Consultation Paper

Draft technical standards on the application for registration as a securitisation repository under the Securitisation Regulation

Responding to this paper

ESMA invites comments on all matters in this paper and in particular on the specific questions summarised in Annex 1. Comments are most helpful if they:

respond to the question stated;

indicate the specific question to which the comment relates;

contain a clear rationale; and

describe any alternatives ESMA should consider.

ESMA will consider all comments received by **23 May 2018.**

All contributions should be submitted online at www.esma.europa.eu under the heading 'Your input - Consultations'.

Publication of responses

All contributions received will be published following the close of the consultation, unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publically disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with ESMA's rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESMA's Board of Appeal and the European Ombudsman.

Data protection

Information on data protection can be found at www.esma.europa.eu under the heading Legal Notice.

Who should read this paper

This Consultation Paper may be of particular interest to securitisation market infrastructures, investors/potential investors, securitisation issuers, as well as public bodies involved in securitisations (market regulators, resolution authorities, supervisory authorities, and standard setters).

Table of Contents

Acronyms and definitions used

ABCP	Asset-Backed Commercial Paper
ABS	Asset-backed security
CRA	Credit Rating Agencies
EBA	European Banking Authority
EMIR	European Market Infrastructure Regulation (Regulation (EU) 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories)
ESMA	European Securities and Markets Authority
ESMA Regulation	Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC, as amended.
ESRB	European Systemic Risk Board
EU	European Union
ITS	Implementing Technical Standards
ISO	International Organization for Standardization
LEI	Legal Entity Identifier
RTS	Regulatory Technical Standards
SFI	Structured Finance Instrument
Securitisation Regulation	Regulation (EU) 2017/2402 of the European Parliament and of the Council laying down common rules on securitisation and creating a European framework for simple, transparent, and standardized securitisation and amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, and Regulations (EC) No 1060/2009 and (EU) No 648/2012
SFTR	Securities Financing Transactions Regulation (Regulation (EU) 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse and amending Regulation (EU) No 648/2012)
SSPE	Securitisation Special Purpose Entity

SWIFT	Society for Worldwide Interbank Financial Telecommunication

1 Executive Summary

Reasons for publication

The Securitisation Regulation was published in the Official Journal of the European Union on 28 December 2017 and has entered into force 20 days after its publication. The Regulation requires the European Commission to adopt delegated acts in a number of areas.

ESMA is mandated to draft Regulatory Technical Standards covering the contents of the application to be submitted to ESMA by firms seeking to provide repository services to originators, sponsors, and/or SSPEs. ESMA is furthermore mandated to draft Implementing Technical Standards outlining the format of this application. ESMA is mandated to submit these draft standards to the Commission by 12 months from the date of entry into force of the Securitisation Regulation.

Contents

Section 2.1 presents ESMA's legal mandate and accompanying background, including the relevant EMIR and SFTR requirements for trade repositories. Some initial considerations are provided, including recalling that ESMA will register securitisation repositories and supervise their continued compliance with the Regulation.

Next, section 2.2 presents the proposed general arrangements for information to be submitted by a candidate securitisation repository, in line with the arrangements set out in Article 78 of EMIR. These proposals include the receipt of information on the securitisation types (ABCP or non-ABCP), risk transfer methods (true sale or synthetic), and underlying exposure types (residential mortgage, commercial mortgage, corporate, leasing, consumer, auto loan/lease, credit card, other) for which the applicant wishes to be registered. In addition, ESMA proposes that an application should provide adequate assurance that the candidate repository will be objective, impartial, and independent when interacting with market participants. This involves obtaining information on the applicant's arrangements regarding conflicts of interest, as well as the applicant's financial position and the profile of its management body. ESMA also considers it necessary to receive information on the applicant's internal controls and ability to ensure its compliance with regulatory requirements, as well as comprehensive information on the applicant's organisational ownership, organisational structure, and provision of ancillary services. This also extends to obtaining details on the applicant's user access arrangements, as well as the prices and fees charged by the applicant.

Section 2.3 contains ESMA's proposed requirements regarding information on applicants' operational arrangements, in line with Article 79 of EMIR. The proposals cover information on the applicant's arrangements to mitigate operational risk, as well as its disaster recovery and data backup (record-keeping) preparations. Other key procedures of interest to ESMA

are the applicant's arrangements for verifying the completeness and consistency of the securitisation standardised reporting templates' contents, calculating data completeness scores, and producing end-of-day reports. ESMA's interest also extends to an applicant's information technology system, including its investment and renewal policies and any outsourcing arrangements entered into by the applicant to provide securitisation repository services. Lastly, ESMA considers it important to understand how the securitisation repository's user arrangements ensure a smooth process for users to extract and process the information necessary for them to fulfil their tasks and obligations under the Securitisation Regulation.

Section 2.4 touches on the applicant's data safeguarding arrangements, with reference to Article 80 of EMIR. The proposals include requirements for the applicant to demonstrate its safeguards against the illegitimate use of information it hosts and produces, as well as the applicant's arrangements for recording data and enabling timely access for reporting entities to correct or modify their data submissions.

Section 2.5 discusses ESMA's proposals regarding the simplified application to be submitted by firms already registered as trade repositories. In ESMA's view, a number of pieces of information have already been provided and need not be re-submitted, thereby simplifying the necessary efforts for existing trade repositories to prepare an application to become a securitisation repository. This includes information on the applicant's organisational structure, on its internal corporate governance policies and processes, information on its management and board members, its financial report and business plans, as well as certain data safeguarding arrangements.

Section 2.6 sets out ESMA's proposed ITS for the securitisation repository application. In this section, ESMA proposes that applicants include a unique reference number to each document submitted. Moreover, ESMA proposes that the information submitted clearly identifies which specific requirement of the draft RTS is being referred to. Finally, ESMA proposes that the applicants be required to justify when the information is not submitted as outlined in the document references section of the Annex to the draft ITS. Arrangements for the simplified application for existing trade repositories are also discussed.

Section 2.7 discusses draft Guidelines for ensuring the orderly substitution of information between securitisation repositories, should the applicant cease (or no longer be authorised) to provide securitisation repository services. The draft Guidelines are similar to ESMA's Guidelines on data portability for trade repositories, which were published in 2017.

Lastly, the full text of the draft RTS is contained in Annex IV (section 3.4), the accompanying draft ITS can be found in Annex V (section 3.5), and the draft Guidelines are in Annex VI (section 3.6).

Next Steps

ESMA will consider the feedback it receives to this consultation in Q2/Q3 2018 and expects to publish a final report and submission of the draft technical standards to the European Commission for endorsement in Q3/Q4 2018.

2 Contents

1. Regulation (EU) 2017/2402 of the European Parliament and of the Council laying down common rules on securitisation and creating a European framework for simple, transparent, and standardized securitisation and amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, and Regulations (EC) No 1060/2009 and (EU) No 648/2012 ('the Securitisation Regulation') was published in the Official Journal of the European Union on 28 December 2017.

2. As set out in the Securitisation Regulation, the European Securities and Markets Authority is obliged to submit, within six and twelve months of entry into force of the Regulation, proposed delegated acts to the European Commission ('the Commission') for adoption.

3. The Securitisation Regulation confers a pivotal role on securitisation repositories, who will help foster transparency in securitisation markets and will be relied upon by all types of investors, public entities, and reporting entities to meet their respective obligations under the Securitisation Regulation. Having access to all details of securitisations is of utmost importance for both investors, potential investors, and public authorities to ensure compliance with the obligations stemming from the Securitisation Regulation.

4. As set out in the Regulation, ESMA will register securitisation repositories and supervise their continued compliance with the Regulation, as well as the draft RTS/ITS contained in Annexes IV and V (sections 3.4 and 3.5, resp.) to this document (once adopted by the Commission). The proposed contents of the draft RTS/ITS have been structured to reflect ESMA's views on what information will enable ESMA to effectively assess a securitisation repository. ESMA has based the proposed information requirements in the draft RTS/ITS on its experiences of performing similar supervisory tasks for trade repositories under EMIR (and under SFTR), as well as from supervising CRAs, while also taking into account the specificities of securitisation products and the Securitisation Regulation.

5. Lastly, the draft texts in this document (Annexes IV, V, and VI, i.e. sections 3.4, 3.5, and 3.6, resp.) occasionally refer and mention "the disclosure RTS", "the disclosure RTS", and/or "the operational standards RTS". For the avoidance of doubt, these references relate to the respective draft legal texts set out and discussed in ESMA's recent Consultation Paper entitled "Draft technical standards on disclosure requirements, operational standards, and access conditions under the Securitisation Regulation".[1]

2.1 Legal mandate and Background

6. Article 10(7)(b)-(c) of the Securitisation Regulation requires ESMA to submit, by 18 January 2019, draft RTS specifying the application procedures for repositories to be registered by ESMA, while also taking into account whether a securitisation repository is already registered as a trade repository for the purposes of EMIR and/or SFTR[2].

---

[1] Available at https://www.esma.europa.eu/sites/default/files/library/esma33-128-107_consultation_paper_disclosure_and_operational_standards_0.pdf

[2] Under Title VI, Chapter 1 of Regulation (EU) No 648/2012 or under Title I, Chapter III of Regulation (EU) No 2365/2015

7. Pursuant to Article 10(2) of the Securitisation Regulation, a securitisation repository must meet the requirements for trade repositories specified in Articles 78, 79, and 80(1) to (3), (5) and (6) of EMIR. These articles cover, respectively:

   (a) General requirements: including robust governance arrangements, effective management of conflicts of interest, policies and procedures to ensure compliance with the Securitisation Regulation, adequate organisational structure to ensure business continuity, operational separation of ancillary services, good repute and experience of the senior management and board, provision of non-discriminatory access, and disclosure of prices and fees charged;

   (b) Operational reliability: including appropriate systems, controls, and procedures to minimise operational risk; appropriate business continuity and disaster recovery arrangements; and appropriate data substitution arrangements in the event that registration is withdrawn; and

   (c) Data safeguarding and recording: including confidentiality, integrity, and protection of information received; use of data received for commercial purposes; recording of data and of data modifications; enabling timely access for correcting data; and prevention of misuse of information maintained in the repository's systems.

8. Furthermore, Article 10(8) of the Securitisation Regulation requires ESMA to develop draft ITS specifying the format of the application, while avoiding duplication of procedures for already-registered trade repositories.

9. ESMA has set out the draft RTS and ITS provisions with a view to ensuring that applicants are able to comply with the above-mentioned requirements in EMIR and the Securitisation Regulation. Furthermore, pursuant to the Securitisation Regulation Article 10(8), ESMA has explicitly set out the additional information that already-registered TRs should provide in order to demonstrate compliance with these Articles, to the extent that such information is not already available to ESMA from earlier applications as per EMIR or SFTR.

10. Lastly, as per Article 10(4) of the Securitisation Regulation, already-registered securitisation repositories shall, without undue delay, notify ESMA of any material changes to the conditions for registration. The same considerations apply to already-registered trade repositories, as per Article 14(4) of EMIR and Article 5(4) of SFTR.

2.2 General requirements (Article 78 of EMIR)

11. As part of its confirmation of an applicant's compliance with the general requirements set out in Article 78 of EMIR, ESMA considers it important to obtain certain initial items of information on the applicant firm. This information includes confirmation from the applicant that its articles of incorporation and, where relevant, other statutory documentation state that the applicant shall provide securitisation repository services, and also information on the securitisation types (ABCP or non-ABCP), risk transfer methods (true sale or synthetic), and underlying exposure types (residential mortgage, commercial mortgage, corporate,

leasing, consumer, auto loan/lease, credit card, other) for which the applicant wishes to be registered.[3]

12. Pursuant to Article 78(1) of EMIR, ESMA also deems it necessary to receive comprehensive information on the applicant's organisational ownership and organisational structure. Such items will facilitate ESMA's understanding of actual and potential conflicts of interest, the operational remoteness of non-repository related services, and the presence of well-defined, transparent and consistent lines of responsibility. Such items will also assist ESMA in assessing whether, pursuant to Article 78(4) of EMIR, the organisational structure of the applicant ensures the continuity and orderly functioning of the securitisation repository.

13. By virtue of their central role in receiving information and providing information to numerous market participants and public authorities, securitisation repositories will form a key pillar of the Securitisation Regulation's implementation. Securitisation repositories must therefore be objective, impartial, and independent when interacting with market participants covered by the Securitisation Regulation and its accompanying proposed delegated acts.

14. In line with Article 78(2) of EMIR, ESMA thus considers it essential that there is full reassurance that both actual and potential conflicts of interest are being sufficiently identified, managed, mitigated, and disclosed by an applicant, and that the application demonstrates that staff are aware of the policies and procedures put in place to achieve this. ESMA also proposes to require information to be provided on the applicant's financial position, as evidenced by revenue streams and financial statements, as well as the independence, good repute, and integrity of the applicant's management body (also to assess the applicant's compliance with Article 78(6) of EMIR).

15. In addition, and in line with Article 78(3) of EMIR, ESMA expects that an applicant should have sufficient internal controls, with clear lines of responsibility, to provide reassurance that compliance with the requirements set out in both the Securitisation Regulation and the draft RTS are being adhered to at all times. Indeed, the Securitisation Regulation and its accompanying proposed delegated acts contain a number of detailed requirements for securitisation repositories, including verifying the completeness and consistency of the detailed transparency templates' contents, aggregating information received, producing end-of-day reports, providing direct and immediate access to specific user groups, and interacting with reporting entities based on their data submissions. Therefore, ESMA considers it important that the applicant provides convincing evidence on its arrangements to monitor how its staff and systems are complying with these regulatory requirements.

