A. Commentaires sur le Modèle d'accord entre autorités compétentes

Introduction

1. Le Modèle AAC associe la NCD et la base juridique (comme la Convention concernant l'assistance administrative mutuelle en matière fiscale ou une convention fiscale bilatérale) qui permet l'échange d'informations relatives aux comptes financiers. Le Modèle AAC se compose d'un préambule et de sept sections, et définit les conditions à réunir pour assurer une communication efficace d'informations. Le préambule inclut les règles nationales en matière de déclaration et de diligence raisonnable qui sous-tendent l'échange de renseignements en vertu du Modèle AAC. Il énonce également des principes relatifs à la confidentialité, aux protections et à l'existence des infrastructures nécessaires à un échange efficace.

2. Le Modèle AAC contient une section de définitions (section 1), détermine le type de renseignements à échanger (section 2), la durée et les modalités des échanges (section 3), la collaboration en matière d'application et d'exécution (section 4), ainsi que les règles de confidentialité et de protection des données qui doivent être respectées (section 5). Les sections 4, 6 et 7 portent sur les consultations entre autorités compétentes, les modifications et la durée de l'accord, y compris sa suspension et sa résiliation.

3. Le Modèle AAC est conçu comme un accord bilatéral réciproque basé sur le principe selon lequel l'échange automatique est réciproque et qu'il sera effectué sur une base bilatérale. Pour réduire les coûts induits par la signature de nombreux accords entre autorités compétentes, l'échange de renseignements peut aussi être mis en œuvre sur la base d'un accord/arrangement multilatéral. L'Annexe 1 contient une version multilatérale du Modèle AAC. Bien que l'accord soit multilatéral, les renseignements seraient échangés sur une base bilatérale. Il se peut également que, dans certains cas, des juridictions souhaitent conclure un accord bilatéral non réciproque entre autorités compétentes (lorsque par exemple une juridiction ne prélève pas

d'impôt sur le revenu). L'Annexe 2 contient une version non réciproque du Modèle AAC. Certains observateurs, dont des pays du G20 et d'autres, ont souligné le fait que les pays en développement peuvent se trouver confrontés à des contraintes spécifiques de capacités en ce qui concerne l'échange automatique de renseignements, et que c'est un aspect important à prendre en considération ; en juillet 2013, le G20 a demandé au Forum mondial sur la transparence et l'échange de renseignements à des fins fiscales de coopérer avec le Groupe de travail de l'OCDE sur la fiscalité et le développement, la Banque mondiale et d'autres acteurs en vue d'aider les pays en développement à cerner leurs besoins en matière d'assistance technique et de renforcement des capacités.

4. Des juridictions peuvent aussi conclure un accord intergouvernemental multilatéral ou plusieurs accords intergouvernementaux qui seraient des traités internationaux à part entière ou une législation régionale couvrant à la fois les obligations déclaratives et les procédures de diligence raisonnable, conjugués à un accord entre autorités compétentes de portée plus limitée.

Commentaires sur le préambule

1. Le préambule (« considérants ») définit le contexte et contient des déclarations, notamment une phrase qui fait référence à la base juridique sous-jacente qui autorise l'échange automatique de renseignements.

2. Le premier paragraphe est une introduction et peut être adapté aux circonstances propres aux juridictions qui concluent l'Accord.

3. Au deuxième paragraphe, les autorités compétentes déclarent que les lois de leurs juridictions respectives imposent ou sont censées imposer aux institutions financières de communiquer des informations concernant certains comptes, conformément à la portée des échanges définie à la section 2 du présent Accord.

4. Les différentes possibilités prévues dans ce paragraphe permettent aux juridictions qui le souhaitent de conclure l'accord entre autorités compétentes avant même que l'une des parties, ou les deux, aient mis en place des règles de déclaration et de diligence raisonnable pertinentes. Voir également la section 3, troisième paragraphe (paragraphe 3 des Commentaires sur la section 3) et la section 7 (paragraphe 1 des Commentaires sur la section 7).

5. Le troisième paragraphe définit la base juridique qui autorise l'échange automatique de renseignements sur les comptes financiers et qui autorise les autorités compétentes à définir la portée et les modalités de ces échanges automatiques. La portée ainsi définie doit être cohérente avec celle de l'échange visée par la section 2 du présent Accord. D'autres instruments juridiques (différents des conventions relatives à l'impôt sur le revenu ou de la Convention concernant l'assistance administrative mutuelle en matière fiscale) qui autorisent l'échange automatique de renseignements en matière fiscale peuvent inclure certains accords d'échange de renseignements fiscaux ou des accords régionaux de coopération fiscale. À l'échelle régionale, l'échange automatique de renseignements peut aussi être mis en œuvre sur la base d'une législation européenne ou d'une législation de la Communauté andine, par exemple, qui couvrirait les éléments du Modèle AAC et de la NCD.

6. Le quatrième paragraphe contient des déclarations selon lesquelles les autorités compétentes ont mis en place *(i)* les protections adéquates pour faire en sorte que les renseignements reçus restent confidentiels, et *(ii)* les infrastructures nécessaires à un échange efficace. Les Commentaires relatifs à la section 5 du Modèle AAC donnent des précisions supplémentaires.

Commentaires sur la section 1 concernant les définitions

Paragraphe 1 – Définitions

1. Le paragraphe 1 contient les définitions des termes qui sont propres à l'Accord. Les définitions de tous les autres termes utilisés dans l'Accord figurent dans la section VIII de la Norme commune de déclaration.

2. Les alinéas 1(a) et (b) définissent les juridictions qui concluent l'Accord. Les autorités compétentes sont libres de s'accorder sur les définitions des termes « [Juridiction A] » et « [Juridiction B] », mais ces définitions doivent être cohérentes avec celles qui figurent dans l'instrument juridique sous-jacent. En outre, les autorités compétentes sont libres de convenir d'inclure une description géographique (notamment une référence au plateau continental) ; toutefois, seule une définition politique est nécessaire, dont voici un exemple : « Mexique signifie les États-Unis du Mexique ».

3. La définition du terme « Autorité compétente » figurant à l'alinéa 1(c) vise à décrire les autorités compétentes aux fins de l'Accord. Elle permet à chaque juridiction de désigner une ou plusieurs autorités compétentes. Toutefois, cette définition doit être cohérente avec celle qui figure dans l'instrument juridique sous-jacent.

4. Les termes contenus aux alinéas 1(d) à (k) alignent la portée de l'échange de renseignements entre les juridictions qui concluent l'Accord sur celle de la Norme commune de déclaration. Ces termes désignent :

- les institutions financières tenues de déclarer : « Institution financière de la [Juridiction A] », « Institution financière de la [Juridiction B] », et « Institution financière déclarante », conformément aux expressions « Institution financière déclarante » et « Institution financière d'une Juridiction partenaire » figurant aux alinéas A(1) et (2) de la section VIII de la Norme commune de déclaration (voir les paragraphes 2-6 des Commentaires sur la section VIII) ;
- les comptes financiers soumis à déclaration : « Compte déclarable », « Compte déclarable de la [Juridiction A] », et « Compte déclarable

de la [Juridiction B] », conformément à l'expression « Compte déclarable » figurant à l'alinéa D(1) de la section VIII de la Norme commune de déclaration (voir le paragraphe 105 des Commentaires sur la section VIII) ; et

- les Titulaires de compte soumis à déclaration : « Personne de la [Juridiction A] » et « Personne de la [Juridiction B] », conformément aux expressions « Personne devant faire l'objet d'une déclaration » et « Personne d'une Juridiction soumise à déclaration » figurant aux alinéas D(2) et (3) de la section VIII de la Norme commune de déclaration (voir les paragraphes 106-116 des Commentaires sur la section VIII).

