



Data management and sharing governance policy and regulations for the Regional Minerals Database (RDBMF) of the ICGLR

February 2025

Author: Daniel Homorodean

This publication of the International Conference of the Great Lakes Region (ICGLR) has been funded by the European Union as part of the Peace and Security in the Great Lakes Region project, implemented by IMPACT. Its contents are the sole responsibility of the ICGLR and IMPACT and do not necessarily reflect the views of the European Union.



**Funded by
the European Union**

Table of Contents

1. Acronyms.....	3
2. General objective	3
3. Approach	4
4. Results of data collection through interviews and surveys.....	7
5. Analysis	10
6. Principles for the implementation of a data management and sharing governance policy at the level of ICGLR.....	17
6.1. Data collection in the National Minerals Database	22
6.2. Data validation into the NMD	23
6.3. Data update in the NMD	23
6.4. Data acquisition into the RDBMF	23
6.5. Data updating into the RDBMF	27
6.6. Data storage in the RDBMF	27
6.7. Data sharing management	29
6.8. Data exporting	30
6.9. Data archiving.....	31
6.10. Data deletion	32
7. Data management and sharing governance policy and regulations for the Regional Minerals Database (RDBMF)	33
7.1. Introduction.....	33
7.2. Approach	33
7.3. General requirements	35
7.3.1. ICGLR Minerals Data Semantic Standard	35
7.3.2. Data validation	35
7.3.3. Data sharing control	35
7.4. Specific requirements for each stage in the data life cycle	36
7.4.1. Data acquisition into the RDBMF	36
7.4.2. Data updating into the RDBMF.....	36
7.4.3. Data storage in the RDBMF	37
7.4.4. Data sharing.....	38
7.4.5. Archiving of data	38
7.4.6. Deletion of data.....	38

1.Acronyms

ICGLR	International Conference on the Great Lakes Region
RDBMF	Regional Database of Mineral Flows
NMD	National Minerals Database
RCM	Regional Certification Mechanism
API	Application programming interface

2.General objective

ICGLR is mandated to govern a system for exploitation, monitoring and verification of natural resources within the Great Lakes Region, defined in the Regional Certification Mechanism and documented in the RCM Manual.

The data collected by each ICGLR member country in relation to their mining activity, in particular related to the mining, processing and trading of the Designated Minerals, should support a regional-level auditing process performed by ICGLR. Such tracking and reporting activities require that the national datasets are collected in a common data repository, the Regional Minerals Database (RDBMF, or RMD).

The RDBMF, including all the processes related to the stored data, should be governed by a comprehensive agreed-upon set of rules, guidelines and regulations, in the form of a Policy, that should support the purpose of the ICGLR and in the same time ensure that the member countries, the data owners, understand, accept and comply with the policies, in a manner that protects their rights and interests.

3.Approach

The development of the policy was prepared through a set of activities including analysis and information collection from the ICGLR member states.

The initial study was focused on the set of documents developed by ICGLR, in particular the following:

- Manual of the Regional Certification Mechanism (RCM) of the International Conference on the Great Lakes Region (ICGLR), first and second (2019) editions
- ICGLR Appendices to the Certification Manual
- Data Transfer Procedures for Regional Database for Mineral Flows developed in 2016
- The set of documents developed in 2016 through ELL-IPIS for the RDBMF, including High-Level Requirements Definition for the ICGLR Regional Mineral Tracking Database, ICGLR Regional Mineral Database_Detailed Requirements, ICGLR_RDBMF_TransferProcedures
- Assessments of the RDBMF developed by GIZ in 2023
- The assessment of the RDBMF developed by Arxia in 2024, contracted by GIZ

The analysis included a direct engagement with the ICGLR member countries, represented by the appointees in the Technical Committee. The interaction was possible with 11 out of the 12 member states. DR Congo did not respond to the engagement requests transmitted through the ICGLR secretariat.

The individual engagement with each member state focused on the following components:

A presentation from Arxia and an initial discussion on the principles of data governance, in order to align the understanding of the topic. It focused on the data management function, emphasizing the essential elements of data governance such as the pursuit of quality, integrity, security and usability of the data collected and shared, on its entire life cycle, the related risks, the impact of the future evolution of regulations and technology, and need for policies.

A data collection form, as a survey, which can either be filled out independently by each member state or completed through a direct interview with the representative of Arxia. In practice, some

preferred to fill out the survey individually, others to answer directly through the interview. The form collected information about:

- The regulatory framework in place in the country that impacts the minerals data lifecycle
- The current status of the data collection and centralized data registries as a “single source of truth”.
- The current status of the digitalization of the minerals data lifecycle, including collection, storage, and processing.
- Existence of data models, standards or other forms that regulate the structure and format of the data that is collected and stored.
- General quantitative data related to mining, in particular those that reflect the entities defined in the RCM and the data structures specified in the RDBMF.
- The actual data structure of each of the relevant entities defined in the RCM, in the form that they are collected and stored at the level of each country, to the extent that this is specified and known.
- The perception of the country representative related to the importance and priority of the following aspects, the meaning of each being
 - data origin (who/when/where has generated the record)
 - data unicity (single source-of-truth, which should be used/accessed/interrogated by all other systems)
 - data accuracy (data is correctly reflecting the actual situation)
 - data integrity (information is consistent and valid and was not tempered or manipulated, and any change can be traced and audited at the level of who/when/what it did)
 - data access control at the national level (different levels of permissions should be in place at the national level to allow access to data, for visualization, reproduction or export)
 - data access traceability (authorized access to information should be logged, accessible for auditors, and reported/notified under specific circumstances - eg. critical data being accessed by a certain role/organization)
 - data access control at inter-national and supra-national levels (specific restricted access to information for foreign nationals or representatives of supra-national organizations)

During the interviews, the consultant emphasized the importance of a strategy and policy related to data sharing at the level of ICGLR and the importance of the input of the representatives of each country in this respect. The following discussion with each country focused on two main aspects:

- The opportunities perceived by each country in relation to the possibilities of having access to data sets provided by the other member countries
- The challenges and risks perceived by each country in relation to their data being shared with the other countries

The analysis further collaborated the information related to the technical evaluation of the RDBMF that was conducted by GIZ in 2023 and 2024 and the initial recommendations for the technical evolution of the RDBMF, as well as the proposed general conceptual architecture of the Data Sharing Solution technical system whose implementation is supported by GIZ.

