OpenPeppol AISBL Internal Regulations Part II

Use of the Peppol Network

Version: 2.0.0
Approved: 2023.11.29

OpenPeppol AISBL
Rond-point Schuman 6, box 5
1040 Brussels Belgium

info@peppol.eu
www.peppol.org

Table of Contents

1 Introduction

1.1 Scope and Structure

The OpenPeppol AISBL Internal Regulations on the Use of the Peppol Network contains a set of Policies that include rules and provisions about the ways to operate in the Peppol Network. The content of these Policies is essential for the proper understanding of the legal obligations assumed through the Peppol Agreements, by further elaborating on the clauses of those Agreements.

The OpenPeppol AISBL Internal Regulations on the Use of the Peppol Network include Policies on the following subjects:

1. Change Management
2. Entity Identification
3. Data Usage and Reporting
4. Service Provider Accreditation
5. Information Security
6. Peppol Authority Specific Requirements
7. Extended Use of Peppol
8. Compliance

1.2 Definitions and Conventions

Whereas:

1. OpenPeppol AISBL has established the Peppol Network as the main means of achieving the Association's purposes. It is defined as: "A logical network enabling secure and reliable exchange of Peppol Dataset Types between End Users via Peppol Service Providers. It is a component in the Peppol Architectural Framework and is based on a set of Peppol specifications which are governed according to the Peppol Governance Framework".
2. OpenPeppol AISBL has developed the Peppol Interoperability Framework in order to regulate the use of the Peppol Network. The Peppol Interoperability Framework is defined as: "The set of agreements, policies and procedures and technical specifications which, taken together, are needed to ensure interoperability. It consists of the Peppol Architectural Framework and the Peppol Governance Framework and is governed by the Peppol Coordinating Authority." The composition of the Peppol Interoperability Framework is included in section 1.3 below.

3. The Peppol Agreements (Peppol Authority Agreement and Peppol Service Provider Agreement) serve as the means of providing legal certainty on the use of the Peppol Network to the contracting parties (The Peppol Coordinating Authority, the Peppol Authorities, and the Peppol Service Providers).
4. The Policies included in the OpenPeppol AISBL Internal Regulations on the Use of the Peppol Network contain rules and provisions that expand in more detail the legal obligations assumed through the Peppol Agreements.
5. Operational details regarding the implementation of the Peppol Agreements and the Policies contained in the OpenPeppol AISBL Internal Regulations on the Use of the Peppol Network are laid out in Operational Procedures.
6. In case of any doubt or the appearance of conflict, the Peppol Agreements shall take precedence over the Policies contained in the OpenPeppol Internal Regulations on the Use of the Peppol Network and these will take precedence over the OpenPeppol Operational Procedures.

1.3 The Peppol Interoperability Framework

1. The Peppol Interoperability Framework includes the following sections:
    a. The Peppol Governance Framework
    b. The Peppol Architectural Framework
2. The Peppol Governance Framework includes the following components:
    a. The Peppol Agreements
        i. Peppol Authority Agreement
        ii. Peppol Service Provider Agreement
    b. Policies for the Use of the Peppol Network (part 2 of the OpenPeppol AISBL Internal Regulations)
    c. Operational Procedures for the Use of the Peppol Network
    d. Peppol Service Domain requirements
        i. List of Applicable Specifications
        ii. Service Level Requirements
    e. Peppol Authority Specific Requirements
3. The Peppol Architectural Framework includes the following components:
    a. Peppol Message Specifications
        i. Peppol Business Interoperability Specifications (Peppol BIS, used globally)

ii. Peppol Authority-governed Specifications

b. Peppol Network Specifications

i. Packaging and Security Specifications

ii. Messaging Specifications

iii. Capability Lookup and Addressing Specifications

1.4 Effective Date of Policies

The Policies contained in the Internal Regulations on the Use of the Peppol Network shall take effect as of publication of each new version, subject to the timelines and conditions set out in a Migration Plan to be published simultaneously.

Back to Table of Contents

2 Change Management Policy

2.1 Introduction

2.1.1 Policy Purpose

This Policy defines the overarching principles and specific provisions, or rules, that must be respected by all actors who take part in activities related to the lifecycle stages concerning artefacts subject to this policy.

2.1.2 Artefacts under this Policy

The following artefact categories are in scope of this Policy:

1. Technical Artefacts which are the specifications and other technology and architecture-related artefacts published as part of the Peppol Architectural Framework, such as the Peppol BIS (Business Interoperability Specifications), and associated validation artefacts and code lists that define the compliance criteria for Peppol Services offered to the market.
2. Internal Regulations on the Use of the Peppol Network, and other governance-related artefacts including, but not limited to, Domain Specific Requirements, which are necessary to regulate use of the Peppol Network, hereinafter collectively referred to as “governance policies” or simply “policies”.
3. Operational Procedures that describe routines and mechanisms for the implementation of Governance Policies and other provisions of the Peppol Interoperability Framework.
4. Agreements between the main actors responsible for the use of the Peppol Network, the Peppol Authority Agreement, and the Service Provider Agreement.

Artefacts developed and used under provisions of the Policy for Extended Use of the Peppol Network may be subject to principles and procedures different than those included in this Policy.

2.1.3 Policy Overview

This policy contains the following parts:

1. Introduction
2. Overarching governance provisions
3. RFC processing
4. Provisions for Technical Artefacts

5. Provisions for Internal Regulations and other Policies
6. Provisions for Operational Procedures
7. Provisions for Peppol Agreements

2.2 Overarching Governance Provisions

2.2.1 Key Principles

1. All artefacts in the Peppol Interoperability Framework are subject to a controlled lifecycle management process respecting the provisions outlined in this Policy. The lifecycle includes the following stages, all of which are subject to the provisions in this Policy, and which may be collectively referred to using the term “change and release management” or simply “change management”:
   a. Introduction of a new artefact
   b. Changing an existing artefact
   c. Releasing a new version of an existing artefact
   d. Migrating from an old to a new version of an artefact
   e. Removal of an artefact
2. Each artefact of the Peppol Interoperability Framework shall be allocated to a responsible Change Management Board (CMB) according to the following table. The CMB is responsible for all stages of lifecycle management related to the artefact under its responsibility. In cases where the nature of artefacts requires it, alternative or combined responsibilities may be set through relevant provisions of the Peppol Governance Framework.

		Type of artefact	Responsible entity
Peppol Interoperability Framework	Peppol Governance Framework	Peppol Authority Agreement	APP CMB
		Peppol Service Provider Agreement	APP CMB
		Internal Regulations on the Use of the Peppol Network and other Governance Policies	APP CMB
		Operational Procedures	APP CMB

		Peppol Service domain Requirements	List of Applicable Specifications	Responsible Domain CMB and APP CMB
			Service Level Requirements	Responsible Domain CMB and APP CMB
		Peppol Authority Specific Requirements		Responsible PA and APP CMB (see also chapter 7)
	Peppol Architectural Framework	Peppol Message Specifications	Peppol Business Interoperability Specifications (global BIS)	Responsible Domain CMB
			Peppol Authority governed specifications (local specifications)	Responsible PA
		Peppol Network Specifications	Packaging, Security and other network-related specifications	eDec CMB
			Messaging specifications	eDec CMB
			Capability Lookup and Addressing specifications	eDec CMB

3. The typical lifecycle management of an artefact is set out in the OpenPeppol Operational Procedures on Change Management. Lifecycle management should not deviate from these, except for good and specific reasons related to the nature of an artefact or the issue(s) requiring resolution.
4. The lifecycle management for any given artefact must allow for adequate involvement and participation of all OpenPeppol Members affected.
5. An artefact in the Peppol Interoperability Framework may contain Annexes or Attachments of a purely informative nature such as, but not limited to, the location of tools and other resources. These Annexes are not subject to the Change Management provisions in this policy but can be updated by the OpenPeppol Operating Office. The responsible CMB must always be notified and give the final approval for a revised version of such an Annex.

6. Changes to any artefact in the Peppol Interoperability Framework that are of a purely informative nature, such as external references etc. may not be subject to the Change Management provisions in this Policy but must always be approved by the responsible CMB.

2.2.2 Principles of Decision Making

1. Decisions along all stages of the artefact lifecycle are always taken by the Change Management Board (CMB) responsible for the artefacts as foreseen in the present Policy. When alternative or additional provisions apply, these are explicitly stated in this Policy.
2. The outcome of the decision-making process must be communicated back to the party requesting a change.
3. Escalation paths are provided in relation to all decisions of accepting or rejecting an RFC, as well as on RFC implementation in an affected artefact, in order to ensure transparency and accountability.
4. All decisions must be justified at all levels, particularly when a request is rejected or a previous decision is overturned.

2.3 RFC processing

2.3.1 Raising an RFC

1. Any OpenPeppol Member or defined organisational entity in OpenPeppol may raise a Request for Change (RFC) related to any artefact in the Peppol Interoperability Framework at any time.
2. The RFC is allocated to the responsible CMB, which will assume ownership of the next steps along the lifecycle, supported by the OO where appropriate. Allocation will be made by the OO based on responsibilities defined in this policy, subject to an assessment that ensures that sufficient information being provided by the RFC submitter.
3. For each step in the RFC processing OpenPeppol ensures that the status of the RFC is updated in an RFC Register. This enables Peppol members and defined organisational entities in OpenPeppol to monitor its status.

2.3.2 Deciding on accepting an RFC

1. The decision on acceptance/rejection of an RFC is made by the responsible CMB.

2. If the RFC is accepted, it will be further processed as foreseen in this Policy. If it is rejected, the responsible CMB must provide a justification outlining the reasons for its rejection.

2.3.3 Processing an RFC

1. Each accepted RFC must be processed in a timely manner according to the severity of the issue raised.
2. For each RFC the responsible CMB must provide the following, with support from the OO where necessary:
   a. a proposed resolution to the issue raised, approved for consultation and potential implementation as defined in this Policy, and
   b. an impact assessment on the implementation of the proposed resolution (or its rejection).
3. Based on the assessment of its impact, each RFC resolution must be classified by the responsible CMB according to the expected severity (major, minor or errata corrigenda) resulting from its implementation in a new release of the artefact effected.

2.3.4 Consultation on proposed RFC resolutions

1. For each proposed RFC resolution, other than errata corrigenda, the responsible CMB must ensure that sufficient consultation takes place with the members of relevant Domain and/or Stakeholder Communities directly affected. The responsible CMB will determine whether such consultation may be initiated for individual RFCs, or in batches, or collectively for all processed RFCs pending at a given time, via the review of a new release candidate of the affected artefact(s).
2. The responsible CMB must ensure that the consultation process is fair and open, and that the duration of the consultation period is proportional to the severity of the RFC.

2.3.5 Implementation of RFC resolutions

1. Implementation of RFC resolutions take place through the development of revised versions of existing artefacts, introduction of new artefacts or removal of existing artefacts.
2. For reasons of stability and practicality, RFCs may be processed, but the implementation of their resolution delayed until a later point in time, when critical mass has developed that will warrant new versions of existing artefacts to be

developed. OpenPeppol should avoid too frequent changes in its artefacts unless there is an urgent need to remedy a situation or to mitigate acute or previously unforeseen risk.

