ASSOCIATION REACTION 19
19, Boulevard Malesherbes
75008 Paris

OPENPEPPOL AISBL

À l'attention du Secrétaire général et des membres du Managing Committee

Rond-point Robert Schuman 6, boîte 5
1040 Bruxelles
Belgique

Par lettre RAR n°RK766811033FR
Et par courrier électronique

Courriels : info@peppol.eu – openpeppol@peppol.eu

À Paris, le 5 août 2026

Objet : contestation de la légitimité et de l'étendue des fonctions exercées par OpenPeppol dans le cadre français – demande de cessation et de suspension conservatoire – demande de communication de documents et de garanties – préservation des preuves.

Madame, Monsieur,

J'interviens en qualité de Président de l'ASSOCIATION REACTION 19 qui compte parmi ses adhérents de nombreuses entreprises soumises à la facturation électronique et elle s'inquiètent au sujet des fonctions exercées par l'association OpenPeppol AISBL dans le cadre de la mise en œuvre de la facturation électronique obligatoire en France.

La présente constitue une interpellation formelle et une mise en demeure de justifier l'ensemble des pouvoirs exercés par votre association à l'égard de la France, de mettre un terme aux présentations et interventions dépourvues de fondement suffisamment établi et, dans l'attente de ces justifications, de suspendre les actes normatifs ou discrétionnaires susceptibles d'affecter les entreprises françaises.

I. Sur la nature juridique d'OpenPeppol et l'importance des pouvoirs qu'elle revendique

OpenPeppol est une association internationale sans but lucratif de droit belge, enregistrée sous le numéro d'entreprise 0848.934.496, dont le siège est établi à Bruxelles. Elle constitue donc une personne morale privée et non une institution de l'Union européenne, une autorité administrative européenne ou une organisation internationale créée par traité.

OpenPeppol affirme cependant être l'entité juridique propriétaire de Peppol et exercer une autorité sur plusieurs composantes centrales du réseau, notamment :

- le Service Metadata Locator, ou SML ;
- l'infrastructure à clés publiques, ou PKI ;
- le cadre d'interopérabilité Peppol ;
- les accords conclus avec les autorités Peppol ;
- les règles applicables aux prestataires de services ;
- les mécanismes de certification, de conformité et, le cas échéant, de révocation des certificats.

OpenPeppol indique elle-même que le SML constitue un service centralisé unique qu'elle fournit et que les certificats PKI peuvent être révoqués en cas de non-respect des accords du réseau.

Il en résulte une concentration particulièrement importante de prérogatives techniques et contractuelles entre les mains d'une association privée : définition de normes, administration d'éléments techniques centraux, délivrance ou révocation de certificats, organisation de la conformité des prestataires et capacité d'influer sur l'accès effectif au réseau.

Cette situation appelle des garanties renforcées de légalité, de transparence, d'indépendance, de sécurité, de continuité et de responsabilité, dès lors que les infrastructures concernées sont appelées à être utilisées dans le cadre d'une obligation légale imposée aux entreprises françaises.

II. Sur l'incertitude affectant actuellement la qualité d'Autorité Peppol pour la France

La DGFiP et OpenPeppol ont annoncé que la Direction générale des finances publiques était devenue Autorité Peppol pour la France le 8 juillet 2025. La page actuelle d'OpenPeppol consacrée aux autorités nationales désigne également la DGFiP comme Autorité Peppol France.

Pourtant, la documentation de gouvernance actuellement publiée par OpenPeppol continue d'identifier, dans le tableau des exigences spécifiques nationales, **OpenPeppol AISBL elle-même comme Autorité Peppol pour la France**. Elle mentionne en outre des exigences françaises, dites « France PASR », approuvées le 25 février 2026.

Cette contradiction est majeure.

Elle ne permet pas de déterminer avec certitude :

1. à quelle date exacte OpenPeppol a cessé d'exercer les fonctions d'Autorité Peppol par intérim pour la France ;
2. si l'ensemble des fonctions exercées antérieurement par OpenPeppol a effectivement été transféré à la DGFiP ;
3. quels pouvoirs OpenPeppol conserve en qualité d'autorité coordinatrice ;
4. sur quel fondement OpenPeppol est encore mentionnée comme Autorité Peppol pour la France dans les PASR publiées en 2026 ;
5. quelle entité a juridiquement approuvé, repris ou validé les exigences françaises actuellement applicables ;
6. quelles décisions peuvent être prises par OpenPeppol sans accord préalable de la DGFiP ;
7. quelle autorité est responsable en cas de défaillance, de compromission ou de révocation affectant un prestataire opérant en France.

OpenPeppol avait précédemment indiqué avoir assumé, sur décision de son propre Managing Committee du 11 décembre 2024, la fonction d'Autorité Peppol intérimaire pour la France, dans l'attente de la reprise de cette fonction par la DGFiP.

Une décision prise par l'organe dirigeant d'une association privée ne saurait cependant, à elle seule, constituer le fondement d'une délégation de puissance publique française ni autoriser cette association à édicter des conditions produisant des effets contraignants à l'égard des entreprises françaises.

Il vous appartient donc d'établir la chaîne complète des décisions, habilitations, accords et transferts de responsabilités sur laquelle reposent vos interventions.

III. Sur les risques structurels résultant de cette organisation

1. Risque tenant à la concentration de fonctions critiques

OpenPeppol déclare exercer son autorité sur la PKI, le SML et le cadre d'interopérabilité. Ces éléments conditionnent l'identification des acteurs, l'adressage des échanges, l'authentification des prestataires et la confiance accordée aux communications.

Toute compromission, indisponibilité, erreur de configuration, révocation injustifiée ou défaillance affectant ces composants pourrait donc provoquer des conséquences en chaîne sur un grand nombre d'opérateurs.

Le caractère fédéré des points d'accès ne supprime pas le risque systémique lié au contrôle central de l'adressage, de la certification et des règles de confiance.

2. Risque de confusion entre gouvernance privée et fonction quasi réglementaire

OpenPeppol présente sa gouvernance comme reposant sur plusieurs catégories de membres, notamment les autorités Peppol, les prestataires de services et les utilisateurs finaux.

Le Managing Committee comprend des représentants issus de ces différentes communautés et le Security Committee est composé de représentants des autorités Peppol et des prestataires de services.

Cette organisation n'est pas illicite en elle-même. Elle soulève néanmoins des questions objectives relatives :

- à l'indépendance des décisions ;
- à la prévention des conflits d'intérêts ;
- à la représentation effective des entreprises obligées d'utiliser le système ;
- à la participation d'entreprises privées aux décisions techniques ou normatives ;
- aux conditions dans lesquelles les intérêts des prestataires sont conciliés avec ceux des utilisateurs captifs ;
- à l'existence de voies de recours indépendantes.

Ces questions sont d'autant plus importantes qu'à compter du 1er septembre 2026, l'émission, la transmission et la réception des factures électroniques relevant du dispositif français doivent s'effectuer par l'intermédiaire d'une plateforme agréée.

3. Risque lié à la modification unilatérale des règles

OpenPeppol a publié une nouvelle version 4.0.0 de ses règles internes relatives à l'utilisation du réseau, approuvée le 24 juin 2026 et déclarée applicable dès sa publication.

L'application immédiate de règles adoptées par les organes internes d'une association privée soulève la question de leur opposabilité aux entreprises françaises et aux prestataires intervenant dans le cadre d'une obligation légale nationale.

Il convient notamment de déterminer :

- si la DGFiP a expressément validé ces nouvelles règles ;
- si elles peuvent modifier les droits et obligations des acteurs français ;
- si un droit de consultation ou de contestation a été organisé ;
- si leur application peut conduire à une suspension ou une révocation ;
- quelles règles prévalent en cas de contradiction avec le droit français ou européen.

4. Risques portant sur la confidentialité et les secrets protégés

Les factures et données associées peuvent révéler l'identité des clients et fournisseurs, les prix pratiqués, les volumes d'activité, les conditions commerciales, la nature des prestations, les habitudes économiques, les difficultés de paiement et, pour certaines professions, des informations couvertes par un secret professionnel.