The analysis considered a comprehensive approach to the entire life cycle of the minerals-related data, both in-country and in the shared form in the RDBMF and related technical components managed by the ICGLR. The data life cycle include the following stages:

- Data collection (primary, at source, in-country)
- Data acquisition into the RDBMF
- Data updating into the RDBMF
- Data storage in the RDBMF
- Data sharing management
- Data access through visual interfaces and APIs by member countries
- Data retrieval by 3rd party through APIs
- Data exporting - specific data can be exported in formats usable for other systems
- Data archiving
- Data deletion

For each of the data lifecycle stages, the consultants aimed to establish the possible approaches, challenges, and risks, taking into account the current status at the level of the ICGLR country members, the results of the interviews, and the development activities that are already in the planning phase, mainly the support of the development of a technical platform for the management of data sharing, the development of a standardized data model and a data standard

for the data exchange between countries and ICGLR secretariat, and the planned evolution of the national systems in the form of National Minerals Databases.

The analysis of the data lifecycle identified a set of questions that are influencing the data-sharing process and are related to the discipline of the data collection and sharing process. These questions were sent to the ICGLR secretariat for consideration in the discussion with the technical committee. Each of the following topics needs to be considered and its potential negative impact should be mitigated by the policy.

These questions relate to the following aspects, considering the input of the member countries into the RDBMF:

- Timing of data entry in relation to the initial data collection
- Continuity and periodicity of data entry from the member countries
- Completeness of reported data
- Repeated/identical reporting
- Reporting of duplicate but inconsistent records
- Data retention timeline
- Data deletion or controlled data hiding requested by a country post reporting

The collected information was the base for the analysis leading to the proposal of the draft policy.

4. Results of data collection through interviews and surveys

The direct discussions with the representatives of the member states and the data collected from them through the survey and direct interviews have provided relevant information for the development of the data management and sharing policy.

In terms of data collection and storage, we have different situations, as follows:

- Data is kept in mixed form, on paper registries and in Excel (Burundi, Central African Republic, and Sudan).

- Data is digitally available, in Excel and a central national system currently in development (Kenya).
- Data is kept in mixed form, on paper registries, in Excel and into a national system (Republic of Congo, Rwanda, Uganda, South Sudan, Zambia, and Angola)
- Data is digitally available, in dedicated software systems that are accessible by authorized personnel (Tanzania).

Where there is a central national digital storage, the following countries expressed the need to enhance or replace the current system: Uganda, South Sudan, Zambia, and the Republic of Congo.

No country currently has an adopted official mining data standard to support the collection, storage, and exchange of data.

Rwanda is in the process of developing its own data standard and has involved private stakeholders active in the supply chain to contribute to this process.

The Republic of Congo has the specific intention of developing its national standard to improve the data quality and allow data exchange.

The Central African Republic mentioned that they are in the process of defining a standardized national data structure, and that they aim to be compatible with the RCM data structure requirements, while their current storage structure (in Excel) is not compatible with the RCM requirements.

Data reliability and consistency were mentioned by several counties to be a matter of great concern, given the traditional paper-based collection of the information on-site, which can lead to errors when being transcribed, which can include misspelling of words, incorrect digits (quantities, locations, etc) The completeness of data records is also of great concern in the case of manual paper-based on-site collection.

Data accuracy was mentioned as an important problem when relying upon the collection of volumes of the lots based on the traders' self-declaration.

Data access control at the national level was also mentioned as a concern.

The consultant has requested the member states to provide the data structures that are used at the national level for each relevant data entity, in particular for mine sites and export certificates. It was expected that they would directly match the RCM requirements, as specified in Appendix 2 and Appendix 3. However, the direct declaration of the member countries has shown that there are substantial variations and divergences from the RCM data structure specification.

As the consultants did not receive actual data samples as reflected in the storage systems, but received the structures as provided by the member states representatives, it might be possible that the actual storage systems might include a larger set of data fields that could be filled, but are not usually collected on site.

In most cases, the data structures included additional information, compared to the mandatory fields defined by the RCM appendices.

Some states (Uganda, and Rwanda) have made specific efforts to adopt and use the structures required by RCM.

Regarding data retention, there is no general policy across the member states, but that follows rules in this respect mentioned minimum retention times of 5 years in an active and accessible system. Some countries mentioned that upon the elapsing of the minimum retention period, the data is archived in a state-owned storage, however there was no available information on how long should the data remain in the archive.

Angola has a specific regulation requiring that the data is kept for 10 years.

All interviewed countries were asked to give their views on the perceived value and opportunity of accessing the data shared by other countries.

Kenya is particularly interested in being able to do cross-border data comparisons, tracing mineral origins, and identifying risks of smuggling. If this is the case, such comparative visualizations could expose inaccuracies in official data, which could highlight smuggling or corruption.

For Rwanda, there is interest in data sharing and collaboration between countries. They are interested in checking if the data reported by other countries is consistent and reliable, which could impact the effectiveness of cross-border coordination and policy-making.

Uganda has explicitly expressed concerns about data sharing. They declared specifically that there is a need for a clear data-sharing policy that needs to be debated. Digital sovereignty is a

very big concern and is taken very seriously. They consider that some of the data is already available publicly, but some data need to remain private, such as individual data of the companies, and how much is produced by each company.

As Uganda is both a producer and a transit country, they see it as very important to be able to trace and match the information about the lots that enter the country and those that get out of the country. They also expressed an interest in receiving training on data governance.

Tanzania expressed the need for guidance from ICGLR regarding which data should be shared.

Sudan expressed no concerns over data sharing and trans-border access control for data.

Zambia expressed interest in information about quantities that are mined and traded.

They consider that all critical data should be hosted under national control. However, having a mutual data access agreement in place would be enough for them to agree to share data with other countries.

When certain data items can be considered “personal data” falling under the national regulation for the protection of personal data, the sharing mechanism shall make sure to adhere to the respective regulations. Specifically, these could include the location and contact data of persons, such as mine owners, if individuals.

5. Analysis

The policy defining data sharing at the level of ICGLR should consider several dimensions:

- Current specific requirements of the RCM manual that institute an obligation to the member states.
- The interests and concerns of the member states, including the perceived opportunities and risks related to the sharing and availability of data for 3rd parties.
- The current state of regulations, data standards, digital data collection and management, technical platforms at the level of member states, and of ICGLR.
- The future evolution of the data standards and technical platforms at country level and ICGLR level.

The RCM includes specific requirements that create obligations for the member countries, as well as for the ICGLR itself, in relation to the sharing of specific data.

The sharing from the member countries to ICGLR refers specifically to several datasets (as detailed below) and rules.

The RCM also introduces the notion of the “Regional Mineral Tracking Database (RMTD)”, where the member states should transfer information, and introduces the obligation to ICGLR to develop and maintain the RMTD.

Both the first edition and the second edition (2019) of the Manual of the Regional Certification Mechanism (RCM) of the International Conference on the Great Lakes Region (ICGLR) specify requirements related to the data transfer from the member states to ICGLR.

While the initial version of the RCM manual provides specific details regarding the requirement to report each type of record, the second edition of the RCM manual, from 2019, expresses the requirement in a more general term.

In between the first and second editions of the RCM manual, the Regional Minerals Database was specified, the data transfer procedures were specified, and the RMD was technically implemented. Thus the more general description of data transfer obligations given in the second edition could be supported by the work done up until that moment, both in terms of analysis and technical implementation.

The expression of the requirements for data sharing in the 2 versions of the RCM manual is coherent, the second edition does not contradict the specific requests of the first edition, as will be the more verbose, explicit formulation of the first edition can still support the nuances of further analysis.

Moreover, since the current implementation of the RMD and related technical specification stems from the analysis based on the first edition of the RCM manual, having an explicit knowledge of the original version could prove useful.

In the extracts cited below, the versions are noted v1 and v2.

The RCM manual firmly requests that each member state shall

- Share the contents and results of the yearly mine site inspections with the ICGLR Secretariat as they occur, **on a regular and timely basis** (v1 3.11).

- Share the database of mine sites and their status (Certified/Un-certified/Yellow Flagged) with the ICGLR Secretariat **on a regular and timely basis** (v1 3.13).
- Share all information regarding exports of Designated Minerals and Certificates and their issuance as may be required and requested by the ICGLR Secretariat for use in its Region Mineral Tracking Database, **in a regular and timely manner** (v1 5.3).
- Share all information from their domestic Chain of Custody Tracking systems **as may be required and requested** by the ICGLR Secretariat for use in its Regional Mineral Tracking Database, **in a regular and timely manner** (v1 4.18).
- Provide **in a timely manner** all information from the domestic Chain of Custody system **as may be requested and required** by an ICGLR Third Party Auditor (v1 4.19).
- Share all information regarding exports of Designated Minerals and Certificates and their issuance **as may be required and requested** by the ICGLR Secretariat for use in its Regional Mineral Tracking Database, **in a regular and timely manner** (v1 5.3).
- Provide **in a timely manner** all information regarding Chain of Custody of mineral consignments, Exports of Designated Minerals and Certificates **as may be requested and required** by an ICGLR Third Party Auditor or the ICGLR Mineral Chain Auditor (v1 5.4).
- **Promptly** supply to the ICGLR Secretariat **such information as it requests or requires** in order to develop and keep up to date the ICGLR Database of Exporters (v1 7.11).
- **Extend full cooperation** to and facilitate the work of ICGLR database officials **in collecting information** within Member States (v1 7.12).

RCM Manual second edition is more explicit in specifying that such transfers need to be done to the RMD.

Each Member State shall [...] Transfer to the RMD **in a compatible format and timely manner**, all country-level mine site, CoC and Exporter data contained within the Member State Mineral Database (v2 5.15).

and

Member states should [...] Transfer export and Certification records to the ICGLR Secretariat for use in the RMD (v2 4.1.7).

And

Transfer to the RMD in a compatible format and timely manner, all country-level mine site, CoC and Exporter data contained within the Member State Mineral Database (v2 5.15).

It can be observed that the requirements are formulated in such a way as to underline the urgency of the data provided, but still leave the timing imprecise.

The following expressions do not provide in themselves the possibility of the application of a procedural escalation or enforcement.

- “as may be required and requested” might be understood as the countries being free to wait for such a specific requirement from the ICGLR and to respond by updating only specific information that might be subject to the explicit request.
- “in a regular and timely manner” does not include any time bounding, as “regular” and “timely” can be interpreted at the discretion of the country, while not complying with a specific request for data sharing is not directly counting against the formulation of the RCM manual.
- “Promptly” does not include any specification of the actual deadline of a positive answer to the request.

It can be noted that section v1 7 Regional Mineral Tracking via an ICGLR database of the RCM formulates again, in an identical or quasi-identical form, the requirements for the member states expressed in sections 3,4,5, but also adds points 7.11 and 7.12 that create general unspecific obligations.

The formulation “supply [...] such information as it requests or requires” can be interpreted as the obligation to “supply ANY” information requested, or as a reinforcement of the requirements already stated on the specific type of data.

To complete the specific requirements extracted from the RCM manual, we also have the relevant obligations of the ICGLR:

ICGLR shall:

Develop and maintain an up-to-date ICGLR Regional Mine Site Database of all mine sites in the region producing Designated Minerals. The database will indicate whether each site is currently Certified (Green Flagged), Un-Certified (Red Flagged) or Yellow Flagged, along with the date and details of the latest inspection by the Member State Government, the Third Party Audit, or any supplementary inspection contracted directly by the mine site operator in case of a Red Flag.

[..]

The ICGLR Regional Mine Site database shall be publicly accessible.

(v1 3.15)

In the second edition of the RCM manual, the transfer of data is explicitly related to the Regional Minerals Database, in a compact form:

(V2 5) ICGLR Regional Mineral Database and Member State Mineral Database Requirements

The RMD and Member State Mineral Databases will host the mine site, CoC and Exporter data, which is to be obtained as part of the Mine Site Inspection, CoC tracking and export components of the RCM.

Member States are required to collect data defined in the RCM **and upload it periodically** to the RMD, in the format and scope specified in the RCM. This data, while held by the Member State, constitutes a Member State Database, with a structure equivalent to the RMD.

[..]

The RMD will be used by relevant RCM stakeholders to verify the latest Status of mine sites, CoC systems and Exporters.

[..]

Specific datasets in the RMD, as defined by the ICGLR Secretariat, will be accessible to the public.

Thus, in between v1 and v2, “in a regular and timely manner” was replaced by “periodically”. The requirement that “Specific datasets in the RMD, as defined by the ICGLR Secretariat, will be accessible to the public” gives full control for public accessibility to the ICGLR Secretariat, thus the Secretariat could, based on its decision, make publicly available all datasets or none at all.

The v1 was more specific in enforcing that “The ICGLR Regional Mine Site database shall be publicly accessible”, which is in v2 not a direct explicit requirement anymore.

While the RCM includes specific obligations for the member countries and for ICGLR in relation to the data collection and storage into the RDBMF, it does not include specific requirements related to data collection into the RDBMF from other parties.

Therefore, it can be assumed that the RDBMF is constituted solely from the data input of the member countries, such input being under the control of the member countries.

Overall, although the RCM manual includes obligations of data reporting from the Member states to the ICGLR, and includes specific requirements of timing expressed generally as “timely” or “promptly”, there is no clear specific requirement for a frequency of updating the RDBMF from the countries.