3. Implementation of an RFC resolution should not be delayed more than 6 months and must not be delayed more than a year since the submission of the RFC, unless duly justified by the responsible CMB. Batch implementation of RFC resolutions must not result in undue delay in the implementation of agreed changes.

2.3.6 Escalation

1. Disagreement on an RFC acceptance or rejection may be escalated by the party that raised the RFC.
2. Disagreement on an RFC resolution as implemented in the affected artefact may be escalated by
    a. any OpenPeppol member that submitted comments during a review process where the resolution was included, or
    b. any defined organisational entity in OpenPeppol, provided that a member review has shown that the resolution severely affects its members and/or the Association itself.
3. An escalation shall be submitted in the same manner as raising an RFC and will be assessed and processed by the OO.
    a. As a first step, the OO should facilitate reconsideration of the escalated issue by the responsible CMB, in consultation with the escalating party.
    b. During the reconsideration, the responsible CMB and the escalating party may agree on resolving the difference of opinion. If not, the escalation will be eligible for consideration by the MC following the statutory provisions for its agenda.
4. An escalation must be raised within 30 days from the decision or resolution being announced and must be properly substantiated so that the appropriate processing of the escalation on its merits is possible.
5. An escalation should be addressed and concluded within 60 days after it is raised. In the meantime, the regular change and release management procedures foreseen in this Policy will continue unaffected, unless a decision to accept an escalation is reached by the relevant CMB or the MC according to provisions stated in this section.

6. Any decision made by the MC is considered as a final conclusion on the matter. If the MC does not consider an escalation, the original CMB decision shall remain as final.

2.4 Provisions for Technical Artefacts

Provisions in this section apply to all technical artefacts of the Peppol Interoperability Framework referred to in section 2.1.2, as well as or instances of essential infrastructure, such as the Service Metadata Locator (SML) or the Peppol Directory.

2.4.1 Introduction of New Artefacts

1. The following provisions concern the introduction of new technical artefacts in existing global Peppol Service Domains. For cases that fall under the provisions of Extended Use (Chapter 8), processes arising from the provisions included in that Policy shall be followed.
2. A proposal to introduce a new artefact must be submitted through an RFC, even when it is initiated by the Managing Committee by issuing a mandate for a work group or task force to be formed with that purpose or taking a decision to use OpenPeppol resources. The provisions about raising, processing, and deciding on an RFC shall apply, as stated in section 2.3.
3. A new artefact may be developed through in-kind contributions of members or OpenPeppol resources, or a combination of the two. Under any circumstances, the availability of sufficient resources to develop a new artefact must be secured before a decision to proceed is taken.
4. A proposal to introduce a new technical artefact in the Peppol Architectural Framework must be based on a positive assessment of the following elements:
    a. Outline of purpose and main benefits,
    b. impact on operations for OpenPeppol to support and maintain the artefact, and
    c. impact on operations for members and other parties that implement, use, or are otherwise affected by the artefact.
5. If a new artefact is based on contributions that have been developed outside OpenPeppol, such external contributions must be licensed to OpenPeppol by the IPR holders under an open license. Furthermore, the content and presentation of such external contributions must be aligned with the Peppol Interoperability Framework through a process that includes consultation with the relevant Communities.

6. Introduction of new Peppol Dataset Types shall be subject to further conditions, as outlined in the Peppol Authority Agreement clause 12.4.

2.4.2 Releasing a New Version of an Existing Technical Artefact

1. A new release of an artefact in the Peppol Architectural Framework must be constructed by applying approved resolutions to RFCs to the existing version. A new release of an existing artefact must be classified as either:
   a. A major release, which may contain significant and/or non-backward compatible changes (e.g., removing or adding mandatory functionality),
   b. A minor release, which will usually contain backward compatible changes (e.g., adding optional functionality), or
   c. A errata corrigenda release, which must be limited to error correction, bug fixing and clarifications.
2. The decision to publish a new release of an existing technical artefact is taken by the responsible CMB.
3. Publication of a new release of a technical artefact is made by the Operating Office, following regular notification procedures and publication tools, as described in the OpenPeppol Operational Procedures.

2.4.3 Migration to a New Release of a Technical Artefact

1. Every new release of a technical artefact must be supported by a migration plan, which must respect the migration requirements of the changes contained in the release and define how older versions of the artefact are to be phased out.
2. A migration plan must contain the following steps:
   a. Phase-in: The new version is introduced in the Peppol Network as optional and relevant parties start to implement it in their systems.
   b. Switch-over: The new version becomes mandatory, and the old version becomes optional in the Peppol Network.
   c. Phase-out: The old version is no longer supported and will be removed from the Peppol Network.
3. The migration plan must contain the above steps as a minimum, clearly identifying what is expected of implementers at the beginning and end of each step and the time periods between milestones that delineate the beginning and end of each phase. Migration plans may contain more steps if relevant and appropriate.

4. Migrations to new versions of technical artefacts may not follow the steps stipulated in this section and may be done in a synchronised manner, provided that there are compelling reasons to do so.

2.4.4 Removing a Technical Artefact

1. A technical artefact may be removed from the Peppol Architectural Framework and its use in the Peppol Network may be discontinued.
2. Removal is decided based on an RFC submitted by a member or defined organisational entity in OpenPeppol and approved by the relevant CMB, after consultation with the Coordinating Committee.
3. An RFC to remove a technical artefact from the Peppol Architectural Framework shall be processed and decided upon according to the provisions set out in this Policy and will be subject to the same rules for escalation.
4. If the artefact is considered irrelevant and no longer valid for use the responsible CMB must issue a plan for how and when the artefact will be removed from the Peppol Architectural Framework which shall include provisions allowing existing users, if any, to terminate their use of the component.
5. Upon completion of the plan for removal, the artefact shall no longer appear within the Peppol Architectural Framework and its further use shall be prevented by suitable means.

2.4.5 Minimum Time for Consultation and Implementation

2.4.5.1 General Provisions

1. The following table defines the minimum time that must be allocated for;
   a. consultation with relevant communities on proposals for changes to an existing technical artefact as outlined in section 2.3.3, and
   b. Relevant actors to implement (migrate to) a new release of an existing technical artefact as outlined in section 2.4.3.

Type of technical artefact	Minimum time that must be allowed for consultation	Minimum time that must be allowed for implementation (migration)
New mandatory technical artefact (other than those explicitly mentioned in this table)	4 weeks	6 months
New optional technical artefact	4 weeks	4 weeks
Network specification, major release	4 weeks	6 months
Network specification, minor release	4 weeks	6 months
Network specification, errata Corrigenda release	N/A	N/A
Adding or changing codes in a code list used in a network specification	4 weeks	3 months
Deprecating or removing code values in a code list used in a network specification	4 weeks	4 weeks
Peppol BIS and associated validation artefacts, major release	2 months	6 months
Peppol BIS and associated validation artefacts, minor release	4 weeks	3 months
Peppol BIS and associated validation artefacts, Errata Corrigenda release	N/A	N/A

Changes to code lists used in a Peppol BIS	4 weeks	4 weeks
Removing an existing technical artefact	4 weeks	4 weeks

2.4.5.2 Special Provisions for Urgent or Alternative Action

1. In cases where urgent action is needed to change technical artefacts, the timelines stated in section 2.4.5.1 may be shorter.
2. Urgent action must be duly justified on grounds of serious impact on the Peppol Network operations that can only be avoided by acting faster than the minimum timelines set forth in section 2.4.5.1 would allow.
3. Alternative action may be warranted in situations including, but not limited to, external dependencies (such as in inherited code lists) and generally when the nature of an artefact and/or the conditions of a proposed changes requires it.
4. Alternative action must be duly justified on grounds of operational feasibility, or implementation requirements and the justification must be properly substantiated.
5. Urgent or alternative action must be initiated by a decision of the responsible CMB. Such decisions shall be subject to the escalation rules described in section 2.3.6 of this Policy.

2.5 Provisions for Governance Policies

This section contains special provisions for lifecycle management of the Internal Regulations on the Use of the Peppol Network and other governance policies, as defined in section 2.1.2.

2.5.1 Introduction of New Policies

1. The provisions in this section concern the introduction of new Policies related to the use of the Peppol Network that shall be added to the Internal Regulations on the Use of the Peppol Network, or otherwise be part of the Peppol Governance Framework.
2. A proposal to introduce a new Policy must be submitted through an RFC, even when it is initiated by the Managing Committee by issuing a mandate for a work group or task force to be formed with that purpose or taking a decision to use OpenPeppol resources. The provisions about raising, processing, and deciding on an RFC shall apply, as stated in section 2.3.

3. A proposal to introduce a new Policy in the Peppol Governance Framework must be based on a positive assessment of the following elements:
    a. Outline of purpose and main benefits,
    b. Impact on operations for OpenPeppol to support and maintain the implementation of the policy,
    c. Impact on operations for members and other parties that are affected by the introduction and implementation of the Policy.
4. The OpenPeppol Managing Committee shall decide on the introduction of a new policy upon recommendation of the APP CMB, after careful consideration of each proposal.
5. After Managing Committee acceptance, the new Policy shall be developed and approved by the APP CMB after being reviewed by members.
6. The final decision to put into effect the new Policy shall be taken by the OpenPeppol Managing Committee.
7. A new Policy may be developed through in-kind contributions of members or OpenPeppol resources or a combination of the two. Under all circumstances, the availability of sufficient resources to develop a new policy, together with any tools that may be necessary to implement it must be secured before a decision to proceed is taken.

2.5.2 Releasing a New Version of an Existing Policy

1. A new release of the Internal Regulations on the Use of the Peppol Network or any other Policy in the Peppol Governance Framework must be constructed by applying approved resolutions to RFCs to the existing version, and be classified as follows:
    a. A major release, which contains new or removes existing rules or obligations, or substantially alters existing provisions.
    b. A minor release, which only elaborates on a rule, without altering the substance and principles of the policy, or without introducing changes that expand the obligations of Open Peppol members.
    c. An errata corrigenda release, which must be limited to error correction and clarifications of ambiguous language.
2. A decision to publish a new release of the Internal Regulations on the Use of the Peppol Network or any other Policy that is part of the Peppol Governance Framework, is taken by the Managing Committee after recommendation of the APP CMB.

3. Publication of a new release of the Internal Regulations on the Use of the Peppol Network or any other Policy that is part of the Peppol Governance Framework is made by the Operating Office, following regular notification procedures and publication tools, as described in the OpenPeppol Operational Procedures.

