Guidance on Peppol End User Identification Policy in Poland

Table of content:

1. General obligations

This guide is based on Peppol's End User Identification policy indicated in sections 3.3.1 and 4.3 of Peppol Internal Regulations. In accordance with these rules „Peppol Service Providers shall ensure that the […] information is known for all End Users (senders and receivers) to which they provide Peppol services". Moreover, Peppol Service Providers shall ensure that these data are reported to the Peppol Coordinating Authority, according to regulations stated above.

This guide sets out how to implement this principle for Service Providers operating in jurisdiction area of Poland, with particular emphasis on the key and largest component of the Peppol network - the national Electronic Invoicing Platform (PEF).

2. End User Identification Process

Peppol Service Providers shall ensure tool to meet the requirements indicated in section 3.3.1 of Internal Regulations, however under certain conditions some of requirements do not have to apply directly, as stated below. Section 3.3.1 indicates following data to be collected:

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 Peppol 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.

b.   Country and (where applicable) territory where the intermediate is legally based.

Such data shall be collected through the information indicated in:

a) written contract between Peppol Service Provider and End User (recommended for commercial services);
    or
b) through the self-declaration signed electronically by the End User representative using Trusted Profile (https://pz.gov.pl/dt/login/login?urlt=ycss5d11cvt0of0dsg37). Moreover, for PEF providers, such self-declaration may be considered as a proof of ownership . (recommended for PEF providers).

3. Verification of data

a) PEF services

Due to the mass nature of the service, PEF providers are not responsible for verification of data provided by the End User representatives. This caveat applies to both onboarding process and periodic review.

Nevertheless, PEF providers shall ensure that End User data can be online and continously updated by End User representatives (administrators) having access to account management. Moreover, obligation to update data by End User must be clearly indicated in regulations of the platform and all users have to read and approve these terms and conditions before starting using PEF services. In addition, the service should force the End User to verify and confirm or update the data at least once a year.

During registration process all users have to sign self-declaration mentioned in section 2 above, using Trusted Profile. Exchange of documents is possible for successfully registered End Users only.

In case of any suspicious activities account can be online blocked or suspended and its administrator can be clearly identified and summoned to explain situation (with the possibility of further legal escalation).

b) Other services

Good practice is recommended, in which the Service Provider will ask End User about the up-to-date data at least once a year. The End User should also update information about itself after each change.

4. Integration with national databases

Service Providers can ensure auxiliary services basing on connection with other national registers such as REGON, CEIDG etc. Such connection may be established via free and public-open API and can be used within End User registration process.

Such solution can ensure better data quality, however can not be used as the sole source of information – due to the fact that the registers may not be updated online and the risk that data presented there may be out of date.

5. Reporting about End Users

As stated in section 3 above, PEF providers are not responsible for personal verification of End Users data but are responsible for providing services that enable such self-verification. Therefore, reporting requirement indicated in section 4.3 of Peppol Internal Regulations can be only applied to the extent resulting from this guide. It means that PEF providers will provide required information to Peppol Coordinating Authority using data delivered by End Users, without additional verification.

Requirement of reporting applies to other Service Providers as well (including other commercial services of entities operating as PEF providers), taking into account rules resulting from OpenPeppol Internal Regulations and this guide accordingly.