



Record Keeping Policy

September 2022



Record Keeping Policy

Scope CRAs

Start Date: 01/09/2022	Version: 1.0
Applies to:	Entities
<input checked="" type="checkbox"/> All covered employees <input checked="" type="checkbox"/> All Departments of Scope's CRAs and outsourced Functions	<input checked="" type="checkbox"/> Scope SE & Co. KGaA <input checked="" type="checkbox"/> Scope Ratings GmbH <input checked="" type="checkbox"/> Scope Ratings UK Ltd. <input type="checkbox"/> Scope Hamburg GmbH <input checked="" type="checkbox"/> All existing and coming subsidiaries and affiliates of the above
<input checked="" type="checkbox"/> This document and any future updates or changes are made available on Scope's Intranet.	
<input checked="" type="checkbox"/> This document and any future updates or changes are made available on Scope's website.	
<input checked="" type="checkbox"/> This document contains defined terms made available in the Defined Terms Glossary available on Scope's intranet and Scope's website.	

Table of Contents

1. Preamble	3
2. Defined Terms	3
3. Principles	3
4. Retention of Business Records	3
4.1 Records to be kept for Credit Rating activities	3
4.2 Other Business Records	4
4.2.1 Commercial Documentation	4
4.2.2 Tax-relevant Documentation	4
4.2.3 Corporate Documentation	4
4.2.4 HR Documentation	4
4.2.5 Information Technology and Information Security	4
5. Disposal of Business Records	4



Record Keeping Policy

Scope CRAs

1. Preamble

This Record Keeping Policy (the "Policy") sets out the principles and standards for Business Records that have to be created and/or retained by all Covered Employees of Scope Ratings and its outsourced functions Scope Group in order to maintain appropriate documentation in line with legal and regulatory requirements that Scope Group is subject to.

2. Defined Terms

Business Records are all records (hard copy or digital) that records an act, condition or event related to the business.

3. Principles

Scope will arrange for adequate Business Records and, where appropriate, audit trails of its Credit Rating activities to be created, retained, or disposed, as required according to the regulations and laws applicable to Scope. Business Records will be retained in accordance with Scope Record Keeping Procedure and its related Record Keeping Appendix.

Business Records will be kept either at Scope's business premises or be filed in electronic form in a manner that such Business Records can be retrieved and made available in a readable format promptly upon request. For all Business Records that are retained electronically, including emails and instant messages, backup files and audit trails will be created to protect against data loss in accordance with Scope's Record Keeping Appendix.

It is generally prohibited to destroy, damage, or alter Scope's Business Records that are not drafts or working papers unless the retention period has expired.

Managers are obliged to oversee that staff are aware of and adhere to the requirements under this Policy and will assign record keeping responsibilities in their area of responsibility in accordance with the Record Keeping Appendix.

All external and internal electronic written communications in relation with Credit Rating Services and Ancillary Services including analytical and commercial correspondence must be done by e-mail and it is not permitted to use any other electronic communications systems or chatrooms (Skype chat, MS teams, etc.).

Employees are required to use Scope's systems provided only for the processing, filing and retention of Business Records and are not permitted to save or store any Business Records on, or transfer these to any private electronic devices (e.g., private computers, memory sticks, or otherwise).

Employees are not permitted to use their personal email accounts or other exchange applications to handle business correspondence, nor to forward Business Record to their personal email address unless formally instructed by Scope Management or People & Organization department.

4. Retention of Business Records

4.1 Records to be kept for Credit Rating activities

Records for regulated activities will be created and retained as required by the relevant regulations.

Scope CRAs mandatory business records include:

- a) For each Credit Rating Action and Credit Rating outlook action:
 - The identity of the rating analysts participating in the determination of the Credit Rating or Credit Rating outlook;
 - The identity of the persons who have approved the Credit Rating Action;
 - Information as to whether the Credit Rating was solicited or unsolicited, and
 - The date on which the Credit Rating action was taken.
- b) Record of the deliberations that lead to the Credit Rating Action;
- c) The account Records relating to fees received by Scope from any rated entity or related third party or any user of Credit Ratings;
- d) The account Records for each subscriber to Scope Ratings' Credit Ratings or related services;

- e) The Business Records documenting the established procedures and rating methodologies used by Scope Ratings to determine Credit Ratings;
- f) The internal Business Records and files, including non-public information and work papers, used to form the basis of any Credit Rating Action taken by Scope Ratings;
- g) Credit analysis reports, credit assessment reports and private Credit Rating reports and internal Business Records, including non-public information and work papers, used to form the basis of the opinions expressed in such reports.
- h) Business Records of the procedures and measures implemented by Scope Ratings to comply with the relevant CRA Regulation; and
- i) Copies of internal and external communications, including electronic communications, received and sent by Scope and its employees, that relate to Credit Rating activities.

4.2 Other Business Records

4.2 Other Business Records will be received, created and maintained in accordance with legal obligations applicable to Scope, as detailed below:

4.2.1 Commercial Documentation

In accordance with applicable laws and regulations, commercial documentation is subject to a retention period of ten years, unless a longer period is required.

4.2.2 Tax-relevant Documentation

In accordance with applicable laws and regulations, tax-relevant documentation is subject to a general retention period of ten years after the end of the business relationship, unless a longer period is required.

4.2.3 Corporate Documentation

Corporate Documentation is subject to an indefinite retention period, except when stipulated otherwise in the Record Keeping Procedure.

4.2.4 Employee relevant Documentation

Employee relevant documentation, as specified in the Record Keeping Procedure, is subject to a general retention period of ten years.

4.2.5 Information Technology and Information Security

Information Technology and Information Security related documents are subject to a general retention period of five years.

5. Disposal of Business Records

Business Records must be disposed of once the retention period, as stipulated in the Record Keeping Appendix and Record Keeping Procedures, has expired, unless such records are subject to an investigation, complaint, dispute or litigation. In such cases, the relevant document will be retained for the period necessary until such investigation, complaint, dispute or litigation has concluded.

In case of any document containing personal data, the retention period and disposal requirements are determined by the applicable general data protection laws and regulations.



Record Keeping Policy

Scope CRAs

Compliance with this Policy and requirements regarding breaches

This Policy reflects the way Scope CRAs 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 CRAs. 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.