2.5.3 Migration to a New Release of a Policy

1. Every new release of the Internal Regulations on the Use of the Peppol Network or any other Policy that is part of the Peppol Governance Framework must be accompanied by a migration plan.
2. A migration plan should contain the following steps:
    a. Phase-in: The new version is introduced in the Peppol Governance Framework as an upcoming rule set and relevant parties start preparing for its implementation, adjusting their internal processes and systems if necessary.
    b. Switch-over: The new policy comes into effect, and the previous version becomes obsolete.
3. The migration plan may contain the above steps as a minimum, clearly identifying what is expected of implementing parties at the beginning and end of each step and what are the time periods between milestones that delineate the beginning and end of each step. Migration plans may contain more steps if relevant and appropriate.
4. If appropriate, the migration plan may foresee that new Policies take effect immediately.

2.5.4 Removing a Policy

1. A governance policy may be removed from the Peppol Governance Framework and its effect may be discontinued in the Peppol Network.
2. Removal is decided on the basis of an RFC submitted by a member or an organisational entity of OpenPeppol.
3. An RFC to remove a policy from the Peppol Governance Framework shall be subject to provisions about raising, processing, and deciding on an RFC, as stated in section 2.3.
4. Sufficient lead time for the removal of a Policy must be foreseen, if appropriate.

2.5.5 Timeline for Consultation and Implementation

1. The following table defines the time that must be allocated for consultation with members on proposals for changes to an existing policy as outlined in section 2.4.3.
2. Implementation of resolutions to RFCs into a new release of an existing policy shall be subject to the provisions in section 2.3.5 and must not be delayed for more than a year since the submission of the RFC.

	Minimum time that must be allowed for consultation
New policy	4 weeks
Major release of an existing policy	4 weeks
Minor release of an existing policy	4 weeks
Errata corrigenda release of an existing policy	N/A
Removal of an existing policy	4 weeks

2.6 Provisions for Operational Procedures

Due to their nature, change management for Operational Procedures will be exempt from certain provisions contained in sections 2.2 and 2.3 and will follow special provisions contained in this section.

2.6.1 Processing and deciding on RFCs

1. A proposal to introduce a new Operational Procedure must be submitted by a member or organisational entity of OpenPeppol through an RFC.
2. Processing of such RFCs will be done by the Operating Office who will present a recommended resolution to the APP CMB for approval.

2.6.2 Introduction of new Operational Procedures

1. A new Operational Procedure shall be developed by the Operating Office and must be approved by the APP CMB before it is published.

2. No member review is expected for the resolution to RFCs against an Operational Procedures.

2.6.3 Releasing a New Version of an Existing Operational Procedure

1. A new release of an Operational Procedure in the Peppol Governance Framework must be constructed by applying approved RFC resolutions to the existing version.
2. A decision to publish a new release of an Operational Procedure that is part of the Peppol Governance Framework is taken by the APP CMB after recommendation of the Operating Office.
3. Publication of a new release of an Operational Procedure is made by the Operating Office, following regular notification procedures and publication tools.

2.6.4 Migration to a New Release of an Operational Procedure

1. A new release of an Operational Procedure takes effect on the date announced, unless explicitly defined differently through a migration plan.
2. If a migration plan is issued to support the implementation of a new release of an Operational Procedure, it must contain the following steps:
    a. Phase-in: The new version is introduced in the Peppol Governance Framework as an upcoming rule set and relevant parties start preparing for its implementation, adjusting their internal processes and systems if necessary.
    b. Switch-over: The new Operational Procedure comes into effect, and the old version becomes obsolete.
3. A migration plan, if needed, must contain the above steps as a minimum, clearly identifying what is expected of implementing parties at the beginning and end of each step and the time periods between milestones that delineate the beginning and end of each step. Migration plans may contain more steps if relevant and appropriate.

2.6.5 Removing an Operational Procedure

1. An Operational Procedure may be removed from the Peppol Governance Framework and its effect may be discontinued in the Peppol Network.
2. Removal is decided based on an RFC submitted by a member or an organisational entity of OpenPeppol.

3. An RFC to remove an Operational Procedure from the Peppol Governance Framework shall be processed and decided upon according to the provisions set out in this section.
4. Sufficient lead time for the removal of an Operational Procedure must be foreseen.

2.7 Provisions for Peppol Agreements

2.7.1 Consultation on RFCs concerning Agreements

1. As a minimum, a review should be initiated, giving the opportunity to all members of Stakeholder Communities to express their views.
2. If, during a review, an RFC is opposed by more than 50% of eligible Stakeholder Community members, the responsible CMB cannot accept the RFC as is, and must provide a revised version or reject it altogether. Eligible members of Stakeholder Communities shall be considered those that are signatories to a given Agreement to which the RFC refers.
3. In addition to a Stakeholder Community review, consultation can be initiated by other means including (but not limited to) a multi-stakeholder Working Group or a vote by Stakeholder Communities. Any vote initiated as part of an RFC review is subject to the majority and eligibility provisions of point 2 above.
4. After consultation is completed, a decision on an RFC will be taken according to the provisions of section 2.3.5.

2.7.2 Introduction of a New Agreement

1. The introduction of a new type of Peppol Agreement is not foreseen under this Policy.
2. Any consideration for the introduction of a new Peppol Agreement would need to be instigated by changes in stakeholder requirements and would necessitate major changes to the Peppol Interoperability Framework and the OpenPeppol Internal Regulations on the Use of the Peppol Network, including (but not limited to) this Policy.

2.7.3 Releasing a New Version of an Existing Agreement

1. A new release of a Peppol Agreement shall be constructed by applying approved RFC resolutions to the existing version.
2. A new release of a Peppol Agreement may be classified as follows:

a. A major release, which contains new or removes existing rules or obligations, or substantially alters existing provisions.

b. An errata corrigenda release, which must be limited to editorial revisions that do not affect the legal obligations or responsibilities of the contracting parties., such as changes to Annexes. An errata corrigenda release can include the following changes:

- Corrections of errors and omissions
- Editorial revisions to clarify inconsistent or ambiguous references, terminology and other language
- Changes to Annexes that are considered to be of operational, but not substantive nature

3. Every new release, other than Error Correction, must be reviewed by members according to the provisions described in section 2.4.3 and the results of such review must be considered by the APP CMB in the production of the final version. All comments shall be processed, and responses will be provided. A member review cannot be shorter than 8 weeks.
4. Decision to publish a new version, other than errata corrigenda, of Peppol Agreements is taken by the Peppol Authorities, following the voting procedures specified in the Peppol Agreements. The Peppol Authorities shall vote on a final version that is submitted to them by the OpenPeppol Managing Committee, following a proposal by the APP CMB, which includes all the agreed changes.
5. Publication of a new release of Peppol Agreements is made by the Operating Office, following standard notification procedures and publication tools, as described in the OpenPeppol Operational Procedures.
6. A certified master copy of the Agreements text will be hosted on the OpenPeppol Website. This will ensure clarity and consistency is maintained and the contracting parties can easily access the “in force” versions of the Agreement documents. Previous versions and notifications of changes will be archived as well.

2.7.4 Migration to New Versions of Peppol Agreements

1. Every new release of the Peppol Agreements, other than errata corrigenda, must be accompanied by a migration plan, which must be constructed and approved following the same procedures as the new Agreement release as described in 2.8.2.

2. The contracting parties will implement approved new versions of the agreements according to the migration plan. The migration plan will stipulate whether the Agreements will need to be re-signed.
3. An Errata Corrigenda release does not require re-signing by the contracting parties and be considered effective 20 days following its publication as part of the Peppol Interoperability Framework.
4. If re-signing of a new Agreement version is not required:
    a. The new versions will automatically replace superseded versions. Clause 13.3 of the Agreements provides that a new signing process is not required for new versions of the Agreements to take effect.
    b. Notification of the revised versions, and acknowledgement of receipt of notification by the contracting parties is deemed to be acceptance of the revised versions by the contracting parties.
    c. If any of the contracting parties consider the revised versions of the agreements to be unacceptable for whatever reason, the only remedy available will be to terminate the Agreement in accordance with the provisions set out in clause 22 of the Service Provider Agreement and clause 24 of the Peppol Authority Agreement.
5. If re-signing of a new Agreement version is required; the migration plan must contain the following steps:
    a. PA sign period: The time needed for OpenPeppol to sign new Agreements with Peppol Authorities.
    b. New SP Agreement Phase-in: The new SP Agreement version starts to be signed with Service Providers in each PA jurisdiction.
    c. Old SP Agreement Termination: When Peppol Authorities are confident that signing of the new SP Agreement will proceed smoothly, a termination notice shall be given for the old SP Agreements remaining in effect.
    d. Old SP Agreement Phase-out: Remaining Service Provides must sign the new SP Agreement, otherwise they are removed from the Peppol Network at the end of the termination notice period.
    e. The migration plan must contain the above steps as a minimum, clearly identifying what is expected of implementing parties at the beginning and end of each step and the time periods between milestones that delineate the beginning and end of each step. Migration plans may contain more steps if relevant and appropriate.

2.7.5 Removing an Agreement

1. The removal of a Peppol Agreement is not foreseen under this Policy.
2. Any consideration for the removal of a Peppol Agreement would necessitate major changes to the Peppol Interoperability Framework and the OpenPeppol Internal Regulations, including (but not limited to) this Policy.

2.7.6 Minimum Time for Consultation and Implementation

The following table defines the minimum time that must be allocated for

1. consultation with members on proposed changes to an existing Agreement as outlined in section 2.8.2, and
2. implicated actors to implement (migrate to) a new release of an existing Agreement as outlined in section 2.8.3.

	Minimum time that must be allowed for consultation	Minimum time that must be allowed for implementation (migration)
New Agreement	N/A	N/A
Major release	8 weeks	6 months
Errata Corrigenda release	N/A	20 business days
Removal of an existing Agreement	N/A	N/A

Back to Table of Contents

3 Entity Identification Policy

3.1 Policy Overview

This policy contains the following parts:

1. Overview
2. Requirements from the Peppol Agreements
3. End User identification and Reporting Requirements
4. Service Provider Identification Requirements

3.2 Requirements from the Peppol Agreements

The legal obligation to ensure proper Entity Identification follows from

- the Peppol Authority Agreement clause 9.2.4 with respect to the PAs responsibility to verify the entity of the SP, and
- the Peppol Service Provider Agreement clause 9.2 with respect to the SPs responsibility to verify the entity of the End User.

3.3 End User Identification

3.3.1 Information to be Collected

Peppol Service Providers shall ensure that the following information is known for all End Users (senders and receivers) to which they provide Peppol services directly or indirectly through intermediaries. As an exception, Service Providers that offer Capability Lookup Services exclusively are not responsible for End User identification, unless they have a direct contract with them:

1. Legal identifier of the End User in the jurisdiction within which it is legally based, and legal identifier Type (e.g., VAT number, company registration number).
    a. The legal identifier has to be active, in jurisdictions when such distinction exists.
    b. In case of End Users that are public organisations and where legal identifiers as such do not exist, other officially issued codes are acceptable.
2. Legal name of the End User, in the jurisdiction within which it is legally based.
3. Legal address, including as a minimum country and (where applicable) territory information.

