Confidential Information Management Policy

December 2022

Confidential Information Management Policy

Scope Group

Start Date:	30/12/2022	End date:	Version:	2.0

Applies to:	Entities affected by:
☒ **All Employees**	☒ Scope SE & Co. KGaA ☒ Scope Ratings GmbH ☒ Scope Ratings UK Ltd. ☐ Scope Hamburg GmbH ☒ All existing and future subsidiaries and affiliates of the above

☒ This document and any future updates or changes are made available on Scope's Intranet.

☒ This document and any future updates or changes are made available on Scope's website.

☒ This document contains defined terms made available in the Defined Terms Glossary available on Scope's intranet.

☒ This document contains defined terms made available in the Defined Terms Glossary available on Scope's website.

Table of Contents

1. Preamble

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[1] 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.

This Policy does not cover:

i. Information shared with media, which is covered by Scope Group Communications Procedures

ii. Material Non-Public Information, which is covered by the Personal Accounts Dealing Policy and Procedure, or

iii. The sharing of commercial information with Analytical Personnel by other Employees, which is covered by the Commercial Separation Policy.

2. Defined terms

Scope non-CRAs: means entities of Scope group which are not registered credit rating agencies nor subsidiaries or affiliates of registered credit rating agencies.

Analytical Information: means Non-public information received or created for the performance of Credit Rating Activities or Ancillary Services, encompassing:

- Non-public information received from Clients and defined as confidential under an agreement with the Client
- Non-public information identifying a person or legal entity as a Client
- Information regarding a pending Credit Rating or Ancillary Service
- Information regarding the credit rating analysis or assessment process

It is a sub-category of Confidential Information of especially sensitive nature .

3. Handling Confidential Information

3.1 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 legitimate business purposes.

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 Group.

3.2 Prohibition from using Confidential Information for personal 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.

[1] This term is defined in Scope Group Defined Terms Glossary

3.3 Individual confidentiality obligations

Employees are required to use Scope's email system and are not permitted to use their personal accounts for electronic transmission of information related to their responsibilities at Scope. Employees are required to store electronic confidential business data, information and records exclusively on Scope's systems and network and are not permitted to use private electronic devices to store, transmit or record confidential business information, data and/or records.

Confidential Information should not be discussed in places where the discussion may be overheard.

Confidential Information should not be displayed on computer screen when visible from unauthorized people. Computers should be locked and set to screen saver mode when left unattended.

Confidential Information in hard copy may not be left unattended in common rooms, or at Employees' desks for a long period of time, should not be copied unless necessary, and when relevant should be kept locked or disposed of using designated bins.

3.4 Protection against unauthorized access

Employees are responsible for protecting Confidential Information used and/or stored on their system accounts against access by unauthorized third parties. Employees are also required to keep their personal access details to Scope's systems, such as passwords, confidential and must not share them with management and/or any other Employee as well as external parties. Further, Employees are required to protect Scope's devices and data.

Employees who work from a location that is not part of Scope's business premises are required to act with the same diligence and care in performing business tasks as on site at Scope's office premises and must take every reasonable measure to protect Confidential Information.

4. Corporate interactions

Legal entities which are part of Scope Group are separated legally and operationally. Employees of Scope Group who belong to different entities do not share information with each other except in the following circumstances:

- The exchange is necessary to perform an outsourcing agreement between Scope group entities
- Each recipient has a need-to-know for the information shared
- The exchange is between Employees of Scope CRAs and is necessary for the performance of Credit Rating Activities or Ancillary Services

4.1 Information sharing between Scope CRAs and Scope non-CRAs

Scope CRAs and its Scope-Non-CRAs may share Confidential Information or otherwise interact with each other where there is a valid business reason for doing so (i.e., need to know) and the interaction does not interfere with or compromise the integrity and independence of Scope CRAs credit rating activities, see section 4.2 'Waivers' below.

Scope CRAs and Scope Non-CRAs may enter into contractual arrangements for the provision of services and the licensing of products, services, and other intellectual property from one entity to the other. The terms of these agreements may permit certain types of information sharing, including Analytical Information.

Scope CRAs and Scope Non-CRAs may not otherwise share Analytical Information.

Employees of Scope CRAs and Scope Non-CRAs may not be granted accesses which would result in the sharing of Analytical Information.

4.2 Waivers

When there is a need-to-know for the sharing of Analytical Information between Scope CRAs and Scope Non-CRAs, and no contractual arrangement is in place, it must be communicated to Compliance. If appropriate, Compliance will provide a waiver.

Analytical Information may not be shared between Scope CRAs and Scope Non-CRAs before the waiver has been granted by Compliance.

5. Communication with external parties regarding Credit Rating Activities

Employees participating in investor calls or other speaker forums must be prepared to support their analyses without revealing Confidential Information.

Employees may not release any portion of any issuer file to any third party without the express consent or direction of the relevant issuer, unless otherwise determined by management.

6. Accidental disclosure of Confidential Information

If Confidential Information has been disclosed to any unauthorized person, such disclosure should be reported immediately to Senior Management and for Scope CRAs' to the respective Compliance department.

7. Information systems and Data Protection

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 tools are made in accordance with the Identity and Access Management Policy. On a regular basis, the IT department in coordination with the Compliance function conduct reviews of system access rights to ensure access to specific data storage networks is limited to Employees who have a legitimate need for such system access.

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 GDPR. Scope is taking all reasonable measures to ensure that personal data is processed and used within the limits of the legal basis for their processing, including but not limited to legal and regulatory obligations, performance of work contracts or contracts with clients, consent from Employees or clients when not covered by the previous basis.

Compliance with this Policy and requirements regarding breaches

This Policy reflects the way Scope implements regulatory requirements.

If case of questions about this Policy or any doubt as to employees' obligations under this Policy, guidance should be sought from Compliance.

Breach of this Policy may lead to breach of regulatory obligations applying to Scope. As a result, any action by employees to whom this Policy applies which breaches or might reasonably be expected to lead to or result in a breach, 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 investigated and reported to Senior Management to determine appropriate intervention.

Employees must immediately report breaches or suspected breaches of this Policy to Compliance.