5. L'alinéa 1(l) contient la définition du terme « NIF », qui est également un terme défini à l'alinéa E(5) de la section VIII de la Norme commune de déclaration. Dans la Norme, cette définition précise qu'un NIF est un numéro d'identification fiscale ou, à défaut, un équivalent fonctionnel (voir les paragraphes 146-149 des Commentaires sur la section VIII), tandis que dans le Modèle AAC, elle désigne les NIF des juridictions qui concluent l'accord. Les expressions « NIF de la [Juridiction A] » et « NIF de la [Juridiction B] » contenus aux alinéas 1(m) et (n) poursuivent le même objectif.

6. L'expression « Norme commune de déclaration » n'est pas définie dans le Modèle AAC, mais est définie dans la version multilatérale de ce Modèle. Il est possible que la Norme commune de déclaration, y compris les modalités informatiques, soit périodiquement mise à jour à mesure que de nouvelles juridictions l'appliqueront et acquerront une expérience correspondante. Dans le contexte d'un accord multilatéral, les autorités compétentes peuvent apposer leur signature à des dates différentes et, de ce fait, la Norme commune de déclaration peut avoir été mise à jour dans l'intervalle. Pour remédier à cette situation, la version multilatérale définit la Norme commune de déclaration en ces termes : « la norme d'échange automatique de renseignements sur les comptes financiers élaborée par l'OCDE aux côtés des pays du G20, présentée aux dirigeants du G20 en 2014 et publiée sur le site Internet de l'OCDE ». En outre, pour indiquer clairement que toutes les juridictions seraient tenues d'appliquer la version la plus récente de la Norme, le troisième considérant dispose que « la législation des Juridictions sera périodiquement modifiée afin de tenir compte des mises à jour de la Norme commune de déclaration, et qu'une fois ces modifications promulguées par une Juridiction, la définition de la "Norme commune de déclaration" sera réputée faire référence à la version mise à jour pour cette Juridiction ». Dans le cadre d'un accord bilatéral, cette question ne se pose pas car les autorités compétentes le signent généralement le même jour. Toutefois, même dans un accord bilatéral, les autorités compétentes peuvent souhaiter prévoir expressément des mises à jour de la Norme commune de déclaration selon des modalités identiques à celles figurant dans la version

multilatérale (définir l'expression « Norme commune de déclaration » et ajouter un considérant stipulant que les juridictions modifieront leur législation pour tenir compte des mises à jour de la Norme).

Paragraphe 2 – Règle générale d'interprétation

7. Le paragraphe 2 définit la règle générale d'interprétation. La première phrase du paragraphe 2 précise que tout terme en majuscule utilisé dans le Modèle AAC mais qui n'y est pas défini aura le sens que lui attribue la Norme commune de déclaration. Cette disposition reflète le fait, également exprimé dans le préambule, que les juridictions ont mis en place des procédures de déclaration et de diligence raisonnable (y compris des définitions correspondantes) conformes à la Norme commune de déclaration.

8. La deuxième phrase du paragraphe 2 dispose que, sauf si le contexte exige une interprétation différente ou si les Autorités compétentes s'entendent sur une signification commune, tout terme qui n'est pas défini dans le présent Accord ou dans la Norme commune de déclaration aura le sens que lui attribue au moment considéré la législation de la juridiction qui applique l'Accord. À cet égard, toute définition figurant dans la législation fiscale applicable de cette juridiction l'emportera sur une définition contenue dans une autre législation de la même juridiction. En outre, lorsqu'elles examinent le contexte, les autorités compétentes doivent tenir compte des Commentaires sur la Norme commune de déclaration et des termes qui y sont définis.

Commentaires sur la section 2 concernant l'échange de renseignements relatifs aux comptes déclarables

1. Cette section dispose que les renseignements qui doivent être échangés sont ceux visés par les règles de déclaration et de diligence raisonnable applicables en vertu de la Norme commune de déclaration. Voir la section I (Obligations déclaratives générales) de la NCD et les Commentaires correspondants.

2. Le premier paragraphe fait référence à la base juridique sur laquelle se fonde l'échange et indique que les renseignements seront échangés sur une base annuelle. Ils peuvent aussi l'être plus fréquemment ; lorsque par exemple une Autorité compétente reçoit des données corrigées d'une Institution financière déclarante, ces informations sont généralement adressées à l'autre Autorité compétente le plus rapidement possible. Les renseignements à échanger sont ceux obtenus en vertu de la NCD et sont précisés plus avant au paragraphe 2.

3. Le paragraphe 1 précise que l'échange de renseignements est soumis aux règles de déclaration et de diligence raisonnable applicables en vertu de la NCD. Ainsi, lorsque par exemple ces règles n'exigent pas la communication d'un NIF relatif à un Compte déclarable en particulier, l'échange de ce renseignement n'est pas obligatoire. Voir les exceptions prévues aux paragraphes C à F de la section I de la NCD et les paragraphes 25 à 35 des Commentaires sur la section I.

4. L'alinéa 2(d) de la section 2 précise qu'une juridiction est tenue de communiquer le solde ou la valeur portée sur le compte à la fin de l'année civile considérée ou d'une autre période de référence adéquate. Toutefois, le paragraphe 11 des Commentaires sur la section I de la NCD dispose que les juridictions peuvent, à défaut, demander aux Institutions financières de communiquer le solde moyen ou la valeur moyenne portée sur le compte au cours de l'année civile considérée ou d'une autre période de référence adéquate. Si une juridiction opte pour cette formule plutôt que pour le solde en fin d'année, l'Accord doit le mentionner, en indiquant les règles à suivre pour calculer le solde moyen ou la valeur moyenne portée en compte, pour que l'on sache clairement sur quoi porte l'échange.

Commentaires sur la section 3 concernant le calendrier et les modalités des échanges de renseignements

Paragraphes 1 et 2 – Montant, qualification et monnaie des paiements

1. Le paragraphe 1 dispose qu'aux fins de l'échange de renseignements prévu à la section 2, le montant et la qualification des versements effectués au titre d'un Compte déclarable peuvent être déterminés conformément aux principes de la législation fiscale de la juridiction qui communique l'information. Le paragraphe 2 dispose que les renseignements échangés indiquent la monnaie dans laquelle chaque montant concerné est libellé.

Paragraphes 3 et 4 – Délai pour l'échange de renseignements

2. Le paragraphe 3 dispose que les renseignements doivent être échangés dans les neuf mois qui suivent la fin de l'année civile à laquelle ils se rapportent. La première année concernée par l'échange de renseignements est laissée en blanc et doit être renseignée par les juridictions. Le délai de neuf mois envisagé au paragraphe 3 est une norme minimale et les juridictions sont libres de fixer des délais plus courts. Par exemple, les États membres de l'UE sont soumis à un délai de 6 mois en vertu de la Directive de l'UE sur l'épargne.