16. Moreover, obtaining information on the breadth of the applicant's services will help ESMA assess their compliance with Article 78(5) of EMIR. To this end, ESMA proposes that an applicant shall provide a description of the ancillary or non-securitisation services that the applicant or its parent group performs or plans to perform. Equally, ESMA proposes that an applicant should provide a description of any agreement that the firm may have with companies offering securitisation related services, as well as copies of such agreements. Furthermore, in ESMA's view, the applicant should set out its procedures and policies that

---

[3] To facilitate reporting entity and user awareness of this information, ESMA's website will indicate the underlying exposure classes, risk transfer types, and securitisation types for which a securitisation repository has been registered.

will ensure the adequate level of operational separation in terms of resources, systems, information and procedures, between the applicant's securitisation repository services under the Securitisation Regulation and other business lines.

17. At the same time, ESMA also believes that it is important, for supervisory purposes, to receive detailed information on the applicant's data access arrangements. Such information will help assess the applicant's compliance with EMIR Article 78(7)'s provisions on non-discriminatory access (including to third-party service providers[4]) and with the Securitisation Regulation's Article 17(2) text on direct and immediate access to specific entities. Insofar as different access arrangements are set out by the applicant for entities listed in Article 17(1) of the Securitisation Regulation (ESMA, EBA, EIOPA, ESRB, the ESCB, national supervisory/competent authorities, national resolution authorities, the SRB, as well as investors and potential investors), ESMA proposes that an applicant should provide details of each access arrangement per user group.

18. Further proposed requirements for data access are also set out in ESMA's draft RTS on operational standards and data access. In the present document, ESMA also proposes to require applicants to set out their procedures to make available the additional information that they produce based on securitisation data received.[5] Lastly, the present RTS proposes information requirements for applicants to demonstrate how 'direct and immediate' access requirements[6] are complied with.

19. Lastly, in line with Article 78(8) of EMIR, ESMA is of the view that precise details on the pricing and fees charged by the applicant for securitisation repository services should be provided at the time of application. Such information is needed to assess the applicant's compliance with the Securitisation Regulation's stipulation[7] that access to a number of specific user types should be direct, immediate, and free of charge. Moreover, in line with Article 78(8), information on pricing and fees charged by the applicant will assist ESMA to confirm that the prices and fees charged by the applicant are "cost-related"[8]. ESMA further believes it would be important, for supervisory purposes, to receive evidence that the prices and fees charged by the applicant are non-discriminatory.

Q 1: Do you agree with the general requirements proposed in the draft RTS? Do you have any further suggestions? If yes, please provide also the reasoning.

---

[4] Such as data analytics companies that obtain information from securitisation repositories and integrate this information in their own products.

[5] For example, as regards the data completeness score and end-of-day reports produced by the repository.

[6] This refers to the provisions in Article 17(2)(d) of the Securitisation Regulation, which stipulates that ESMA should specify, in an RTS, the terms and conditions under which specific entities referred to in the Regulation are to have direct and immediate access to data held in securitisation repositories. In its draft RTS and Consultation Paper handling these provisions, ESMA sets out its interpretation of 'direct and immediate', which in ESMA's view provides for a sufficiently-short turnaround time for users to rapidly obtain the necessary information (see section 2.2.5.1 of https://www.esma.europa.eu/sites/default/files/library/esma33-128-107_consultation_paper_disclosure_and_operational_standards_0.pdf)

[7] Article 17(1)

[8] Article 78 of Regulation (EU) No 648/2012

2.3 Operational reliability (Article 79 of EMIR)

2.3.1 General considerations

20. ESMA believes it would be important, for supervisory purposes, to receive reassurance that an applicant's organisational structure is conducive to the smooth functioning of securitisation repository-related services required under the Securitisation Regulation and the accompanying proposed delegated acts. As mentioned above, the Securitisation Regulation and its accompanying proposed delegated acts contain a number of detailed requirements for securitisation repositories, including verifying the completeness and consistency of the detailed transparency templates' contents, producing end-of-day reports, providing direct and immediate access to specific user groups, and interacting with reporting entities based on their data submissions. These requirements in turn necessitate extensive and robust operational arrangements by applicants, also with a view to mitigating operational risk and the financial consequences in case of materialised operational risks.

21. Therefore, in line with Article 79(1) of EMIR, ESMA proposes that an application for registration as a securitisation repository should contain information on the applicant's resources (financial, human, technical) and procedures to identify and mitigate operational risks, including a copy of any relevant policies, methodologies, internal procedures and manuals. Furthermore, an application should describe the financial resources available to cover potential losses due to operational risks materialising.

22. In relation to Article 79(2) of EMIR, ESMA proposes to receive detailed information on the applicant's business continuity plan and disaster recovery arrangements. Such information would include an identification of the applicant's business processes, resources, escalation procedures and related systems which are critical to ensuring the securitisation repository services of the applicant, including any relevant outsourced service and including the applicant's strategy, policy and objectives towards the continuity of these processes. Clarity on the applicant's periodic testing programme and the results and follow-up actions resulting from any tests are also proposed to be required, in order to help gauge the applicant's efforts to adapt itself to a variety of possible scenarios. ESMA considers it important to also ensure that the business continuity plan describes alternative technical and operational sites available, and more generally the applicant's arrangements to manage crises and recover its systems.

23. ESMA also believes it important, for supervisory purposes, to receive the detailed procedures used by the applicant to perform specific actions on the securitisation information received from reporting entities. In particular, the applicant should provide its procedures for verifying the completeness and consistency of the securitisation standardised reporting templates' contents, calculating data completeness scores, producing end-of-day reports, and handling historical data[9].

24. Furthermore, (also in relation to EMIR Article 78(4)) ESMA considers it crucial to receive a detailed description of the applicant's information technology system, to enable ESMA to

---

[9] Pursuant to Recital 12 of the Securitisation Regulation, which states the necessity of ensuring that investors and potential investors 'have access to all the relevant information over the entire life of the securitisation.'

consider the applicant's capabilities to host the various securitisation types (true sale or synthetic; ABCP or master trust or standalone), underlying exposure classes, as well as the volume of information contained in particular in the draft templates set out in ESMA's proposed RTS on disclosure[10]. In ESMA's view, information should be provided on the investment and renewal policies and procedures on information technology resources of the applicant, as well as the outsourcing arrangements entered into by the applicant to provide securitisation repository services.

25. In addition, ESMA deems it necessary to obtain, as part of the applicant's application package, reassurance that the securitisation repository has taken the necessary steps towards providing a smooth process for users to extract and process the information necessary for them to fulfil their tasks and obligations under the Securitisation Regulation. Therefore, ESMA proposes that applicants should provide a copy of any user manual explaining how to access, extract, and use information (including historical information) hosted by the securitisation repository, and also including internal procedures to provide services to the relevant users. Similarly, ESMA proposes that a copy of the reporting manual used to guide reporting entities also be included in an application for registration.

Q 2: Do you agree with the operational reliability provisions set out in the draft RTS? Do you have any further suggestions?

2.3.2 Demonstration of compliance with RTS and ITS on disclosure requirements and operational standards

26. Elsewhere, the need for applicants to demonstrate adequate operational capacity is driven not only by the content, but also the format, of the securitisation information to be received and made available by applicants. In this regard, ESMA recalls that its proposed draft RTSs on disclosure and operational standards[11] include provisions on the use of ISO 200222 and, within this, XML as a common format for the reporting templates.

27. As set out therein[12], and in line with Article 17(2)(b) of the Securitisation Regulation, ESMA's proposals aim to enable securitisation repositories to collect data in a timely, structured, and comprehensive manner. Moreover, ESMA proposes in the above-mentioned draft RTSs that securitisation repositories conduct a number of validation checks on submitted XML templates. However, these checks are premised *inter alia* upon

---

[10] See in particular Section 3.5 (Annex V – draft ITS on securitisation disclosure standards and Annexes 2-11 therein) of the Consultation Paper available here: https://www.esma.europa.eu/sites/default/files/library/esma33-128-107_consultation_paper_disclosure_and_operational_standards_0.pdf

[11] See in particular sections 2.1.7, 2.2.2.2, and 2.2.3.5-2.2.3.6 (pages 44, 48, and 54-56, resp.) in the Consultation Paper available here: https://www.esma.europa.eu/sites/default/files/library/esma33-128-107_consultation_paper_disclosure_and_operational_standards_0.pdf

[12] See in particular section 2.2.2 (pages 46-48) in the Consultation Paper available here: https://www.esma.europa.eu/sites/default/files/library/esma33-128-107_consultation_paper_disclosure_and_operational_standards_0.pdf

securitisation repositories having correctly implemented the common XML schema (which will be made available on ESMA's website). Errors of conversion of the templates set out in ESMA's proposed draft ITS on disclosure requirements [13] constitute an important operational risk in ESMA's view.

28. To this end, ESMA expects to provide, in time for the European Commission's publication of the final RTSs and ITSs on disclosure and operational standards, corresponding model XML schema/messages for each applicable disclosure template. These model schema and messages would be available on ESMA's website, and ESMA proposes that securitisation repositories would, as part of their application for registration, submit evidence of their incorporation in their own systems. The models are proposed to be used by ESMA as a basis for assessing an applicant's correct implementation of the reporting requirements and standards set out in the above-mentioned RTSs and ITSs. To avoid inconsistencies across repositories and ensure a level playing field and smooth transition (where desired/necessary) for market participants switching across repositories, ESMA notes that it may, as part of its application assessment, request any necessary adjustments to repositories' XML schema and messages.

29. ESMA believes that this centralised approach (i.e. ESMA developing model schema/messages that are then implemented by applicants and included in their application package) would improve certainty for potential applicants as to the implementation of a key technical component of the Securitisation Regulation—thus also helping simplify the application process. This centralised approach would also, in ESMA's view, improve the chances of industry-wide models being available in time for the entry into force of both the present draft RTS and the aforementioned disclosure requirements and operational standards RTSs. The centralised approach would also translate into fewer risks of inconsistencies across securitisation repositories, and, furthermore, would assist ESMA's supervisory efforts in ensuring a level playing field for all actual and potential applicants.

30. In setting out these considerations, ESMA notes that in any case industry participants remain free to use any securitisation model XML schema/messages and complement them for their own internal, bilateral, or multilateral purposes.

Q 3: Do you agree with a centralised approach to develop ISO 20022-compliant XML messages/schema? Do you agree that ESMA is best placed to develop ISO 20022-compliant XML messages/schema? Please explain why if not and provide an alternative proposal.

---

[13] See in particular Section 3.5 (Annex V – draft ITS on securitisation disclosure standards and Annexes 2-11 therein) of the Consultation Paper available here: https://www.esma.europa.eu/sites/default/files/library/esma33-128-107_consultation_paper_disclosure_and_operational_standards_0.pdf

2.4 Data safeguarding (EMIR Article 80)

31. In addition to the above-mentioned requirements regarding providing timely access to reporting entities for correcting data, ESMA considers it important that an application for registration as a securitisation repository should disclose the applicant's policies and procedures to prevent information stored and produced to be used for illegitimate purposes[14], to prevent the disclosure of confidential information, and to prevent the use of information in ways not permitted for commercial use[15], in line with Articles 80(1), 80(2), and 80(6) of EMIR, respectively. Such information would include details of the applicant's arrangements for managing staff access to information, as well as arrangements to protect the reported data from cyber-risks and cyber-attacks. ESMA proposes that applicants should also specify their arrangements for recording each staff member accessing the data, the time of access, the nature of data accessed and the purpose.

32. Pursuant to Article 80(3) of EMIR, ESMA also proposes that applicants should include information on their recordkeeping systems, policies and procedures used in order to ensure that data reported is stored in line with Article 80(3) of Regulation (EU) No 648/2012. In addition, ESMA considers that such recordkeeping requirements could also be extended to cover not only information reported to securitisation repositories, but also information produced by the securitisation repository as set out in ESMA's draft RTS on operational standards.[16] In ESMA's view, in light of the experience on data completeness gained with securitisation reporting arrangements over recent years, the data completeness and consistency checks, unique securitisation identifiers, and end-of-day reports produced by securitisation repositories contain additional useful information for investors, potential investors, and public authorities.

33. Furthermore, in line with Article 80(5), ESMA proposes to request information on the applicant's procedures to ensure that, where a reporting entity identifies factual errors in information that it has reported, it may submit, without undue delay, a corrected information item.

Q 4: Do you agree with the data safeguarding provisions set out in the draft RTS?

2.5 Simplified application format for securitisation repositories already registered as trade repositories under EMIR and/or SFTR

34. Applicants for registration as a securitisation repository that have already been registered as trade repositories under EMIR and/or SFTR have already provided substantial information to ESMA. For this reason, as required by Article 10(7)(c), ESMA proposes that

---

[14] For example, specific information on securitisations uploaded prior to deal closing being used by employees for personal gain.

[15] For example, contacting potential users not registered with the securitisation repository and specifically identifying the information provided by a particular reporting entity.

[16] See section 2.2 of the Consultation Paper available here: https://www.esma.europa.eu/sites/default/files/library/esma33-128-107_consultation_paper_disclosure_and_operational_standards_0.pdf

already-registered trade repositories shall not be required to provide a number of pieces of information which they have been provided otherwise at the time of the application as a TR. This redundant information includes:

(a) information on any pending judicial, administrative, arbitration or any other litigation proceedings;

(b) the applicant's ownership structure and ownership chart;

(c) information regarding the applicant's internal corporate governance policies and processes, as well as identification of any corporate governance code of conducts adhered to by the applicant;

(d) the identity of the internal bodies in charge of evaluating any relevant internal control findings;

(e) a description of the roles of the persons responsible for regulatory compliance, how the independence of the compliance function from the rest of the business is ensured, and the most recent internal compliance report;

(f) the staffing policies and procedures of the applicant;

(g) the applicant's financial report and business plans; and

(h) the applicant's procedures to prevent the use of information stored for illegitimate purposes, for disclosure of confidential information, or in ways not permitted for commercial use.

