ANTI-MONEY LAUNDERING & SANCTIONS POLICY

Version 1.0
Date: April 2019

Approved by Creditinfo Group CEO

CREDITINFO

TABLE OF CONTENT

I. Countering Corruption

A. Compliance Policies

Our Creditinfo Compliance Policies define the business and ethical behaviours that we all need to demonstrate when working for Creditinfo Group hf. and any other entity, subsidiary, and/or affiliate within the Group umbrella (the "Group" or "Creditinfo Companies"). They are mandatory. While these are for internal use, we also publish them externally in support of transparency.

Our Compliance Policies are available to the general public at http://www.creditinfo.com/policies. However, in certain circumstances, a Policy may use or reveal information which is not available to the general public and which could be considered of some importance internally and/or to Group shareholders, customers, business partners, and others. In such cases, the Policy will not be available at the URL above.

Employees may request a comprehensive list of the Group's Compliance Policies (including any policies that are unavailable at the URL above) via email at compliance@creditinfo.com. Any compliance-related questions may be directed to this inbox.

The Group's Compliance Officer, Carly Souther, can be contacted at +34.691.043.161, or via email at c.souther@creditinfo.com.

B. Anti-money Laundering & Sanctions: Background and Definition

Creditinfo Companies do not do business with, whether directly or indirectly, individuals or entities associated with money laundering, terrorism financing, white-collar crime, or other unusual activities (collectively "AML activity"). Furthermore, the Group does not do business in a sanctioned country or with a sanctioned person without prior clearance from the Group's Compliance Department.

Money laundering is the term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source.

Terrorist financing refers to activities that provide financing or financial support to terrorists. Transactions associated with terrorist financing tend to be in smaller amounts than in the case of money laundering. It may involve funds raised from legitimate sources, such as personal donations, profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping, and extortion.

Economic sanctions are the withdrawal of customary trade and financial relations for foreign and security policy purposes. They may be comprehensive (i.e., prohibiting commercial activity with regard to an entire country), or they may be targeted (i.e., blocking transactions of, and with, particular businesses, groups, or individuals.

Governments and multinational bodies impose economic sanctions to deter or alter the conduct or strategic decisions of state or non-state actors whose decisions violate international norms of behaviour, or otherwise threaten against domestic, regional, and/or international security and peace.

To optimize Creditinfo's compliance and to better identify employees or contractors, customers or partners, or any other affiliates who may be associated with AML activity or economic sanctions, each Creditinfo Company shall implement procedures related to the following compliance areas:

- **Employee Onboarding** – Identify and report patterns indicative of money laundering and terrorism financing, then screen against appropriate Politically Exposed Persons (PEPs) and global sanctions lists.

- **Monitoring/Look-Back** – Have your Customer portfolio continually screened/monitored against PEPs and global sanctions lists for changes, receiving alerts when changes to the selected data sources are found.

- **Oversight** - Streamline alerting, tasks, and reporting for Creditinfo Governance body (e.g. Country Manager, Country Compliance

Officer, Group Compliance Officer, Group Chief Executive Officer and Group Board of Directors) and/or internal auditors.

Any unusual activities must be rejected immediately and reported to an employee's Supervisor/Manager and the Group's Compliance Officer, Carly Souther, at +34.691.043.161, or via email at c.souther@creditinfo.com.

II. Anti-Money Laundering

To protect Creditinfo's reputation and avoid criminal liability, it is important not to become associated – however innocently – with the criminal activities of others. In particular, Creditinfo and its employees must ensure Creditinfo does not receive the proceeds of criminal activities, as this can amount to the criminal offence of money laundering. This Policy sets out essential steps employees must take to avoid being implicated in money laundering.

MUSTS

All Creditinfo employees **must** immediately notify the Group's Compliance Officer if they have any suspicions about actual or potential money laundering activity.

All Creditinfo employees **must** look out for warning signs of money laundering, such as:

Supplier requests to:

- Pay funds to a bank account in the name of a different third-party or outside the country of their operation;
- Make payments in a form outside the normal terms of business;
- Split payments to several bank accounts;
- Overpay.

Customer payments to Creditinfo:

- From multiple bank accounts;
- From bank accounts overseas when not a foreign customer;

- Made in cash when normally made by cheque or electronically;
- Received from other third parties;
- Made in advance when not part of normal terms of business.

All Creditinfo employees involved in engaging or contracting with third parties such as new suppliers and customers **must**:

- Ensure that the third parties in question are subject to screening to assess their identity and legitimacy before contracts are signed or transactions occur. Various factors will determine the appropriate forms and levels of screening;

- Determine, with guidance from their Supervisor/Manager, which tools and processes should be used to facilitate appropriate screening and record-keeping;

- Carefully consider, where necessary in consultation with their Supervisor/Manager or the Group's Compliance Officer, screening outcomes before deciding whether to do business with the third-party;

- Finance managers who support Supply Chain Management and Customer Development must regularly monitor and/or review suppliers, customers, and other third-party service providers, to identify business activity or governance that could indicate money laundering is taking place.

MUST NOTS

All Creditinfo employees **must not**:

- participate in money laundering in any form;
- participate in terrorist financing in any form;
- do any business in a sanctioned country without prior clearance from the Group's Compliance Department;
- do any business with a sanctioned person.

All Creditinfo employees **must not** simply assume relevant third-party screening has already taken place: Failure to check or update screenings periodically may put Creditinfo and its employees at risk.

CREDITINFO

SIGNATURE PAGE

Name: Mr. Stefano M. Stoppani

Title: Creditinfo Group CEO

Date: 9 April 2019

Signature: