# Data and Service Sovereignty

## Purpose

The Critical Infrastructure Workgroup (CIWG) has been formed to assess the Peppol Network's critical infrastructure needs and propose solutions to improve its dynamic discovery architecture, including mitigating identified risks to the Service Metadata Locater (SML). Three groups were setup as below.

* CIWG A: Technical - Insourcing the Peppol SML in full or partly.
* CIWG B: Architectural/Technical - SML federation + Future Architecture.
* CIWG C: Business – Data and service sovereignty + Business Requirements.

This document is the output of CIWG Workgroup C which sets out a proposed policy statement, and set of principles in relation to data and service sovereignty, to assist the technical working groups as they consider options for the evolution or federalization of the SML.

## Objective

Peppol is continuing to gain popularity for jurisdictions to adopt as a national platform for digital document exchange. Confidence in Peppol as a means to allow a jurisdictions’ specific needs to be met and sustain network operations independently of external dependencies, while at the same time continuing to benefit from community-based shared experiences and operations is an important factor for decision makers.

The CIWG’s initiative is a unique opportunity to have future Peppol infrastructure by-design cater for this bi-modal need.

The objectives for the data and sovereignty requirements guide the design of the infrastructure to achieve these desired outcomes:

1. The ability to have a full functioning infrastructure to serve domestic participants and where possible foreign participants without any dependency on non-jurisdictional systems and personnel. Where a transitioning process is required to achieve this, the process should ensure acceptable business continuity.
2. The Ability to host systems and data for the above within the borders of the jurisdiction or region.

A proposed policy statement, to capture the purpose and objectives of the CIWG is set out below.

## Data and Service Sovereignty Requirements

### 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.

### Data Access Controls

Access to data shall be restricted based on a "need-to-know" principle.

Businesses should have granular control over who can access any information about them that is stored within their designated SML. This may involve functionalities for:

* Defining user roles with specific access permissions (e.g., view-only, edit)
* Implementing time-bound access controls

### Data Transfer and Processing

Any transfer or processing of stored information 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

### Data Residency Reporting

The SML shall provide reports or dashboards for businesses to verify the location of any information about them (if any) that is being stored.

Businesses should be able to track any instances where their data is accessed or transferred outside their designated region.

### 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 information 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.

### Audit Logging

The SML must maintain comprehensive audit logs that track all access, transfer, and processing activities related to any stored information.

Audit logs should be readily available for compliance purposes and potential investigations to authorised parties only.

### Data Deletion

Businesses shall have the right to request the deletion of their stored information 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.

### Proposed Policy Statement on Operational Independence

The SML can be subdivided and implemented in a distributed manner where the SML can be fully functioning for the businesses within a jurisdiction without dependency on components residing in external jurisdictions.

The jurisdiction has the option to fully own the subdivided SML required to serve the jurisdiction.

Jurisdictions can have full operational control of the subdivided SML where it can be operated by commercial parties and technologies freely chosen by the local jurisdiction. If a transition process is needed to achieve this, business operations should not be disrupted.

Changes and upgrades on the subdivided SML can be under jurisdiction’s sole discretion and process.