35. At the same time, in order to ensure that ESMA's assessment of an existing applicant trade repository's compliance with the present draft securitisation repository registration RTS is based on updated information, ESMA proposes that the above-mentioned items should be provided if those items have been updated since they were last provided to ESMA.

Q 5: Do you agree with the contents of the simplified application?

2.6 Proposed ITS requirements (application format)

36. Annex V sets out ESMA's proposed draft ITS for securitisation repository applications.

37. ESMA proposes therein that an application for registration should be provided in a durable medium[17], and contain a unique reference number to each document submitted. Moreover, ESMA proposes that the information submitted clearly identifies which specific requirement of the draft RTS is being referred to. Finally, ESMA proposes that the applicants be required

---

[17] I.e. as defined in Article 2(1)(m) of Directive 2009/65/EC of the European Parliament and of the Council: durable medium' means an instrument which enables an investor to store information addressed personally to that investor in a way that is accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored;

to justify if the information is not submitted as outlined in the document references section of the Annex to the draft ITS.

38. In light of the simplified application requirements for already-registered trade repositories, ESMA has specified a separate Annex in order to comply with the provisions of the Securitisation Regulation that a simplified format should also be set out in cases of an application for extension of registration for existing trade repositories. In practice, this second Annex is identical to the first, but would involve less information completion, as set out in the immediately-preceding section of this paper.

Q 6: Do you agree with the proposed requirements for the ITS?

2.7 Draft Guidelines on transfer of data between securitisation repositories

39. In line with Article 79(3) of EMIR, and consist with its existing arrangements for trade repositories[18], ESMA also included draft Guidelines covering procedures to ensure the orderly substitution of the securitisation repository if its registration is subsequently withdrawn, including procedures for the transfer of data to other securitisation repositories and the redirection of reporting flows to other securitisation repositories. As per Article 13 of the Securitisation Regulation, ESMA shall withdraw the registration of a securitisation repository under certain conditions[19]. At the same time, it is recalled that securitisation repositories will form a critical part of the securitisation market infrastructure. In the specific case of a registration being withdrawn due to the repository renouncing its registration, false statements having been made, or a repository no longer meeting the conditions under which it was registered, it may be necessary to avoid undesirable cliff effects following the registration withdrawal.

40. Similarly, ESMA also considers it important that securitisation repositories should ensure that, where a reporting entity decides to report to another securitisation repository, orderly substitution of the old securitisation repository information occurs, including the transfer of data and the redirection of reporting flows to the other securitisation repository. In addition to being linked with Article 79(3) of EMIR, ESMA also considers that such arrangements are important as part of ESMA specifying "the operational standards required, to allow the timely, structured, and comprehensive collection of data by securitisation repositories". Finally, recital 12 of the Securitisation Regulation recalls the necessity of ensuring that investors and potential investors "have access to all the relevant information over the entire

---

[18] https://www.esma.europa.eu/sites/default/files/library/esma70-151-552_guidelines_on_transfer_of_data_between_trade_repositories.pdf

[19] Article 13(1) stipulates that ESMA shall withdraw the registration of a securitisation repository where a repository either renounces the registration, has provided no securitisation repository services for the preceding six months, obtained the registration by making false statements or by other irregular means, or no longer meets the conditions under which it was registered.

life of the securitisation". Lastly, it appears worthwhile to ensure that reporting entities are not 'locked in' to a particular repository's arrangements.

41. To avoid such cliff effects and ensure sufficient flexibility for reporting entities, ESMA's draft Guidelines propose a set of procedures, which draw on ESMA's guidelines on data portability for Trade Repositories[20], in light of the important overlap between securitisation repositories and trade repositories. This overlap arises both legally (between EMIR and the Securitisation Regulation [21]) and technically [22]. In ESMA's view, two cases must be distinguished and covered in an application to be registered as a securitisation repository:

(a) A reporting entity requests to transfer its data from one securitisation repository to another, and

(b) The registration of a securitisation repository is withdrawn (either voluntarily or involuntarily)

2.7.1 Legal framework

42. The guidelines are providing additional clarification for securitisation repositories on how to ensure compliance at all times with the following EMIR provisions (via the Securitisation Regulation's Article 10(2)): Article 79(3)[23] and Article 80(3)[24]. Furthermore, Article 16(1) of the ESMA Regulation stipulates that "*The Authority shall, with a view to establishing consistent, efficient and effective 9 supervisory practices within the ESFS, and to ensuring the common, uniform and consistent application of Union law, issue guidelines and recommendations addressed to competent authorities or financial market participants.*"

43. The following sub-sections further delineate ESMA's clarifications.

2.7.2 Procedures following a request to transfer data to another repository

44. Following a request to transfer data[25], two securitisation repositories are involved: the repository from which data is leaving (the 'old' securitisation repository) and the repository receiving the data (the 'new' repository). ESMA considers that securitisation repositories establish a mutually-agreed migration plan within five working days of the transfer request. The plan should contain a detailed timeline and description of the required controls in place to transfer the data. For example, the plan should include the scope of the data transfer

---

[20] https://www.esma.europa.eu/sites/default/files/library/esma70-151-552_guidelines_on_transfer_of_data_between_trade_repositories.pdf

[21] Article 10 of the Securitisation Regulation refers to several EMIR articles as eligibility requirements for securitisation repositories.

[22] i.e. the technical overlap in reporting requirements between EMIR and ESMA's proposed draft RTSs on disclosure and operational standards, such as the use of ISO 20022 formats and XML templates for making information available (see in particular sections 2.1.7, 2.2.2.2, and 2.2.3.5-2.2.3.6 (pages 44, 48, and 54-56, resp.) in the Consultation Paper available here: https://www.esma.europa.eu/sites/default/files/library/esma33-128-107_consultation_paper_disclosure_and_operational_standards_0.pdf)

[23] *A trade repository from which registration has been withdrawn shall ensure orderly substitution including the transfer of data to other trade repositories and the redirection of reporting flows to other trade repositories*

[24] A trade repository shall promptly record the information received under Article 9 and shall maintain it for at least 10 years following the termination of the relevant contracts. It shall employ timely and efficient record keeping procedures to document changes to recorded information.

[25] Which can include actual data and/or documents stored by the securitisation repository the securitisations in question

(e.g. reporting entities whose securitisations are involved, securitisations, etc.), as well as the roles and responsibilities of the entities involved. Moreover, the plan should include timelines for the transfer and also controls to ensure confidentiality, integrity, and accuracy of the transferred data. In ESMA's view, establishing a plan will ensure the smooth operation, as well as accountability, for each necessary stage in the transfer of data.

45. As regards the content to transfer, all of the information provided by the reporting entity to the old repository should be included in the transfer. In addition, ESMA is of the view that information relating to modifications of information on the reporting entity's securitisations recorded by the old repository, as well as the unique securitisation identifier associated with the transferred information, is necessary to transfer. Including such information in the transfer will facilitate the ability of investors and potential investors to "have access to all the relevant information over the entire life of the securitisation". Furthermore, including such information in the transfer will also facilitate the storage of all relevant information on a securitisation in a centralised location—a key component of the "comprehensive system" envisaged in recital 12 of the Securitisation Regulation. At the same time, ESMA is of the view that transferring such already-recorded information would not risk disclosing the old securitisation repository's business strategy, operational arrangements, or other proprietary information.

46. ESMA also considers it useful to set out, at this stage, arrangements for how data should be transferred. To this end, and in line with the arrangements proposed in the draft RTS on operational standards[26], ESMA considers that data should be transferred using XML format and templates, using secure machine-to-machine protocols and advanced encryption methods.

47. In order to facilitate the smooth transfer of data, ESMA considers that the transfer should generally take place on a non-working day, unless explicitly agreed by the old and new securitisation repository. Where it is not possible to transfer all of the identified data in the same instance, priority should be given to securitisations that are still outstanding as at the date of the transfer, in order to minimise disruption for market participants and public authorities.

48. According to the draft Guidelines, the new securitisation repository should confirm the successful transfer to both the reporting entity having made the request, the old securitisation repository, and also the users registered[27] with the new securitisation repository. On its side, the old securitisation repository would confirm the transfer to its own users. Such confirmations are also necessary, in ESMA's view, to ensure the "timely, structured, and comprehensive aggregation of data".

49. As a further safeguard, ESMA also considers that the old securitisation repository should continue to store (but not make available to its users) the transferred data for a period of

---

[26] See the Consultation Paper available here: https://www.esma.europa.eu/sites/default/files/library/esma33-128-107_consultation_paper_disclosure_and_operational_standards_0.pdf

[27] See in particular section 2.2.5 and Article 9 of the draft operational standards and access conditions RTS (pages 61-65 and 242-244, resp.) in the Consultation Paper available here: https://www.esma.europa.eu/sites/default/files/library/esma33-128-107_consultation_paper_disclosure_and_operational_standards_0.pdf

10 years (in line with the recordkeeping arrangements set out in EMIR Article 80(3)), in the event that it becomes necessary to retrieve them.

50. Finally, to ensure the appropriate alignment of incentives between the various participants in the data transfer process and beyond, and in line with its existing guidelines on portability of information across Trade Repositories[28], ESMA considers that any fees charged by either the new or the old securitisation repository for the data transfer process should be cost-related, non-discriminatory and included in the fee schedule of the relevant repositories (which is proposed to be made public as set out in the draft RTS on application requirements for registration).

Q 7: Do you agree with the considerations on transferring information following a request to transfer data to another repository?

Q 8: Do you consider that any other aspects should be considered regarding the fees charged by the new or old repository for the data transfer process?

2.7.3 Procedures following withdrawal of repository registration

51. ESMA's draft operational arrangements for transfer of information following the withdrawal of a repository's registration are in many respects identical to the above-mentioned arrangements. A migration plan is also established and agreed between the new securitisation repository receiving the information and the old securitisation repository (i.e. the repository whose registration is being withdrawn). However, in this second case, ESMA must be presented with the migration plan as part of the repository's winding-down arrangements.

52. Another distinct proposal for this scenario is that ESMA and the old repository's users must be notified in advance of the intended date of cessation of operations. In order to help mitigate any disruption to securitisation market participants due to the withdrawal of registration, ESMA considers that securitisation repositories with more than 50 reporting entities or 100 registered users at the time of repository's decision to cease operations or the notice of intention to withdraw registration (whichever is earlier), should provide notice at least nine months in advance of the intended date. In other cases, the advance notice should be at least six months in advance.

53. Elsewhere, in cases where the registration of a repository is withdrawn, ESMA considers that, at the date of actual cessation of operations, the old securitisation repository should perform a secure destruction/deletion of the data, with the aim of ensuring that data cannot be undeleted or recovered after that date. In setting out this draft Guideline element, ESMA understands that, following the withdrawal of a repository's registration, the entity would no longer be deemed to be a "securitisation repository" and, therefore, that the provisions of

---

[28] https://www.esma.europa.eu/file/22897/download?token=yMHqxB91

Article 80(3) of EMIR (via Article 10(2) of the Securitisation Regulation) would no longer apply.[29]

Q 9: Do you agree with the draft arrangements for transferring information from one securitisation repository to another following a withdrawal of registration?

---

[29] EMIR Article 80 (3): A trade repository shall promptly record the information received under Article 9 and shall maintain it for at least 10 years following the termination of the relevant contracts. It shall employ timely and efficient record keeping procedures to document changes to recorded information.

3 Annexes

3.1 Annex 1: Summary of questions

Q 1: Do you agree with the general requirements proposed in the draft RTS?

Q 2: Do you agree with the operational reliability provisions set out in the draft RTS? Do you have any further suggestions?

Q 3: Do you agree with a centralised approach to develop ISO 20022-compliant XML messages/schema? Do you agree that ESMA is best placed to develop ISO 20022-compliant XML messages/schema? Please explain why if not and provide an alternative proposal.

Q 4: Do you agree with the data safeguarding provisions set out in the draft RTS?

Q 5: Do you agree with the contents of the simplified application?

Q 6: Do you agree with the proposed requirements for the ITS?

Q 7: Do you agree with the considerations on transferring information following a request to transfer data to another repository?

Q 8: Do you consider that any other aspects should be considered regarding the fees charged by the new or old repository for the data transfer process?

Q 9: Do you agree with the draft arrangements for transferring information from one securitisation repository to another following a withdrawal of registration?

3.2 Annex II: Legislative mandate to develop technical standards

Article 10 of the Securitisation Regulation:

[…]

7.   In order to ensure consistent application of this Article, ESMA shall develop draft regulatory technical standards specifying the details of all of the following:

[…]

(b)   the application for registration referred to in point (a) of paragraph 5;

(c)   a simplified application for an extension of registration referred to in point (b) of paragraph 5.

ESMA shall submit those draft regulatory technical standards to the Commission by … [one year from the date of entry into force of this Regulation].

The Commission is empowered to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1095/2010.

8. In order to ensure uniform conditions of application of paragraphs 1 and 2, ESMA shall develop draft implementing technical standards specifying the format of both of the following:

(a)   the application for registration referred to in point (a) of paragraph 5;

(b)   the application for an extension of registration referred to in point (b) of paragraph 5.

With regard to point (b) of the first subparagraph, ESMA shall develop a simplified format avoiding duplicate procedures.