4. End User's capability to receive and/or send Peppol Dataset Types (Document Type ID).
5. All identifiers used in the Peppol Network by the End User, related only to the Peppol Services which that particular Service Providers offers to them. If these are associated with different trade names or legal entities within the same organization, associations must likewise be mapped.
6. Contact information sufficient for the End User to be reachable by the Service Provider.
7. Proof of ownership – i.e., that the information has been provided by the entity it concerns.
8. Which intermediaries, if any, intermediate the End User's access to the Peppol Services. The following information must be known about each intermediary:
    a. Legal identifier of the Intermediary in the jurisdiction within which it is legally based, and legal identifier Type (e.g., VAT number, company registration number).
    b. Legal name of the Intermediary, in the jurisdiction within which it is legally based.
    c. Country and (where applicable) territory where the intermediate is legally based.

Service Providers must verify the above information concerning End Users to which they provide Peppol Services, except in cases when this is not feasible with reasonable efforts. Such cases may include, but are not limited to, the lack of automated means to retrieve or verify End User information through lookup or API connection to authoritative sources of information in specific jurisdictions. Service Providers may not be held accountable for lack of proactive verification when they can demonstrate that this was not feasible with reasonable effort.

If and when it comes to the attention of a Service Provider that one of their End Users is trading under names different from its legal name, these may be documented. In particular, when the Service Provider becomes aware that different trade names, business units, etc. are associated with different endpoints, this should be adequately documented.

The Service Providers remain responsible for the correctness of End User information for the time during which they provide Peppol Services to them. End User information shall be collected and verified at the time of enrolment in the Peppol Network and when it changes. Furthermore, it must be periodically checked at least on an annual basis, provided that mechanisms to that effect are available, e.g., through lookup or API connection to authoritative sources of information in specific jurisdictions. For the

avoidance of doubt, this clause does not require the Service Providers to make such checks for each transaction or more generally in runtime.

3.3.2 Requirements for the Peppol Authorities

Peppol Authorities shall provide, to the best of their ability, guidance to Service Providers on how to reliably obtain or verify End User information such as the legal identifier, type, and alternate trade names for businesses or persons resident in their jurisdiction, as well as what constitutes proof of ownership, through authoritative services such as national business registers that offer automated (e.g., through an API) and free of charge services. Where such services exist, Service Providers must use them.

In the absence of such a description (e.g., because there is no Peppol Authority for the End User's jurisdiction, or because the process for accessing the information is costly or otherwise onerous), the Service Provider must exercise all reasonable effort to obtain and validate information required for End Users to which they provide services, as well as proof of ownership of that information. OpenPeppol will support the Service Providers, to the best of its ability, to obtain information that is necessary for them to complete this task in jurisdiction where there is no established Peppol Authority.

3.4 Peppol Service Provider Identification

As part of the process to establish the Peppol Service Provider Agreement the Peppol Authority must secure the following minimum data about the Peppol Service Provider:

1. Legal identifier of the Service Provider in the jurisdiction within which it is legally based, and legal identifier Type (e.g., VAT number, company registration number).
2. Legal name of the Service Provider, in the jurisdiction within which it is legally based.
3. Legal address, including country and (where applicable) territory information.
4. Contact information for formal notices.
5. Any other names the Service Provider trades under.
6. Name and identifier of the legal representative of the Service Provider, authorised to act on its behalf.
7. Name and contact details for Service Provider representative(s) responsible for the Peppol Service, at a minimum both email and telephone number.
8. Proof of ownership – i.e., that the information has been provided by the entity it concerns.

Peppol Authorities must verify the above information concerning Service Providers with which they are contracted.

Service Provider information shall be collected and verified at the time of signing a Service Provider Agreement and when it changes. Furthermore, it must be periodically checked, at least before each renewal of production certificate.

A Peppol Authority shall not enter into any Peppol Service Provider Agreement with an entity which, in the good faith judgment of the Peppol Authority, cannot bear the legal responsibilities of a Peppol Service Provider.

The Peppol Authority may make signing with a prospective Service Provider contingent on the Peppol Authority completing a satisfactory audit of the financial and technical capabilities of the prospective Service Provider. The Peppol Authority shall bear the cost of performing the audit, which must be conducted in the minimally invasive manner feasible. However, the prospective Service Provider shall make reasonable accommodations for facilitating the audit and shall carry any costs they themselves incur in making such accommodations.

Back to Table of Contents

4 Data Collection, Reporting and Usage Policy

4.1 Policy Overview

The purpose of this Policy is to provide a comprehensive frame of reference regarding the data that is collected, processed, and made available regarding the use of the Peppol Network.

This policy contains the following parts:

1. Overview
2. Requirements from the Peppol Agreements
3. Data Collection Purposes
4. Service Provider Reporting on End User Statistics
5. Service Provider Reporting on Transaction Statistics
6. OpenPeppol SML analytics
7. Data Usage
8. The Peppol Directory
9. Data protection

4.2 Requirements from the Peppol Agreements

The legal obligations related to data usage and reporting follows from

- the Peppol Authority Agreement clause 8.1.8 with respect to the Peppol Coordinating Authority responsibility for collecting data and making aggregated statistics available, and
- the Peppol Service Provider Agreement clause 9.4.8 with respect to the responsibility of the SP to make such data available related to the use of their Peppol Services.

4.3 Data Collection Purposes

Under this policy, OpenPeppol may collect information through End User and Transaction Statistics Reporting, as well as through Peppol Network Analytics. OpenPeppol will also aggregate, and make available, certain data on End Users, available from Service Metadata Publishers, via the Peppol Directory.

OpenPeppol will use the collected data for certain operational, strategic and compliance purposes, specifically the following:

1. Capacity planning, assessing stress capabilities and load management of the Peppol Network and all its components, including identification of trends in volume changes, peak usage areas and peak usage times.
2. Ensuring the resilience and proper operation of the Peppol Network and all its components, notably through risk analysis, threat detection, and other measures to prevent fraud.
3. Measuring historic and current usage of the Peppol Network, in order to have the capability to determine trends and evolutions, and assess current and future needs and requirements of various stakeholders, including the identification of potential future use cases and Service Domains for the Peppol Network.
4. Assessing and improving the internal organization and the quality of services and processes, specifically to:
    a. Improve service quality to End Users.
    b. Improve the experience of actors involved in the use, operations, and governance of the Peppol Network.
    c. Conduct market segmentation analysis of current or potential user groups (without identifying individual End Users).
5. Monitoring and ensuring compliance with the requirements expressed through the Peppol Interoperability Framework including, but not limited to, monitoring the use of datasets defined through a Peppol BIS to measure compliance to the “mandatory BIS” requirement.

4.4 Service Provider Reporting on End User Statistics

To monitor the evolving use of the Peppol Network, OpenPeppol needs to collect statistical information about the End Users exchanging datasets over the Peppol Network. This will help OpenPeppol to monitor the volume and type of usage in different countries and for different business processes, allowing monitoring of growth in adoption, or the lack thereof.

Information on the areas and type of adoption is essential for OpenPeppol to be able to set targets and have sufficient information to perform business analysis about the direction it takes. It is also needed to identify business risks that should be mitigated and opportunities that should be explored.

Only aggregated, statistical information, which should be based on the application of the End User Identification Policy in clause 3.3.1, must be reported.

The data reported must be entirely anonymous and not directly linkable to any natural persons or individual legal entities, including any (contact persons of) End Users.

The Peppol Service Provider is responsible for ensuring that the reported data are collected in an accurate and reliable manner, using whatever methods the Peppol Service Provider deems most efficient in its own infrastructure and operational environment. Prior to submitting it, the Peppol Service Provider must take reasonable measures to verify that the data reported is anonymous and not directly linkable to any natural persons or individual legal entities.

Peppol Service Providers must ensure that a range of statistics on the number of End Users that have been involved in dataset exchanges is reported to OpenPeppol for each reporting period.

The exact nature and format of aggregated statistics to be reported by Service Providers is defined in the technical specification of **End User Statistics Reporting**, based on the data scope and in line with collection purposes and usage principles laid out in this Policy.

The reporting period, applicability conditions and other terms and conditions will be described, if necessary, in Operational Procedures or other context-specific documents. If such documents contain provisions that affect the obligations of OpenPeppol members with respect to this Policy, they must be subject to change and release management procedures as foreseen for in the Internal Regulations for the Use of the Peppol Network.

All reported data will be collected by OpenPeppol through a centralised reporting mechanism. OpenPeppol will then provide Peppol Authorities with access to desired statistics on data that concerns End Users based in their own jurisdiction.

4.5 Service Provider Reporting on Transaction Statistics

To monitor the evolving usage of the Peppol Network, OpenPeppol needs to collect information about the Peppol Dataset Types actually being exchanged over the Peppol Network, considering each such exchange as a transaction between End Users. This information must be reported by Service Providers according to the provisions of this Policy.

Only statistical information will be collected and reported to OpenPeppol under this Policy. No information from the actual business content of individual datasets will be collected for the purposes of this Policy or reported to OpenPeppol.

The data reported must be entirely anonymous and thus not be directly linkable to any natural persons or individual legal entities, including any (contact persons of) End Users.

The Peppol Service Provider is responsible for ensuring that the relevant data can be collected in an accurate and reliable manner, using whatever methods the Peppol Service Provider deems most efficient in its own infrastructure and operational environment.

The exact nature and format of aggregated statistics to be provided by Service Providers is defined in the technical specification of **Transaction Statistics Reporting**, based on the data scope listed above and in line with collection purposes and usage principled laid out in this Policy.

The reporting period, applicability conditions and other terms and conditions will be described, if necessary, in Operational Procedures or other context-specific documents. If such documents affect the obligations of OpenPeppol members with respect to this Policy, they must be subject to change and release management procedures as foreseen in the Internal Regulations for the Use of the Peppol Network.

All reported data will be collected by OpenPeppol through a centralised reporting mechanism. OpenPeppol will then provide to relevant Peppol authorities access to desired statistics on data that concerns end users based in their own jurisdiction.

4.6 Peppol Network Analytics

OpenPeppol will regularly analyse information that is available via the Service Metadata Locator and from Peppol Service Providers offering Peppol Addressing and Capability look-up oriented Peppol Services, for the purpose of meeting operational and strategic needs as described in this Policy as well as verifying compliance with the rules of the Peppol Network including, but not limited to, the following:

1. That End User capabilities have been registered for authorised Peppol Dataset Types only, and that only the allowed capabilities are being used.
2. That End Users have been registered with authorised identifier schemes only.
3. That Peppol Service Providers are using the agreed transport protocol(s).

OpenPeppol may establish a mechanism for the automatic retrieval of information from Service Providers within the scope of this section and engage in the processing of such information for the purposes of data collection stated in this Policy. Such Service Providers may not engage in any action that reduces or stops OpenPeppol's ability to retrieve such information.

OpenPeppol will provide Peppol Authorities access to desired statistics on data that concerns End Users based in their own jurisdiction.

