**Data and Service Sovereignty Requirements**

**1. Data Location**

* Service metadata for a specific business entity should where possible, be stored, processed, and replicated within the jurisdiction of their home Peppol Authority, or the same geographical region. This ensures compliance with national, and/or regional privacy and data residency laws and regulations.
* Businesses shall be able to specify their preferred data storage location during registration.

**2. Data Access Controls**

* Access to service metadata shall be restricted based on a "need-to-know" principle.
* Businesses should have granular control over who can access their service metadata within their designated SML. This may involve functionalities for:
  + Defining user roles with specific access permissions (e.g., view-only, edit)
  + Granting access to specific business partners or other external parties on a case by case basis.
  + Implementing time-bound access controls

**3. Data Transfer and Processing**

* Any transfer or processing of service metadata outside the designated jurisdiction or region is permitted subject to adherence to strict data security protocols. This may involve:
  + Encryption of data in transit and at rest
  + Utilizing secure data transfer mechanisms
  + Obtaining explicit consent from businesses before transferring data outside their designated region

**4. Data Residency Reporting**

* The SML shall provide reports or dashboards for businesses to verify the location of their stored service metadata.
* Businesses should be able to track any instances where their data is accessed or transferred outside their designated region.

**5. Legal Compliance**

* The SML must comply with all applicable data privacy regulations in the jurisdiction in which the business entity operates, and the geographical region where service metadata is stored and processed. As a minimum, this may involve adherence to:
  + General Data Protection Regulation (GDPR) in the European Union
  + Similar data protection laws in other regions

**6. Audit Logging**

* The SML must maintain comprehensive audit logs that track all access, transfer, and processing activities related to service metadata.
* Audit logs should be readily available for compliance purposes and potential investigations.

**7. Data Deletion**

* Businesses shall have the right to request the deletion of their service metadata from the SML upon transfer or termination of Peppol.
* The SML shall implement a clear data deletion policy outlining the process and timelines for deleting data upon request.