ESMA shall submit those draft implementing technical standards to the Commission by … [one year from the date of entry into force of this Regulation].

The Commission is empowered to adopt the implementing technical standards referred to in the first subparagraph in accordance with Article 15 of Regulation (EU) No 1095/2010.

EMIR Article 78 (General Requirements):

1. A trade repository shall have robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of responsibility and adequate internal control mechanisms, including sound administrative and accounting procedures, which prevent any disclosure of confidential information.

2. A trade repository shall maintain and operate effective written organisational and administrative arrangements to identify and manage any potential conflicts of interest concerning its managers, employees, or any person directly or indirectly linked to them by close links.

3. A trade repository shall establish adequate policies and procedures sufficient to ensure its compliance, including of its managers and employees, with all the provisions of this Regulation.

4. A trade repository shall maintain and operate an adequate organisational structure to ensure continuity and orderly functioning of the trade repository in the performance of its services and activities. It shall employ appropriate and proportionate systems, resources and procedures.

5. Where a trade repository offers ancillary services such as trade confirmation, trade matching, credit event servicing, portfolio reconciliation or portfolio compression services, the trade repository shall maintain those ancillary services operationally separate from the trade repository's function of centrally collecting and maintaining records of derivatives.

6. The senior management and members of the board of a trade repository shall be of sufficiently good repute and experience so as to ensure the sound and prudent management of the trade repository.

7. A trade repository shall have objective, non-discriminatory and publicly disclosed requirements for access by undertakings subject to the reporting obligation under Article 9. A trade repository shall grant service providers non-discriminatory access to information maintained by the trade repository, on condition that the relevant counterparties have provided their consent. Criteria that restrict access shall only be permitted to the extent that their objective is to control the risk to the data maintained by a trade repository.

8. A trade repository shall publicly disclose the prices and fees associated with services provided under this Regulation. It shall disclose the prices and fees of each service provided separately, including discounts and rebates and the conditions to benefit from those reductions. It shall allow reporting entities to access specific services separately. The prices and fees charged by a trade repository shall be cost-related.

EMIR Article 79 (Operational reliability):

1. A trade repository shall identify sources of operational risk and minimise them through the development of appropriate systems, controls and procedures. Such systems shall be reliable and secure and have adequate capacity to handle the information received.

2. A trade repository shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan aiming at ensuring the maintenance of its functions, the timely recovery of operations and the fulfilment of the trade repository's obligations. Such a plan shall at least provide for the establishment of backup facilities.

3. A trade repository from which registration has been withdrawn shall ensure orderly substitution including the transfer of data to other trade repositories and the redirection of reporting flows to other trade repositories.

EMIR Article 80 (Safeguarding and recording), sub-paragraphs (1)-(3) and (5)-(6):

1. A trade repository shall ensure the confidentiality, integrity and protection of the information received under Article 9.

2. A trade repository may only use the data it receives under this Regulation for commercial purposes if the relevant counterparties have provided their consent.

3. A trade repository shall promptly record the information received under Article 9 and shall maintain it for at least 10 years following the termination of the relevant contracts. It shall employ timely and efficient record keeping procedures to document changes to recorded information.

…

5. A trade repository shall allow the parties to a contract to access and correct the information on that contract in a timely manner.

6. A trade repository shall take all reasonable steps to prevent any misuse of the information maintained in its systems. A natural person who has a close link with a trade repository or a legal person that has a parent undertaking or a subsidiary relationship with the trade repository shall not use confidential information recorded in a trade repository for commercial purposes.

3.3 Annex III: Cost-benefit analysis

3.3.1 Introduction

54. As discussed in section 2 above, the Securitisation Regulation tasks ESMA with developing RTSs on the application requirements for securitisation repositories. As part of its mandate to conduct an analysis of the costs and benefits of these proposed RTSs, ESMA has prepared a preliminary analysis in this Consultation Paper, on which it welcomes views from market participants and other stakeholders.

55. ESMA is of the view that its proposed draft RTSs are purely technical and do not imply strategic decisions or major policy choices. Indeed, ESMA considers that its options are limited to its specific mandate for drafting these particular RTSs, and the need to ensure compliance with the objectives set out in Securitisation Regulation. The main policy decisions taken under the Regulation have already been assessed and published by the European Commission in its own impact assessment work.[30]

56. ESMA furthermore recalls that it has a mandate to conduct a CBA on Level 2 requirements (i.e. these draft RTSs), and not Level 1 (i.e. the Securitisation Regulation).

57. The following section reflects the key issues carrying, in ESMA's view, different options for implementation.

3.3.2 Scope of information to be submitted to ESMA

58. The draft RTS discussed in this consultation paper propose a substantial amount of information to be provided to ESMA. Generally-speaking, from ESMA's perspective this reflects an orientation to obtain, ex ante, information on many aspects of the applicant's business.

Objective	*Obtaining sufficient information to assess an application to be registered as a securitisation repository*
Option 1	Specify limited information requirements in the draft RTS
Option 2	Specify comprehensive information requirements in the draft RTS
Preferred option	**Option 2:** Despite the higher up-front effort required from applicants, ESMA is of the view that it is preferable to request a comprehensive set of information at the outset in the present RTS. ESMA prefers this proposed approach in order to minimize the frequency of follow-up exchanges for supplementary information between ESMA and the applicant. Although leading to higher up-front costs for applicants (in relation to the up-front costs for option 1), in terms of total costs of information provision the

---

[30] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015SC0185&from=EN

	efficiency gains under option 2 are expected to imply lower total costs under option 2 in compared with option 1.

Option 1	*Specify limited information requirements in the draft RTS*
Benefits	• Potentially lower up-front cost for applicants .
Costs	• Higher potential costs for ESMA and applicants due to duplication of efforts required when requesting supplementary information to be provided (such as additional technical documentation, evidence of compliance with technical provisions set out in the Securitisation Regulation and accompanying technical standards and guidelines).

Option 2	*Specify comprehensive information requirements in the draft RTS*
Benefits	• Lower potential costs for ESMA and applicants due to avoided duplication of efforts (arising from the expected need for fewer repeated exchanges). • Greater ex ante clarity for all market participants, including reporting entities and data users, on what is expected of securitisation repositories. • Consistent in terms of the extent/detail of requirements for Trade Repositories and Credit Rating Agencies.
Costs	• Potentially higher up-front cost for applicants.

3.3.3 Is it important to assess outsourcing and ancillary services?

59. The draft RTS proposes to obtain substantial information on securitisation repositories' reliance on outsourcing for providing key functions, as well as their provision of ancillary services. The following options have been considered when drafting the relevant sections of the proposed RTS.

Objective	*Obtaining necessary information as regards the applicant's operational robustness*
Option 1	Do not include information on outsourcing arrangements and ancillary services provision
Option 2	Include information on outsourcing arrangements and ancillary services provision

Preferred option	**Option 2:** Securitisation repositories may find it cost effective to outsource the performance of a number of functions, such as the development and maintenance of certain critical components of their systems. Similarly, the information hosted and associated expertise may also lead to additional ancillary services to be provided to market participants. In both respects, ESMA considers that this information is pertinent to assess the complete organisational profile of an applicant, with a view to ensuring its operational robustness for the provision of expected securitisation repository services throughout a variety of market conditions and technical events.

Option 1	*Do not include information on outsourcing arrangements and ancillary services provision*
Benefits	• Lower initial amount of information would need to be gathered by applicants, potentially leading to additional interest in applying.
Costs	• Less clarity on operational robustness to market events and technical events. • Possibly greater efforts required from applicants if ESMA seeks to obtain further information on a specific application (leading also to higher overall application assessment costs for ESMA).

Option 2	*Include information on outsourcing arrangements and ancillary services provision*
Benefits	• Greater clarity on operational robustness to market events and technical events. • Possibly fewer efforts required from applicants if ESMA seeks to obtain further information on a specific application (leading also to higher overall application assessment costs for ESMA). • Clearer set of requirements, thus facilitating applicants' initial efforts for preparing application materials. • In line with updated requirements for Trade Repositories.
Costs	• Possibly greater up-front application costs for securitisation repository applicants to prepare the necessary materials.

3.3.4 Is it important to assess knowledge of securitisations as part of an application?

60. The draft RTS proposes to obtain information on the knowledge and experience of the securitisation repository applicant's senior management and board on information technology and on securitisation matters. The following options have been considered when drafting the relevant sections of the proposed RTS.

Objective	*Assessing the knowledge and experience of the applicant's senior management and board on information technology and on securitisation matters*
Option 1	Do not assess knowledge and experience of securitisation
Option 2	Assess knowledge and experience of securitisation
Preferred option	**Option 2:** Securitisations are complex instruments and developing/managing the resources (human and technical) needed to provide certain required securitisation repository services—especially on data quality—in turn necessitates substantial knowledge of these products.

Option 1	*Do not assess such knowledge and experience*
Benefits	• Less initial amount of information would need to be gathered by applicants, potentially leading to additional interest in applying for registration.
Costs	• Risk of less effective securitisation repository services provided in the future, due to the presence of less qualified/experienced staff (if this is not set out as a condition for registration). • Possibly greater effort required from applicants in the event that ESMA seeks to obtain further information on a specific application (leading also to higher overall application assessment costs for ESMA).
Option 2	*Assess such knowledge and experience*
Benefits	• Greater reassurance on ability of repositories' management bodies to effectively steer the firm on its core business activities, as well as evolve alongside securitisation market practices (thus also saving future supervisory resources in ESMA and, consequently, lower-than-otherwise fees charged to securitisation repositories). • Possibly less effort required from applicants in the event that ESMA seeks to obtain further information on a specific application (leading also to lower overall application assessment costs for ESMA). • Clearer up-front set of requirements for applicants.
Costs	• Possibly greater up-front application costs for securitisation repository applicants to prepare the necessary materials.

3.4 Annex IV: Draft RTS on information to be provided in the application for the registration of a securitisation repository

Draft

COMMISSION DELEGATED REGULATION (EU) …/..

supplementing Regulation 2017/2042/EU of the European Parliament and of the Council with regard to Regulatory Technical Standards on information to be provided in the application for the registration of a securitisation repository

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2017/2402 of the European Parliament and of the Council of 12 December 2017 laying down common rules on securitisation and creating a European framework for simple, transparent, and standardized securitisation and amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, and Regulations (EC) No 1060/2009 and (EU) No 648/2012 ('the Securitisation Regulation'), and in particular Article 10 thereof,

Whereas:

(1) The Securitisation Regulation requires the European Securities and Markets Authority (ESMA) to submit by 18 January 2019 draft RTS, to be adopted by the Commission, that specify the application procedures for repositories to be registered and supervised by ESMA.

(2) Establishing a comprehensive and sound framework for registration of securitisation repositories and extension of registration of trade repositories is essential for the achievement of the Securitisation Regulation's objectives and for the adequate provision of repository functions.

(3) In order to minimise additional operational costs for market participants, the rules and standards for the registration of securitisation and the extension of registration of trade repositories for the purposes of the Securitisation Regulation build on pre-existing infrastructures, operational processes, and formats, each of which were introduced with regard to reporting securities financing transactions and derivative contracts to trade repositories. The provisions for registration of trade repositories under Regulation (EU) No

648/2012 and Regulation (EU) 2015/2365 constitute sound starting points to build the framework for registration of securitisation repositories under the Securitisation Regulation.

(4) Securitisation repositories will play a pivotal role in fostering transparency in securitisation markets, as per the Securitisation Regulation, and will be relied upon by all manner of investors, public entities, and reporting entities to meet their respective obligations under the Securitisation Regulation. It is therefore essential that firms applying to be registered as securitisation repositories demonstrate the adequacy of their staff, systems, controls, and procedures, in order to comply with the requirements set out in the Securitisation Regulation and its accompanying delegated acts.

(5) Securitisations are highly complex instruments involving many different types of information, including information on the underlying exposures' features, information on their cash flows, information on the structure of the securitisation, and information on the legal and operational arrangements entered into with third parties. It is therefore essential that securitisation repository applicants demonstrate sufficient experience of these products, and capacity to receive, process, and make available the required information set out in the Securitisation Regulation and its accompanying technical standards.

(6) The use of common resources within a securitisation repository between securitisation reporting services on the one hand and ancillary services on the other may lead to contagion of operational risks across services. Whereas the validation, reconciliation, processing and recordkeeping of data may require an effective operational separation to avoid such contagion of risks, practices such as a common front-end of systems, a common access point to data for authorities or the use of the same staff working in sales, compliance, or a client services helpdesk may be less prone to contagion and hence do not necessarily require operational separation. Securitisation repositories should therefore establish an appropriate level of operational separation between the resources, systems or procedures used in different business lines, including where those business lines comprise the provision of services subject to other Union or third country legislation, and ensure that detailed and clear information on the ancillary services, or other business lines that the securitisation repository offers outside its core activity of repository services under the Securitisation Regulation, is provided to ESMA in the application for registration or extension of registration.

(7) The fees associated with the services provided by securitisation repositories are essential information for enabling market participants to make an informed choice and should therefore form part of the application for registration as securitisation repository.

(8) The effective payment of the registration fees by securitisation repositories at the time of application is essential to cover ESMA's necessary expenditure relating to the registration or extension of registration of the securitisation repository.

(9) This Regulation provides a simplified application for an extension of registration, to allow trade repositories already registered under Regulation (EU) No 648/2012 or under Regulation (EU) 2015/2365 of the European Parliament and of the Council to file a simplified application in order for their registration to be extended under the Securitisation Regulation. Therefore, to avoid any duplicate requirements in the case of an application for an extension of registration, the information to be provided by the trade repository as

part of an extension of registration should include detailed information on the adaptations necessary to ensure it complies with the Securitisation Regulation.