4.7 Data Usage

The data collected and/or generated as described in this Policy can be made available to and used by relevant stakeholders with defined roles in the Peppol Interoperability Framework, to the extent and for the purposes set out below.

4.7.1 Data Usage by OpenPeppol

OpenPeppol may choose, at its own and sole discretion, to publish or otherwise publicly disclose aggregate statistical information based on the data collected, provided that these do not permit the direct linking of any published or disclosed information to the identity or business practices of individual Peppol Service Providers or End Users without their explicit consent.

OpenPeppol must not process statistical data received from the Service Providers under sections 4.4 and 4.5 with the objective of identifying individual End Users without the explicit prior agreement of the Service Provider(s) that provided the statistical data.

In this data collection and processing, each Peppol Authority, Service Provider and End User in the Peppol Network must be treated in the same manner as its comparable peers.

OpenPeppol may not combine or link data from different reporting data streams except for the purposes included in this Policy.

OpenPeppol will not disclose any personal confidential information collected under this policy to any third parties except where legally compelled to do so.

OpenPeppol must take all reasonable security measures to prevent unauthorised access to the data collected and processed under the provisions of this Policy. Operational Procedures for granting and revoking access to authorised internal Operating Office resources and authorised Members must be defined and made available to OpenPeppol members.

OpenPeppol will implement appropriate logging and audit trailing procedures to verify that access and use complies with this Policy. Relevant sections of these logs and audit trails will be made available by OpenPeppol to a neutral third party at the request and at the expense of a Peppol Authority and/or a Service Provider, solely for the purposes of assessing compliance with this Policy.

4.7.2 Data Usage by Peppol Authorities

Respecting the provisions in the Peppol Agreements, OpenPeppol shall, on a regular basis, provide to Peppol Authorities, access to statistics based on information collected or derived according to the provisions of this Policy related to the End Users and Service Providers based within their jurisdiction.

Peppol Authorities may request from OpenPeppol particular data aggregation views to enhance their understanding of the information available, provided that these do not permit the linking of any published or disclosed information to the identity of individual End Users or the business practices of individual Peppol Service Providers or End Users without their explicit consent, except in cases of non-compliance.

Peppol Authorities may publish or disclose the information made available to them under their own legal responsibility and to the extent that they have a legal basis for doing so in their own jurisdiction, provided that the published or disclosed information do not permit the direct linking to the identity or business practices of individual Peppol Service Providers or End Users without their explicit consent.

4.8 The Peppol Directory

Service Providers will be given the ability to submit to OpenPeppol metadata from the SMP(s) in which their End Users' endpoints are listed.

This information, as provided by the Service Providers, may be bundled, and collected in the Peppol Directory, which shall be hosted and made available by OpenPeppol. Prior to making data available to OpenPeppol for inclusion in the Peppol Directory, Service Providers shall ensure that it is current and correct and that making such data available is compliant with applicable law, including local data protection law.

A Service Provider that displays in the Peppol Directory some or all End Users they provide services to, shall be responsible for maintaining the information displayed there. A provider of Peppol Addressing and Lookup Services who relays data about the End Users listed in the SMP to the Peppol Directory shall be responsible for ensuring that the information is accurately relayed.

4.9 Data Protection

For the avoidance of doubt, nothing in this Policy shall be construed as mandating any entity to take any action that would place it in breach of any applicable law, including, but not limited to, applicable data protection regulation. Nor shall this Policy be construed as restricting any otherwise lawful data analysis by OpenPeppol, a Peppol Authority or a Service Provider.

With respect to this Policy, it is likely that, in many jurisdictions, some limited parts of the data to be collected, reported and analysed may qualify as personal data or as personally identifiable information (depending on the law), which may be subject to specific safeguards and requirements.

Where the processing of such data would fall within the scope of European data protection law, under this policy OpenPeppol shall be the data controller for the data processing activities set out in sections 4.3, 4.4 and 4.5 - notwithstanding the possibility that participants in these data processing activities may process the same data for their own purposes as well, acting as independent data controllers under their sole legal responsibility and subject to their applicable laws, outside the scope of this Policy. Where OpenPeppol acts as a data controller, it shall adhere to the requirements of European data protection law. If other participants in these data processing activities become

aware of data protection compliance challenges in the execution of this Policy, they shall raise them with OpenPeppol as soon as reasonably practicable.

With respect to data processing activities set out in section 4.8, OpenPeppol and the Service Providers shall act as joint data controllers, under an arrangement set out between them, formalised by way of this Policy and the privacy policy that's published in conjunction with the Peppol Directory.

Back to Table of Contents

5 Service Provider Accreditation Policy

5.1 Policy Purpose and Overview

This Policy contains provisions that describe the requirements for allowing Peppol Service Providers to obtain and maintain access to the Peppol Network. These provisions must be followed by all actors involved, i.e., Service Providers, Peppol Authorities, and the Peppol Coordinating Authority.

The purpose of this Policy is to increase confidence that the services offered across the Peppol Network respect the relevant technical specifications and thus provide the level of interoperability expected.

This Policy consists of the following parts:

1. Purpose and Overview
2. Requirements from the Peppol Agreements
3. Entering the Peppol Network
4. Remaining in the Peppol Network
5. Leaving the Peppol Network

This Policy relates only to accreditation procedures that are performed across the entire Peppol Network in all jurisdictions and does not include any local accreditation procedures that are administered by Peppol Authorities as part of their PA specific requirements.

5.2 Requirements from the Peppol Agreements

The legal obligation to undertake such testing and certification is expressed in the Peppol Service Provider Agreement clause 9.5.1.

5.3 Entering the Peppol Network

5.3.1 Preconditions

Before a Service Provider obtains access to the Peppol Network, the following preconditions must be met:

1. The Service Provider must have passed the onboarding test foreseen for the type of Peppol Services intended to be offered on the Peppol Network.
2. The Service Provider must have signed a Peppol Service Provider Agreement with the relevant Peppol Authority.

a. A Peppol Authority is relevant to a Service Provider when its jurisdiction includes both dimensions below:
    i. The country or territory where the Service Provider is legally based.
    ii. The Peppol Service Domain(s) in which the Service Provider plans to offer Peppol Services.
b. Where no Peppol Authority can be considered as relevant, according to the conditions of point 7.a.i-ii above, the Service Provider Agreement shall be signed directly with the Peppol Coordinating Authority, which assumes the role and responsibilities of a Peppol Authority according to the provisions of the Peppol Authority Agreement (clause 8.1.7).
c. As an exception, the Peppol Coordinating Authority may grant to a Peppol Authority the right to sign a Service Provider Agreement with a Service Provider legally based outside its territorial jurisdiction, provided that:
    i. No other Peppol Authority has territorial jurisdiction in the country or territory where the Service Provider is legally based.
    ii. The Service Domain in which the Service Provider intends to provide Peppol Services is within the jurisdiction of the Peppol Authority in question.

3. The Service Provider must be a member of OpenPeppol AISBL, in the category appropriate for the type of Peppol Services intended to be offered on the Peppol Network.
4. The Service Provider's membership must be in good standing, including (but not limited to) payment of applicable fees, otherwise the Peppol Coordinating Authority retains the right to deny access to the Peppol Network.
5. For the avoidance of doubt, the Service Provider Agreement may be signed at any time between the time of accession of a Service Provider as a member of OpenPeppol AISBL and the time when the Service Provider gains access to the Peppol Network.

5.3.2 Accreditation process

The accreditation process will start after the Service Provider has been admitted as an OpenPeppol Member in the category appropriate to the type of Peppol Services they want to offer.

To gain access to the Peppol Network, a Service Provider must follow the necessary steps as described below:

1. Determine the relevant Peppol Authority to relate with.

a. The Service Provider should contact the Peppol Authority, the jurisdiction of which meets the requirements of section 5.3.1. If none of the existing Peppol Authorities meets those requirements, OpenPeppol will assume the role of Peppol Authority for that Service Provider.

b. Initiating a relationship with the relevant Peppol Authority is a prerequisite for the successful execution of the accreditation process. The Peppol Authority will indicate whether it accepts the relationship before it is initiated.

2. Request and obtain a test PKI certificate.

   a. The Service Provider shall request and obtain a test PKI certificate from OpenPeppol, so that they can begin testing.

   b. The request for a test PKI certificate must be approved by the relevant Peppol Authority and the Peppol Coordinating Authority.

   c. If no Service Provider Agreement has been signed, a basic entity identification process must take place as a minimum, usually by the Service Provider submitting the information contained in Annex 3 of the Peppol Authority Agreement and a copy of their business register statutes or equivalent. A more comprehensive identification procedure according to the provisions of the Entity Identification Policy may be undertaken if the Peppol Authority so chooses but is not mandatory at this point in time.

   d. As an exception, OpenPeppol may issue test certificates to interested parties that are not Service Providers or even OpenPeppol Members, provided that their enablement to test Peppol Services is to the interest of OpenPeppol. No production certificates shall be issued to such parties.

3. Pass the onboarding test.

   a. The Service Provider shall perform, and must successfully pass, the required onboarding test as appropriate for the Service Domain in which they intend to offer Peppol Services.

   b. Proof of successful test completion will be the test report generated by the OpenPeppol Testbed.

4. In case the relevant Peppol Authority has additional requirements for local accreditation that have been accepted as PA specific requirements, a local accreditation process must be followed and successfully completed before the Service Provider signs the Service Provider Agreement and before production certificate(s) are issued.

5. Sign the Service Provider Agreement.

a. The Service Provider shall sign the Peppol Service Provider Agreement with the relevant Peppol Authority, to be determined according to the provisions of section 5.3.1.

b. The Service Provider Agreement can be already signed before testing is completed or before testing even starts.

6. Request and obtain production PKI certificate(s).

a. After passing the required onboarding tests and signed a Peppol Service Provider Agreement, the Service Provider can request a production PKI certificate from the Peppol Coordinating Authority.

b. The request must be approved by the Peppol Authority with which the Service Provider has signed an Agreement, as well as by the Peppol Coordinating Authority.

c. Once the request is approved, the Service Provider will be issued production PKI certificate(s) for the Peppol Service Domain(s) in which they intend to offer Peppol Services.

Once the Service Provider has obtained production certificate(s) for the Service Domain(s) in which it intends to offer Peppol Services, the accreditation process is complete, and the Service Provider can start operations.

5.4 Remaining in the Peppol Network

To retain access to the Peppol Network, the following conditions must always be met:

1. All Service Providers must be compliant with all requirements for the use of the Peppol Network as stated in the Service Provider Agreement, the Internal Regulations and Operating Procedures.
2. All Service Providers must pass the relevant tests, as appropriate for the Service Domain(s) in which they offer Peppol Services, at least once, and no earlier than 2 months before their production certificate(s) need to be renewed.
3. Production PKI certificate(s) must be re-issued at least every two years, following the provisions specified in the Operational Procedures.
4. A Service Provider Agreement must be in effect with the relevant Peppol Authority.
5. OpenPeppol membership in the category appropriate to the Peppol Service offered must remain valid.

