with all laws. Any employee who violates the rules in this Policy or who permits anyone to violate those rules may be subject to appropriate disciplinary action, up to and including dismissal, and may be subject to personal civil or criminal fines.

1.3 If you have any questions about this Policy you should contact the Group Head of Financial Shared Services.

2. POLICY STATEMENT ON ANTI-MONEY LAUNDERING

2.1 It is Bodycote Group policy to comply with all applicable AML Laws in our operations worldwide. To this end, Bodycote will only conduct business with customers who are involved in legitimate business activity and whose funds are derived from legitimate sources.

2.2 This Policy is intended to help employees, contractors, and other third parties acting on the Group's behalf to understand where breaches of AML Laws might arise and to support them in making the right decisions in line with our corporate position as stated in this Policy.

3. WHO IS SUBJECT TO THIS POLICY

3.1 This Policy applies to the Bodycote Group operations globally, including all legal entities worldwide owned or controlled by Bodycote Plc, and to all directors, officers, employees, contractors, and other third parties acting on behalf of the foregoing.

4. WHAT IS MONEY LAUNDERING

4.1 Money laundering means exchanging money or assets that were obtained criminally for money or other assets that are 'clean'. The clean money or assets don't have an obvious link with any criminal activity. Money laundering also includes money that is used to fund terrorism, however it's obtained.

4.2 The following types of activities are considered to be "money laundering" and are prohibited under this Policy:

a) the conversion or transfer of property (including money), knowing or suspecting that such property is derived from criminal or certain specified unlawful activity ("criminal property"), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;

b) conducting a financial transaction which involves criminal property;

c) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, ownership or control of criminal property;

d) the acquisition, possession or use of criminal property;

e) promoting the carrying on of unlawful activity; and

f) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.

4.3 The broad definition of money laundering means that anybody (including any Bodycote employee) could be in violation of the law if he/she becomes aware of, or suspects, the existence of criminal property within the business and becomes involved in or continues to be involved in a matter which relates to that property being linked to the business without reporting his/her concerns.

4.4 Property can be criminal property where it derives from any criminal conduct, whether the underlying criminal conduct has taken place in the country where you are situated or overseas.

4.5 Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

5. THE RED FLAGS

5.1 Where any suspicions arise that criminal conduct may have taken place involving a customer, colleague or third party, you should consider whether there is a risk that money laundering or terrorist financing has occurred or may occur.

5.2 Some examples of red flags to be reported include:

- A customer provides insufficient, false or suspicious information or is reluctant to provide complete information.
- Methods or volumes of payment that are not consistent with the payment policy or that are not customarily used in the course of business, e.g., payments with money orders, traveller's checks, and/or multiple instruments, and payments from unrelated third parties.
- Receipts of multiple negotiable instruments to pay a single invoice.
- Requests by a customer or partner to pay in cash.
- Early repayments of a loan, especially if payment is from an unrelated third party or involves another unacceptable form of payment.
- Orders or purchases that are inconsistent with the customer's trade or business.
- Payments to or from third parties that have no apparent or logical connection with the customer or transaction.
- Payment to or from countries considered high risk for money laundering or terrorist financing.
- Payments to or from countries considered to be tax havens or offshore jurisdictions.
- Payments from countries unrelated to the transaction or not logical for the customer.
- A customer's business formation documents are from a tax haven, or a country that poses a high risk for money laundering, terrorism or terrorist financing, or a country that is not logical for the customer.
- Overpayments followed by directions to refund a payment, especially if requested to send the payment to a third party.
- Any customer for whom you cannot determine the true beneficial owner.

- Structuring transactions to avoid government reporting or record keeping requirements.
- Unusually complex business structures, payment patterns that reflect no real business purpose.
- Wire transfer activity that is not consistent with the business activities of the customer, or which originates or terminates with parties unrelated to the transaction.
- Unexpected spikes in a customer's activities.

5.3 The above is not intended to be an exhaustive list. Deviation from customer and accepted business practice should alert you to further investigate the activity in accordance with this Policy.

6. BODYCOTE'S OBLIGATIONS

6.1 Bodycote has a responsibility to:

- Appoint a Money Laundering Reporting Officer (MLRO) to receive, consider and report as appropriate the disclosure of any suspicious activity reported by employees. See below for further details in respect of the MLRO.
- Maintain Due Diligence procedures for all Customers and Vendors to identify procedures to identify Anti-Money Laundering relevant business partners.
- Facilitate Anti-Money Laundering training to all employees.
- Maintain adequate records of transactions.

7. EMPLOYEE OBLIGATION

7.1 You have the obligation to read and follow this Policy, to understand and identify any red flags that may arise in business activities and to escalate potential compliance concerns related to the MRLO without notifying anyone involved in the transaction and should not take any actions prior to receiving advice and/or instructions.