The specific time-bound requirements for reporting from the member states can be found:

In the Responsibilities of Regional Certification Mechanism Actors

Each Member state shall:

1.14. Publish Mine Site Inspection reports and mine site Status on the Member State Mineral Database **within 2 weeks of completion** by the Mine Site Inspector **for onward transfer to the RMD.**

1.15. Where a mine site has been declared Not Valid (Red) Status, **inform the ICGLR Secretariat within 7 days.**

As a general corollary, we could not agree with the assumption formulated in the “Data Transfer Procedures for the Regional Database of Mineral Flows (RDBMF)”(2016) that “A frequency of approximately monthly data transfers from the Member States **seems to be a general expectation** in the Manual, in order to support these queries and reports.”(2.5.5)

In terms of data retention in the RMD, the requirements are in

(v2) Appendix D: Data Requirements for Regional Mineral Database and Member State Database Shall hold [...] **Current and historic (last 5 years)** RCM Status (Green, Yellow, Red, Blue) of Mine Sites, CoC Systems and Exporters.

What data is subject to sharing

The RCM manual explicitly defines the information that needs to be shared from the member states to ICGLR.

The specific data to be shared in the RMD includes, as defined by Appendix D of the RCM manual:

1. All Mine Site data is required by the Regional Mineral Database (RMD) as part of the Mine Site Inspection and Certification process.
2. All CoC data required by the RCM as part of CoC tracking.
3. All Exporter data required by the RCM for export of Designated Mineral / ICGLR Certificate Issuance.

4. All reports produced by ICGLR bodies, including reports by the Regional Committee and Third-Party Auditors (TPAs).
5. Current and historic (last 5 years) RCM Status (Green, Yellow, Red, Blue) of Mine Sites, CoC Systems and Exporters.
6. A scanned copy of ICGLR Certificates issued as well as scanned copies of any paper-based Validation of mine sites, traders, Exporters, etc.
7. On-the-ground Mine Site Risk Assessment reports produced by Exporters.

There is no explicit requirement from the RCM on the possibility of data being shared with the other member countries for visualization or processing. Such a possibility is indicated in the documents developed by GIZ as a vision of a Data Sharing Solution, however its requirement is not specifically reflected by a document related to the RCM manual or RDBMF out of the original set developed in 2016.

However, during the interviews with the member countries, it was revealed that they see the possibility of accessing specific shared data sets from other countries as a substantial opportunity.

The RCM manual sets the ground for such possibility through its specification:

5. ICGLR Regional Mineral Database and Member State Mineral Database Requirements)

[..]

The RMD will have an interface that supports data interpretation by performing all queries required by the RCM. Queries will permit, for example, an overview of flows of Designated Minerals within, between and exiting ICGLR Member States. It will therefore be used for the purpose of identifying and understanding anomalies related to the Purpose of the RCM that may warrant further investigation.

*In addition, the RMD **will be used by relevant RCM stakeholders** to verify the latest Status of mine sites, CoC systems and Exporters.*

6. Principles for the implementation of a data management and sharing governance policy at the level of ICGLR

A Data management and sharing governance policy should provide a comprehensive set of rules and guidelines, formulated as requirements (must) and recommendations (should), that will support the ICGLR and the member states in conducting the processes related to managing their data.

The Data management should ensure that all data that is collected, processed and shared by each involved actor adheres to specific qualitative and quantitative objectives related to the following four main pillars:

- Quality - data is consistent, well formatted, correct, and complete for the required purpose
- Integrity - data is original, attributable, and accurate
- Security - data is secured
- Usability - data is usable for the required purposes, directly or through processing

These major pillars are defining a set of more specific requirements that need to be considered:

- Data is attributable: The producer (person or system, the source) of the data is known and uniquely identifiable
- Data is original: The data preserves its original state. It was not tempered in ways that would create problems or risks
- Data is complete for the required purpose, all data records include all required information
- Data is correct/accurate: It reflects correctly the reality.
- Data is unique when its storage relies on an individual entity that is uniquely identifiable, thus, there is no duplication in data registries.
- Data is well-formatted: adhering to a specified format or standard.
- Data is consistent: a data record referring to a data entity is found in the same form everywhere where the record is found.
- Data is accessed only by permitted stakeholders in permitted ways

- Data is auditable: all operations performed on the data, even all data access requests, are logged and can be audited.
- Data is compliant with legal regulations.

The data governance will cover the entire lifecycle of the data that needs to be shared in the context of the RCM from the Member States to ICGLR, specifically to be transmitted to the RDBMF. The data lifecycle related to RDBMF includes:

- Data acquisition into the RDBMF
- Data updating into the RDBMF
- Data storage in the RDBMF
- Data sharing management
- Data access through visual interfaces and APIs by member countries
- Data retrieval by 3rd party through APIs
- Data exporting - specific data can be exported in formats usable for other systems
- Data archiving
- Data deletion

Since the data in the RDBMF is consolidated based on the input of the Member States, the RCM Manual specifies that the respective data needs to be collected initially in a National Minerals Database, which has the same data structure as the RDBMF, or can be made compatible through a direct data mapping process.

It is important therefore to consider that relevant data governance components need to be subject to guidelines at the national level, at the level of the National Minerals Database, for the data collection, processing and preparation for submission to RDBMF.

At RDBMF level, the data governance policy needs to ensure the proper coverage over the following characteristics:

- Access control - who can access the data and in what way
- Retention rate - how long is the data kept and what happens with it in time, on long term
- Formatting - how is the data formatted semantically and technically
- Processing rules - how the data can be processed, according to the data processing & transformation use-cases that are permitted

- Residency - where is the data hosted
- Sovereignty - who has property over the data and who exercises control over it
- Protection - special and sensitive data, such for example personal data, that can be subject to additional regulations (such as the Personal Data Protection Act, etc).

Establishing a Data Management Plan will require the coverage of the following:

- Detailing how data is managed, described and stored
- Identify the data to be captured (automatically, from an analogous context, such as through sensors) or collected (manually or electronically by an operator), acquired (imported into a system from a different system)
- Define how data would be organized
- Document a data storage and preservation process
- Define data policies
- Define roles and responsibilities for the establishment, adoption and enforcement of the data management plan

The Data Management Plan is part of a larger process, which we can define as a Data Governance Framework, that includes all the phases for the definition and implementation of the plan. The following list of activities is organized chronologically, in a logical sequence.

1. Align on the objectives, success indicators and perceived challenges
2. Document guiding principles
3. Get management buy-in
4. Develop the operating model - define the data governance roles and responsibilities, describe the processes and procedures
5. Develop a framework for accountability - clear checks to make sure that everyone is accountable
6. Establish the semantic structure: taxonomies and ontologies
7. Assemble the right technology stack
8. Establish education and training process

As can be seen, the current assignment for the definition of the data management and sharing process will not cover all the points above, however all need to be taken into consideration in the bigger picture.