5.5 Leaving the Peppol Network

A Service Provider may leave the Peppol Network under the following circumstances:

1. Voluntarily, when the Service Provider no longer wishes to provide Peppol Services.
2. When the Service Provider is subject to the penalty of removal from the Peppol Network under the provisions of the Compliance Policy (section 9).
3. When the Service Provider Agreement is terminated for whatever reason that is compliant to the provisions of that Agreement, resulting in a situation where no valid Service Provider Agreement is in effect.
4. When, for any valid reason, the membership of the Service Provider to OpenPeppol is terminated.

In all such circumstances, the production certificate(s) issued to the Service Provider shall be revoked.

Back to Table of Contents

6 Information Security Policy

6.1 Policy Overview

This policy contains the following parts:

1. Overview
2. Requirements from the Peppol Agreements
3. Purpose
4. Security provisions

6.2 Requirements from the Peppol Agreements

The legal obligation to have security measures in place is expressed in the Peppol Service Provider Agreement clause 17.1. The provisions based on this clause are stated in section 6.4. Furthermore, there are other obligations on security measures stated in the Peppol Service Provider Agreement clauses 9.5 and its sub-clauses, 10.3, 10.4, 10.5, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9 and 17.10.

6.3 Policy purpose

This policy describes the minimum security provisions Service Providers must have in place. The reasons for having these security provisions are:

1. To Protect the Peppol Network.
2. To Protect End Users.
3. To Protect Service Providers.
4. To increase confidence and trust in the governance of the Peppol Network.

6.4 Security provisions

Service Providers must have technical and organizational measures in place to secure the integrity and continuous operation of the Peppol Interoperability Framework and all data exchanged across the Peppol Network. These measures have to protect against:

1. Accidental or unlawful destruction.
2. Accidental loss.
3. Alteration.
4. Unauthorized disclosure or access.

5. All other forms of processing contrary to obligations as stated in the Peppol Governance framework.

The measures in place shall ensure a level of security appropriate to the risks represented by the data exchange and the nature of the data to be protected.

Back to Table of Contents

7 Peppol Authority Specific Requirements

7.1 Policy Purpose and Overview

The purpose of this Policy is to define the rules and provisions that must be respected by all actors participating in the definition, approval and enforcement of specific requirements for the use of the Peppol Network, which are applicable within the jurisdiction of a given Peppol Authority (PA), and which will be hereinafter referred to as “PA Specific Requirements”.

This Policy contains the following parts:

1. Purpose and Overview
2. Requirements from the Peppol Agreements
3. General Provisions on the:
   a. Definition of PA Specific Requirements
   b. Applicability of PA Specific Requirements
4. Categories of PA Specific Requirements
5. Approval and Change Management of PA Specific Requirements
6. Availability of PA Specific Requirements

7.2 Requirements from the Peppol Agreements

In accordance with clause 11 of the Peppol Authority Agreement and the Peppol Service Provider Agreement, the Peppol Coordinating Authority has the ability to approve PA Specific Requirements applicable for a given jurisdiction (clause 11.1).

Both the Peppol Authority Agreement and Peppol Service Provider Agreement impose a strong obligation on PAs to ensure that PA Specific Requirements do not hamper interoperability for Service Providers (SPs) and End Users operating actively in more than one jurisdiction or engaged in message exchange across jurisdictions (clause 11.2).

7.3 General Provisions

7.3.1 Definition of PA Specific Requirements

1. Peppol Authorities may define PA Specific Requirements applicable to the use of the Peppol Network within their jurisdiction only when:
   a. either they need to ensure compliance with legislation, regulation, or market conditions particular to that jurisdiction, or

b. they need to manage issues and risks as legitimately perceived by regulating authorities within the particular jurisdiction, and

c. in all cases, such requirements cannot be met by those specifications or other provisions that are universally enforced through the Peppol Interoperability Framework.

2. When defining and enforcing PA Specific Requirements, Peppol Authorities should strive to minimize the additional compliance costs and increased regulatory burden that such requirements will place on Service Providers.
3. PA Specific Requirements cannot be used to impose changes to any component of the Peppol Interoperability Framework but may be used to constrain their use, such as making an optional Peppol Dataset Type mandatory.
4. PA Specific Requirements must not be defined in a way that creates obstacles for global interoperability in the market of message exchange across jurisdictions by preventing Service Providers from offering services within a given jurisdiction, by measures such as requiring the use of specific tools or procedures that cannot be accessed by Service Providers located outside that jurisdiction.
5. PA Specific Requirements must not be defined in a way that creates obstacles for global interoperability in the market of message exchange across jurisdictions by preventing End Users based within their jurisdiction from accessing Peppol Services offered by service Providers located outside their jurisdiction, or from exchanging datasets with End Users in other jurisdictions.
6. The provisions in this section will constitute criteria for the approval of the PA Specific Requirements and must be taken into account when the OO produces a Compliance Report as described in section 7.5.

7.3.2 Applicability of PA Specific Requirements

1. PA Specific Requirements apply to Peppol Services offered to End Users (senders or receivers) which are legally based within the territorial jurisdiction of a Peppol Authority.
2. PA Specific Requirements must be respected by all Service Providers who provide Peppol Services to End Users (senders or receivers) which are legally based within the territorial jurisdiction of a Peppol Authority, irrespectively of the location of the Service Provider and independently of whether a Service Provider has signed a Peppol Service Provider Agreement with that Peppol Authority.

3. For the avoidance of doubt, PA Specific Requirements apply to all Service Providers who provide Peppol Services to End Users (senders or receivers) within the PA's jurisdiction, and not only to the Service Providers who have signed an agreement with that Peppol Authority.

7.4 Categories of PA Specific Requirements

PA Specific Requirements may be defined along the following categories:

1. Applicable or allowed identifier or identification schemes
2. Information security
3. Reporting on End User information and transaction statistics
4. Mandatory use of centralised services and global specifications
5. Service Level Requirements
6. Use of local interoperability specifications
7. Service Provider Accreditation

7.4.1 Applicable or allowed identifier or identification schemes

1. A Peppol Authority may need to express specific requirements related to the actual use of one or more specific identifier schemes for End Users legally based in its jurisdiction, such as a VAT number (or other unique and official identifier).
2. Only identification schemes allowed according to the Peppol Policy for Identifiers may be mandated as PA Specific Requirements.
3. Further to the provisions included in the Entity Identification Policy as set out in section 3, a Peppol Authority may however see a need to define and enforce further requirements, such as the use of a specific authoritative source for verification of Entity identification within the Jurisdiction.
4. If a Peppol Authority defines and enforce PA Specific Requirements under this category, it must provide sufficient information, guidance and access to any tools and resources necessary to enforce identification and verification obligations as stated in the Entity Identification Policy (section 3).

7.4.2 Information security

Any requirements on Information Security above and beyond what is stated in the Peppol Architectural Framework, which a Peppol Authority wants to enforce, must be defined, or incorporated by reference as part of the PA Specific Requirements.

7.4.3 Reporting on End User information and transaction statistics

PA Specific Requirements on reporting must not be defined when a uniform reporting mechanism is applied throughout the Peppol Network other than to support specific legislative and/or regulatory requirements applicable within a PA jurisdiction.

7.4.4 Mandatory use of centralised services and global specifications

1. A Peppol Authority may require, as part of its PA Specific Requirements, the use of centralised Peppol Addressing and Capability Look-up services for all or specific type of End Users legally based within its territorial jurisdiction. In such an event, the Peppol Authority must provide sufficient information/guidance for Service Providers, as well as access to all relevant tools or procedures.
2. A Peppol Authority may make the use of the Peppol Directory mandatory for End Users which are legally based within its territorial jurisdiction.
3. A Peppol Authority may make the use of optional global specifications (e.g. Invoice Response) mandatory for End Users which are legally based within its territorial jurisdiction.

7.4.5 Service Level Requirements

A Peppol Authority may apply, within its jurisdiction, stricter Service Level Requirements than those foreseen in the Peppol Interoperability Framework.

7.4.6 Use of local interoperability specifications

1. A Peppol Authority may request the use of local datasets or other interoperability specifications within its jurisdiction.
2. PA Specific Requirements under this category must comply with the requirements for Extended Use of Peppol as set out in section 8 and, more particularly, to the general provisions for Extended Use and specific provisions relevant to Local Extension.
3. The Peppol Coordinating Authority may grant an exception to the obligation for End Users to support the relevant Peppol BIS, subject to the provisions outlined in clause 12.3 of the Peppol Authority Agreement and Peppol Service Provider Agreement.

7.4.7 Service Provider Accreditation

1. Clause 11.3 of the Peppol Authority Agreement and Service Provider Agreement provides the PA with the authority to define and enforce its own

specific accreditation scheme to ensure compliance to their PA Specific Requirements.

2. The use of any such accreditation scheme to be enforced by the Peppol Authority must be defined or incorporated by reference as part of the PA Specific Requirements.

7.5 Approval and Change Management of PA Specific Requirements

7.5.1 Overarching Governance Provisions

1. PA Specific Requirements must be subject to a controlled lifecycle management process respecting the provisions outlined in this Policy. The lifecycle includes the following stages, all of which are subject to the provisions in this Policy:
   a. Introduction of a new or updated version of PA Specific Requirements.
   b. Releasing a new or updated version of a PA Specific Requirements.
   c. Migration from an old to a new version of a PA Specific Requirements.
2. The governance and lifecycle management for the content of PA Specific Requirements is allocated to the responsible Peppol Authority, while the responsibility for introduction of a new or updated version of PA Specific Requirements is allocated to the Agreements, Policies and Procedures Change Management Board (APP CMB).
3. The lifecycle management and governance of PA Specific Requirements must allow for adequate involvement and participation of all OpenPeppol Members affected.
4. PA Specific Requirements may contain annexes or attachments of a purely informative nature such as, but not limited to, the location of tools and other resources. These annexes and attachments are not subject to the Change Management provisions in this section but can be updated by the responsible PA. The APP CMB must be notified at all times and give the final approval for a revised version of such an annex.

7.5.2 Introduction of a new or updated version of PA Specific Requirements

The provisions in this section concern the introduction of a new set of PA Specific Requirements as well as the introduction of an updated version of PA Specific Requirements to become applicable within a jurisdiction.

7.5.2.1 Constructing a new or updated version of PA Specific Requirements

1. An updated version of PA Specific Requirements must be constructed by the responsible PA by applying approved RFCs to the current version.
2. A new version of PA Specific Requirements must be classified as follows:
   a. A major release, which contains new or removes existing rules or obligations, or substantially alters existing provisions.
   b. A minor release, which only elaborates on a rule, without altering the substance and principles of the PA Specific Requirements.
   c. A errata corrigenda release, which must be limited to error correction and clarifications of ambiguous language.

   An initial new set of PA Specific requirements is always considered a major release.
3. Before finalising a new or updated version of its PA Specific Requirements, the responsible PA should consult with OpenPeppol Members active within its jurisdiction, and should, to the extent possible, address the feed-back and comments provided through the consultation before submitting the final version of its proposed PA Specific Requirements for approval.