Ces informations sont susceptibles de constituer des données à caractère personnel ou des secrets d'affaires protégés par le règlement général sur la protection des données, par la directive européenne relative aux secrets d'affaires et par les articles L. 151-1 et suivants du Code de commerce français.

Or la politique de confidentialité publiquement accessible sur le site d'OpenPeppol paraît principalement consacrée aux données collectées à l'occasion de la consultation de son site internet. Elle ne permet pas, à elle seule, de connaître précisément le rôle d'OpenPeppol dans les traitements liés au SML, à la PKI, aux journaux techniques, aux statistiques du réseau et aux opérations de conformité.

5. Risques portant sur la souveraineté, la continuité et la responsabilité

Il doit également être établi :

- où sont matériellement exploités les composants centraux du réseau ;
- quelles personnes y ont accès ;
- quels sous-traitants techniques interviennent ;
- dans quels États les données, métadonnées, journaux et sauvegardes sont conservés ;
- quelles mesures permettent de prévenir l'accès par des autorités étrangères ;
- quelles solutions de continuité existent en cas de défaillance d'OpenPeppol ;
- quelles garanties de réversibilité sont prévues ;
- quelle assurance couvre les conséquences d'un incident majeur ;
- quel droit et quelle juridiction seraient applicables aux recours des entreprises françaises.

IV. Demandes formelles de communication

En conséquence, je vous mets formellement en demeure de me communiquer, dans un délai de **quinze jours calendaires à compter de la réception de la présente**, les documents et informations suivants.

1. Habilitation et accords avec la France

La copie intégrale, datée et signée :

- du Peppol Authority Agreement conclu avec la DGFiP ;
- de ses annexes, avenants et exigences particulières ;
- de toute convention ayant autorisé OpenPeppol à intervenir provisoirement pour la France ;

- de tout acte organisant la fin de cette période intérimaire ;
- de tout acte transférant à la DGFiP les responsabilités antérieurement exercées par OpenPeppol ;
- de toute décision publique française ayant autorisé la signature de ces accords.

2. Répartition actuelle des compétences

Un tableau exhaustif indiquant, pour chaque fonction, l'entité actuellement compétente entre la DGFiP et OpenPeppol, notamment pour :

- l'adoption et la modification des PASR françaises ;
- l'accréditation et la surveillance des prestataires ;
- les tests de conformité ;
- la délivrance et la révocation des certificats PKI ;
- la gestion des incidents ;
- la gestion des non-conformités ;
- le traitement des plaintes ;
- la conservation des journaux ;
- l'administration du SML ;
- l'interruption ou la suspension d'un accès au réseau.

3. Contradiction affectant les PASR françaises

Une explication circonstanciée sur le maintien, dans la documentation publiée par OpenPeppol, de la mention « OpenPeppol AISBL » comme Autorité Peppol pour la France, alors que la DGFiP est présentée ailleurs comme l'autorité nationale compétente.

Vous préciserez si cette mention résulte :

- d'une erreur documentaire ;
- d'une compétence résiduelle conservée par OpenPeppol ;
- d'un régime transitoire ;
- d'un nouvel accord ;
- ou d'une autre cause juridique ou technique.

En cas d'erreur, vous devrez procéder immédiatement à sa rectification sur l'ensemble de vos documents et supports.

4. Gouvernance et conflits d'intérêts

La communication :

- de la liste des membres ayant participé aux décisions relatives à la France ;
- des déclarations d'intérêts correspondantes ;
- des règles de prévention et de traitement des conflits d'intérêts ;
- des procès-verbaux et décisions du Managing Committee concernant la France ;
- des avis et votes intervenus sur les PASR françaises ;
- des observations reçues durant les consultations ;
- des réponses apportées à ces observations ;
- de l'identité des prestataires privés ayant participé à la définition de l'architecture française.

