Confidential Information Management Policy

Scope Group

April 2021

1. Introduction

While conducting its business activities, Scope SE & Co. KGaA and its subsidiaries (hereinafter also referred to as “Scope” or “Scope Group” and including Scope CRAs) may be exposed to Confidential Information regarding Scope or regarding issuers, investors and other parties. Scope has established the Confidential Information Management Policy to set forth requirements related to the handling and management of such Confidential Information.

Scope and its Employees will protect Confidential Information by imposing restrictions on the disclosure and use of Confidential Information. Scope will also protect Confidential Information from being disclosed in publications, at conferences or outside events, or in conversations with investors, other issuers, other persons, or otherwise.

2. Applicability

This Policy and its requirements apply to all Employees. Associated individuals must acknowledge to abide by this policy.

The contents of this Policy and any future updates or changes are published on Scope’s website and are made available on Scope’s intranet.

Note:

For defined terms used in this Policy please see Scope Defined Terms Glossary that is available on Scope’s website and intranet.

3. Handling Confidential Information / the “need to know” principle

In accordance with Scope’s Code of Ethics, Employees are required to treat all Confidential Information on Scope, its clients and Employees ethically, with discretion and in line with applicable laws, rules and regulations. Employees must handle Confidential Information with care to ensure such information is used only for the legitimate business purposes.

Employees who have access to Confidential Information are not permitted to use or share that information for purposes of trading Securities or for any other purpose except the conduct of Scope’s business. Insider trading (or dealing) laws and regulations globally prohibit buying or selling a company’s Securities while in possession of Material Non-Public Information about that company. Employees can also violate these laws by disclosing Material Non-Public Information to another person. If an Employee makes such a disclosure or use such information, this Employee can be punished, even if this Employee stands to make no financial gain.

Scope has adopted procedures to establish effective information barriers and to protect Scope and its Employ- ees from legal, regulatory and reputational risks. Access to Confidential Information is restricted to authorized persons who should be aware of their confidentiality obligations and who have signed confidentiality agreements where required by Scope.

Employees at Scope are required to discuss Confidential Information and/or to disclose it only to those people who have a legitimate business need to know such information. The “need to know” principle applies to information sharing between Employees and third parties as well as to information sharing within Scope and different teams or department/divisions.

While handling Confidential Information, each Employee is responsible to ensure adequate protection against unauthorized access by third parties. Further, Employees are required to protect Scope’s devices and data.

For communications with the media and other external parties reference is made to Scope’s “Group Communications Procedures” for further guidance.

If Confidential Information and/or Material Information has been disclosed to any unauthorized person, such disclosure should be reported immediately to Senior Management and for Scope CRAs’ to Compliance for further action.

4. Information systems

Scope uses distinct information technology storage platforms for maintaining and processing data as part of its daily business activities. Requests for access to specific drives or sub-folders needs to be approved by the relevant authorized employee.

Remote access to Scope systems and servers from outside the offices is granted on an individual basis. Any Employee or designated person who is granted remote access privileges must remain constantly aware that connections between their location and Scope are literal extensions of Scope’s corporate network, and that they provide a potential pathway to the Scope's most

sensitive information. The Employee and/or designated person must take every reasonable measure to protect Confidential Information.

On a regular basis, a review of system access rights will be conducted to ensure access to specific data storage networks is limited to Employees who have a legitimate need for such system access.

5. Data Protection

Scope has implemented systems and technical solutions to prevent impairment of privacy rights of Employees or clients through the handling of their personal data, as defined by the German Laws, in particular the German Bundesdatenschutzgesetz (“BDSG”). Scope is taking all reasonable measures to ensure that personal data is processed and used within the limits of the permissions granted by the Employee or client and with his or her explicit consent.

Scope employs technical solutions to allow the identification and review of events where data stored on Scope’s platforms has been added, modified or deleted, and by which user.

6. Violation of this policy

Employees must immediately report violations or suspected violations of this Policy to their manager, and for Scope “CRAs’ Employees to Compliance.

Any action by Scope or by any Employee which violates, or might reasonably be expected to lead to or result in a violation of, the provisions set forth in this Policy is strictly prohibited and can result in disciplinary action, up and including, termination of employment. Any potential infringements of these requirements will be inves- tigated and reported to Senior Management to determine appropriate intervention.

Scope Management will be responsible for the implementation and the enforcement of this policy.

Scope SE & Co. KGaA
Lennéstraße 5
D-10785 Berlin
info@scopegroup.com

Scope Ratings GmbH
Lennéstraße 5
D-10785 Berlin
info@scoperatings.com

Scope Ratings UK Limited
111 Buckingham Palace Road
UK-London SW1W 0SR
info@scoperatings.com

Scope Hamburg GmbH
Stadthausbrücke 5
20355 Hamburg
info@scopehamburg.com

Scope ESG Analysis GmbH
Lennéstraße 5
D-10785 Berlin
esg@scopegroup.eu

Scope Analysis GmbH
Lennéstraße 5
D-10785 Berlin
info@scopeanalysis.com

Scope Investor Services GmbH
Lennéstraße 5
D-10785 Berlin
info@scopeinvestors.com

www.scopegroup.com
www.scoperatings.com
www.scopehamburg.com
www.scopeanalysis.com
www.scopeinvestors.com