

Peppol Authority Specific Requirements – Approval 2022

MC167 Decision – 2022.06.21

The Managing Committee discussed the PA Specific Requirements in two meetings over three different sessions: MC165 (24.05.2022) and MC166 (31.05.2022, continued on 07.06.2022). After detailed deliberations, it decided the following:

1. Decision to approve PASR
 - a. All Peppol Authorities Specific Requirements from Australia, Belgium, Germany, Iceland, Italy, Japan, New Zealand, the Netherlands, Norway, Poland, and Singapore are hereby approved, with some exception
 - b. Exceptions are stated in point 2 below and are based on comments by MC members, having as starting point recommendations from the Operating Office included in the Assessment and Compliance Reports which have been provided to the MC ahead of the meetings.
 - c. As part of this decision, the MC agreed on certain guidelines that should be considered by Peppol Authorities in future development, refinement, and update of PA Specific Requirements, but also in the manner in which they will enforce them. These guidelines are stated in point 3 below.
2. Exceptions include:
 - a. Mandatory Use of the Peppol Directory (Australia, Germany, New Zealand, Netherlands, Italy, Belgium):
 - i. Approval postponed until a legal opinion has been obtained by OpenPeppol about the possible liability of the Association and the conditions, if any, that must be applied to the notification of end users and their explicit consent, if needed.
 - ii. The MC instructs the OO to prioritize such legal analysis and have it completed until September 2022.
 - b. Mandatory use of the Message Level Response (Germany, Netherlands):
 - i. Approval postponed until the beginning of 2023 until progress is made in a new work group that is being initiated shortly by PoAC, SPC and PAC.
 - ii. The MC urges the Communities to speed up work and adopt a policy for the entire Peppol Network so that there is no need for

individual PASR going forward and the Network takes the time to migrate and adapt with minimal disruptions

- c. End-to end security (encryption, authentication) in the Post-award Service Domain (Netherlands):
 - i. The MC requests that NPa provide more details regarding the impact on the global Peppol Network, the mechanisms that can be used to comply with this requirement, the way to enforce it and the cost incurred by Service Providers offering services, particularly those outside NL.
 - ii. The MC also suggest that the NPa consider promoting enhanced end-to-end security through positive incentives and market awareness measures.
- d. Data Quality in the Post-award Service Domain (Netherlands):
 - i. The MC requests that NPa provide more details regarding the impact on the global Peppol Network, the mechanisms that can be used to comply with this requirement, the way to enforce it and the cost incurred by Service Providers offering services, particularly those outside NL.
 - ii. The MC also suggest that the NPa consider promoting enhanced data quality through positive incentives and market awareness measures.
- e. Mandatory use of the AS4 transmission protocol (Netherlands):
 - i. The MC recommends that the NPa reconsider the wording of the requirement and confirm what is the actual intention, given that mandatory support of AS4 is a global rule for Peppol.
 - ii. The MC instructs the OO to ensure that there are no SPs remaining in the Peppol Network after 1 July, unless they are confirmed as compliant with AS4.
 - iii. The MC requests from eDEC to take the necessary steps to phase out AS2 completely.

3. Guidelines for the future:

- a. Guidance: The Peppol Authorities should clearly separate the actual rule, to be considered as obligations, from guidance offered to Service Providers on how to comply. Ideally, there should be different documents for PA Specific Requirements (PASR) and PA Specific Guidance (PASG)
- b. Identifiers: When Peppol Authorities mandate specific identifier schemes for their jurisdiction, they should also make all reasonable efforts to support market requirements expressed by Service Providers, such as the registration on lower-level units within a legal entity using different identifiers (e.g., in retail sector). The topic should be further discussed in the Communities.
- c. Centralized SMPs: When mandating the use of a centralized SMP in their jurisdiction, Peppol Authorities shall provide guidance to Service Providers on how to use it, particularly when Service Providers are based outside their jurisdiction.
- d. Reporting: Given that OpenPeppol is in the process of establishing a centralized reporting mechanism, national reporting schemes now approved as PASR should be phased out when the centralized mechanism is operational and implemented by Service Providers in the following months. In the interim transition period, Peppol Authorities shall have a pragmatic approach and ideally not to extend these schemes to Service Provider that have not been reporting to them under the TIA framework.
- e. Security: Given that there is a Security work group now operational, aiming to adopt a Peppol-wide security policy, Peppol Authorities should refrain from introducing through PASR new security requirements from what go beyond what they have today.
- f. Accreditation Policies: As clearly stated in clause 11.3 of the PA Agreement (The Peppol Authorities should use national Accreditation Policies in order to ensure compliance with their other PASR and not to introduce new PASR through Accreditation. In particular, certain business requirements that are currently part of national Accreditation Policies should be expressed as a different category of PASR. Since this is not currently foreseen in the Internal Regulations, it could be introduced following the provisions of the Change Management Policy.
- g. Local interoperability specifications: When Peppol Authorities introduce local interoperability specifications as part of their PASR they should make sure they apply them only to Service Providers that offer relevant services. For example, if there is a local invoice specification in a

jurisdiction, the Peppol Authority should not ask compliance from a Service Provider that offers only eOrders.

4. Future handling of PA Specific Requirements:

- a. The MC instructs the OO to develop a proposal for a change management policy with respect to PA Specific Requirement.
- b. In doing so the OO should consult all relevant stakeholders and especially the APP CMB, which should be requested to review and approve the policy.