(10)   [This Regulation is based on the draft Regulatory Technical Standards submitted by ESMA to the Commission in accordance with Article 10 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council[31].]

(11)   [ESMA has conducted an open public consultation on the draft RTS on which this Regulation is based, analysed the potential related costs and benefits and requested the opinion of the Securities and Markets Stakeholder Group established by Article 37 of Regulation (EU) No 1095/2010.]

HAS ADOPTED THIS REGULATION

Article 1

Definitions

1. 'user' shall refer to any client of the securitisation repository, including user types listed in Article 17(1) of the Securitisation Regulation, and reporting entities as defined in [ref. to disclosure RTS].

Article 2

Identification, legal status and types of securitisations

1. An application for registration as a securitisation repository shall identify the applicant and the activities it intends to carry out which require it to be registered as a securitisation repository.

2. The application for registration as a securitisation repository shall in particular contain the following information:

    (a) the corporate name of the applicant and legal address as well as the address of all its offices within the Union;

    (b) Legal Entity Identifier (LEI) registered with the Global Legal Entity Identifier Foundation;

    (c) Uniform Resource Locator (URL) of the applicant's website;

    (d) an excerpt from the relevant commercial or court register, or other forms of certified evidence of the place of incorporation and scope of business activity of the applicant, valid at the application date;

---

[31] OJ L 331, 15.12.2010, p. 84

(e) information on the securitisation types (ABCP or non-ABCP), risk transfer methods (true sale or synthetic), and underlying exposure types (residential mortgage, commercial mortgage, corporate, leasing, consumer, auto loan/lease, credit card, other) for which the applicant wishes to be registered;

(f) information on whether the applicant is authorised or registered by a competent authority in the Member State where it is established and, in such case, the name of the authority and any reference number related to the authorisation or registration;

(g) the articles of incorporation and, where relevant, other statutory documentation stating that the applicant is to conduct securitisation repository services;

(h) the name and contact details of the person(s) responsible for compliance, or any other staff involved in compliance assessments for the applicant;

(i) the name, title, address, e-mail address and the telephone number(s) of the contact person for the purposes of the application;

(j) the programme of operations, including the location of the main business activities; and

(k) any information on any pending judicial, administrative, arbitration or any other litigation proceedings irrespective of their type, that the applicant may be party to, particularly as regards tax and insolvency matters and where significant financial or reputational costs may be incurred, or any non-pending proceedings that may still have a material impact on costs of providing securitisation repository services.

3. Upon request by ESMA, the applicant shall also provide additional information during the examination of the application for registration where such information is needed for the assessment of the applicants' capacity to comply with the applicable requirements set out in the Securitisation Regulation and its accompanying delegated acts and for ESMA to duly interpret and analyse the documentation to be submitted or already submitted.

4. Where an applicant considers that a requirement of this Regulation is not applicable to it, it shall clearly indicate that requirement in its application and also provide an explanation why such requirement does not apply.

Article 3

Organisational chart

1. An application for registration as a securitisation repository shall contain the organisational chart detailing the organisational structure of the applicant, including that of any ancillary services.

2. That chart shall include information about the identity of the person responsible for each significant role, including senior management and persons who direct the activities of any branches.

Article 4

Corporate governance

1. An application for registration as a securitisation repository shall contain information regarding the applicant's internal corporate governance policies and the procedures and terms of reference which govern its senior management, including the board, its non-executive members and, where established, committees.

2. That information shall include a description of the selection process, appointment, performance evaluation and removal of senior management and members of the board.

3. Where the applicant adheres to a recognised corporate governance code of conduct, the application for registration as a securitisation repository shall identify the code and provide an explanation for any situations where the applicant deviates from the code.

Article 5

Internal control

1. An application for registration as a securitisation repository shall contain detailed information relating to the internal control system of the applicant. This shall include information regarding its compliance function, risk assessment, internal control mechanisms and arrangements of its internal audit function.

2. That detailed information shall include:

   (a) the applicant's internal control policies and respective procedures related to their consistent and appropriate implementation;

   (b) any policies, procedures and manuals regarding the monitoring and evaluation of the adequacy and effectiveness of the applicant's systems;

   (c) any policies, procedures and manuals regarding the control and safeguard of the applicant's information processing systems; and

   (d) the identity of the internal bodies in charge of evaluating the relevant internal control findings.

3. An application for registration as a securitisation repository shall contain the following information with respect to the applicant's internal audit activities:

   (a) the composition of any Internal Audit Committee, its competences and responsibilities;

   (b) its internal audit function charter, methodologies, standards and procedures;

   (c) an explanation how its internal audit charter, methodology and procedures are developed and applied, taking into account the nature and extent of the applicant's activities, complexities and risks; and

   (d) a work plan for three years following the date of application focusing and addressing the nature and extent of the applicant's activities, complexities and risks.

Article 6

Conflicts of interest

1. An application for registration as a securitisation repository shall contain the following information on the policies and procedures put in place by the applicant to manage conflicts of interest:

    (a) policies and procedures with respect to the identification, management, elimination, mitigation, and disclosure without delay of conflicts of interest;

    (b) a description of the process used to ensure that the relevant persons are aware of the policies and procedures;

    (c) the separation of duties and business functions within the applicant including:

        i. measures to prevent or control the exchange of information where a risk of conflicts of interest may arise;

        ii. the separate supervision of relevant persons whose main functions involve interests that are potentially in conflict with those of a client; and

    (d) any other measures and controls put in place to ensure the requirements referred to in point (a) on conflicts of interest management are met.

2. An application for registration as a securitisation repository shall contain an up-to-date inventory, at the time of the application, of existing and potential material conflicts of interest in relation to any ancillary or other related services provided or received by the applicant and a description of how these are being managed. The inventory of conflicts of interest shall include conflicts of interest arising from situations where the applicant:

    (a) may realise a financial gain or avoid a financial loss, to the detriment of a client;

    (b) may have an interest in the outcome of a service provided to a client, which is distinct from the client's interest in that outcome;

    (c) may have an incentive to prioritise its own interests or the interest of another user or group of users rather than the interests of a client to whom the service is provided;

    (d) receive or may receive from any person other than a client, in relation to the service provided to a client, an incentive in the form of money, goods or services, other than commission or fees received for the service.

3. Where an applicant is part of a group, the inventory shall include any existing and potential material conflicts of interest arising from other undertakings within the group and how these conflicts are being managed and mitigated.

Article 7

Ownership of the securitisation repository

1. An application for registration as a securitisation repository shall contain:

(a) a list containing the name of each person or entity who directly or indirectly holds 5 % or more of the applicant's capital or of its voting rights or whose holding makes it possible to exercise a significant influence over the applicant's management; and

(b) a list of any undertakings in which a person referred to in point (a) holds 5 % or more of the capital or voting rights or over whose management they exercise a significant influence.

2. Where the applicant has a parent undertaking, the applicant shall:

(a) identify the name, LEI registered with the Global Legal Entity Identifier Foundation, and legal address of the parent undertaking;

(b) indicate whether the parent undertaking is authorised or registered and subject to supervision and, when this is the case, state any reference number and the name of the responsible supervisory authority.

3. Where the applicant has an ultimate parent undertaking different to the undertaking named in paragraph 2 of this Article, the applicant shall:

(a) identify the name, LEI registered with the Global Legal Entity Identifier Foundation, and legal address of the ultimate parent undertaking; and

(b) indicate whether the ultimate parent undertaking is authorised or registered and subject to supervision, and when this is the case, state any reference number and the name of the responsible supervisory authority.

Article 8

Ownership chart

1. An application for registration as a securitisation repository shall contain a chart showing the ownership links between the ultimate parent undertaking, parent undertaking, subsidiaries and any other associated entities or branches.

2. The undertakings shown in the chart referred to in paragraph 1 shall be identified by their full name, legal status, legal address, and LEI registered with the Global Legal Entity Identifier Foundation.

Article 9

Policies and procedures

1. Policies and procedures that are provided as part of an application shall contain the following items:

(a) an indication that the Board approves the policies, that the senior management approves the procedures and that the senior management is responsible for the implementation and maintenance of the policies and procedures;

(b) a description of how the communication of policies and procedures within the applicant is organised, how compliance with the policies will be ensured and

monitored on a day to day basis, and the person or persons responsible for compliance in that regard;

(c) any records indicating that employed and dedicated staff are aware of the policies and procedures;

(d) a description of the measures to adopt in the event of a breach of policies and procedures together with an indication of the procedure for reporting such breaches to ESMA;

(e) an indication of the procedure for reporting to ESMA any material breach of policies or procedures which may result in a breach of the initial conditions for registration; and

(f) a description of arrangements to promptly notify ESMA of any planned material changes to the applicant's information technology systems prior to their implementation.

Article 10

Regulatory compliance

1. An application for registration as a securitisation repository shall contain the following information regarding an applicant's policies and procedures for ensuring compliance with the Securitisation Regulation and its accompanying delegated acts:

    (a) a description of the roles of the persons responsible for compliance and of any other staff involved in the compliance assessments, including how the independence of the compliance function from the rest of the business will be ensured;

    (b) the internal policies and procedures designed to ensure that the applicant, including its managers and employees, comply with all the provisions of the Securitisation Regulation and its accompanying delegated acts, including a description of the role of the board and senior management; and

    (c) where available, the most recent internal report prepared by the persons responsible for compliance or any other staff involved in compliance assessments within the applicant.

Article 11

Staffing policies and procedures

1. An application for registration as a securitisation repository shall contain the following policies and procedures:

    (a) a copy of the remuneration policy for the senior management, board members and the staff employed in risk and control functions of the applicant; and

    (b) a description of the measures put in place by the applicant to mitigate the risk of over-reliance on any individual employees.

Article 12

Fitness and properness

1. An application for registration as a securitisation repository shall contain the following information about the applicant's staff:

   (a) a general list of the staff directly employed by the securitisation repository, including their role and qualifications per role;

   (b) a specific description of the information technology staff directly employed to provide securitisation repository services, together with the role and the qualifications of each individual;

   (c) a description of the roles and qualifications of each individual who is responsible for internal audit, internal controls, compliance and risk assessment;

   (d) the identity of the dedicated staff members and those members of the staff that are operating under any outsourcing arrangement; and

   (e) details of the training on the applicant's policies and procedures as well as the securitisation repository business, including any examination or other type of formal assessment required for staff regarding the conduct of securitisation repository activities.

   The description referred to in point (b) shall include written evidence of the experience in information technology of at least one staff member responsible for information technology matters.

Article 13

Financial reports and business plans

1. An application for registration as a securitisation repository shall contain the following financial and business information about the applicant:

   (a) a complete set of financial statements, prepared in conformity with either:

      i. international standards adopted in accordance with Article 3 of Regulation (EC) No 1606/2002 of the European Parliament and of the Council of 19 July 2002 on the application of international accounting standards[32]; or

      ii. national accounting standards of the Member State in which the applicant is established, as required by Directive 2013/34/EU[33];

---

[32] OJ L 243, 11.9.2002, p. 1.

[33] Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC. OJ L 182, 29.6.2013, p. 19–76.

(b) where the financial statements of the applicant are subject to statutory audit within the meaning given in Article 2(1) of the Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts[34], the financial reports shall include the audit report on the annual and consolidated financial statements; and

(c) if the applicant is audited, the name and the national registration number of the external auditor;

2. An application for registration as a securitisation repository shall contain a financial business plan contemplating different business scenarios for the securitisation repository services over a minimum three years' reference period and including the following additional information:

(a) the expected level of reporting activity in number of transactions,

(b) the relevant fixed and variable costs identified with respect to the provision of repository services under the Securitisation Regulation and its accompanying delegated acts, and

(c) positive and negative variations of at least 20 % from the base activity scenario identified.

3. Where the historical financial information referred to in paragraph 1 is not available, an application for registration as a securitisation repository shall contain the following information about the applicant:

(a) the pro-forma statement demonstrating proper resources and expected business status in the following six months after registration is granted;

(b) an interim financial report where the financial statements are not yet available for the requested period of time;

4. An application for registration as a securitisation repository shall contain the audited annual financial statements of any parent undertaking for the three financial years preceding the date of the application, where available.

5. An application for registration as a securitisation repository shall also contain the following financial information about the applicant:

(a) an indication of any future plans for the establishment of subsidiaries and their location;

(b) a description of the business activities which the applicant plans to carry out, specifying the activities of any subsidiaries or branches.

Article 14

Information Technology resources

1. An application for registration as a securitisation repository shall contain:

---

[34] OJ L 157, 9.6.2006, p. 87.

(a) a detailed description of the information technology system, in conjunction the information provided in point 2(e) of Article 2;

(b) the relevant business requirements, functional and technical specifications, storage capacity, system scalability (both for performing its functions and handling increases in information to process and access requests), maximum limits on the size of data submissions made in accordance with [ref. to disclosure RTS and ITS], system architectural and technical design, data model and data flows, and operations and administrative procedures and manuals;

(c) a detailed description of user facilities developed by the applicant in order to provide services to the relevant users, including a copy of any user manual and internal procedures;

(d) the investment and renewal policies and procedures on information technology resources of the applicant, including the review and development cycle of the applicant's systems and versioning and testing policies;

(e) the applicant's implementation (XML schema) of the reporting templates set out in the Annexes of [ref. to disclosure ITS] and of any additional XML messages, using the available models made available by ESMA; and

(f) the policies and procedures for handling changes to the reporting templates set out in the Annexes of [ref. to disclosure ITS].