The discussion with the Member States has revealed several aspects that are particularly of interest to them:

- The member states are interested to have access to the data that is shared, to the extent that the data owners (other states) allow it, or the respective data is intended to be shared with them based on the RCM policy, according to their adherence to the RCM.
- The member states consider that when accessing data from other states for visualisation and comparison with their own data, the data of the other states should be correct, complete and up to date, so that comparisons could be made possible.
- The member states consider that the data that is visualized from other states needs to be original and authentic, thus having the assurance that the data is coming from the respective states and that the data was not altered by a third party or by a technical system after it was shared.
- The member states consider that it is important to maintain the sovereignty over their data, in the sense that the property over data is theirs and that they should be able to manage how and to whom they share data, to be able to choose if they share the data according to the agreements that they have adhered to, and to be able to revoke such sharing, if it would be imposed by the evolution of the situation, for example by the evolution of the political relations between states.
- The member states consider that all laws and regulations that apply nationally should also be applicable to the way they share data and the way the data is available to other stakeholders. For example, a particular attention needs to be given to the sharing of personal data, such as contact information and addresses belonging to persons.

In summary, 4 elements will need to be taken into account in order to satisfy the member states:

- Shared data should be authentic, to have a clear proof-of-origin
- Shared data should have integrity, thus to not have been mutated by systems or third parties after being shared
- Sovereignty over their own data should be a right preserved also after the data is shared
- Personal data should be protected according to the applicable national regulatory framework

Discussion points for the preparation of a data management and sharing plan

The policy and guidelines will follow the data life cycle. Although the purpose of the policy is the management and sharing in relation with the ICGLR, following the RCM and within the Regional Minerals Database, it is relevant to extend the analysis at the national level, as the way data is collected and processed in the National Minerals Database can greatly influence the sharing and following data processing activities.

Thus the life cycle of interest will be extended as follows:

1. Data collection into the NMD (National Minerals Database)
2. Data validation into the NMD
3. Data update in the NMD
4. Data acquisition into the RDBMF
5. Data updating into the RDBMF
6. Data storage in the RDBMF
7. Data sharing management
8. Data access through visual interfaces and APIs by member countries
9. Data retrieval by 3rd party through APIs
10. Data exporting - specific data can be exported in formats usable for other systems
11. Data archiving
12. Data deletion

The life cycle approach needs to follow the specific data entities that are shared and their correlation.

These correlations can be illustrated by one of the relevant data entities. According to the RCM manual,

“All Mine Site data is required by the Regional Mineral Database (RMD) as part of the Mine Site Inspection and Certification process”

Thus, as the Member States should report their data to the ICGLR through the RMD, they will need to report “all mine site data”.

Further, the life cycle applied to “all mine site data” is illustrated:

6.1. Data collection in the National Minerals Database

The Mine Site data is initially entered in the NMD. The data might be current or presumed current, as collected in the past from the field or from a system or a registry.

The Mine Site data includes three types of information:

- Immutable information (data attributes that uniquely define the mine site and cannot be altered): These are: Identification number (at the country level) and Mine site location
- Mutable information (data attributes that are not changed with a periodicity or based on a predetermined type of action, but whose change can occur in time as part of the normal evolution of the mine site). These are: Owner, License, Operator, Designated mineral (in case other designated minerals are identified)
- Updatable information (data that is changed periodically based on the requirements of the RCM or by national regulations. These are: Certification status, and Activity status.
- Appendable information (data that is added periodically based on specific occurrences of different events). This type of information builds up the history of specific data records. Examples of such information are: Mine Site Inspection (forming a history of Inspections), and Mine Site Status change (forming a Status Change History).

The same classification in three categories can be generally applied to all data entities: Immutable, Mutable, and Updatable.

Possible risks:

Data can be doubled by mistake: Due to the collection process that might be done manually or lack of validation at the input, a data record (Mine Site in our example) is doubled. At subsequent processing, one of the records can be updated, or the other. Thus the records can diverge (they are not entirely the same) but are inconsistent (at least one, or both, are not reflecting the true state of facts).

Data is not current: Records that are created in the NMD might come from old data sources (paper registries, Excel files) and might not reflect the current state of the respective data records.

Incomplete records: Collected data might not include all the information required by the RCM manual. Some data (eg. the mine site location) might not have been collected in the first place and is missing at the transfer from the original format (paper registry, Excel) into the NMD.

Incorrect records: The collected data might be incorrect due to mistakes in writing names, addresses, geocoordinates, or other information. This might include misspelling or losing of a digit or incorrect digits.

6.2. Data validation into the NMD

Data validation is the responsibility of the Member State. There should be checks in place to identify records that are incomplete and records that are duplicated.

6.3. Data update in the NMD

As the NMD reflects the structure of the RDBMF, the data records should be updated in the NMD and then the updated information should be pushed to the RDBMF.

6.4. Data acquisition into the RDBMF

Data that is created or updated in the NMD should be sent to the RDBMF.

Any data entry variant that is not fully automated is prone to introduce inconsistencies, due to possible mistakes or omissions.

The RDBMF was initially designed, based on the 2016 specification, to accept manual data entry (record by record) and import of Excel spreadsheets.

Both variants are prone to error and inconsistencies, as they require processing through direct typing or copy/paste from a primary source. At the national level, such manual or semi-manual input through Excel, can be hard to track. Records might be doubled if the monitoring of the local data source is not disciplined (which records were loaded, which not etc) and mistakes can be entered. Updates to existing records (for example, the owner of a mine site) can be very difficult, as they require identification of the record to be updated. If data is entered manually, it would be required to implement advanced automatic analysis on the RDBMF side to identify potential

duplicates, and cases when a data record was entered again, with some attributes being modified, instead of updating the initial data record.

Instead, the data transmission from the member country to the RDBMF should be done through direct submission via API, on a set periodicity and in a standardized format. The standardized format should be fully defined at semantic level and should have a commonly understood technical representation.

The technical representation can be in the form of JSON, JSON-LD, or XML based on a purposely defined schema.

The standardization and technical representation are out of the scope of the present document, but several aspects need to be mentioned:

- The ID of records, in particular the ID of mine sites, should be standardized at the level of ICGLR and used consistently by the member states and their systems, as well as the RDBMF and other systems under the operation of ICGLR.
- The data records should be semantically linked and this should reflect into the format that is transmitted from the member states to ICGLR and in the RDBMF, to allow information to be updated without having to retransmit the entire structure of data to which a record belongs (see next point for examples).
- The values of the data attributes should strictly respect formatting rules established by the standard.