3. Le paragraphe 3 ajoute que nonobstant l'année choisie par les Autorités compétentes pour le premier échange de renseignements, l'obligation d'échanger les renseignements pour une année civile s'applique uniquement si les deux juridictions sont dotées d'une législation qui prévoit la communication d'informations pour cette année civile conforme à la portée de l'échange définie à la section 2 et dans la Norme commune de déclaration. Cette phrase sera sans effet si, au moment de la signature de l'Accord, les deux juridictions disposent d'une législation interne conforme à la Norme commune de déclaration. Si ce n'est pas le cas pour l'une des juridictions ou pour les deux, cette phrase a pour objet de préciser qu'une fois l'Accord en vigueur, si l'une des juridictions applique la Norme commune de déclaration depuis plus longtemps que l'autre, les seuls renseignements qui doivent être échangés sont ceux qui se rapportent

aux années durant lesquelles les obligations déclaratives correspondantes étaient en vigueur dans les deux juridictions. Toutefois, une juridiction peut choisir, dans la mesure où sa législation interne le permet, d'échanger des renseignements se rapportant aux années antérieures, ce qui est également conforme à la NCD et au Modèle AAC.

4. L'exemple suivant illustre la logique du paragraphe 3 ; dans cet exemple, une juridiction n'est pas dotée de la législation exigeant la communication de renseignements pour l'année civile convenue à la première phrase du paragraphe 3. Les juridictions A et B signent le Modèle AAC le 30 avril 2015 et conviennent d'échanger des renseignements se rapportant à l'année 2016 et aux années suivantes. La juridiction A fait savoir, le 7 juin 2015, que sa législation exige désormais la communication de renseignements se rapportant à l'année 2016. Le 1er novembre 2015, la juridiction B fait savoir qu'elle s'est dotée d'une législation exigeant la communication de renseignements se rapportant à l'année 2017. En pareil cas, la dernière phrase du paragraphe 3 aura pour effet que la juridiction A n'est pas tenue d'échanger des renseignements se rapportant à l'année 2016. Les deux juridictions A et B devront échanger des renseignements portant sur l'année 2017. Toutefois, la juridiction A peut choisir, dans la mesure où son droit interne le permet, de communiquer des renseignements à la juridiction B portant sur l'année 2016, même si la juridiction A ne recevra pas de renseignements pour cette même année.

5. Le paragraphe 4 contient une exception concernant l'année au titre de laquelle les produits bruts doivent être déclarés. Il peut être plus difficile pour des Institutions financières déclarantes de mettre en œuvre les procédures permettant de calculer le produit brut total de la vente ou du rachat d'un bien. Aussi, lorsqu'elles appliquent la Norme commune de déclaration, les juridictions peuvent décider d'introduire progressivement la déclaration de ces produits bruts. Si aucune période de transition n'est prévue, le paragraphe 4 ne sera pas nécessaire. Si une transition est prévue par l'une des juridictions, le paragraphe 4, qui dispose que nonobstant le paragraphe 3, les renseignements à échanger pour l'année indiquée dans le paragraphe 3 sont ceux décrits au paragraphe 2 de la section 2, à l'exception des produits bruts décrits à l'alinéa 2(e)(2) de la section 2, doit être inséré. En pareil cas, les juridictions doivent préciser l'année au titre de laquelle les produits bruts doivent être déclarés.

6. Aucune disposition de l'Accord n'empêche l'application des dispositions des sections 2 et 3 au titre des renseignements obtenus avant la date d'entrée en vigueur de l'Accord, dès lors que ces renseignements sont communiqués après l'entrée en vigueur de l'Accord et des dispositions des sections 2 et 3. Néanmoins, les Autorités compétentes peuvent juger utile de préciser dans quelle mesure les dispositions des sections 2 et 3 s'appliquent à ces renseignements.

Paragraphes 5 et 6 – Modalités relatives aux technologies de l'information

Schéma de la NCD et guide de l'utilisateur

7. Le paragraphe 5 dispose que les Autorités compétentes échangeront automatiquement les informations décrites à la section 2 selon un schéma de norme commune de déclaration et en langage XML. Le Guide de l'utilisateur de la NCD, dont une copie figure à l'Annexe 3, contient des indications sur le schéma en question et sur son utilisation.

Transmission de données et cryptage

8. Le paragraphe 6 dispose que les Autorités compétentes s'accorderont sur une ou plusieurs méthodes de transmission de données, y compris sur des normes de cryptage.

Normes minimales appropriées

9. Toute méthode de transmission doit obéir à un certain nombre de normes minimales afin que la confidentialité et l'intégrité des données soient assurées tout au long de la transmission. Par confidentialité, on entend que les données ou les informations ne doivent pas être accessibles à des personnes non autorisées ou leur être communiquées. Par intégrité, on entend que les données ou les informations ne doivent pas être modifiées ou altérées de manière non autorisée. Ces normes doivent être susceptibles d'adaptation aux évolutions des capacités techniques au fil du temps. Elles doivent prévoir l'utilisation de canaux de transmission et de protocoles sécurisés capables d'assurer la confidentialité et l'intégrité des données, au moyen d'un cryptage ou de mesures physiques, ou d'une combinaison des deux.

10. Le Modèle AAC n'impose pas une solution unique pour la transmission ou pour le cryptage des données, car pour les Autorités compétentes cela risquerait de compliquer l'alignement avec des pratiques ou des systèmes éprouvés ou susceptibles de convenir pour une situation spécifique. Comme la responsabilité des données continue d'incomber à la juridiction expéditrice jusqu'à ce qu'elles parviennent à la juridiction destinataire, il se peut également que, selon les impératifs nationaux, des processus différents soient approuvés pour les deux parties d'un échange bilatéral (expéditrice et destinataire). Par exemple, la juridiction A peut utiliser une transmission via un navigateur alors que la juridiction B utilise un serveur avec acheminement via un réseau sécurisé pour l'échange de données. Toutefois, comme chaque juridiction va, en principe, créer des relations d'échange automatique à la norme NCD avec plusieurs autres juridictions, il faudra penser à concevoir une architecture internationale de transmission viable, qui évite autant que possible que chaque juridiction ait à

adopter et faire évoluer une multitude de méthodes de transmission et/ou de cryptage.

Cryptage

11. Le cryptage a pour but de protéger la confidentialité et l'intégrité des données. Il consiste à transformer les données afin qu'elles soient inintelligibles à quiconque ne possède pas la clé de décryptage. Tous les fichiers de données à échanger doivent donc être cryptés avec un niveau de sécurité minimum, l'itinéraire de transmission doit être soit crypté, soit sécurisé physiquement, et des contrôles d'audit doivent être en place pour garder trace des accès et les copies de fichiers. Une méthode de chiffrement très utilisée pour échanger des informations est la cryptographie asymétrique, avec une clé publique et une clé privée. La cryptographie à clé publique est pratiquée depuis plusieurs décennies et permet aux parties d'échanger des données cryptées sans qu'il faille communiquer de clé secrète à l'avance. L'expéditeur crypte le fichier de données à l'aide d'une clé publique, et seul le destinataire possède la clé privée sécurisée nécessaire pour le décrypter. Il existe des normes internationales régissant la longueur de la clé de chiffrement utilisée pour assurer le niveau de sécurité approprié pour des données financières personnelles, tant actuellement que pour un avenir prévisible, comme par exemple la norme *advanced encryption standard* (AES 256).