Article 15

Data collection and availability mechanisms

1. An application for registration as a securitisation repository shall contain:

(a) a procedure and a description of the resources, methods and channels that the securitisation repository will employ in order to facilitate the timely, structured, and comprehensive collection of data from reporting entities;

(b) a description of the resources, methods and channels that the applicant will use to facilitate access to the information under Articles 7 and 17 of the Securitisation Regulation, and in accordance with Article 17 of the Securitisation Regulation and its accompanying delegated acts:

(c) a description of the procedures to calculate the data completeness scores in accordance with [ref to operational standards RTS]; and

(d) with regards to sub-paragraphs (b) and (c), a description of the resources, methods and channels that the securitisation repository will employ in order to facilitate access to the data contained therein to the entities listed in Article 17(1) of the Securitisation Regulation, in accordance with [ref to operational standards RTS], along with a copy of any specific manuals and internal policies.

Article 16

Ancillary services

1. Where an applicant, an undertaking within its group, or an undertaking with which the applicant has a material agreement relating to securitisation services offers, or plans to offer any ancillary or non-securitisation services, its application shall contain:

   (a) a description of the ancillary or non-securitisation services that the applicant, or the undertaking within its group, performs or plans to perform, and a description of any agreement that the securitisation repository may have with companies offering securitisation related services, as well as copies of such agreements; and

   (b) the procedures and policies that will ensure the necessary degree level of operational separation in terms of resources, systems, information and procedures, between the applicant's securitisation repository services under the Securitisation Regulation and the applicant's other business lines, including those business lines that comprise the provision of securitisation repository services under Union or third country legislation, irrespective of whether that separate business line is run by the securitisation repository, a company belonging to its holding company, or any other company within which the applicant has a material agreement in the context of the securitisation business line.

Article 17

Senior management and members of the board

1. An application for registration as a securitisation repository shall contain detailed information on the knowledge and experience of the members of the senior management and the board on securitisation matters and on information technology management, operations, and development.

2. An application for registration as a securitisation repository shall contain the following information in respect of each member of the senior management and each member of the board:

   (a) a copy of the curriculum vitae, including:

   i. an overview of the member's post-secondary education;

   ii. the member's complete employment history with dates, identification of positions held and a description of the functions occupied; and

   iii. any professional qualification held by the member, together with the date of acquisition and, if applicable, status of membership in the relevant professional body;

   (b) details regarding any criminal convictions in connection with the provision of financial or data services or in relation to acts of fraud or embezzlement, in particular in the form of an official certificate if available within the relevant Member State;

   (c) a signed declaration from each member of the senior management and the board that states whether or not they:

i. have been convicted of any criminal offence in connection with the provision of financial or data services or in relation to acts of fraud or embezzlement;

ii. have been subject to an adverse decision in any proceedings of a disciplinary nature brought by a regulatory authority or government bodies or agencies or are the subject of any such proceedings which are not concluded;

iii. have been subject to an adverse judicial finding in civil proceedings before a court in connection with the provision of financial or data services, or for impropriety or fraud in the management of a business;

iv. have been part of the board or senior management of an undertaking whose registration or authorisation was withdrawn by a regulatory body;

v. have been refused the right to carry on activities which require registration or authorisation by a regulatory body;

vi. have been part of the board or senior management of an undertaking which has gone into insolvency or liquidation while this person was connected to the undertaking or within a year of the person ceasing to be connected to the undertaking;

vii. have been part of the board or senior management of an undertaking which was subject to an adverse decision or penalty by a regulatory body;

viii. have been disqualified from acting as a director, disqualified from acting in any managerial capacity, dismissed from employment or other appointment in an undertaking as a consequence of misconduct or malpractice;

ix. have been otherwise fined, suspended, disqualified, or been subject to any other sanction in relation to fraud, embezzlement or in connection with the provision of financial or data services, by a government, regulatory or professional body; and

x. is subject to any investigation, or pending judicial, administrative, disciplinary or other proceedings, including relation to fraud or embezzlement by a regulatory authority, government body, agency, or professional body.

(d) a declaration of any potential conflicts of interests that the senior management and the members of the board may have in performing their duties and how these conflicts are managed.

Article 18

Access conditions

1. An application for registration as a securitisation repository shall contain:

(a) the policies and procedures pursuant to which different types of users report and access the data in a securitisation repository, including any process for relevant users to access, view, consult, or modify the information maintained by the securitisation repository (including historical information), as well as the procedures used to authenticate the identity of users accessing the securitisation repository;

(b) a copy of the terms and conditions which determine the rights and obligations of the different types of users in relation to information maintained by the securitisation repository;

(c) a description of the different categories of access available to users;

(d) the access policies and procedures pursuant to which users shall have non-discriminatory access to information maintained by the securitisation repository;

(e) the access policies and procedures pursuant to which other service providers may have non-discriminatory access to information maintained by the securitisation repository where the relevant reporting entities have provided their written, voluntary, and revocable consent;

(f) a description of the channels and mechanisms used by the securitisation repository to disclose to users information on accessing the securitisation repository and to disclose to reporting entities information on making data available via the securitisation repository; and

(g) the procedures for providing immediate access to ESMA on all elements required for ESMA to fulfil its responsibilities set out in the Securitisation Regulation.

The information referred to in points (a)-(d) shall be specified for each the following categories of users:

    i.   internal users;

    ii. originators, sponsors, and SSPEs;

    iii. entities listed in Article 17(1) of the Securitisation Regulation;

    iv. non-reporting third parties;

    v. other service providers; and

    vi. other categories of users.

Article 19

Pricing policy transparency

1. An application for registration as a securitisation repository shall contain a description of the applicant's:

(a) pricing policy, including any existing discounts and rebates and conditions to benefit from such reductions;

(b) fee structure for providing any securitisation repository and ancillary services including the estimated cost of the securitisation repository services and ancillary services, along with the details of the methods used to account for the separate cost that the applicant may incur when providing securitisation repository services and ancillary services; and

(c) methods used to make the information available for users, including a copy of the fee structure where securitisation repository services and ancillary services shall be unbundled.

For the purposes of point (b), the fee structure shall include the fees charged by the repository for transferring data to another securitisation repository or receiving data transferred from another securitisation repository.

2. An application for registration as a securitisation repository shall contain evidence that, in the event of a transfer of data at the request of a reporting entity registered with the applicant, the fees charged by the applicant for transferring or receiving such data are cost-related and non-discriminatory.

3. An application for registration as a securitisation repository shall contain evidence that, in the event that the registration of the securitisation repository is withdrawn, neither the new nor the old securitisation repository(s) should charge any fees or require other compensation or remuneration for the transfer of data.

Article 20

Operational risk

1. An application for registration as a securitisation repository shall contain:

(a) a detailed description of the resources available and procedures designed to identify and mitigate operational risk and any other material risk to which the applicant is exposed, including a copy of any relevant policies, methodologies, internal procedures and manuals;

(b) a description of the liquid net assets funded by equity to cover potential general business losses in order to continue providing services as a going concern,

(c) an assessment of the sufficiency of the applicant's financial resources with the aim of covering the operational costs of a wind-down or reorganisation of the critical operations and services over at least a six-months period;

(d) the applicant's business continuity plan and an indication of the policy for updating the plan. In particular, the plan shall include:

i. all business processes, resources, escalation procedures and related systems which are critical to ensuring the securitisation repository services of the applicant, including any relevant outsourced service and including the securitisation repository strategy, policy and objectives towards the continuity of these processes;

ii. the arrangements in place with other financial market infrastructure providers including other securitisation repositories;

iii. the arrangements to ensure a minimum service level of the critical functions and the expected timing of the completion of the full recovery of those processes;

iv. the maximum acceptable recovery time for business processes and systems, having in mind the deadline for reporting to securitisation repositories as provided

for in Article 7(1) of the Securitisation Regulation and the volume of data that the securitisation repository needs to process within the quarterly period;

    v. the procedures to deal with incident logging and reviews;

    vi. periodic testing programme and the results and follow-up actions resulting from any tests. Such tests shall cover an adequate range of possible scenarios, in the short and medium term, including but not limited to system failures, natural disasters, communication disruptions, loss of key staff and inability to use the premises regularly used. The tests shall also identify how hardware, software, and communications respond to potential threats, specifying systems unable to cope with the scenarios;

    vii. the number of alternative technical and operational sites available, their location, the resources when compared with the main site and the business continuity procedures in place in the event that alternate sites need to be used;

    viii. information on access to a secondary business site to allow staff to ensure continuity of the service if a main office location is not available;

    ix. plans, procedures and arrangements for emergencies handling and personnel safety;

    x. plans, procedures and arrangements to manage crises, to coordinate the overall business continuity efforts and to determine their timely (within given recovery time objective) and effective activation, mobilisation and escalation capabilities;

    xi. plans, procedures and arrangements to recover the applicant's system, application and infrastructure components within the prescribed recovery time objective;

    xii. details on staff training on the operation of the business continuity arrangements, individuals' roles including specific security operations personnel ready to react immediately to a disruption of services;

(e) a description of the arrangements for ensuring the applicant's securitisation repository activities in case of disruption and the involvement of securitisation repository users and other third parties in those arrangements;

(f) a description of the applicant's arrangements for publishing on its website and promptly informing ESMA as well as the applicant's users, of any service interruptions or connection disruptions as well as the time estimated to resume a regular service;

(g) a description of the applicant's arrangements permitting its staff to continuously monitor in real-time the performance of its IT systems.

2. An application for registration as a securitisation repository shall include procedures to ensure the orderly substitution of the securitisation repository where requested by a reporting entity or where a securitisation repository's registration is to be withdrawn, and shall include procedures for:

(a) the transfer of data to other securitisation repositories; and

(b) the receipt of data from other securitisation repositories.

Article 21

Security

1. An application for registration shall demonstrate the applicant's procedures and arrangements for physical and electronic security designed to:

    (a) protect its IT systems from misuse or unauthorised access;

    (b) minimise the risks of attacks against the information systems as defined in Article 2(a) of Directive 2013/40/EU of the European Parliament and of the Council[35];

    (c) prevent unauthorised disclosure of confidential information;

    (d) ensure the security and integrity of the data.

2. The application shall demonstrate the applicant's arrangements to promptly identify and manage the risks identified in paragraph 1.

3. In respect of breaches in the physical and electronic security measures referred to in paragraphs 1 and 2, the application shall demonstrate the applicant's arrangements to promptly notify:

    (a) ESMA and provide an incident report, indicating the nature and details of the incident, the measures adopted to cope with the incident and the initiatives taken to prevent similar incidents; and

    (b) its users that have been affected by the security breach.

Article 22

Outsourcing

1. Where an applicant arranges for activities to be performed on its behalf by third parties, including undertakings with which it has close links, it shall ensure that the third party service provider has the ability and the capacity to perform the activities reliably and professionally.

2. The applicant shall specify which of the activities are to be outsourced, including:

    (a) the scope of those services, the granularity of the activities as well as conditions under which those activities are rendered, and their timelines;

    (b) service level agreements with clear roles and responsibilities, metrics and targets for every key requirement of the securitisation repository that is outsourced, the methods employed to monitor the service level of the outsourced functions, and the measures or actions to be taken in the event of not meeting service level targets;

    (c) a copy of the contracts governing such arrangements, including the identification of the third party service provider;

---

[35] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

(d) external reports on the outsourced activities, where available; and

(e) the organisational measures and policies with respect to outsourcing and the risks posed by it as specified in paragraph 4.

3. The application for registration shall demonstrate that the outsourcing does not reduce the applicant's ability or power to perform senior management or management body functions.

4. The application for registration shall demonstrate how the applicant remains responsible for any outsourced activity and the applicant's organisational measures to ensure:

(a) that it assesses whether the third party service provider is carrying out outsourced activities effectively and in compliance with applicable laws and regulatory requirements and adequately addresses identified failures;

(b) the identification of risks in relation to outsourced activities and adequate periodic monitoring;

(c) adequate control procedures with respect to outsourced activities, including effectively supervising the activities and their risks within the applicant;

(d) adequate business continuity of outsourced activities;

For the purposes of point (d), the applicant shall provide information on the business continuity arrangements of the third party service provider, including an assessment of its quality and, where needed, improvements that have been requested.

5. Where the third party service provider is supervised by a regulatory authority, an applicant shall provide information demonstrating that the third party service provider cooperates with that authority in connection with outsourced activities.

Article 23

Verification of completeness and consistency of information submitted

1. An application for registration as a securitisation repository shall contain the procedures put in place by the applicant in order to:

(a) authenticate the identity of the user accessing the securitisation repository;

(b) authorise and permit the recording of data reported for the relevant securitisation;

(c) verify the completeness and consistency of the schema definition of the data reported to the securitisation repository, in accordance with [ref to disclosure ITS], including the individual checks used by the applicant to achieve these aims as well as procedures for interacting with reporting entities following the checks;

(d) verify that the logical sequence of the data is maintained at all times;

(e) verify the completeness and consistency of the content of the information submitted, in accordance with [ref to operational standards RTS], including:

i. the written confirmation as regards documentation submitted under Article 7(1)(b), 7(1)(c), 7(1)(d), 7(1)(f) and sub-paragraph 3 of Article 7(1) of the Securitisation Regulation ,

ii. a list and description of the checks used by the applicant to assess the completeness and consistency of data submitted under Articles 7 and 17 of the Securitisation Regulation and as set out in [ref to operational standards RTS];

(f) verify and highlight duplicate submissions;

(g) identify unreported information on which there is an obligation to report under Articles 7 and 17 of the Securitisation Regulation;

(h) produce the following items, in accordance with [ref to operational standards RTS]:

i. unique securitisation identifiers;

ii. data completeness scores; and

iii. end-of-day reports.

