GLOBAL SANCTIONS & ANTI-MONEY LAUNDERING POLICY

Version 2.0

Date: April 2022

Revised: March 2025

TABLE OF CONTENTS

I. Introduction

Our Creditinfo Compliance Policies define the business and ethical behaviours that we all need to demonstrate when working for Creditinfo Group including any of its entities, subsidiaries, and/or affiliates within the Group umbrella ("Creditinfo"). All Creditinfo directors, officers, employees (collectively, "**Creditinfo Employees**"), and any person providing services for or on behalf of the Group must comply with this Policy at all times and act with the highest ethical standards. This Policy should be read in conjunction with any local sanctions, AML policies, and due diligence procedures which, if applicable, shall be annexed as an appendix to this Policy. Local policies and procedures may expand upon and supplement the requirements set forth herein but may not derogate or relax the provisions of this Policy.

While the Compliance Policies 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 Creditinfo 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 Creditinfo'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.

Creditinfo's Central Compliance team can be contacted via email at compliance@creditinfo.com.

This Policy has been reviewed and approved by the Group Chief Executive Officer.

II. Purpose

Creditinfo has adopted this Sanctions & Anti-Money Laundering Policy to ensure compliance with applicable financial and trade sanctions laws and regulations administered and enforced by governments and supranational bodies, including, amongst others, Her Majesty's Treasury ("HMT"), the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), and the European Union ("EU") (collectively, "**Sanctions**"), as well as applicable anti-money laundering and counter-terrorist financing laws and regulations. These laws and regulations restrict what Creditinfo may import from or export to certain countries, regulate business and financial transactions with certain countries, and prohibit dealings with certain named individuals, entities, groups and organisations.

The Creditinfo Legal & Compliance team, which includes local in-house counsel, local compliance officers, central legal in-house counsel, central compliance officers and the Creditinfo Group General Counsel, is responsible for the review, approval and oversight of this Policy. Creditinfo Employees should contact their local compliance team as a point of first reference should they have any questions or concerns about any aspect of this Policy, otherwise, queries may be addressed to *compliance@creditinfo.com*.

III. Policy Statement

Creditinfo Companies are committed to doing business in the right way, to continually earn the trust of customers, other stakeholders, and the wider marketplace. In accordance with the Creditinfo Code of Conduct, the Creditinfo Group Board of Directors and Group Chief Executive Officer expect all Creditinfo Employees and anyone carrying out work for or on behalf of the Group to maintain the highest standards of ethical business conduct and personal behavior, and to act honestly, responsibly, safely, lawfully, and with integrity.

Creditinfo Companies must at all times conduct business in compliance with applicable Sanctions. Creditinfo Companies do not do business with, whether directly or indirectly, individuals or entities associated with money laundering or terrorist financing.

This Creditinfo Sanctions & Anti-Money Laundering Policy outlines the standards that must be observed at Creditinfo to protect Creditinfo and Creditinfo Employees from involvement in money laundering, facilitating money laundering, terrorist financing or violating Sanctions.

Failure to meet the required standards of compliance with applicable anti-money laundering, terrorist financing and Sanctions laws and regulations may expose Creditinfo to reputational damage, criminal and civil fines, operational delays, and even the loss of applicable trade licenses and privileges. Individuals may also be subject to criminal, regulatory and civil prosecution, including fines and even imprisonment. Employees who fail to comply with this Policy may also be subject to disciplinary action, up to and including termination.

Creditinfo expects you to make sure that you understand and follow this policy, any applicable local policies, and any relevant supporting policies or procedures, whether issued at central or local level.

IV. Sanctions

a. *What Are Sanctions?*

Sanctions are restrictive measures aimed at achieving foreign policy or national security objectives. 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 Sanctions to deter or alter the conduct or strategic decisions of state or non-state actors whose actions violate international norms of behaviour, or otherwise threaten domestic, regional, and/or international security and peace. Sanctions may be applied against countries, individuals, companies, or trading activities.

Most Sanctions apply on an extra-territorial basis, meaning that they can apply to persons or entities for conduct anywhere in the world.

Sanctions can take the form of any of a range of restrictive measures. The most important types of Sanctions which may affect Creditinfo are:

- Broad-based U.S. Sanctions that apply country or territory-wide restrictions, such as those currently in force in relation to Iran, North Korea, Cuba, Syria, and Crimea/Sevastopol ("**Restricted Territories**"). These sanctions may also apply to non-U.S. persons to the extent that transactions have a connection to the U.S., such as payments in U.S. dollars or through U.S. banks and their subsidiaries or branches abroad, or transactions involving U.S. nationals (including U.S. national or green card-holding Employees, for example) or companies, or U.S. origin goods;

- Entering into transactions with individuals or entities that have either been directly designated as sanctions targets (meaning their name appears on a list of sanctions targets published by a relevant government), or they must be treated as subject to sanctions because of their known involvement in or affiliation with sanctions targets, or with certain criminal activities or groups (e.g. members of the Taliban, the Islamic State in Iraq and the Syria ("ISIS/ISIL"), al Qaeda, the Iranian Revolutionary Guards Corps) ("**Sanctioned Persons**").

- In addition to the Restricted Territories, certain countries are subject to targeted sanctions, meaning that although there is no blanket ban on doing business with individuals or entities from or based in those countries, there is a higher prevalence of Sanctioned Persons in those countries than may be the case in other countries ("**Sanctioned Countries**"). A list of Sanctioned Countries is maintained in the Sanctions Procedure, set out in the Appendix to this Policy.

It is important to note that Sanctions may range beyond the examples set out above. They are also constantly changing to reflect the evolving political and military situations in targeted countries, as well as the political objectives of the countries that impose such restrictions. In certain circumstances, the restrictions under U.K., E.U., and U.S.