Méthodes de transmission électroniques

12. Il était naguère d'usage d'envoyer des fichiers de données cryptés sur des disquettes, des cartes mémoire ou des disques compacts, avec remise en main propre ou par courrier recommandé entre Autorités compétentes, mais le transfert de ces supports physiques entraîne un traitement administratif et un risque supplémentaire (même si l'intégrité et la confidentialité sont assurées grâce au cryptage). Aujourd'hui, la technologie permet tout aussi simplement de transférer des données à l'aide d'un navigateur Internet qui peut également, à peu de frais, assurer des fonctions de cryptage, de non-révocation et de non-répudiation. Par conséquent, l'utilisation d'un support physique ne passe plus pour une bonne pratique. La bonne pratique aujourd'hui est d'utiliser une méthode permettant un transfert intégré de bout en bout pour la transmission de fichiers électroniques, soit de serveur à serveur, soit avec accès via un navigateur[1]. Un système sécurisé de courrier

1. Les services web avec ws-security constituent une autre famille de normes abordables et de plus en plus employées dans des environnements sécurisés, composées d'un ensemble de services utilisant le protocole HTTP au moyen de méthodes standard de type GET et POST. Comme exemples de protocoles de transmission reconnus internationalement comme répondant aux exigences de

électronique, avec des normes et spécifications minimales, peut aussi être utilisé, mais les coûts d'installation peuvent être plus lourds, et il peut entraîner une plus grande complexité d'utilisation pour la gestion des accès utilisateurs et la sécurité des données, imposer une taille limite des fichiers et entrer en conflit avec les systèmes pare-feu. Il importe de ne pas négliger l'évaluation et la réévaluation constante du risque.

Dimension opérationnelle de la sécurité

13. À côté des mesures techniques reposant sur le matériel et les outils logiciels, la confidentialité et la sécurité des données transmises nécessitent également l'application de bonnes pratiques managériales, organisationnelles et opérationnelles. Le respect d'une norme particulière n'est pas impératif, mais idéalement la sécurité doit être gérée en conformité avec des normes de bonnes pratiques reconnues telles que la série des normes ISO 27000 sur la sécurité de l'information, en tenant compte des modifications qui interviennent périodiquement. En l'espèce, les données ne doivent être accessibles qu'à des personnes autorisées tout au long du processus de transmission, et l'accès aux clés de cryptage – en particulier la clé privée – doit être étroitement contrôlé. Un journal d'audit doit garder trace de tout accès autorisé aux données ou aux clés. On trouvera des informations complémentaires sur la sauvegarde des données et la confidentialité dans les Commentaires sur la section 5.

canaux de transmission sécurisés et de protocoles garants de la confidentialité et de l'intégrité des données, on peut citer la Transport Layer Security (TLS) v 1.1 pour la sécurisation des échanges sur serveurs, et le Secure File Transfer Protocol (SFTP) pour les transferts en bloc programmés, mais ce ne sont pas les seuls protocoles susceptibles d'offrir des solutions adéquates.

Commentaires sur la section 4 concernant la collaboration en matière d'application et de mise en œuvre de l'Accord

1. Cette section concerne la collaboration entre Autorités compétentes en matière d'application et de mise en œuvre de l'Accord. Elle dispose que si une Autorité compétente a des raisons de croire qu'une erreur peut avoir eu pour conséquence la communication de renseignements erronés ou incomplets ou qu'une Institution financière déclarante ne respecte pas les obligations déclaratives en vigueur, elle doit transmettre une notification à l'autre Autorité compétente. L'Autorité compétente ainsi notifiée appliquera toutes les dispositions appropriées de son droit interne pour corriger ces erreurs ou remédier aux manquements décrits dans la notification. Voir les Commentaires sur la Section IX de la Norme commune de déclaration concernant les règles et procédures administratives que les juridictions doivent mettre en place pour garantir une mise en œuvre effective de la NCD.

2. La notification doit se faire par écrit et doit indiquer clairement l'erreur ou le manquement en cause, ainsi que les raisons pour lesquelles l'Autorité compétente pense qu'ils se sont produits. L'Autorité compétente notifiée doit répondre ou réagir le plus rapidement possible, au plus tard 90 jours civils après avoir été avisée par l'Autre autorité compétente. Si le problème n'est pas résolu, l'Autorité compétente doit tenir l'autre autorité compétente informée tous les 90 jours. Si toutefois, après avoir examiné la notification en toute bonne foi, l'Autorité compétente notifiée ne reconnaît pas l'existence de l'erreur ou du manquement qui y est décrit, elle doit en aviser par écrit l'autre autorité compétente le plus rapidement possible et préciser ses raisons.

3. La section 4 ne prévoit pas de contact direct entre l'Autorité compétente d'une juridiction et une Institution financière déclarante de l'autre juridiction. Deux Autorités compétentes peuvent aussi souhaiter autoriser les contacts directs entre une Autorité compétente d'une juridiction et une Institution financière déclarante de l'autre juridiction en cas d'erreurs administratives ou d'autres erreurs minimes. La décision en ce sens dépendra du droit interne des juridictions concernées, mais éventuellement aussi du nombre de demandes qu'une Autorité compétente s'attend à recevoir. Si les

Autorités compétentes conviennent d'une telle approche, le contenu actuel de la section 4 doit être remplacé par le texte suivant :

1. Une Autorité compétente peut adresser une demande directement à une Institution financière déclarante de l'autre juridiction si elle a des raisons de croire que des erreurs administratives ou d'autres erreurs minimes peuvent avoir eu pour conséquence la communication de renseignements erronés ou incomplets. L'Autorité compétente avise l'Autorité compétente de l'autre partie lorsque la première Autorité adresse une telle demande à une Institution financière déclarante de l'autre juridiction.

2. Une Autorité compétente avise l'Autorité compétente de l'autre partie lorsque la première Autorité a des raisons de croire qu'une Institution financière déclarante ne respecte pas les obligations déclaratives en vigueur et les procédures de diligence raisonnable au titre de la Norme commune de déclaration. L'Autorité compétente ainsi notifiée applique toutes les dispositions appropriées de son droit interne pour remédier aux manquements décrits dans la notification.

4. C'est le droit interne de la juridiction de l'Institution financière déclarante, y compris les dispositions relatives à la protection des données personnelles, qui s'applique à de tels contacts directs.

Commentaires sur la section 5 concernant la confidentialité et la protection des données

1. La confidentialité des renseignements sur les contribuables a toujours été la pierre angulaire des systèmes fiscaux. Les contribuables comme les administrations fiscales ont le droit juridiquement reconnu de s'attendre à ce que les données échangées demeurent confidentielles. Pour qu'ils aient confiance en leurs systèmes fiscaux et respectent la loi, les contribuables doivent avoir l'assurance que les informations financières les concernant, souvent de nature sensible, ne seront pas divulguées de façon inopportune, ni intentionnellement ni par accident. Les citoyens et les États n'auront confiance dans l'échange international de renseignements que si les données sont utilisées et divulguées exclusivement selon les termes de l'accord sur lequel se fonde cet échange. Il est nécessaire pour cela de disposer d'un cadre juridique et de systèmes et procédures qui garantissent son respect dans la pratique et empêchent toute divulgation non autorisée. La capacité de protéger la confidentialité des renseignements fiscaux est également le fruit d'une « culture de l'attention » au sein de l'administration fiscale, qui englobe l'ensemble des systèmes, procédures et processus propres à garantir que le cadre juridique est respecté en pratique et que la sécurité et l'intégrité des informations sont assurées lorsque celles-ci sont traitées. À mesure que l'administration fiscale gagne en complexité, les processus et pratiques nécessaires à la confidentialité doivent évoluer pour que les renseignements échangés restent confidentiels[2]. Plusieurs juridictions sont dotées de règles spécifiques en matière de protection des données personnelles qui s'appliquent aussi aux renseignements sur les contribuables.