(i) provide feedback to the securitisation reporting entities on the verifications performed;

(j) notify ESMA of any errors, omissions, or failure to submit information that is required to be reported under Articles 7 and 17 of the Securitisation Regulation;

(k) in exceptional circumstances, amend information in an information item upon request from the reporting entity, when that entity cannot amend its own information for technical reasons.

Article 24

Check of consistency of information stored

1. With respect to information produced by the applicant, pursuant to [ref to operational standards RTS], an application for registration as a securitisation repository shall contain the procedures put in place by the applicant in order to:

(a) ensure that it accurately and successfully publishes the information received from reporting entities, without itself introducing any errors or omitting information;

(b) ensure that it corrects information containing errors or omissions, and notifies its users and ESMA of any errors or omissions.

Article 25

Confidentiality

1. An application for registration as a securitisation repository shall contain the internal policies, procedures and mechanisms preventing any use of information maintained in the prospective securitisation repository:

(a) for illegitimate purposes;

(b) for disclosure of confidential information;

(c) not permitted for commercial use.

2. The internal policies, procedures and mechanisms shall include the internal procedures on the staff permissions for using passwords to access the data, specifying the staff purpose and the scope of data being viewed and any restrictions on the use of data.

3. Applicants shall provide ESMA with information on the processes to keep a log identifying each staff member accessing the data, the time of access, the nature of data accessed and the purpose.

Article 26

Recordkeeping policy

1. An application for registration as a securitisation repository shall contain information:

   (a) on the recordkeeping systems, policies and procedures that are used in order to ensure that data reported is stored in line with Article 80(3) of Regulation (EU) No 648/2012,

   (b) on the recordkeeping systems, policies and procedures that are used in order to ensure that that data reported is modified appropriately and in accordance with relevant legislative or regulatory requirements;

   (c) about the receipt and administration of data, including any policies and procedures put in place by the applicant to ensure:

   i.   a timely and accurate registration of the information reported;

   ii. the record-keeping of all reported information relating to the receipt, modification, or termination of a securitisation in a reporting log ;

   iii. that the data is maintained both online and offline; and

   iv. that the data is adequately copied for business continuity purposes.

2. The application for registration shall include the applicant's policies and procedures to promptly record the information produced by the securitisation repository under [ref. to operational standards RTS] and maintain it for at least 10 years following the termination of the securitisation.

Article 27

Payment of fees

1. An application for registration as a securitisation repository shall contain proof of payment of the relevant registration fees as established in [insert reference to Commission Delegated Regulation to be adopted based on ESMA's technical advice under Article 14 of the Securitisation Regulation].

Article 28

Verification of the accuracy and completeness of the application

1. Any information submitted to ESMA during the registration process shall be accompanied by a letter signed by a member of the board of the securitisation repository and of the senior management, attesting that the submitted information is accurate and complete to the best of their knowledge, as of the date of that submission.

2. The information shall also be accompanied, where relevant, with the relevant corporate legal documentation certifying the accuracy of the application data.

Article 29

Information requirements for a registered trade repository seeking to provide securitisation repository services

1. Notwithstanding paragraphs (3) and (4) of Article 2, an application for an extension of registration for the purposes of Article 7 of the Securitisation Regulation in the case of a trade repository already registered under Chapter 1 of Title VI of Regulation (EU) No 648/2012 or under Chapter III of Regulation (EU) 2015/2365 of the European Parliament and of the Council[36] shall include information with regards to the following provisions of this Regulation:

    (a) Article 2, except point (d) of paragraph (2);

    (b) Article 3;

    (c) Article 5, except point (d) of paragraph (2);

    (d) Article 6;

    (e) Article 9;

    (f) Article 10(b);

    (g) Article 12;

    (h) Article 13(2);

    (i) Article 14;

    (j) Article 15;

    (k) Article 16;

    (l) Article 17(1) and Article 17(2)(d);

    (m) Article 18;

    (n) Article 19;

    (o) Article 20;

---

[36] Regulation (EU) 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse and amending Regulation (EU) No 648/2012 (OJ L 337, 23.12.2015, p. 1).

(p) Article 21;

(q) Article 22;

(r) Article 23;

(s) Article 24;

(t) Article 25(2);

(u) Article 26;

(v) Article 27 ; and

(w) Article 28.

2. Information elements that are required according to this Regulation's provisions and are not mentioned in point 1 shall be provided if there is a difference between the specific element at the time of the application for registration and the version of that same element provided to ESMA most recently prior to the time of application.

Article 30

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, […]

For the Commission

The President

3.5 Annex V: Draft ITS on information to be provided in the application for the registration of a securitisation repository

Draft

COMMISSION DELEGATED REGULATION (EU) …/..

supplementing Regulation (EU) 2017/2402 of the European Parliament and of the Council with regard to Implementing Technical Standards on information to be provided in the application for the registration of a securitisation repository

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2017/2402 of the European Parliament and of the Council laying down common rules on securitisation and creating a European framework for simple, transparent, and standardized securitisation and amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, and Regulations (EC) No 1060/2009 and (EU) No 648/2012 ('the Securitisation Regulation'), and in particular Article 10 thereof,

Whereas:

(1) Article 10(8) of the Securitisation Regulation requires the European Securities and Markets Authority (ESMA) to submit by 18 January 2019 draft ITS to be adopted by the Commission, specifying the format of the application for securitisation repositories, pursuant to Article 10(7)(b)-(c) of the Securitisation Regulation. These securitisation repositories will be registered and supervised by ESMA.

(2) Pursuant to the first sub-paragraph of Article 10(8), ESMA shall develop a simplified format for the securitisation repository application, where an applicant is a trade repository already registered under Title VI, Chapter 1 of Regulation (EU) No 648/2012 or under Title I, Chapter III of Regulation (EU) No 2015/2365.

(3) Any information submitted to the European Securities and Markets Authority (ESMA) in an application for registration of a securitisation repository should be provided in a durable medium, which enables its storage for future use and reproduction.

(4) In order to facilitate the identification of the information submitted by a securitisation repository, documents included with an application should bear a unique reference number.

(5) [This Regulation is based on the draft Implementing Technical Standards submitted by ESMA to the Commission in accordance with Article 10 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council[37].]

(6) [ESMA has conducted an open public consultation on the draft ITS on which this Regulation is based, analysed the potential related costs and benefits and requested the opinion of the Securities and Markets Stakeholder Group established by Article 37 of Regulation (EU) No 1095/2010.]

HAS ADOPTED THIS REGULATION

Article 1

Identification, legal status and types of securitisations

1. An application for registration shall be provided in an instrument which stores information in a durable medium as defined in Article 2(1)(m) of Directive 2009/65/EC of the European Parliament and of the Council[38].

2. An application for registration shall be submitted in English.

3. An application for registration shall be submitted using the formats set out in Annex 1.

4. An application for an extension of registration in the case of a trade repository already registered under Chapter 1 of Title VI of Regulation (EU) No 648/2012 or under Chapter III of Regulation (EU) 2015/2365 of the European Parliament and of the Council[39] shall be submitted using the formats set out in Annex 2.

5. A securitisation repository shall give a unique reference number to each document it submits and shall ensure that the information submitted clearly identifies which specific requirement of the delegated act, with regard to RTS specifying the details of the application for registration of securitisation repositories adopted pursuant to Article 10(6) of the Securitisation Regulation it refers to, in which document that information is provided, and also provides a reason if the information is not submitted as outlined in the document references section of the Annex.

---

[37] OJ L 331, 15.12.2010, p. 84

[38] OJ L 302, 17.11.2009, p. 32.

[39] Regulation (EU) 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse and amending Regulation (EU) No 648/2012 (OJ L 337, 23.12.2015, p. 1).

Article 2

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, […]

For the Commission

The President

Annex 1 – Formats for an application for registration

Table 1

GENERAL INFORMATION	
Date of application	
Corporate name of securitisation repository	
Legal Entity Identifier (LEI) registered with the Global Legal Entity Identifier Foundation	
Legal address	
The securitisation types, risk transfer methods, and underlying exposure types for which the applicant repository is applying to be registered	
If the applicant is authorised or registered by a competent authority in the Member State where it is established, the name of the authority and any reference number related to the authorisation or registration	
Name of the person assuming the responsibility of the application	
Contact details of the person assuming the responsibility of the application	
Name of other person(s) responsible for the securitisation repository compliance	
Contact details of the person(s) responsible for the securitisation repository compliance	
LEI of any parent company registered with the Global Legal Entity Identifier Foundation	
LEI of any ultimate parent company (if different from parent) registered with the Global Legal Entity Identifier Foundation	

Table 2

DOCUMENT REFERENCES			
Article of the delegated act with regard to RTS specifying the details of the application for registration of securitisation repositories adopted pursuant to Article 10(7) of the Securitisation Regulation	Unique reference number of document	Title of the document	Chapter or section or page of the document where the information is provided or reason why the information is not provided

Annex 2 – Formats for an application by a trade repository for extension of registration

Table 1

GENERAL INFORMATION	
Date of application	
Corporate name of securitisation repository	
Legal Entity Identifier (LEI) registered with the Global Legal Entity Identifier Foundation	
Legal address	
The securitisation types, risk transfer methods, and underlying exposure types for which the applicant repository is applying to be registered	
If the applicant is authorised or registered by a competent authority in the Member State where it is established, the name of the authority and any reference number related to the authorisation or registration	
Name of the person assuming the responsibility of the application	
Contact details of the person assuming the responsibility of the application	
Name of other person(s) responsible for the securitisation repository compliance	
Contact details of the person(s) responsible for the securitisation repository compliance	
LEI of any parent company registered with the Global Legal Entity Identifier Foundation	
LEI of any ultimate parent company (if different from parent) registered with the Global Legal Entity Identifier Foundation	

Table 2

DOCUMENT REFERENCES			
Article of the delegated act with regard to RTS specifying the details of the application for registration of securitisation repositories adopted pursuant to Article 10(7) of the Securitisation Regulation	Unique reference number of document	Title of the document	Chapter or section or page of the document where the information is provided or reason why the information is not provided

3.6 Annex VI: Draft Guidelines on transfer of data between securitisation repositories

Section 1 - Procedure for transfer of data at the request of a securitisation repository reporting entity

1. In the case of transfer of data requested by a reporting entity, a securitisation repository should transfer data according to the provisions set out in this Section.

2. For the purposes of this Section, data should be understood to refer to any of the items stored by the old securitisation repository.

3. Only the old securitisation repository and the new securitisation repository should carry out the transfer of securitisation data.

4. The transfer of data should be carried out by the securitisation repositories in accordance with a mutually-agreed migration plan.

5. The migration plan should contain a detailed plan (timeline) and a description of the required controls in place to ensure the timely, complete and accurate transfer of designated data.

6. All securitisation repositories involved should use a standardised migration plan template mutually agreed across the securitisation repositories and that is compliant with the content included in this Section.

7. The migration plan should contain the following information:

    (a) the scope of the data transfer, including the reporting entities whose securitisations are involved and the securitisations to be transferred;

    (b) detailed roles and responsibilities of the involved entities;

    (c) timeline and relevant milestones for the transfer;

    (d) the controls required to ensure the confidentiality of the transferred data, including the type of encryption used;

    (e) the controls required to ensure the integrity and accuracy of the transferred data, including cryptographic checksums and hashing algorithms;

    (f) the controls required to ensure continuity of operations and the inter-securitisation repository reconciliation status of the elements under transfer;

    (g) cut-off time of data to be transferred;

    (h) availability of data once received; and

(i) any other information that will facilitate and secure the smooth transfer of data.

8. The securitisation repositories should transfer data to each other by using the XML format and template defined in accordance with [insert ref. to disclosure ITS and operational standards RTS].

9. The securitisation repositories should use secure machine-to-machine protocols, including the SSH File Transfer Protocol, to transfer data between each other.

10. The securitisation repositories should use advanced encryption protocols and should exchange the relevant public encryption keys with their peers. To ensure the seamless functioning of data encryption, the securitisation repositories should test in advance that they are able to encrypt and decrypt each other's data files.

11. The old securitisation repository should identify the number of securitisations and the number of corresponding files (by unique securitisation identifier, item code and submission timestamp) that will be transferred to the new securitisation repository. The old securitisation repository should request the reporting entity's sign-off of the files to be transferred to the new securitisation repository and should resolve all discrepancies at the earliest convenience and no later than in five working days.

12. For every file generated and transferred, the old securitisation repository should generate and include in the data transfer a cryptographic checksum according to a mutually-agreed hashing algorithm.

13. The transfer of data should be carried out, as a general principle, on a non-working day. The old and the new securitisation repository can however agree on carrying it out on a working day depending on the expected volume of the transfer.

14. As soon as the transfer of securitisations is confirmed by the new securitisation repository, the old securitisation repository should not accept further data submissions relating to the securitisation subject to transfer to the new securitisation repository.

15. Until the transfer of all the relevant files subject to the transfer is completed, the new securitisation repository should not accept further data submissions relating to the securitisation subject to transfer to the new securitisation repository.

16. Once the data transfer is completed, the new securitisation repository should treat the data in the same way as other data received from reporting entities. The data should be subject to the provisions set out in these Guidelines, in [ref. to operational standards RTS] and in [ref. to disclosure RTS/ITS].

17. In the case of transfer of data requested by a reporting entity, and when the registration of the old securitisation repository is not withdrawn nor in the process to be withdrawn, the scope of the data should comprise at least:

(a) all information received by the old securitisation repository on that reporting entity's securitisations as set out in [ref. to disclosure RTS];

(b) the unique securitisation identifiers produced by the old securitisation repository, as per [ref. to operational standards RTS]. for that reporting entity's securitisations;

(c) the reporting log on that reporting entity's securitisations which records the reason or reasons for any modification, the unique securitisation identifier, item code, submission timestamp, date, timestamp and a clear description of the changes (including the old and new contents of the relevant data) pertaining to the securitisation(s).