7.5.2.2 Submitting a new or updated version of PA Specific Requirements for introduction as part of the Peppol Interoperability Framework

1. A proposal to introduce a new or updated version of PA Specific Requirements as part of the Peppol Interoperability Framework must be submitted by the responsible PA through an RFC following the RFC process outlined in section 2.4.
2. Upon successful submission of an RFC to an RFC Register, the RFC must be allocated to the APP CMB, which shall be responsible for the next steps in the process.

7.5.2.3 Approval of a new or updated version of PA Specific Requirements as part of the Peppol Interoperability Framework

1. Each proposal for a new or updated version of PA Specific Requirements must undergo a compliance review by the Operating Office to ensure that they comply with the rules and provisions included in this Policy. The Compliance Report and recommendation from the Operating Office must be made available to the APP CMB as part of the basis for decision together with the final version of the proposed new version of PA Specific Requirements.

2. Each major or minor version of PA Specific Requirements must be made available for review by OpenPeppol Members. Any comments raised during the review must be addressed and resolved by the APP CMB in consultation with the responsible PA.
3. The final decision to put into effect a new or updated version of the PA Specific Requirements as part of the Peppol Interoperability Framework shall be taken by the APP CMB.
4. For PA Specific Requirements on the use of local interoperability standards, the provision of Extended Use (section 8) applies to the approval process.
5. If PA Specific Requirements fall into the category of “Mandatory use of centralised services and global specifications” (section 7.4.4) and a similar precedent has already been established for other PAs, these will be approved automatically without requiring the approval by the APP CMB. They will be directly published as part of PA Specific Requirements within the Peppol Interoperability Framework by the Operating Office, which will be acting in a delegated role to facilitate the process.
6. At any stage in the process a disagreement on a decision may be escalated according to the provisions in section 2.4.6 (Escalation).

7.5.3 Releasing a new or updated version of PA Specific Requirements

1. In accordance with clause 11.1 of the Peppol Authority Agreement and the Peppol Service Provider Agreement, PA Specific Requirements will be documented as part of the Peppol Interoperability Framework.
2. Upon their approval, the Operating Office shall be responsible for publishing all PA Specific Requirements and their supporting migration plan on the Peppol website as part of the Peppol Interoperability Framework description.

7.5.4 Migration from an old to a new version of PA Specific Requirements

1. Every release of PA Specific Requirements must be supported by a migration plan, which must respect the phase-in requirements of the changes contained in the release.
2. A migration plan must define the following steps:
    a. Phase-in: The new version is introduced in the Peppol Governance Framework as an upcoming rule set and relevant parties start preparing for its implementation, adjusting their internal processes and systems if necessary.

b. Switch-over: The new version of the PA Specific Requirements comes into effect, and the old version becomes obsolete.

3. The migration plan must contain the above steps as a minimum, clearly identifying what is expected of implementing parties at the beginning and end of each step and the time periods between milestones that delineate the beginning and end of each step. Migration plans may contain more steps if relevant and appropriate.

7.5.5 Timeline for Consultation and Implementation

The following table defines the time that must be allocated for consultation with OpenPeppol members on proposals for changes to the content of an existing set of PA Specific Requirements as outlined in section 7.5.2 above, and consultation on the introduction of a new version of PA Specific Requirements as part of the Peppol Interoperability Framework outlined in section 7.5.3 above.

	Minimum time that must be allowed for consultation
Resolution on RFC for content changes	4 weeks
Introducing a new major release	4 weeks
Introducing a new minor release	4 weeks
Introducing a errata corrigenda release	Na

Back to Table of Contents

8 Extended Use of Peppol

8.1 Policy Statement

In addition to the global Peppol Service Domains, which cover all jurisdictions within the Peppol Network, individual Peppol Authorities may develop and implement additional services, or extend the use of the Peppol Network.

OpenPeppol shall encourage and facilitate such initiatives, with a view to the gradual integration of Extended Use cases as global Peppol Service Domains, subject to sufficient interest and uptake from Peppol Authorities, Service Providers and End Users.

In all cases, any proposed additional Peppol Services or extension(s) of the Peppol Network must be able to integrate fully with the existing governance, operations and policies applying to the Peppol Network.

8.2 General Provisions

8.2.1 Types of Extended Use

Global Service Domains in OpenPeppol are the ones that are in use across the entire Peppol Network and are governed by OpenPeppol.

Extended use of Peppol can occur beyond the global Service Domains, built around use cases that can be categorized into one of three groups:

1. **Local Extensions to global Service Domains** which are already established across all jurisdictions within the Peppol Network:
    a. They are unique to the territorial jurisdiction of a specific Peppol Authority, as defined by that Peppol Authority.
    b. They do not involve changes to the Peppol technical specifications which are applicable within the existing global Service Domain in question.
    c. Such cases may include localized customisations of globally applicable technical specifications or bespoke local Datasets required for End Users to comply with local laws, regulations, or standards.
2. **Local Service Domains** newly established within the jurisdiction of a Peppol Authority:
    a. Their business process scope falls outside existing Peppol Service Domains.
    b. They do not require support outside a given local jurisdiction or cross-border capabilities.

c. Such cases may include national usage scenarios relevant to local stakeholders and processes, not relevant to stakeholders outside a specific geographical jurisdiction, which can be defined to include a country or a multi-country region.

3. **Incubations** of new global Service Domains:
   a. Aim to establish an entirely new Peppol Service Domain with potential to be relevant across the entire Peppol Network.
   b. Incubation will take place under the responsibility of a Peppol Authority when the prospect is deemed beneficial and preferable for OpenPeppol or if OpenPeppol lacks the capacity to develop a new Service Domain centrally and scale it to a global level.

8.2.2 Basic principles and requirements

1. All cases of Peppol Extended Use must be approved by the OpenPeppol Managing Committee.
2. They can be initiated either by OpenPeppol itself or by a Peppol Authority that wishes to embark on such a prospect.
3. Approval of Extended Use will be based on the fulfilment of required criteria, as stated below.
   a. To be approved, Extended Use must:
      i. Cause no foreseeable conflict with:
         - any global Service Domains already existing,
         - any Peppol Services already approved for Extended Use,
         - any promising prospects for new such Service Domains already considered by OpenPeppol for global or local use.
      ii. Describe the impact of the proposed Extended Use on the use of technical specifications that are applicable and mandatory in existing Peppol Service Domains, so that it can be determined that no negative impact is caused on interoperability across the Peppol Network.
      iii. Be feasible within the organizational and financial capacity and capability of the proposing Peppol Authority and/or OpenPeppol as may be relevant.
   b. To be approved, Extended Use should:

i. Extend the coverage and usage of the Peppol Network in terms of users, transaction types, Service Providers, new stakeholder constituencies, application areas and technology fields, increasing the value of the Peppol Network.

ii. Increase the potential of Peppol to play the role of a robust interoperability environment that can be dependably considered as essential IT infrastructure within and among national jurisdictions.

iii. Enhance the reputation of OpenPeppol and build trust in internal and external stakeholders, strengthening the Peppol brand.

4. A proposal for approval of Extended Use must meet the criteria stated above and include, inter alia:
   a. Use case description.
   b. Stakeholder analysis – who are the end users, the potential Service Providers, the Peppol Authority (if different than the proposing one).
   c. Growth potential for the Peppol Network – high-level indications pointing to the addition of new users, transactions, service providers.
   d. Technical specifications to be used, including terms of availability and IPR status. Differences with existing, globally applicable specifications must be highlighted and justified.
   e. Change management responsibilities for the proposed Extended Use, intended to be assumed either by a Peppol Authority or by another relevant body within the jurisdiction concerned, if applicable.
   f. Peppol Authority responsibilities related to the proposed Extended Use.
5. The OpenPeppol Managing Committee shall decide on all submitted proposals for Extended Use, based on the criteria included under point 2 above.
6. OpenPeppol shall maintain a public list of approved Extended Use cases, and the Peppol Authorities that are responsible for each.

8.3 Particular Provisions and Governance

8.3.1 Local Extensions and Service Domains

Local Extensions to existing global Service Domains are adopted by Peppol Authorities through their PA Specific Requirements.

Local Service Domains are adopted through inclusion to the Domain jurisdiction of Peppol Authorities by listing them in Annex 2 of the Peppol Authority Agreement.

Onboarding Service Providers to a Local Service Domain can be done through Annex 2 of the Peppol Service Provider Agreement.

Subject to the general rules set out above, individual Peppol Authorities may construct their Local Extensions and Domains, subject to the principles outlined in clause 11.2 and 11.4 as well as 12.4 of the PA Agreement.

In case other Peppol Authorities may wish to adopt any approved Local Extension or Local Service Domain, the Peppol Authorities concerned and OpenPeppol shall first consider the possibility of moving to a global specification or Service Domain before the Managing Committee takes a final decision on further Extended Use at a local level.

8.3.2 Incubation

8.3.2.1 Function and goal

A successful incubation process leads to the establishment of a new global Service Domain in Peppol, conforming to all the relevant governance structures and processes of existing Service Domains that are applicable across the entire Peppol Network. Unlike local types of Extended Use, an incubation is therefore an inherently and explicitly temporary construct.

8.3.2.2 Incubation Charter

An Incubation is founded upon a project charter, which shall be called the Incubation Charter.

The structure of the Incubation Charter and the requirements it must fulfil are laid out in the OpenPeppol Operational Procedures. They must include at least such tangible deliverables as to demonstrate that the Incubated Service Domain is ready to graduate into full global Service Domain status.

The Incubation Charter may be developed after an initial, in principle approval of the incubation prospect by the Managing Committee. It must be submitted to and approved by the Managing Committee prior to the start of the undertaking. Such approval shall not be withheld except for specific and compelling reasons.

8.3.2.3 Incubation Monitoring Committee

An incubation is overseen by a Monitoring Committee, which is established for the purposes of a particular incubation project and is therefore transient in nature. Its function is to monitor on a regular basis the progress of an incubation, according to stated objectives and deliverables laid out in the Incubation Charter.

The Incubation Monitoring Committee is composed of:

- A representative of the proposing Peppol Authority.
- A representative of the Managing Committee or, in case no MC member is available, a representative of the Operating Office.
- Depending on relevance and availability, representatives of other Peppol Authorities, Service Providers or Domain Communities. External subject matter experts may also be included.

The Incubation Monitoring Committee composition will be decided as part of the Incubation Charter at the time of incubation approval. Communities will be consulted during this process.

The Incubation Monitoring Committee is a consulting body and does not make formal decisions. The final decision about the incubation results will be made by the Managing Committee based on achievement of goals stated in the Incubation Charter. Full adoption shall not be denied to any incubation which has fulfilled the requirements laid out in its charter, unless conditions have materially changed since the approval of the charter, in a manner that could not have reasonably been foreseen at the time of approval. The Management Committee shall without delay notify the Incubation Monitoring Committee of such developments as may come to its attention.