5. Sécurité informatique

La communication, sous une forme permettant d'en vérifier l'existence, la portée et les conclusions :

- des certifications de sécurité dont bénéficie OpenPeppol ;
- des rapports d'audit de la PKI et du SML ;
- des audits d'architecture ;
- des tests d'intrusion ;
- des audits de code ;
- des analyses de risques ;
- des plans de réponse aux incidents ;
- des plans de continuité et de reprise d'activité ;
- des audits portant sur les sous-traitants ;
- de la liste des vulnérabilités critiques identifiées au cours des cinq dernières années ;
- de la liste des incidents ayant affecté la disponibilité, l'intégrité ou la confidentialité du réseau.

Les éléments strictement sensibles pourront, le cas échéant, être communiqués dans le cadre d'un dispositif de confidentialité approprié. Le secret de la sécurité ne saurait néanmoins justifier une absence totale de preuve de l'existence et du sérieux des audits.

6. Protection des données

Vous indiquerez :

- la qualification d'OpenPeppol au regard du RGPD pour chacun des traitements concernés ;
- les catégories exactes de données et métadonnées traitées ;
- les finalités de chaque traitement ;
- les durées de conservation ;
- la localisation des traitements et sauvegardes ;
- l'identité des responsables du traitement, responsables conjoints et sous-traitants ;
- l'existence d'une analyse d'impact relative à la protection des données ;
- les mesures de protection dès la conception et par défaut ;
- les éventuels transferts hors de l'Espace économique européen ;
- les procédures d'exercice des droits ;
- l'identité et les coordonnées du délégué à la protection des données compétent pour les activités du réseau.

7. Secret des affaires et secrets professionnels

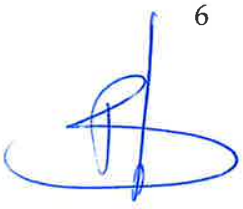
Vous préciserez les mesures permettant :

- d'empêcher l'accès aux factures ou métadonnées par OpenPeppol et ses sous-traitants lorsque cet accès n'est pas strictement nécessaire ;
- de cloisonner les informations ;
- de prévenir toute réutilisation statistique ou commerciale ;
- d'assurer la traçabilité des accès ;
- de protéger les professions soumises à un secret professionnel ;
- de traiter les demandes provenant d'autorités publiques ;
- d'informer les personnes et entreprises concernées en cas d'accès ou de divulgation.

8. Responsabilité et assurance

Vous communiquerez :

- le régime contractuel de responsabilité applicable à OpenPeppol ;
- les éventuelles clauses limitatives ou exonératoires ;
- les plafonds d'indemnisation ;
- les polices d'assurance souscrites ;



- les montants garantis ;
- la procédure d'indemnisation des entreprises victimes ;
- le droit applicable et les juridictions compétentes ;
- les mécanismes de règlement indépendant des différends.

9. Cadre européen de cybersécurité

Vous indiquerez si OpenPeppol considère relever, directement ou indirectement, du champ d'application de la directive NIS 2 ou de ses mesures nationales de transposition, notamment au titre de ses activités d'infrastructure numérique, de service géré, de gestion de certificats ou de service essentiel au maintien d'activités économiques critiques.

Dans la négative, vous exposerez les motifs juridiques et techniques de cette position.

10. Continuité et réversibilité

Vous communiquerez le dispositif prévu en cas :

- de dissolution ou d'insolvabilité d'OpenPeppol ;
- de défaillance prolongée du SML ;
- de compromission de l'autorité de certification ;
- de révocation massive de certificats ;
- de rupture avec un sous-traitant critique ;
- de retrait d'un État du réseau ;
- de contestation judiciaire de l'accord conclu avec une autorité nationale ;
- de nécessité pour la France de reprendre souverainement l'exploitation des composants indispensables.

V. Mise en demeure de cessation et de suspension

Dans l'attente de la communication complète de ces éléments et de la levée des incertitudes exposées, je vous mets en demeure :

À titre principal

1. de **cesser immédiatement de vous présenter, directement ou indirectement, comme Autorité Peppol pour la France**, si cette fonction a effectivement été transférée à la DGFiP ;
2. de cesser d'adopter, modifier, approuver ou imposer des exigences particulières à la France sur le fondement d'une qualité d'Autorité Peppol nationale qui ne serait plus la vôtre ;
3. de cesser toute décision d'accréditation, de suspension, de non-conformité ou de révocation concernant un prestataire relevant de la juridiction française, lorsqu'une telle décision ne repose pas sur une compétence clairement identifiée et démontrée ;
4. de cesser toute communication susceptible de laisser croire qu'OpenPeppol constituerait une institution publique européenne ou disposerait, par elle-même, d'un pouvoir réglementaire à l'égard des entreprises françaises ;
5. de rectifier immédiatement les documents publics contradictoires relatifs à l'identité de l'Autorité Peppol France.