The data under points (a) and (b) should be transferred, on a best effort basis, in a single instance.

18. In case all the data in the scope of the migration plan cannot be transferred in a single instance, the securitisation repositories should transfer the data in accordance with the following order:

(a) Securitisations whose data is to be transferred and that have not matured as at the date of transfer:

    i.   the latest submission of the templates set out in [ref. to disclosure RTS];

    ii.   the latest submission of the available items referred to in Table 2 in Annex 1 in [ref. to operational standards RTS], with the exception of the templates set out in [ref. to disclosure ITS];

    iii.   all other information received by the securitisation repository as set out in [ref. to disclosure RTS and operational standards RTS]; and subsequently

    iv.   the reporting log which records the reason or reasons for any modification, the unique securitisation identifier, item code, submission timestamp, date, timestamp and a clear description of the changes (including the old and new contents of the relevant data) pertaining to the securitisation(s).

(b) Securitisations whose data is to be transferred and that have already matured as at the date of transfer:

    i.   the latest submission of the templates set out in [ref. to disclosure ITS];

    ii.   the latest submission of the available items referred to in Table 2 in Annex 1 in [ref. to operational standards RTS], with the exception of the templates set out in [ref. to disclosure ITS];

    iii.   all other information received by the securitisation repository as set out in [ref. to disclosure RTS and operational standards RTS]; and subsequently

iv. the reporting log which records the reason or reasons for any modification, the unique securitisation identifier, item code, submission timestamp, date, timestamp and a clear description of the changes (including the old and new contents of the relevant data) pertaining to the securitisation(s).

19. The old and the new securitisation repository should each adhere to the following process:

(a) The securitisation repositories should agree the migration plan for the data transfer as soon as possible and no later than in five working days after the request is received.

(b) As soon as the elements for the securitisations of the reporting entity are transferred to the new securitisation repository, the new securitisation repository should confirm this, including the date of transfer completion, to the affected reporting entity, the old securitisation repository, and the users registered with the new securitisation repository. The old securitisation repository should confirm this, including the date of transfer completion, to the users registered with the old securitisation repository.

(c) If a transfer of data is requested by a reporting entity, the old securitisation repository should isolate and keep safely the transferred data, by applying the same recordkeeping policies, procedures and safeguards to the transferred data as to the rest of securitisation data reported to and made available by that securitisation repository, for as long as prescribed according to Article 26 and should ensure the retrieval of data in no more than seven calendar days.

(d) After signing the relevant contractual agreement with the reporting entity, the new securitisation repository communicates to and agrees with the old securitisation repository the migration plan elaborated in accordance with this Section.

(e) The new securitisation repository notifies ESMA by email about the transfer.

(f) The old securitisation repository determines and agrees with the reporting entity the following aggregate information regarding the securitisations of the reporting entity subject to transfer:

i. the total number of securitisations

ii. the total number of items (using the codes set out in Table 2 in Annex 1 in [ref. to operational standards RTS] and the associated submission timestamps)

(g) The old securitisation repository should request the reporting entity's confirmation of the accuracy of the information above vis-à-vis the reporting entity's own records. In case of a mismatch, the old securitisation repository should reconcile the relevant numbers with the reporting entity and agree on the final list of items reports that will be migrated. The old securitisation repository should solve all discrepancies at the earliest convenience and in no later than five working days.

(h) Once the number of securitisations and records are confirmed, the old securitisation repository should proceed with generating the relevant file(s) in accordance with this Section. The old and new securitisation repositories execute the migration plan. The old securitisation repository should transfer the files generated to the new securitisation repository, which acknowledges the file transfer.

(i) In case the volume of files is manageable, the old securitisation repository should transfer all files at the same time.

(j) In case the volume of files does not allow the simultaneous transfer, the sequence included in paragraph 18 of this Section should be followed.

(k) The files should be transferred within a predetermined weekend or, in case the volume of files does not allow the simultaneous transfer, within a predetermined weekend and at the earliest opportunity within the next calendar week.

(l) The new securitisation repository should determine the following figures and information for the received records and verify the completeness of the transfer:

  i. the total number of securitisations

  ii. the total number of items (using the codes set out in Table 2 in Annex 1 in [ref. to operational standards RTS] and the associated submission timestamps)

(m) The new securitisation repository should request the reporting entity's confirmation of the accuracy of the information above vis-à-vis the reporting entity's own records. In case there is a mismatch, the two securitisation repositories should together try to reconcile the relevant numbers with the reporting entity until an agreement is achieved—the old securitisation repository should initiate and coordinate this process.

(n) The new securitisation repository should inform its registered users that the reporting entity has switched to it.

(o) The old securitisation repository should remove the migrated securitisations from any data aggregations or other reports produced as set out in [ref. operational standards RTS].

(p) The old securitisation repository should retain the reporting logs for each securitisation that has been transferred for at least 10 years following the maturity of the relevant securitisation.

Section 2 - Procedure for migration in case of withdrawal of registration

2. When the registration of a securitisation repository is to be withdrawn, it should transfer its data according to the provisions set out in this Section.

3. For the purposes of this Section, data should be understood to refer to any of the items stored by the old securitisation repository.

4. Only the old securitisation repository and the new securitisation repository should carry out the transfer of securitisation data.

5. The transfer of data should be carried out by the securitisation repositories in accordance with a mutually-agreed migration plan. The migration plan should contain a detailed plan (timeline) and a description of the required controls in place to ensure the timely, complete and accurate transfer of designated data.

6. All securitisation repositories involved should use a standardised migration plan template mutually agreed across the securitisation repositories and that is compliant with the content included in this Section.

7. The migration plan should contain the following information:

   (a) the scope of the data transfer, including the reporting entities whose securitisations are involved and the securitisations to be transferred;

   (b) detailed roles and responsibilities of the involved entities;

   (c) timeline and relevant milestones for the transfer;

   (d) the controls required to ensure the confidentiality of the transferred data, including the type of encryption used;

   (e) the controls required to ensure the integrity and accuracy of the transferred data, including cryptographic checksums and hashing algorithms;

   (f) the controls required to ensure continuity of operations and the inter-securitisation repository reconciliation status of the elements under transfer;

   (g) cut-off time and data availability; and

   (h) any other information that will facilitate and secure the smooth transfer of data.

8. The securitisation repositories should transfer data to each other by using the XML format and template defined in accordance with [insert ref. to disclosure ITS and operational standards RTS].

9. The securitisation repositories should use secure machine-to-machine protocols, including the SSH File Transfer Protocol, to transfer data between each other.

10. The securitisation repositories should use advanced encryption protocols and should exchange the relevant public encryption keys with their peers. To ensure the seamless functioning of data encryption, the securitisation repositories should test in advance that they are able to encrypt and decrypt each other's data files.

11. The old securitisation repository should identify the number of securitisations and the number of corresponding files (by unique securitisation identifier, item code and submission timestamp) that will be transferred to the new securitisation repository. The old securitisation repository should request the reporting entity's sign-off of the files to be transferred to the new securitisation repository and should resolve all discrepancies at the earliest convenience and no later than in five working days.

12. For every file generated and transferred, the old securitisation repository should generate and include in the data transfer a cryptographic checksum according to a mutually-agreed hashing algorithm.

13. The transfer of data should be carried out, as a general principle, on a non-working day. The old and the new securitisation repository can however agree on carrying it out on a working day depending on the expected volume of the transfer.

14. As soon as the transfer of securitisations is confirmed by the new securitisation repository, the old securitisation repository should not accept further data submissions relating to the securitisation subject to transfer to the new securitisation repository.

15. Until the transfer of all the relevant files subject to the transfer is completed, the new securitisation repository should not accept further data submissions relating to the securitisation subject to transfer to the new securitisation repository.

16. Once the data transfer is completed, the new securitisation repository should treat the data in the same way as other data received from reporting entities. The data should be subject to the provisions set out in these Guidelines, in [ref. to operational standards RTS] and in [ref. to disclosure RTS/ITS].

17. Following the transfer of records of a reporting entity to another securitisation repository, the old securitisation repository should not charge any fees or require other compensation or remuneration for the recordkeeping of these records.

18. The transfer of data should comprise:

    (a) all the details of securitisations reported to the securitisation repository, including the rejected ones, and

    (b) the associated reporting logs which records the reason or reasons for any modification, the unique securitisation identifier, item code, submission timestamp, date, timestamp and a clear description of the changes (including the old and new contents of the relevant data) pertaining to the securitisation(s).

19. In case all the data in the scope of the migration plan cannot be transferred in a single instance, the securitisation repositories should transfer the data in accordance with the following order:

   (a) Securitisations whose data is to be transferred and that have not matured as at the date of transfer:

      i.   the latest submission of the templates set out in [ref. to disclosure ITS];

      i.   the latest submission of the available items referred to in Table 2 in Annex 1 in [ref. to operational standards RTS], with the exception of the templates set out in [ref. to disclosure ITS];

      ii.   all other information received by the securitisation repository as set out in [ref. to the disclosure RTS/ITS and operational standards RTS]; and subsequently

      ii.   the reporting log which records the reason or reasons for any modification, the unique securitisation identifier, item code, submission timestamp, date, timestamp and a clear description of the changes (including the old and new contents of the relevant data) pertaining to the securitisation(s).

   (b) Securitisations whose data is to be transferred and that have already matured as at the date of transfer:

      i.   the latest submission of the templates set out in [ref. to disclosure ITS];

      iii. the latest submission of the available items referred to in Table 2 in Annex 1 in [ref. to operational standards RTS], with the exception of the templates set out in [ref. to disclosure ITS];

      iv.   all other information received by the securitisation repository as set out in [ref. to disclosure RTS and operational standards RTS]; and subsequently

      ii.   the reporting log which records the reason or reasons for any modification, the unique securitisation identifier, item code, submission timestamp, date, timestamp and a clear description of the changes (including the old and new contents of the relevant data) pertaining to the securitisation(s).

20. The migration plan(s) for data transfer should be included as part of the wind-down plan presented by the securitisation repository to ESMA.

21. The following procedure should be followed by the old securitisation repository and the new securitisation repository. The old securitisation repository should provide to ESMA enough evidence that any and all transfers required under this Section have been successful.

   (a) Notification:

i. In the event of a voluntary withdrawal of registration (i.e. withdrawal is requested by the old securitisation repository), the old securitisation repository should notify ESMA in advance of the intended date of cessation of operations and should then immediately notify the affected reporting entities and registered users. For securitisation repositories with more than 50 reporting entities or 100 registered users at the time of repository's decision to cease operations or the notice of intention to withdraw registration (whichever is earlier), notice should be at least nine months. In other cases, the advance notice should be at least six months.

ii. In the event of a non-voluntary withdrawal of registration (i.e. withdrawal is not requested by the old securitisation repository), ESMA notifies the other registered securitisation repositories that they should receive data that was originally reported to the old securitisation repository.

(b) The old securitisation repository(s) prepares the migration plan, as detailed in this Section, and submits it to ESMA and the new securitisation repository(s). ESMA and the other involved securitisation repositories raise any potential objections or concerns and after resolving them all parties agree on the migration plan details.

(c) The old securitisation repository identifies the securitisations subject to transfer, and provides ESMA and the other involved securitisation repositories (as part of the migration plan or separately) the following information regarding the elements subject to transfer per securitisation repository:

i. the total number of securitisations

ii. the total number of items (using the codes set out in Table 2 in Annex 1 in [ref. to operational standards RTS] and the associated submission timestamps)

(d) Once the number of securitisations and records are confirmed, the old securitisation repository should proceed with generating the relevant file(s) in accordance with this Section. The old and new securitisation repositories execute the migration plan. The old securitisation repository should transfer the files generated to the new securitisation repository, which acknowledges the file transfer. The sequence prioritisation included in paragraph 18 of this Section is followed.

(e) The files should be transferred within a predetermined weekend or, in case the volume of files does not allow the simultaneous transfer, within a predetermined weekend and at the earliest opportunity within the next calendar week. Securitisations to be transferred should be segmented per reporting entity.

(f) Any issues identified and progress made are reported regularly to ESMA in a timely manner.

(g) The new securitisation repository(s) should determine the following figures and information for the received records and verify the completeness of the transfer:

i. the total number of securitisations

ii. the total number of items (using the codes set out in Table 2 in Annex 1 in [ref. to operational standards RTS] and the associated submission timestamps)

(h) The new securitisation repositories should notify ESMA and the old securitisation repository of the result of the verification. In case of verification failure, the root cause is investigated by both parties (old and new securitisation repositories) and the transfer process is repeated until the data transfer is deemed successful by ESMA.

(i) Once the transfer(s) has been completed, the new securitisation repository(s) should notify the relevant reporting entities and the registered users (by email) of the successful conclusion of the transfer.

(j) The old securitisation repository should isolate and keep safely the transferred data for as long as stipulated in Article 26, by applying the same recordkeeping policies, procedures and safeguards to the transferred data as to the rest of the data, until the date of actual cessation of operations and should ensure the timely retrieval of data in no more than seven calendar days. At the date of actual cessation of operations, the old securitisation repository should perform a secure destruction/deletion, in accordance with leading practices and the most reliable available techniques, with the aim of ensuring that data cannot be undeleted or recovered after that date.

(k) The old securitisation repository should destroy/delete the transferred data when this is permitted and following the relevant principles for secure deletion/destruction set out in this Section.