2. La section 5, la section 7 et le quatrième paragraphe du préambule reconnaissent expressément l'importance de la confidentialité et de la protection des données en lien avec l'échange automatique de renseignements sur les comptes financiers. La partie restante de ces Commentaires passe succinctement en revue les paragraphes 1 et 2 avant d'étudier en détail les modalités de protection de la confidentialité et des données en lien avec la Norme commune de déclaration.

2. OCDE (2012), *Garantir la confidentialité* OCDE, Paris, disponible sur www.oecd.org/fr/ctp/echange-de-renseignements-fiscaux/rapport-garantir-la-confidentialite.pdf.

Paragraphe 1 – Confidentialité et protection des données personnelles

3. Tous les renseignements échangés sont soumis aux règles de confidentialité et aux autres protections prévues par l'instrument juridique applicable, y compris en ce qui concerne l'usage qui peut être fait de ces renseignements et les personnes qui peuvent en être destinataires.

4. De nombreuses juridictions ont mis en place des règles spécifiques sur la protection des données personnelles qui s'appliquent aux renseignements sur les contribuables. Par exemple, des règles spéciales relatives à la protection des données s'appliquent aux informations échangées par les États membres de l'UE (que le destinataire soit un autre État membre de l'UE ou un pays tiers). Ces règles incluent notamment le droit d'information, d'accès, de correction et de recours de la personne concernée par l'échange de données, et l'existence d'un mécanisme de surveillance destiné à protéger les droits de cette personne. Le paragraphe 1 de la section 5 dispose que l'Autorité compétente qui communique les renseignements peut, dans la mesure où cela est nécessaire pour garantir le degré requis de protection des données personnelles, indiquer dans l'Accord entre autorités compétentes les dispositions particulières qui doivent être exigées, en vertu de son droit interne. L'Autorité compétente qui reçoit les renseignements doit veiller à la mise en œuvre et au respect des protections éventuellement spécifiées. Elle doit traiter ces renseignements conformément à son droit interne, mais également dans le respect des dispositions supplémentaires qui peuvent être exigées pour protéger les données en vertu du droit interne de l'Autorité compétente qui transfert l'information. Ces dispositions supplémentaires, telles que définies par l'Autorité compétente qui communique les renseignements, peuvent se référer à l'accès individuel aux données. L'Autorité compétente qui communique les renseignements ne spécifiera pas nécessairement des dispositions de protection particulières si elle a l'assurance que l'Autorité compétente destinataire garantit le niveau requis de protection des données communiquées. En tout état de cause, ces dispositions ne doivent pas aller au-delà de ce qui est nécessaire pour assurer la protection des données personnelles et ne doivent pas empêcher ou retarder indûment l'échange effectif de renseignements.

5. En règle générale, les instruments relatifs à l'échange de renseignements disposent que la communication de renseignements à une autre juridiction n'est pas obligatoire si elle devait être contraire à l'*ordre public* de la juridiction qui les fournit[3]. Ce cas de figure survient rarement dans le contexte de l'échange de renseignements entre Autorités compétentes, mais certaines juridictions peuvent

3. Voir par exemple le point 3(c) de l'article 26 du Modèle de Convention fiscale de l'OCDE et le point 2(d) de l'article 21 de la Convention multilatérale concernant l'assistance administrative mutuelle en matière fiscale.

demander à leurs Autorités compétentes de préciser que les renseignements communiqués ne doivent pas être utilisés ou divulgués dans des procédures susceptibles d'aboutir à la prononciation ou l'exécution de la peine de mort, d'actes de torture ou d'autres violations graves de droits de l'homme (lorsque par exemple les enquêtes fiscales sont motivées par des persécutions politiques, raciales ou religieuses) car cela serait contraire à l'ordre public de la juridiction qui fournit les renseignements. En pareil cas, une disposition à cet effet pourrait être incluse dans l'Accord entre autorités compétentes.

Paragraphe 2 – Violation de la confidentialité

6. Il est essentiel d'assurer la confidentialité des renseignements reçus en vertu de l'instrument juridique applicable. Le paragraphe 2 de la section 5 dispose qu'en cas de violation de l'obligation de confidentialité ou des dispositions relatives à la protection des données (y compris des dispositions supplémentaires éventuelles spécifiées par l'Autorité compétente qui fournit les renseignements), l'Autorité compétente doit en informer immédiatement l'Autorité compétente de l'autre partie et lui notifier toute sanction ou action corrective qui en résulte. Le contenu de cette notification doit respecter les règles de confidentialité et être conforme au droit interne de la juridiction dans laquelle la violation ou le manquement se sont produits. En outre, la section 7 indique expressément que le non-respect des obligations de confidentialité et des dispositions relatives à la protection des données (y compris des dispositions supplémentaires éventuelles spécifiées par l'Autorité compétente qui fournit les renseignements) serait considéré comme un manquement grave et un motif de suspension immédiate de l'Accord entre autorités compétentes.

Confidentialité et protection des données en vertu de la Norme commune de déclaration

7. Trois éléments sont essentiels pour garantir l'existence de dispositions adéquates pour protéger les renseignements échangés automatiquement : *(i)* le cadre juridique, *(ii)* les pratiques et procédures visant à assurer la sécurité des données, et *(iii)* le suivi de l'observation et les sanctions en cas de violation de la confidentialité. Chacun de ces aspects est examiné ci-après. L'Annexe 4 de ce document est un questionnaire[4] qui convertit cette analyse en une série de questions et que les juridictions pourraient utiliser afin d'évaluer le respect des règles en matière de confidentialité et de protection des données. Les juridictions peuvent choisir d'élaborer leur propre questionnaire sur

4. L'exemple de questionnaire à l'Annexe 4 est le questionnaire utilisé par les États-Unis aux fins de la loi FATCA au 20 mars 2014 après suppression des spécificités américaines.

les aspects de la NCD relevant de la confidentialité et de la protection des données. D'autres peuvent décider de ne pas utiliser de questionnaire dans la mesure où elles ont déjà conclu un accord d'échange automatique de renseignements avec une autre juridiction et ont obtenu l'assurance que celle-ci a pris des dispositions adéquates pour protéger les renseignements échangés automatiquement.

1. Cadre juridique

8. Le cadre juridique doit garantir la confidentialité des renseignements fiscaux échangés et limiter leur utilisation aux fins prévues par les dispositions de l'instrument d'échange. Les deux piliers de ce cadre sont les dispositions de l'instrument applicable et le droit interne des juridictions concernées.