The Incubation Monitoring Committee may submit deliverables foreseen in the Incubation Charter to a peer review by Peppol Authorities and Service Providers, or all OpenPeppol Members.

Back to Table of Contents

9 Compliance Policy

9.1 Policy purpose and overview

This policy is focused on the responsibilities of the Peppol Authorities and the Peppol Service Providers with a view to ensure interoperability across the full Peppol Network and to improve the communication and convergence between all parties.

This can only be achieved if the OpenPeppol community maintains a common rule set, i.e. principles and compliance criteria, as a baseline for all parties involved.

It contains the following parts:

1. Purpose and overview
2. Requirements from the Peppol Agreements
3. Compliance supervision and enforcement
4. Claim escalation and dispute resolution
5. Authority delegation

9.2 Requirements from Peppol Agreements

1. The legal obligation on SPs to ensure that Peppol Services offered to the market comply to the relevant components of the Peppol Interoperability Framework follows from the Peppol Service Provider Agreement clause 9.5.
2. Furthermore, clause 7.1.2 of the Peppol Service Provider Agreement provides that the PA shall ensure that Peppol Services offered within their jurisdiction are in compliance with the components of the Peppol Interoperability Framework.
3. Reactions to cases of non-compliance are defined in clause 18 of the Peppol Service Provider Agreement.

9.3 Compliance supervision and enforcement

1. Compliance of a Peppol Authority is measured against the Peppol Authority Agreement and the Internal Regulations on the Use of the Peppol Network.
2. Compliance of a Service Provider is measured against the Service Provider Agreement and the Internal Regulations on the Use of the Peppol Network.

9.3.1 Peppol Network supervisory bodies

The compliance supervisory bodies are:

1. Peppol Coordinating Authority: It is the main governing body in the Peppol Network. The Peppol Coordinating Authority is responsible for the supervision and enforcement of the policies and procedures for the Peppol Authorities and for the issue resolution of claims that may affect more than one Peppol Authority.
2. Peppol Authorities: As defined in the Peppol Authority Agreement, the Peppol Authorities are responsible for the supervision of Service Providers within their jurisdiction. They are the entities that shall enforce the OpenPeppol policies and procedures on their Service Providers. They shall also enforce on their Service Providers, the Peppol Authority Specific Requirements of all Peppol Authorities.

9.3.2 Types of supervisory procedures

There is a proactive and a reactive type of supervision and respective ways to enforce compliance.

1. Reactive supervision and enforcement are initiated as a result of a non-compliance complaint raised to a Peppol Authority or the Peppol Coordinating Authority, subject to provisions described in section 9.3.4. Such complaints may be related to:
   a. an alleged breach of any rules stated in the Peppol Agreements or Internal Regulations for the use of the Peppol Network,
   b. any actors or bodies allegedly not following due process in the execution of their duties and responsibilities as described in the Peppol Interoperability Framework.
2. Proactive supervision and enforcement are continuous, and relevant actions are executed by the supervisory body analysing the Peppol Network infrastructure and the data obtained from the Service Providers. Specific provisions are described in section 9.3.3 related to actions taken by the Peppol Coordinating Authority, but this does not preclude similar or other proactive supervision procedures to be established and executed by Peppol Authorities within their jurisdiction.

9.3.3 Continuous and proactive supervision

9.3.3.1 Monitoring Compliance

1. Continuous supervision and monitoring of compliance is done by the Peppol Coordinating Authority and Peppol Authorities through the use of the data gathered from the Peppol Network and the data reported by Service Providers according to the provisions of the Data Usage and Reporting Policy.

2. Checks on available data will be done regularly by the OpenPeppol Operating Office, which acts on behalf of the Peppol Coordinating Authority. Results will be made available to Peppol Authorities in relation to the Service Providers and End Users within their jurisdiction. Specific controls on behalf of Peppol Authorities can be performed by the Operating Office through the tools available to and by the Peppol Coordinating Authority.
3. The goal of the monitoring process is to determine whether the rules for the use of the Peppol Network are followed, focusing on (but not limited to) the following:
    a. Applicable Specifications, as determined by the Peppol Architectural Framework.
    b. End User Identification, as foreseen by the Entity Identification Policy.
4. When a migration process is in progress, the Operating Office shall take into account the deadlines for the phase-in of the new specification and phase-out of the deprecated one.

9.3.3.2 Managing non-compliance detected through monitoring

1. Derived from the above monitoring process, the supervisory body shall describe the non-compliance issues with the list of End Users and Service Providers in breach.
2. Each Peppol Authority shall act on issues concerning the Service Providers they have signed SP Agreements with and/or End Users based in its jurisdiction. Issues can be derived both from the proactive monitoring of the Peppol Coordinating Authority or from its own proactive monitoring processes.
3. To manage non-compliance, the supervisory bodies shall follow the provisions below:
    a. When the Peppol Coordinating Authority discovers an incident of non-compliance, it shall open a non-compliance issue in the Peppol Service Desk reporting the breach. The ticket shall explain the breach of compliance and identify the Service Provider(s) and, if relevant, End user(s) involve in the issue. The ticket shall be assigned to the Peppol Authority responsible for the Service Provider.
    b. When a Peppol Authority discovers an incident of non-compliance or receives notification of such an incident from the Peppol Coordinating Authority, it shall contact the Service Provider or Service Providers and address the non-compliance, proceeding to its resolution. The Peppol Authority shall set the non-compliance issue resolution deadline as may be appropriate.

c. Once resolved, the supervisory body shall process to closing the issue.

d. Any party affected by the complaint and its resolution, or lack thereof, can escalate the issue to the Peppol Coordinating Authority as defined in section 9.4.2 if the party considers the problem of non-compliance is not resolved in a satisfactory manner.

9.3.4 Supervisory procedure based on a complaint

1. When a non-compliance incident occurs, a direct discussion among the involved parties should take place in an attempt to resolve the issue.
2. In case no agreement can be reached on a resolution, any affected party has the right to raise the non-compliance to its Peppol Authority or to the Peppol Authority/Authorities of the other party/parties involved in the incident.
3. The Peppol Authority shall mediate between the parties trying to find a resolution to close the issue according to the Peppol Agreements, Internal Regulations and Operational Procedures.
4. Once resolved, the Peppol Authority shall close the issue.
5. Should the issue not be resolved because it affects more than one Peppol Authority, due to its complexity or for any other reason, the Peppol Authority shall escalate the issue as described in section 9.4.2.
6. Any party affected by the complaint and its resolution, or lack thereof, can also escalate the issue to the Peppol Coordinating Authority as defined in section 9.4.2 if the party considers the problem of non-compliance is not resolved in a satisfactory manner.

9.4 Enforcement of policies and procedures

9.4.1 General Provisions

1. A supervisory body has the power to enforce the procedures and policies on the set of entities it is responsible for, as defined in this policy.
2. Procedures and policies can be enforced through the penalties specified in section 9.4.3.
3. As a result of penalty enforcement, End Users may be removed from the Peppol Network and added to a blacklist of End Users so that they will not be allowed to become a Peppol End User again.
4. For Service Providers, the ultimate penalty is to remove them from the Peppol Network by revoking their technical capability to exchange datasets.

9.4.2 Escalation process in case of dispute

1. In case of dispute, the issue, the resolution, and the dispute arguments from the party raising the dispute shall be filed in the Peppol Service Desk.
2. The Peppol Coordinating Authority, through the Operating Office shall try to resolve the issue, and in case the issue cannot be resolved, they shall escalate it to the Managing Committee with a pre-analysis and a suggested resolution.
3. The Managing Committee shall assess the case and provide a final decision. The Operating Office shall communicate the final decision to the parties through the Peppol Service Desk.
4. The resolution from the Managing Committee shall be considered final, and there is no other body to appeal.
5. While a dispute resolution process is in progress, deadlines foreseen as part of the escalation process shall be considered as paused. This provision does not apply to the 5 working day deadline for a Service Provider to respond with a reasonable plan and to cases where the supervisory body takes immediate action under the conditions of clause 18.5 of the Service Provider Agreement.

9.4.3 Penalties

1. Penalties are the means to support the enforcement of the policies and procedures. The penalties that may be enforced by the supervisory body are defined in the Peppol Agreement clause18 as follows:
    a. Internal blacklisting on an area of the OpenPeppol website accessible to members only, i.e. publication of the fact that the Service Provider or the End User is in a non-compliance situation on the closed member site of OpenPeppol.
    b. Public blacklisting, i.e. publication of the fact that the Service Provider or the End User is in a non-compliance situation on the public website of OpenPeppol (www.peppol.eu) and on the website used by the relevant PA for market communication.
    c. Temporary suspension of a Service Provider’s access to the Peppol Network. This requires the revocation of the certificate and re-issuance of a new one after the established period of suspension. End Users may also be temporarily deregistered from the SMP.
    d. Permanent removal from the Peppol Network, i.e. permanent revocation of the Peppol certificate.

2. Penalties are applied gradually and with an increasing level of severity following the escalation levels mentioned in point 1 above, and after adequate warnings have been issued in compliance with article 18 of the Peppol SP Agreement.
3. The Peppol Authority may extend an initially limited suspension, depending on conditions set up by the Peppol Authority or ultimately exclude the Service Provider from the Peppol Network by revoking their Peppol Certificate. Any extension in suspension shall be documented by a warning note.
4. The Peppol Authority may take immediate action to suspend a Service Provider's access to the Peppol Network in line with the provisions of clause 18.5 of the Service provider Agreement.

9.5 Authority delegation

Every Peppol supervisory body can delegate the role of supervision to an entity or team within their internal organization.

The Peppol Coordinating Authority delegates the compliance processing to the Operating Office and its authority to the Managing Committee.

Back to Table of Contents

Version control

Version	Date	Comments
1.0	16.11.2021	Approved by the OpenPeppol Managing Committee (MC159 meeting)
1.0.1	21.06.2022	Postponement of applicability for the Reporting Policy and the Semantic Versioning Guidelines Annex
2.0.0	29.11.2023	**This version introduces changes to the following policies:** • Change Management Policy • Data Collection, Reporting and Usage Policy • PA Specific Requirements • Removal of the Semantic versioning Annex Further details are provided in the accompanying Release Note.

List of Terms and Abbreviations

Term	Definition
API	Application Programming Interface
APP CMB	Agreements, Policies and Procedures Change Management Board
BIS	Peppol Business Interoperability Specifications
CC	OpenPeppol Coordinating Committee
CMB	Change Management Board
EN	European Norm
IPR	Intellectual Property Rights
MC	OpenPeppol Managing Committee
OO	OpenPeppol Operating Office
PA	Peppol Authority
PCA	Peppol Coordinating Authority (OpenPeppol AISBL)
PKI	Public Key Infrastructure
RFC	Request for Change
SBDH	Standard Business Document Header
SML	Service Metadata Locator
SMP	Service Metadata Publisher
SP	Peppol Service Provider
XML	Extensible Markup Language