Sanctions may also differ. If you are in any doubt as to the potential relevance of Sanctions to any activity you are engaged in for or on behalf of Creditinfo, you should seek advice from a member of the Creditinfo Legal & Compliance team **before** engaging in that activity.

b. *Sanctions: what should I do?*

Creditinfo **must not** do business connected to a Restricted Territory, Sanctioned Country or with a Sanctioned Person without first complying with the Sanctions Procedure, set out in the Appendix to this Policy.

A connection to a Restricted Territory, Sanctioned Country or Sanctioned Person may include, for example, where:

- a customer or supplier is a Sanctioned Person, or is owned or controlled by a Sanctioned Person;
- a customer or supplier is based or incorporated in a Restricted Territory or Sanctioned Country;
- a customer or supplier's owner or controller is in a Restricted Territory or Sanctioned Country;
- a customer is not based or incorporated in a Restricted Territory or Sanctioned Country but has requested that software, technology or services be sent, directly or indirectly, to, or made available for use in, a Restricted Territory or Sanctioned Country; or
- a customer is purchasing software, technology or services for onward sale or use in a Restricted Territory or Sanctioned Country, or by a Sanctioned Person, whether or not the software, technology or services are incorporated into the customer's own products first.

V. Money Laundering and Terrorist Financing

a. *What is money laundering?*

Money laundering is a serious criminal offence and a term used to describe the process by which criminals disguise the original ownership and control of the proceeds of crime to make assets appear legitimate.

Money laundering may consist of:

- Converting, transferring or disguising criminal property;
- Possessing, using or controlling criminal property; or
- Being involved in transactions to facilitate the acquisition, use or retention of criminal property.

Criminal property is not limited to the proceeds of such things as drug trafficking or terrorism—the definition extends to any property flowing from any crime, including tax evasion, bribery and corruption, and fraud.

Money laundering offences present serious risks for businesses. Breaches of anti-money laundering ("**AML**") laws and regulations can lead to significant fines for companies and individuals, and even imprisonment for individuals. Creditinfo's reputation could be severely damaged by a failure to detect any relationships or transactions that use criminally tainted or otherwise illegitimate funds to pay for Creditinfo's products and services or to fund projects for Creditinfo. Creditinfo Employees who engage in money laundering related offences or breaches of this Policy may face criminal or civil prosecution, and/or disciplinary action up to and including termination.

b. *What is terrorist financing?*

Terrorist financing refers to activities that provide financing or financial support to terrorists. 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.

c. *Money laundering and terrorist financing: what should I do?*

All Creditinfo Employees must immediately notify your local in-house counsel or local compliance team.if they have any suspicions about actual or potential money laundering or terrorist financing activity. If your local market does not have an in-house

counsel or compliance function, you should instead consult with the central Legal & Compliance team. Local in-house counsel or local compliance teams should report any such notifications to central Legal & Compliance without delay.

All Creditinfo Employees must look out for warning signs of money laundering and terrorist financing, 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; or
    - overpay.
- Customer seeks to pay Creditinfo:
    - from multiple bank accounts or in multiple currencies without obvious justification for doing so;
    - from bank accounts overseas when not a foreign customer;
    - in a form outside the normal terms of business, such as deposits of cash or cash equivalents or made on a party's behalf by another unknown party;
    - indirectly via other third parties; or
    - in advance when not part of normal terms of business.
- Diligence indicates a previous criminal, civil, or regulatory breach or reputational concerns linked to a customer or supplier, or a Creditinfo Employee becomes aware of such information, for example from the employees of the customer or supplier, or from other sources.

If a red flag (including any of the above) is detected prior to entering into or during the course of any business relationship, the transaction in question must not proceed and the suspicious activity must be reported immediately to the relevant Finance Director and your local in-house counsel or local compliance team for further review, investigation and approval.

Any "red flag" transactions approved in accordance with the above procedures must be appropriately documented, detailing clearly the reason for proceeding, including how the red flags have been addressed, and the details of the relevant transaction.

VI. Ongoing Monitoring/Look Back

Each Creditinfo Company shall implement procedures to periodically monitor and refresh due diligence on customers, suppliers, agents, distributors, introducers, joint venture partners, and other third parties on a risk-appropriate basis.

VII. Record-Keeping—Screening

Records reflecting the result of screening searches must be maintained in the sharepoint system for the relevant Creditinfo market. This includes records of all approvals under the Sanctions Procedure, or decisions not to proceed. Records should be kept for 5 years, unless you think the information may be required for legal proceedings or where you have knowledge or suspicion of money laundering or terrorist financing or potential Sanctions breaches, in which case it must be retained.

VIII. Reporting Concerns

If any Group Employee has a suspicion, arising in the context of their work for Creditinfo, that money laundering or a Sanctions violation may have taken place, this should be reported immediately to that individual's line manager or direct report. The line manager or direct report must then report the matter to the local in-house counsel or compliance function and to Creditinfo Group's General Counsel.

The Group has also implemented a Whistleblowing Policy to enable Creditinfo Employees to highlight concerns (a non-exhaustive list is described in the policy), whilst protecting Creditinfo Employees from victimisation by their employer. It provides guidance for dealing with these and other whistleblowing issues in a safe and constructive way. It encourages Creditinfo Employees to raise concerns internally in the first instance. For further detail refer to the Whistleblowing Policy.

IX. Training

Sanctions and AML training forms part of annual compliance training provided to all employees.

Creditinfo will arrange enhanced training for employees as appropriate and on a risk-based basis, which will include more in depth training for compliance team and for senior local, regional and Group management and those with core roles in finance, procurement and sales.

Contact Information

Group Compliance Department

compliance@creditinfo.com

Group Executive team

ci.group.directors@creditinfo.com