9. Toutes les conventions fiscales bilatérales et multilatérales ainsi que d'autres instruments juridiques prévoyant l'échange de renseignements fiscaux doivent prévoir l'obligation que les données échangées restent confidentielles et qu'elles soient utilisées à certaines fins uniquement. Le Modèle de Convention fiscale de l'OCDE en est l'illustration. Aux termes du paragraphe 2 de l'article 26, les renseignements sur les contribuables reçus par une Autorité compétente doivent être tenus secrets de la même manière que les renseignements sur les contribuables obtenus en application du droit interne de cet État. Ils ne doivent être communiqués qu'aux « personnes ou autorités (y compris les tribunaux et organes administratifs) » concernées par l'établissement, le recouvrement, l'administration ou l'exécution des impôts couverts, par les procédures ou poursuites concernant ces impôts, par les décisions sur les recours relatifs à ces impôts, ou par le contrôle de ce qui précède. Ils peuvent également être utilisés à d'autres fins si les Autorités compétentes des deux juridictions l'autorisent et si le droit des deux États le permet. De même, l'article 22 de la Convention multilatérale concernant l'assistance administrative mutuelle en matière fiscale prévoit que les renseignements obtenus par une Partie doivent être tenus secrets et protégés dans les mêmes conditions que celles prévues pour les renseignements obtenus en application du droit interne de cette Partie, et impose des restrictions à l'usage et à la divulgation de ces renseignements.

10. Le droit interne doit comporter des dispositions suffisantes pour protéger la confidentialité des renseignements sur les contribuables et prévoir des circonstances spécifiques et limitées dans lesquelles ces renseignements peuvent être divulgués et utilisés. Le droit interne doit également fixer des pénalités ou des sanctions efficaces en cas de divulgation ou d'utilisation non autorisée de ces renseignements. En outre, le droit interne doit disposer que les instruments internationaux d'échange adoptés par la juridiction sont juridiquement contraignants et que les obligations de confidentialité qui y

figurent le sont aussi. Enfin, le droit interne d'une juridiction prévoyant la protection des données sur les contribuables doit s'appliquer aux renseignements reçus d'une autre juridiction en vertu d'un instrument d'échange.

2. Gestion de la sécurité de l'information : pratiques et procédures

11. Pour que les protections juridiques accordées par l'instrument d'échange et par le droit interne soient efficaces, les juridictions doivent mettre en place des pratiques et des procédures qui garantissent que les renseignements échangés seront utilisés uniquement en matière fiscale (ou à d'autres fins spécifiées) et qui empêchent leur transmission à des personnes ou à des autorités publiques qui ne sont pas concernées par l'établissement, le recouvrement, l'administration ou l'exécution des impôts couverts, par les procédures ou poursuites concernant ces impôts, par les décisions sur les recours relatifs à ces impôts, ou par le contrôle de ce qui précède.

12. Un système de gestion de la sécurité de l'information est un ensemble de règles, pratiques et procédures portant sur la gestion de la sécurité de l'information et sur les risques informatiques associés. Cette question n'est pas seulement technique, mais elle touche aussi des aspects économiques, culturels et organisationnels. Comme on le verra plus en détail ci-après, les pratiques et procédures mises en œuvre par les administrations fiscales doivent englober tous les aspects pertinents pour garantir la confidentialité, y compris un processus de sélection du personnel qui traite l'information, des restrictions quant aux personnes autorisées à accéder aux renseignements et des systèmes capables de détecter et d'identifier les divulgations non autorisées. Les pratiques et procédures relatives à la gestion de la sécurité de l'information suivies par l'administration fiscale de chaque juridiction doivent respecter les normes reconnues internationalement ou les pratiques exemplaires qui garantissent la protection des données confidentielles sur les contribuables[5]. En l'occurrence, elles doivent comporter les vérifications fondamentales suivantes :

5.. Les normes acceptées internationalement qui régissent la sécurité de l'information sont connues sous l'appellation « suite ISO/CEI 27000 » et sont publiées conjointement par l'Organisation internationale de normalisation (ISO) et par la Commission électrotechnique internationale (CEI). Cette série définit les pratiques exemplaires en matière de gestion de la sécurité de l'information, de risque et de contrôles dans le contexte d'un système global de gestion de la sécurité de l'information. Une administration fiscale doit être en mesure de prouver qu'elle se conforme aux normes de la suite ISO/CEI 27000 ou qu'elle dispose d'un cadre équivalent pour la sécurité de l'information, et que les renseignements sur les contribuables obtenus en vertu d'un instrument juridique sont protégés par ce cadre.

2.1. Personnel (vérification des antécédents, contrats de travail, formation)

13. Les administrations fiscales doivent s'assurer que les personnes exerçant des responsabilités et ayant accès aux données sur les contribuables sont dignes de confiance et ne représentent pas un risque pour la sécurité, et que leurs droits d'accès sont dûment gérés et contrôlés. Les membres du personnel, les consultants et autres intervenants ayant accès à des renseignements confidentiels doivent également faire l'objet d'une enquête de sécurité. Les consultants ayant accès aux renseignements sur les contribuables doivent être contractuellement tenus de respecter les mêmes obligations que le personnel en ce qui concerne la confidentialité des renseignements fiscaux.

14. Les administrations fiscales doivent veiller à ce que les membres du personnel ayant accès aux données soient informés des obligations de confidentialité qui leur incombent, des risques que leurs activités font peser sur la sécurité, ainsi que des lois, politiques et procédures applicables en matière de sécurité et de confidentialité. Les membres du personnel qui ont accès aux données doivent bénéficier d'une formation annuelle ou plus fréquente.

15. En outre, des procédures doivent permettre de mettre rapidement un terme à l'accès aux renseignements confidentiels pour les membres du personnel qui sont licenciés, transférés ou qui partent en retraite et qui n'ont donc plus besoin de cet accès. En outre, l'obligation de confidentialité doit rester en vigueur après la fin de la relation d'emploi.

2.2. Accès aux locaux et stockage des documents physiques

16. Les administrations fiscales doivent adopter des mesures de sécurité visant à restreindre l'accès à leurs locaux. Parmi les mesures fréquentes figurent la présence d'agents de sécurité, l'accompagnement obligatoire des visiteurs, les badges de sécurité, les entrées à code pour le personnel et les dispositifs qui limitent son accès aux espaces abritant des informations sensibles.

17. Les administrations fiscales doivent également disposer de systèmes sécurisés de stockage des documents confidentiels. Les données peuvent être conservées dans des unités ou pièces verrouillées : armoires (à code ou à clé), coffres et chambres fortes. Des règles devraient régir l'accès aux codes et clés. Le degré de sécurité des armoires de stockage doit varier en fonction de la classification de leur contenu, et les données fiscales échangées en bloc automatiquement doivent avoir une classification de sécurité appropriée. Les administrations fiscales doivent également garantir cette sécurité lorsque les données sont transférées sur d'autres sites de travail.

2.3. Planification

18. Les administrations fiscales doivent établir un plan visant à élaborer, documenter, mettre à jour et déployer des mesures de sécurité pour leurs systèmes d'information.

2.4. Gestion de la configuration

19. Les administrations fiscales doivent contrôler et gérer la configuration des systèmes d'information. À cette fin, elles doivent mettre en place, documenter, diffuser et mettre à jour des contrôles de sécurité adéquats.

2.5. Contrôle d'accès

20. Les administrations fiscales doivent limiter l'accès des systèmes aux utilisateurs et aux équipements (autres systèmes d'information compris) autorisés. Ces utilisateurs ne doivent pouvoir accéder qu'aux transactions et aux fonctions qu'ils sont autorisés à accomplir.