À titre subsidiaire

Dans l'hypothèse où vous soutiendriez conserver certaines compétences concernant la France, je vous mets en demeure de **suspendre tout nouvel acte normatif ou discrétionnaire affectant la France**, notamment toute modification des PASR, toute nouvelle exigence obligatoire et toute mesure de suspension ou de révocation non urgente, jusqu'à ce que :

- le fondement juridique de cette compétence ait été publiquement établi ;
- la répartition des responsabilités avec la DGFiP ait été clarifiée ;
- un audit indépendant ait été produit ;
- les garanties de sécurité, de responsabilité et de continuité aient été rendues vérifiables.

Cette demande de suspension ne concerne pas les opérations techniques strictement nécessaires pour éviter une interruption immédiate des échanges déjà en cours, sous réserve qu'elles soient licites, nécessaires, proportionnées et entièrement traçables.

VI. Demande d'expertise indépendante

Je vous demande également de proposer, dans le même délai, les modalités d'une expertise technique et juridique indépendante portant notamment sur :

- l'architecture PKI ;
- le SML ;
- la gouvernance des certificats ;
- la résistance aux compromissions ;
- la séparation des responsabilités ;
- la protection des données et métadonnées ;
- la protection des secrets d'affaires ;
- la continuité du réseau ;
- la réversibilité ;
- les mécanismes de contrôle et de recours.

L'expert devra être indépendant d'OpenPeppol, de la DGFiP, des plateformes agréées et des prestataires ayant participé à la conception du dispositif.

VII. Mise en demeure de préserver les éléments de preuve

Vous êtes formellement mis en demeure de préserver, sans suppression ni altération :

- les courriels et échanges intervenus avec la DGFiP et les autorités françaises ;
- les versions successives des accords et PASR ;
- les procès-verbaux et enregistrements des réunions ;
- les déclarations d'intérêts ;
- les rapports d'audit ;
- les journaux de sécurité ;
- les décisions de délivrance ou de révocation de certificats ;
- les historiques de modification des documents ;
- les dossiers relatifs aux incidents ;
- les contrats conclus avec les sous-traitants ;
- les documents relatifs à la transition entre OpenPeppol et la DGFiP.

Cette obligation de préservation s'étend aux documents détenus par vos dirigeants, salariés, prestataires, hébergeurs et conseils.

VIII. Conséquences d'une absence de réponse satisfaisante

À défaut de réponse complète, documentée et vérifiable dans le délai imparti, toutes procédures utiles seront envisagées, notamment :

- saisine de la DGFiP et des autorités françaises compétentes ;

- saisine de l'autorité belge de protection des données et, selon les traitements concernés, de la CNIL ;
- saisine des autorités nationales chargées de la cybersécurité ;
- signalement aux institutions européennes compétentes ;
- demande judiciaire de communication forcée de documents ;
- demande de désignation d'un expert indépendant ;
- demande de suspension ou d'interdiction des actes insuffisamment justifiés ;
- action en responsabilité en cas de préjudice ;
- publication des contradictions et insuffisances documentaires constatées, dans le respect des règles applicables.

La présente est adressée sans renonciation à aucun droit, moyen, action ou demande indemnitaire.

Copie de la présente lettre est adressée à la DGFiP en sa qualité d'adhèrent de votre structure, ainsi qu'à la Commission Européenne.

Je vous demande de confirmer la bonne réception de cette mise en demeure dans un délai de quarante-huit heures et de désigner la personne chargée d'y répondre.

Je vous prie d'agréer, Madame, Monsieur, l'expression de ma considération distinguée.

REACTION 19

Le Président

Carlo Alberto BRUSA

Association Loi 1901

N°. P. W751256495