Your report should include as much detail as possible including:

a) Full details of the people and/or companies involved including yourself and other members of staff if relevant.

b) Full details of the transaction and nature of each person's involvement in the transaction.

c) The suspected type of money laundering activity or use of proceeds of crime with exact reasons as to why you are suspicious.

d) The dates of any transactions, where they were undertaken, how they were undertaken, and the likely amount of money or assets involved.

7.2 Once you have reported your suspicions to the MLRO you must follow any instructions given to you. You must not make any further enquiries unless instructed to do so by the MLRO. At no time and under no circumstances should you voice any suspicions to the person(s) you suspect of money laundering, nor should you discuss this matter with any colleagues.

7.3 If appropriate the MLRO will refer the case to the respected national criminal bodies who will undertake any necessary investigation. This may include consent to continue with a particular

transaction and care should be taken not to 'tip off' the individuals concerned, otherwise you may be committing a criminal offence which may result in severe penalties to you.

8. MONEY LAUNDERING REPORTING OFFICER (MLRO)

8.1 The Group has appointed a Money Laundering Reporting Officer (the "MLRO"), who is the Group Head of Finance Shared Services, and a Deputy MLRO, who is the Chief Administration officer to act in his absence. The MLRO is the officer nominated to receive disclosures in respect of suspected transactions or activity within the Bodycote Group.

8.2 On receipt of a disclosure report the MLRO will:

- Note the date of receipt and acknowledge receipt of it.
- Assess and advise the individuals concerned when a response can be expected.
- Consider the report and any other relevant information, undertaking further enquiries if necessary to decide if a report should be made to national criminal bodies.

8.3 Once the MLRO has evaluated the case, a timely determination will be made as to whether:

- There is actual or suspected money laundering taking place.
- There are reasonable grounds to know or suspect that is the case.
- Consent is required from national criminal bodies for a particular transaction to proceed.

8.4 Where the MLRO concludes that the case should be disclosed this needs to be done:

- In a timely manner.
- In the prescribed manner on a standard report format provided.

8.5 Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then consent will be given for transactions to proceed and the disclosure report will be marked accordingly.

8.6 Where any suspicions arise that criminal conduct may have taken place involving a customer, colleague or third party, you should consider whether there is a risk that money laundering or terrorist financing has occurred or may occur

9. CUSTOMER AND SUPPLIER DUE DILIGENCE INCLUDING FINANCIAL SANCTION TARGETS

9.1 In order to confirm that Bodycote Plc only deals with legitimate business partners the Company has engaged with 3rd party screening tool – DESCARTES. This tool validates every Business partner versus all available sources (AML, Sanction lists etc), including validation of beneficial owners of the company. The tool is fully operated by Finance SSC.

As a part of Business partner due diligence process the SSC validates:

- Every new customer before addition to Customer database.
- Every new supplier before addition to Supplier database.

The SSC has also established an instant real time validation of the Group's complete Business partner database.

The validation effectively confirms that:

- The Business partner is a legitimate business.

- The Business partner beneficial owners are not part of any official AML or Sanction list.

10. COMMUNICATION

10.1 This Policy ensures staff understand their responsibilities under the Anti-Money Laundering regime, the Company's due diligence procedures and how to report suspicious activity. The Policy is published on the Group's intranet and communicated to staff via internal communication.

record keeping

10.2 By keeping comprehensive records Bodycote is able to show that we have complied with the Money Laundering Regulations. This is crucial if there is a subsequent investigation into one of our customers or transactions.

10.3 The types of records kept may include:

- Daily records of transactions.
- Receipts.
- Cheques.
- Paying-in books.
- Customer correspondence.

10.4 Records may be kept in any of the following formats:

- Originals.
- Photocopies.
- Microfiche.
- Scanned.
- Computerised or Electronic.

10.5 Records must be kept for five years beginning on either:

- The date a business relationship ends.
- The date a transaction is completed.

10.6 The MLRO will retain any disclosure reports and any associated relevant documents in a confidential file for a minimum of five years.

10.7 The Group is required to retain records for at least seven years after ceasing to transact with an employee, supplier or customer including records of risk assessment, identity and verification and ongoing monitoring. These records are required for other purposes, such as tax compliance, as well as anti-money laundering.

If you have any further questions please contact the Group Head of Shared Services at email petr.jelinek@bodycote.com or phone +420 602491633

Policy owner:	Group Head of Shared Services
Second policy owner:	Group Chief Administration Officer
Approved by:	Bodycote plc Board
Version number and date:	1.0 27/10/2022
ate of last review:	New Issue