2.6. Identification et authentification

21. Les systèmes d'information doivent être munis de fonctions permettant de stocker et d'authentifier l'identité d'utilisateurs et d'équipements qui en demandent l'accès. Ils doivent être en mesure d'identifier un utilisateur non autorisé et de l'empêcher d'accéder aux renseignements confidentiels.

2.7. Audit et responsabilité

22. La responsabilité des utilisateurs non autorisés ne peut être engagée que si leurs actions sont identifiables. C'est pourquoi il est essentiel que les administrations fiscales créent et conservent des dossiers d'audit des systèmes d'information afin de contrôler, d'analyser, d'enquêter et de signaler toute activité illégale, non autorisée ou inappropriée.

2.8. Maintenance

23. Les administrations fiscales doivent procéder à une maintenance des systèmes à intervalles périodiques et en temps voulu, et mener des vérifications efficaces des outils, techniques et mécanismes de maintenance et du personnel qui les utilise.

2.9. Protection des systèmes et des communications

24. Les administrations fiscales doivent suivre, contrôler et protéger les communications au niveau des frontières internes et externes des systèmes d'information. Ces contrôles doivent comporter des procédures visant à supprimer les données résiduelles, assurer la confidentialité des transmissions et valider la cryptographie.

2.10. Intégrité des systèmes et de l'information

25. Les administrations fiscales doivent identifier, signaler et corriger (ou prendre des mesures d'amélioration) en temps voulu les incidents impliquant la sécurité des technologies de communication de l'information, se prémunir contre les logiciels malveillants et suivre les alertes et avis de sécurité du système.

2.11. Évaluations de sécurité

26. Les administrations fiscales doivent élaborer et actualiser périodiquement une politique d'examen des processus utilisés pour tester, valider et autoriser les contrôles de sécurité nécessaires à la protection des données, à la correction des défaillances et à la réduction des risques. La fréquence de ces mises à jour dépendra des risques, mais elles doivent intervenir à intervalles appropriés, conformément aux normes reconnues internationalement ou aux pratiques exemplaires. Les administrations fiscales doivent également se doter d'une politique d'examen des modalités d'autorisation des transactions et connexions du système d'information, ainsi que des procédures de suivi des contrôles de sécurité du système.

2.12. Planification des interventions d'urgence

27. Les administrations fiscales doivent élaborer et mettre en œuvre des plans d'intervention d'urgence, d'opérations de sauvegarde et de récupération des données des systèmes après une catastrophe.

2.13. Évaluation des risques

28. Une administration fiscale doit évaluer le risque potentiel d'accès non autorisé aux renseignements sur les contribuables, ainsi que le risque et l'ampleur du préjudice causé par l'utilisation, la divulgation, l'altération, la modification ou la destruction non autorisées de ces renseignements ou des systèmes d'information sur les contribuables. Elle doit actualiser son évaluation des risques à intervalles périodiques ou lorsque le système d'information ou les installations qui l'hébergent subissent d'importantes

modifications, ou encore lorsque surviennent d'autres conditions susceptibles d'avoir un impact négatif sur la sécurité ou le statut d'accréditation du système.

2.14. Acquisition de systèmes et de services

29. Les administrations fiscales doivent s'assurer que les prestataires extérieurs engagés pour traiter, stocker et transmettre les renseignements échangés en vertu de l'instrument juridique applicable effectuent des contrôles conformes aux exigences de sécurité propres aux systèmes informatiques.

2.15. Protection des supports

30. Les administrations fiscales doivent protéger les renseignements au format papier ou sur supports numériques, restreindre leur accès aux seuls utilisateurs autorisés, et effacer le contenu des supports numériques ou les détruire avant leur élimination ou leur réutilisation.

2.16. Identification des données

31. Les données échangées en vertu de l'instrument juridique applicable doivent être systématiquement protégées contre une divulgation fortuite. Si les données sont enregistrées dans un fichier contenant d'autres données et qu'une séparation physique est impossible, des procédures doivent être en place pour faire en sorte que l'ensemble du fichier soit sauvegardé et pour indiquer clairement qu'il contient des données échangées aux termes d'un instrument juridique. Les renseignements proprement dits doivent aussi être clairement signalés.

32. Il faut instaurer des procédures garantissant que toutes les données contenues dans un tel fichier soient effacées avant que ce fichier soit remis à une personne ou à une autorité qui n'est pas autorisée à accéder aux données échangées en vertu d'un instrument juridique. Si les données sont stockées dans une base de données, il faut prévoir des procédures garantissant que toutes ces données sont bien effacées de la base avant consultation par une personne ou une autorité qui n'est pas autorisée à accéder aux renseignements échangés en vertu d'un instrument juridique (ou que ces données soient dûment séparées/protégées de manière à empêcher la personne ou l'autorité non autorisée d'y accéder).

2.17. Règles de suppression des données

33. Les administrations fiscales doivent se doter de règles imposant la destruction des données devenues inutiles et garantissant la suppression en toute sécurité des informations confidentielles. Le déchiquetage, l'incinération

ou l'utilisation de conteneurs à déchets verrouillés sont appropriés pour les documents imprimés, et les documents électroniques doivent être effacés lorsqu'ils ne sont plus utiles. Des mesures doivent être prises pour effacer les données confidentielles quand les ordinateurs et appareils de stockage sont mis au rebut.

3. Contrôle de conformité et sanctions en cas de violation de la confidentialité

34. Les administrations fiscales doivent non seulement tenir confidentiels les renseignements échangés en vertu d'un instrument juridique, mais aussi s'assurer qu'ils seront utilisés uniquement aux fins prévu par l'accord d'échange de renseignements applicable. Aussi, le respect d'un cadre de sécurité de l'information acceptable ne suffit pas à protéger les données fiscales échangées. Le droit interne doit en outre prévoir des pénalités ou des sanctions en cas de divulgation ou d'utilisation inappropriée des renseignements sur les contribuables. Pour garantir leur mise en œuvre, cette législation doit être complétée par des ressources et des procédures administratives adéquates.

3.1. Pénalités et sanctions

35. Le droit interne doit comporter des pénalités ou des sanctions en cas de divulgation ou d'utilisation inappropriée des renseignements sur les contribuables, et les administrations fiscales doivent, dans les faits, les appliquer à l'encontre du personnel qui enfreint les règles et procédures de sécurité afin de dissuader les contrevenants potentiels. Pour garantir leur mise en œuvre, cette législation doit être complétée par des ressources et des procédures administratives adéquates. Les administrations fiscales devraient établir un processus formel de sanctions visant le personnel et les prestataires extérieurs qui ne respectent pas les règles et procédures établies en matière de sécurité de l'information, prévoyant des sanctions civiles et pénales ou cas de consultation ou de divulgation non autorisée.

3.2. Répression de l'accès et de la divulgation non autorisés

36. Outre l'adoption de règles en matière d'accès aux renseignements confidentiels, les administrations fiscales doivent également mettre en place des processus pour contrôler le respect de ces règles et détecter tout accès et toute divulgation non autorisés. En cas de divulgation non autorisée, une enquête doit être menée et un rapport établi à l'intention de la direction. Ce rapport doit comporter :

- des recommandations sur les moyens d'atténuer les répercussions de l'incident ;
- une analyse de ce qu'il faudrait faire pour éviter qu'il se reproduise ;
- des recommandations sur les mesures et sanctions à prendre à l'encontre du/des responsable(s) de l'infraction, en soulignant qu'en cas de présomption de divulgation intentionnelle, autorités répressives pourraient intervenir ;
- les raisons qui conduisent à penser, avec un degré d'assurance élevé, qu'une fois mises en œuvre, les modifications du système et les sanctions recommandées empêcheront que des infractions similaires se reproduisent.