The member state should transmit strictly the information that needs to be updated, not the entire structure of information. For example, reporting the new Mine Site Inspections should transmit only the information regarding the inspections, not all the information regarding the Mine Site, certainly not the immutable information. Based on the semantic linkage through ID, the RDBMF can recognize that the inspection information belongs to a certain mine site and can append it into the database in the corresponding place.

Validation is an important aspect that needs to be handled at the moment of data transmission. Data should be validated before being accepted for storage into the RDBMF.

It is preferable that the validation is performed at the member state level, before the data is transmitted. This way, corrective actions can be taken directly at the level of the data storage belonging to the member state, thus ensuring further the consistency of data at the national level.

However, the validation should be performed also before the storage in the central data vault. In case the central (ICGLR side) validation encounters problems in a data record, that specific data record will be rejected, thus not imported. However, the member state should receive, automatically, a clear message that allows a clear corrective action and a resubmission of a record, otherwise the incorrect record will not be updated and the parties involved (member state and ICGLR might remain unaware of the missing data).

The validation should be automated. A Data Import Validator should be a technical artefact that operates in exactly the same way at the level of the systems of the member state and of the ICGLR (RDBMF).

The validator should perform the following checks:

- Completion of records: All required attributes of the data record should be filled
- Value formatting of data attributes: All value formats should adhere to the rules as expressed by the standard
- Length of values: All values should respect the maximum length as prescribed by the standard, if the case

Updates in the rules established by the standard should reflect in the validator.

In between two systems, the National Minerals Database and the RDBMF, a protocol of automatic data exchange can be established. This needs to take into account:

- Who initiates the transfer requests
- When are the transfer requests initiated

The initiator of the transfer needs to request the transfer through the API of the other party. Thus, such callable APIs should be in place, in order to be called.

The data source, the member state, might want to exercise its direct control over the information that is transferred, thus in order to respect the digital sovereignty principle and control exercised by the data owner, the transfer should always be initiated by the country.

It should not be presumed that having technical systems in place and the technical means of managing the data transfer, the member country will transmit all the information required by the RCM manual. Ultimately, it remains the responsibility of the country to respect the requirements of the RCM manual, and failing to do so maintains it accountable in relation to the agreements to which it explicitly adhered.

The control of the member state over what it shares (transmits to the RDBMF) should be complete. That means that the member state should be able to control what data records they transmit to the ICGLR. Therefore, the transfer should always be initiated and controlled by the member state.

The periodicity of transmitting data from the member state to ICGLR is in practice restricted by the feasibility of using a certain means of transfer.

Manual entry or preparation of Excel files for import are time consuming tasks, that require discipline, focus and adherence to time slots.

Therefore, transmission of the data “on a regular and timely basis” as required by the RCM manual, would explicitly require a time-bound approach.

In between two technical systems, an API-based transmission can be scheduled, or triggered in real time. Both approaches are feasible and could be applied for different reasons.

A real-time update can be triggered for example when a new data record is entered in the NMDB, of the type that needs to be reported to the ICGLR, for example an inspection of a mine site, the changing of the certification of a mine sites, and other such specific fields and records, as required by the RCM manual.

A scheduled transmission could happen in batches, thus records that are collected since the last transmission are sent as a package to the collector system (RDBMF). However, the batch transmission is still formed by sequential transmission of individual records that are validated and accepted or rejected individually.

An intermediary approach could be delayed individual transmission, in order to allow possible manual verifications at the national level, if it is the case.

Transmitting data in batches might also be a way to handle unstable internet connection at the source site, at the member state level. However, this temporary downtime can be mitigated by the implementation of a transmission queuing at the level of the member state, which adds technical complexity to the NMD implementation.

There would be no impediment for real-time transmission once a record is added at the member state level into their data storage (NMD), aside from the need of creating a fallback queuing process for transmission, which would be recommended also for batch transmission as the sequential transfer mode might be prone to risks of connection interruption.

Although in the future, as soon as possible, the data transmission should rely on system to system transmission through API, the immediate reality is not supporting such transmission, therefore a general rule should be in place.

We can thus say that data records should be transmitted at once or in batched daily transmissions when an API-based system to system connection is in place, or in periodical batches using a standardized form in Excel, with a delay that should not exceed 2 weeks from the registration of the record at the national level.

On a strictly standardized approach, an Excel-based evidence of records can also be the basis for data transmission, thus maintaining the same format for national-level management and for transmission. The data set to be transmitted can be iteratively built during a short period of time based on the new records entered in the master file. The “2 weeks” periodicity does not have a specific justification, in comparison to “1 week” or “once a month”, but given the relatively small number of new records at the level of each member state, it can also be feasible.

6.5. Data updating into the RDBMF

Data updating refers to the modification of records that are already stored and that need to be changed due to certain occurrences of events. These types of data attributes are referred to above as “mutable” and “updatable” data.

The timing and technical mechanisms for updating records should be the same as for the “Data acquisition”.

The update should not include a full data record, but the record identifier and the value of the attribute(s) to be changed, including the clear reference to the name of the attribute for easy identification.

The preparation for such an update can easily be done through a technical system at the member state side, however, when done in Excel, it needs to be conducted with great care, as might be prone to accidental duplication if the data operator is not careful.

6.6. Data storage in the RDBMF

All data transmissions are to be considered as being performed for the specific purpose of their transmission at the time of their transmission. The member state should remain the owner of the

data and should continue to be able to exercise the manner in which the data is processed and visualized by other parties, including ICGLR, other countries or 3rd party auditors or other stakeholders.

However, once the information is transmitted, through an exchange of information between two technical systems, the transmission itself cannot be revoked. Even if the data record could be deleted, willingly or accidentally, either by its owner the member state, or by ICGLR, or by a third party, the fact that it was transmitted is maintained and possible copies, for backup or other purposes, could occur outside the control of the member state.

This can lead to the perception of a member state that it cannot exercise complete control over what happens with the respective data records in the future, in any given context that can induce changes in the interest and willingness of sharing data with other stakeholders, and that this lack of future control might be detrimental to the state and contrary to the principle of its digital sovereignty.

As well, while most member states expressed their interest to visualise the data shared by other countries, for comparative analysis purposes, some also expressed their concern that all their data might be available for all the other states, which could be in the present or could become in the future in contradiction with the interest of member states. While this topic will be extended in the next point (data sharing management), the storage is relevant in supporting the data sharing control process.

The data storage should also respond to the essential aspects of the origin and authenticity of the data record, which should be preserved during the lifetime of the data records in the storage.

