

Anti-Money Laundering Policy

1. Introduction

- 1.1** Digi Communications N.V. (***DIGI***) and its subsidiaries (the ***DIGI Group***) are committed to exercising high ethical standards and conducting business with fairness, honesty and integrity.
- 1.2** This commitment includes requiring all officers, directors, employees and contractors of the DIGI Group (***Personnel***) and partly-owned companies within the DIGI Group's control to comply with all applicable laws and regulations requiring reporting of cash transactions.

2. Money Laundering and Terrorism Financing

- 2.1** Personnel must not engage in, or help others engage in, money laundering or terrorism financing.
- 2.2** Personnel must not do business with persons or entities known or suspected to be involved in money laundering or terrorism financing.

3. Cash Transaction Reporting Principles

- 3.1** Personnel must avoid cash transactions unless there is no reasonable alternative payment mechanism available.
- 3.2** Personnel must report cash payments over specified thresholds to the DIGI Compliance Group, which will in turn comply with applicable requirements to report verified cash receipts to the Financial Intelligence Units in relevant jurisdictions.
- 3.3** Personnel must not tell the person or company who made the cash payment about their report. This can be a serious violation of the law in some countries (sometimes called 'tipping off').

4. Due Diligence

- 4.1** The DIGI Group conducts enhanced due diligence in connection with any customer relationship in which the DIGI Group anticipates receiving a cash payment of €10,000 or more.
- 4.2** The DIGI Group conducts risk-based due diligence in respect of other customers and business partner.

5. Concerns

- 5.1** Personnel must report any cash transactions in amount of or exceeding 10,000EUR and any money laundering or terrorism financing suspected operations to the DIGI Compliance Group.
- 5.2** Personnel must not tell the person or company that is the subject of their concern about their report. This can be a serious violation of the law in some countries (sometimes called 'tipping off').

5.3 The DIGI Compliance Group will review each report submitted and, where appropriate, will conduct further investigation, make recommendations for remedial action and/or reporting potential issues to relevant law enforcement or regulatory authorities.

6. Further Information

6.1 All questions about these principles or other matters of compliance and ethics may be directed to the DIGI Compliance Group via email (grup.conformitate@digicomunications.ro).