37. En outre, les administrations fiscales devraient mettre en place un processus d'examen et d'approbation des recommandations de modification des règles et procédures afin d'éviter de nouvelles infractions à l'avenir. L'autorité chargée de l'enquête ou l'autorité hiérarchique doit veiller à ce que l'administration fiscale applique bien les recommandations approuvées.

Commentaires sur la section 6 concernant les consultations et modifications

1. Cette section porte sur les consultations entre Autorités compétentes et sur les modifications apportées à l'Accord entre autorités compétentes.

Paragraphe 1 – Consultations

2. Ce paragraphe dispose qu'en cas de difficulté dans l'application ou l'interprétation du présent Accord, chaque Autorité compétente peut solliciter des consultations en vue d'élaborer des mesures appropriées pour garantir l'exécution de l'Accord. Des consultations peuvent également se tenir en vue d'analyser la qualité des renseignements reçus.

3. Les Autorités compétentes peuvent communiquer entre elles par courrier, fax, téléphone, rencontre directe ou par tout autre moyen pratique permettant de parvenir à un accord sur les mesures appropriées pour garantir l'exécution du présent Accord.

Paragraphe 2 – Modifications

4. Ce paragraphe précise que l'Accord peut être modifié par consentement écrit des Autorités compétentes. Sauf disposition contraire entre les Autorités compétentes, une telle modification entre en vigueur le premier jour du mois suivant l'expiration d'une période d'un mois après :

- la date des signatures de cet accord écrit ou
- la date des notifications échangées aux fins de cet accord écrit.

5. Comme l'indique l'introduction aux Commentaires sur le Modèle AAC, des juridictions peuvent conclure un accord intergouvernemental multilatéral ou plusieurs accords intergouvernementaux qui seraient des traités internationaux à part entière couvrant à la fois les obligations déclaratives et les procédures de diligence raisonnable, conjugués à un accord entre Autorités compétentes de portée plus limitée. Dans ce cas, les modifications peuvent être soumises à des règles différentes.

Commentaires sur la section 7 concernant la durée de l'Accord

Paragraphe 1 – Entrée en vigueur

1. Le paragraphe 1 prévoit deux dates d'entrée en vigueur possibles. En premier lieu, lorsque les juridictions concluent cet accord après avoir adopté la législation nécessaire pour mettre en œuvre la Norme commune de déclaration, elles fixent une date d'entrée en vigueur de l'Accord. En second lieu, si les Autorités compétentes concluent l'Accord avant la mise en place de la législation nécessaire dans l'une des juridictions ou dans les deux, elles peuvent recourir à la deuxième option, auquel cas l'accord entre en vigueur à la date de la dernière notification effectuée pour indiquer que la juridiction a adopté les règles nécessaires pour appliquer l'accord.

Paragraphe 2 – Suspension

2. Le paragraphe 2 contient des précisions sur la possibilité pour une Autorité compétente de suspendre l'accord si elle juge que l'autre Autorité compétente commet ou a commis un manquement grave. Dans la mesure du possible, les Autorités compétentes doivent s'efforcer de remédier aux manquements, même à ceux ayant un niveau élevé de gravité, avant de notifier la suspension de la validité de l'Accord.

3. Pour suspendre l'Accord, une Autorité compétente doit adresser un préavis écrit en ce sens à l'autre Autorité compétente. Ce préavis doit décrire en détail le manquement grave constaté, et mentionner si possible les mesures qui devraient être prises pour y remédier. La suspension est à effet immédiat.

4. L'Autorité compétente ainsi notifiée doit engager le plus rapidement possible les mesures nécessaires pour remédier au manquement grave. Elle doit informer l'autre Autorité compétente dès que le problème est résolu. L'Autorité compétente qui a envoyé le préavis de suspension doit alors confirmer par écrit à l'autre Autorité compétente que l'Accord n'est plus suspendu et que les échanges de renseignements peuvent reprendre le plus tôt possible.

5. Le paragraphe 2 indique que le concept de manquement grave désigne notamment :

- le non-respect des obligations de confidentialité ou des dispositions relatives à la protection des données du présent Accord (y compris des protections supplémentaires précisées dans l'Accord entre Autorités compétentes), par exemple l'utilisation des renseignements à des fins non autorisées par l'instrument juridique applicable ou une modification du droit interne qui compromet la confidentialité des renseignements ;
- le fait pour l'Autorité compétente de ne pas communiquer des informations appropriées ou en temps voulu comme le prévoit le présent Accord ;
- une définition de Comptes exclus ou d'Institutions financières non déclarantes allant à l'encontre des objectifs de la Norme commune de déclaration ;
- le fait de ne pas mettre en place des règles et des procédures administratives garantissant la mise en œuvre effective des procédures de déclaration et de diligence raisonnable établies dans la Norme commune de déclaration.

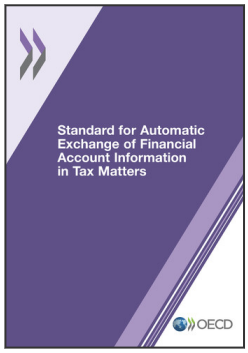
6. Au cours de la période de suspension, tous les renseignements préalablement reçus en vertu de cet Accord restent confidentiels et soumis aux dispositions de la section 5 de l'Accord, y compris aux dispositions supplémentaires en matière de protection des données spécifiées par l'Autorité compétente qui communique les renseignements et à celles prévues par l'instrument juridique applicable.

Paragraphe 3 – Résiliation

7. Le paragraphe 3 contient la clause de résiliation. Chacune des Autorités compétentes peut dénoncer le présent Accord moyennant préavis écrit adressé à l'Autorité compétente de l'autre partie. Cette dénonciation prend effet le premier jour du mois suivant l'expiration d'un délai de douze mois à compter de la date du préavis. Par exemple, une Autorité compétente peut décider de résilier cet Accord dans le cas où il a été suspendu et où l'autre Autorité compétente n'a pas remédié au manquement grave dans un délai raisonnable.

8. La résiliation de l'instrument juridique qui sous-tend l'Accord entre Autorités compétentes entraîne la résiliation automatique de cet Accord. Dans ces circonstances, il n'est pas nécessaire de résilier séparément l'Accord entre Autorités compétentes.

9. Le paragraphe 3 précise qu'en cas de résiliation, toutes les informations déjà reçues au titre du présent Accord restent confidentielles et soumises aux dispositions de la section 5 de l'Accord, y compris aux dispositions supplémentaires en matière de protection des données spécifiées par l'Autorité compétente qui communique les renseignements et à celles prévues par l'instrument juridique applicable.



Extrait de :

Standard for Automatic Exchange of Financial Account Information in Tax Matters

Accéder à cette publication :
https://doi.org/10.1787/9789264216525-en

Merci de citer ce chapitre comme suit :

OCDE (2014), « Commentaires sur le Modèle d'accord entre autorités compétentes », dans *Standard for Automatic Exchange of Financial Account Information in Tax Matters*, Éditions OCDE, Paris.

DOI: https://doi.org/10.1787/9789264222090-6-fr