There are different types of technical architecture that can be implemented to support the storage and data sharing control. Such architectures are not in the scope of the present document, but their design should adhere to several relevant principles, as follows:

- Data origin should be clearly preserved: Which member state transmitted the data record and when. Data origin should not be modifiable. Data origin should be kept in a log that is separated from the main data storage.
- Data authenticity should be firmly ensured. Once transmitted, the data can be modified only by the rightful updaters and a clear record of such updates should be kept. Data should not be modifiable by accidental technical means (eg. incorrect database queries) or non-authorized users, persons or systems. Therefore, the immutability should be a

function of the data storage and each change should be auditable through the change logs, which should preserve the previous status of the data attribute. The technologies used for storage should ensure this possibility.

- Data storage and data accessibility should not be presumed equivalent. Once a member state transmits the information, it remains the owner of that information and should be able to revoke the accessibility of the respective data records or attributes in relation to any type of permissible types of stakeholders (ICGLR, member states, 3rd party stakeholders).

Of specific concern is data that can be classified as personal information, and can therefore be subject, at the time of transmission or in the future, to specific regulation regarding the protection of personal data. Specifically in the case of the data referred by the RCM data, these are the contact phone number and contact email of the legal representative of business entities, such as mine site owners or operators.

In terms of storage, the treatment of the personal data needs to ensure the following:

- It should be secured, meaning that it should not be extractable by unauthorized persons or systems, including cyber attackers
- It should not be stored in technical storage structures that make deletion of data impossible. For example, blockchain storage should never be used to hold personal data. In case blockchain is used to store the data transmitted by member states, there should be a clear separation of the storage of relevant mining data and the personal data which should be stored outside the blockchain and referenced through logical pointers from the blockchain.

6.7. Data sharing management

Each member state remains the owner of its data and should be able to determine at any time who has access to their data, either by type of stakeholder (ICGLR, member states as a whole, 3rd party stakeholders as a whole) or individually (certain specific member states, etc).

This data sharing control needs to be granular and in full control of the member states.

Specific technical architectures for the implementation of a data vault and a data sharing mechanism can support the solving of this aspect in different degrees. The scope of the present

document includes the principles and usage mechanisms, not the technical specification for implementation.

The data sharing should be performed by each member state, including at least the following:

- Direct control over the types of stakeholders that can access their data: ICGLR, Member states, and 3rd party stakeholders.
- Direct control over the individual stakeholders that can access their data: states that can access their data and states that cannot access their data.
- Direct control over what data should be shared. As we are referring specifically to the data shared in the context of the RCM, the concern is specific on the data entities shared as described by the RCM manual. The sharing should be granular at the level of each data entity and sub-entity. For example, a state might be willing to share with the other states the general information of a mine site, but not the business identification information of the operator of the site.

Such direct sharing control should allow two operations at each level: Grant and Revoke access. Access to personal data (specifically, the contact information of owners and operators of the mine sites and of exporters and importers) should be treated separately and explicitly.

Data access through visual interfaces and APIs by member countries

The Regional Minerals Database is thought to allow forms of data view, interrogation and export through technical interfaces, either visually or programmatically.

The information that is included in these forms of visualisation should strictly adhere to the sharing principles described above and should reflect the current access status granted by the originator member country to the stakeholder that views the data.

In case the visualisation mechanism makes use of a data caching that preserves a temporary copy of all or a part of sharable data, the caching needs to be technically updated each time a member state changes the access rights.

6.8. Data exporting

Data exporting - specific data can be exported in formats usable for other systems

Once data is accessed by one stakeholder aside from its member state owner, it can be considered that the respective stakeholder has and will retain access to the respective data in the state current at the moment of visualisation or export. Visualisation in itself is equivalent to an export in terms of the data sharing effect, since it can be saved through various technical means. A general difference can be that data visualisation is usually a processed subset of data that could be aggregated, while the data exporting is done usually in a raw form reflecting the storage format. Data exporting should adhere to the same rules set through the data sharing. Data exporting and formatting are not subject to regulation. It might be beneficial that the data sharing system would use an export format that adheres to the standard of data representation established at the level of the ICGLR.

6.9. Data archiving

Data archiving consists of separating the active data from inactive (old) data, by leaving the active data in the scope of processing (visualisation, search, filtering, export) and storing the old data separately. Generally, the data archive is built incrementally, thus adding data in time, based on certain rules, such as the age of the data or the loss of relevancy of the data.

The guiding information in the RCM manual mentions that the Regional Minerals Database should hold “ Current and historic (last 5 years) RCM Status (Green, Yellow, Red, Blue) of Mine Sites, CoC Systems and Exporters”.

This does not exclude necessarily the possibility to hold the data for a longer period of time.

At the level of each member state, their storage and archiving systems should adhere to the national regulatory framework regulations.

We can therefore consider that all transmitted data should remain in active status for at least 5 years, being available for processing and interrogation. After the elapse of the 5 years, data records can be added to a data archive, which should be technically accessible to the main storage system and should be unitary maintained.

The access rights to the data in the archive should follow the same rules as the main storage system as described above.

6.10. Data deletion

While archiving, simply move the data into a storage that is not going to be interrogated for processing needs but it can be audited and restored if the need arises, deletion is an act that will make the data unavailable for any kind of queries.

There are two types of deletion that can be considered in technical terms: the “hard delete” removes the data record from the database and makes its retrieval impossible, while the “soft delete” marks the data record as deleted, while still maintaining the possibility of retrieving it in the future. A soft delete has a different effect compared with archiving, as an archive can still be interrogated and data queries can be performed on it, while the soft-deleted records are invisible for general queries.

Technically the hard deletion is possible when using technical storage mechanisms that are not immutable and appendable by design. A blockchain storage for example does not allow hard deletion. Performing full deletion in a blockchain would require the reconstruction of the blockchain record by record and omitting the “deleted” records in the reconstruction process, which in itself is a very complex technical task.

Thus, if hard deletion would be envisioned as a possibility, the storage solution should not be based on blockchain.

The hard deletion goes against the auditability principle, as data will not be retrievable anymore. Even if there might be no current interest in having a deletion mechanism, the member states might see as a potential concern for the future on long-term the permanency of their data being stored in a mechanism outside of their control.

Thus, an answer should be given if a future concern will arise asking for certain data to be “completely removed” from the storage.

As hard-deletion impedes auditability, it should be avoided. However, the soft-delete can be triggered as a function of the data sharing process, making certain data unavailable to all stakeholders, based on the occurrence of an event. This can be time-bound, and automatically executed, for example, “make all Mine Site Owners records unavailable after 5 years since their initial insertion in the central data vault”.

Based on the above considerations, the Policy is defined in the following:

7. Data management and sharing governance policy and regulations for the Regional Minerals Database (RDBMF)

7.1. Introduction

The purpose of this policy document is to define and standardize the processes related to the data collected from the ICGLR member states into the Regional Minerals Database (RDBMF).

7.2. Approach

The policy will follow a complete life-cycle approach in relation to the RDBMF, including the following stages:

- Data acquisition (transmission, import) into the RDBMF
- Data updating into the RDBMF
- Data storage in the RDBMF
- Data sharing management
- Data access through visual interfaces and APIs by member countries
- Data exporting - specific data can be exported in formats usable for other systems
- Data archiving
- Data deletion

The policy provides a comprehensive set of rules and guidelines, formulated as requirements (Must) and recommendations (Should), that will support the ICGLR and the member states in conducting the processes related to managing the data specified in the RCM manual to be transmitted by the member states into the RDBMF.

The policy supports the following four main characteristics related to the data collected in the RDBMF:

- Quality - data is consistent, well formatted, correct, and complete for the required purpose.

- Integrity - data is original, attributable, and accurate.
- Security - data is secured.
- Usability - data is usable for the required purposes, directly or through processing.

The following general requirements are considered:

- Data is attributable: The producer (person or system, the source) of the data is known and uniquely identifiable.
- Data is original: The data preserves its original state. It was not tempered in ways that would create problems or risks.
- Data is complete for the required purpose, all data records include all required information.
- Data is correct/accurate: It reflects correctly the reality
- Data is unique when its storage relies on an individual entity that is uniquely identifiable, thus there is no duplication in data registries.
- Data is well-formatted: adhering to a specified format or standard
- Data is consistent: a data record referring to a data entity is found in the same form everywhere where the record is found.
- Data is accessed only by permitted stakeholders in permitted ways.
- Data is auditable: all operations performed on the data, even all data access requests, are logged and can be audited.
- Data is compliant with legal regulations.

The policy includes the rules describing the answers to the following points:

- Access control - who can access the data and in what way?
- Retention rate - how long is the data kept and what happens with it in time, on long term
- Formatting - how is the data formatted semantically and technically?
- Processing rules - how the data can be processed, according to the data processing & transformation use-cases that are permitted?
- Residency - where is the data hosted?
- Sovereignty - who has property over the data and who exercises control over it?
- Protection - special and sensitive data, for example personal data, that can be subject to additional regulations (such as Personal Data Protection Act, etc).

7.3. General requirements

7.3.1. ICGLR Minerals Data Semantic Standard

All data transmitted to the Regional Minerals Database should adhere strictly to a Semantic Standard that is provided by the ICGLR.

The ICGLR Minerals Data Semantic Standard defines all data entities, all data attributes, formatting rules, restriction of values available for attributes, and semantic relationships between data entities.

The Standard also defines an uniform rule for the formatting of the identifier of the Mine Sites, to be applied by all member states.

The Standard can be transposed into a technical representation that is to be used for the transmission of the minerals data from the member states to the RDBMF.

7.3.2. Data validation

Data validation is the responsibility of the member states, prior to its transmission to the RDBMF.

Data validation should include at least the following aspects:

- There should be no duplication of data records.
- All data records should be completed, in the sense that all required attributes as specified by the RCM manual are present and have value.
- All values should strictly adhere to the formatting rules as specified in the Standard
- All attributes should take value from the set of admissible values, if such rules are specified by the Standard.

Member states should strive, through their best due diligence, to ensure that all data is current and correct.

7.3.3. Data sharing control

All member states should be able to exercise their full right of managing the sharing of their data with ICGLR, with the other member states and 3rd party stakeholders, in an explicit and detailed way, assisted by technical means offered by the technical systems of the ICGLR.

7.4. Specific requirements for each stage in the data life cycle

7.4.1. Data acquisition into the RDBMF

The ICGLR member states will transmit the specific data as required by the RCM manual to the ICGLR RDBMF by strictly adhering to the ICGLR semantic standard.

The transmission should be performed by technical means through an API, system to system, without involving manual data entry.

The national systems (National Minerals Databases) should implement the ICGLR semantic standard, or should include a technical mapping mechanism from their internal format to the Standard.

Transmission should be done automatically, either at once when a data record is created or updated or in batched daily transmissions.

In case a technical system is not available at the national level, or until such a technical system is available, the member states will transmit data to the RDBMF in periodical batches using a standardized form in Excel, with a delay that should not exceed 2 weeks from the registration of the record at the national level.

Each member state is responsible for the technical validation of the sent records, before being sent.

7.4.2. Data updating into the RDBMF

Each data entity can include four types of information, as follows

- Immutable information (data attributes that uniquely define the mine site and cannot be altered): For a Mine site, these are: Identification number and Mine site location.
- Mutable information (data attributes that are not changed with a periodicity or based on a predetermined type of action, but whose change can occur in time as part of the normal evolution of the mine site). For a Mine site, these are: Owner, License, Operator, Designated mineral (in case other designated minerals are identified).

- Updatable information (data that is changed periodically based on the requirements of the RCM or by national regulations. For a Mine site, these are: Certification status, and Activity status.
- Appendable information (data that is added periodically based on specific occurrences of different events). This type of information builds up the history of specific data records. Examples of such information are: Mine Site Inspection (forming a history of Inspections), and Mine Site Status change (forming a Status Change History).

Once a data record has been created in the RDBMF, further changes will be transmitted by the Member State, including a clear indication of the corresponding record that is changed or to which information is appended, without retransmitting the full data record.

7.4.3. Data storage in the RDBMF

The data storage will ensure:

- Data origin: Which member state transmitted the data record and when. Data origin should not be modifiable. Data origin should be kept in a log that is separated from the main data storage
- Data authenticity. Once transmitted, the data can be modified only by the rightful updaters and a clear record of such updates should be kept. Data should not be modifiable by accidental technical means (eg. incorrect database queries) or non-authorized users, persons or systems. Therefore the immutability should be a function of the data storage and each change should be auditable through the change logs, which should preserve the previous status of the data attribute.
- Control over data. Once a member state transmits the information, it remains the owner of that information and should be able to revoke the accessibility of the respective data records or attributes in relation to any type of permissible types of stakeholders (ICGLR, member states, 3rd party stakeholders).

Storage of personal data such as the contact information (email, phone) of persons should allow the setting of special access rights and deletion, as an exception from the other data, which by default are not fully deletable.

7.4.4. Data sharing

Each member state remains the owner of its data and should be able to determine at any time who has access to their data, either by type of stakeholder (ICGLR, member states as a whole, 3rd party stakeholders as a whole) or individually (certain specific member states, etc).

This data sharing control needs to be granular and in full control of the member states.

7.4.5. Archiving of data

Data should be kept accessible in the ICGLR RDBMF for at least 5 years, after which it can be optionally archived in an incremental storage that remains accessible to audit and can allow data records to be restored.

7.4.6. Deletion of data

Full deletion from the RDBMF should not be allowed. Revoking of access rights should be done through the data sharing settings.