FORUM MONDIAL SUR
LA TRANSPARENCE ET L'ÉCHANGE DE RENSEIGNEMENTS À DES FINS FISCALES

Termes de référence pour l'examen des mesures de confidentialité et de protection des données

OCDE
DES POLITIQUES MEILLEURES POUR UNE VIE MEILLEURE

Termes de référence pour l'examen des mesures de confidentialité et de protection des données

Les exigences en matière de confidentialité et de sauvegarde des données de la Norme EAR

1. L'Exigence fondamentale 3 des évaluations par les pairs de l'EAR prévoit que "les juridictions doivent garder les informations échangées confidentielles et correctement sauvegardées, et les utiliser conformément à l'accord d'échange en vertu duquel elles ont été échangées".[1] Une juridiction doit satisfaire à cette exigence pour pouvoir recevoir des informations (c'est-à-dire pour être considérée comme un "Partenaire approprié" pour recevoir des informations).

2. Ces exigences figurent, dans la Norme EAR, à la section 5 du Modèle d'accord entre autorités compétentes (Modèle d'AAC) et de son commentaire. La section 7 reconnaît l'importance de maintenir le respect de ces exigences et envisage la possibilité pour les autorités compétentes de suspendre les échanges automatiques d'informations en cas de non-respect.

3. Les éléments de l'Exigence fondamentale 3 sont les suivants (i) un cadre juridique qui garantit la confidentialité et l'utilisation appropriée des informations échangées conformément aux instruments juridiques internationaux (**Exigence fondamentale 3.1**) ;[2] (ii) un système de gestion de la sécurité de l'information (GSI) qui respecte les normes ou les meilleures pratiques reconnues au niveau international (**Exigence fondamentale 3.2**) ;[3] et (iii) des dispositions et des procédures d'application pour faire face aux violations de la confidentialité et à l'utilisation abusive de l'information (**Exigence fondamentale 3.3**).[4] Ces exigences se déclinent en neuf sous-exigences (SE) pour les évaluations.

4. L'objectif des évaluations est de donner l'assurance que les juridictions gardent les informations confidentielles et les sauvegardent correctement. Pour ce faire, il est nécessaire de protéger les informations tout au long de leur cycle de vie. Les juridictions peuvent gérer le cycle de vie de l'information de différentes manières au niveau opérationnel. Le champ d'application opérationnel des évaluations, en particulier en ce qui concerne les Exigences fondamentales 3.2 et 3.3, peut donc varier d'une juridiction à l'autre. Les juridictions doivent décrire leurs processus de gestion des données et du cycle de vie des

---

[1] *Le cadre du deuxième cycle d'examens par les pairs de l'EAR, Annexe A, Termes de référence de l'EAR* [CTPA/GFTEI(2022)5/FINAL].

[2] Paragraphes 8 à 10 du commentaire sur la section 5 du Modèle d'AAC

[3] Paragraphes 11 et 12 du commentaire sur la section 5 du Modèle d'AAC. Un système GSI est un ensemble de politiques, de pratiques et de procédures relatives à la gestion de la sécurité de l'information, y compris les risques liés aux technologies de l'information. Les normes internationalement reconnues ou les meilleures pratiques en matière de GSI font référence à la "série ISO/IEC 27000", publiée conjointement par l'Organisation internationale de normalisation (International Organisation for Standardisation - ISO) et la Commission électrotechnique internationale (International Electrotechnical Commission - IEC), ou à une autre norme équivalente, ou au cadre de GSI d'une juridiction qui est équivalent à ces normes.

[4] Paragraphes 34-37 du commentaire sur la section 5 du Modèle d'AAC.

informations échangées dès le début des évaluations afin de s'assurer que le champ d'application approprié des opérations est évalué. Les évaluations peuvent être utilisées par les organismes chargés du suivi et de l'examen de la mise en œuvre des normes relatives à l'échange de renseignements à des fins fiscales autres que la Norme EAR, afin de minimiser les coûts globaux d'évaluation et de créer des gains d'efficacité.[5] Les juridictions devraient donc décrire les processus et le cycle de vie des renseignements échangés dans le cadre de ces autres normes, le cas échéant, dans la mesure où ils diffèrent de ceux des informations échangées dans le cadre de la Norme EAR.

[5] Au mois d'octobre 2024, ces organes n'incluent que le Cadre inclusif sur le BEPS en ce qui concerne ses normes relatives à la transparence, comme en témoignent les documents suivants : OCDE (2017), Action 5 du BEPS sur les pratiques fiscales dommageables – « Termes de référence et méthodologie pour la conduite des examens par les pairs du cadre de transparence de l'Action 5 », Projet OCDE/G20 sur l'érosion de la base d'imposition et le transfert de bénéfices, OCDE, Paris. www.oecd.org/tax/beps/beps-action-5-harmful-tax-practices-peer-review-transparency-framework.pdf, Méthodologie au paragraphe 7 ; OCDE (2017), "Termes de référence pour la conduite des examens par les pairs de la norme minimale de l'Action 13 sur la déclaration pays par pays" dans l'Action 13 du BEPS sur la déclaration pays par pays - Documents d'examen par les pairs, Projet OCDE/G20 sur l'érosion de la base d'imposition et le transfert de bénéfices, OCDE, Paris. www.oecd.org/tax/beps/beps-action-13-on-country-by-country-reporting-peer-review-documents.pdf, Méthodologie au paragraphe 7.

Exigence fondamentale 3.1 : Les juridictions doivent disposer d'un cadre juridique garantissant la confidentialité et l'utilisation appropriée des renseignements échangés dans le cadre d'un accord d'échange international

SE 3.1.1 : Le cadre juridique interne des juridictions doit comprendre des dispositions suffisantes pour protéger la confidentialité des informations relatives aux contribuables, y compris les renseignements échangés dans le cadre d'une convention, et ne prévoir que des circonstances spécifiques et limitées dans lesquelles ces informations peuvent être consultées, divulguées et utilisées, ces circonstances étant conformes, en ce qui concerne les renseignements échangés dans le cadre d'une convention, aux termes de l'instrument d'échange international applicable (bilatéral ou multilatéral) dans le cadre duquel les renseignements ont été échangés

Exigence fondamentale 3.2 : Les juridictions doivent disposer d'un cadre de gestion de la sécurité de l'information (GSI) qui respecte les normes ou les meilleures pratiques internationalement reconnues et garantit la protection des renseignements échangés dans le cadre d'une convention

5. Les autorités fiscales[6] qui sont autorisées à accéder aux informations échangées conformément au paragraphe 2 de l'article 22 de la Convention concernant l'assistance administrative mutuelle en matière fiscale ou à des dispositions équivalentes dans d'autres accords internationaux d'échange doivent disposer d'une politique et de systèmes de gestion des informations afin de garantir que les informations ne peuvent être utilisées qu'aux fins prévues et d'empêcher leur divulgation à des personnes non autorisées. Un système GSI est un ensemble de dispositions, de politiques, de procédures et de pratiques de gouvernance concernant les risques liés à la sécurité de l'information, y compris les risques liés aux technologies de l'information. Les systèmes GSI doivent respecter les normes ou les meilleures pratiques reconnues au niveau international.

6. Les normes internationalement reconnues en matière de sécurité de l'information sont connues sous le nom de "série ISO/IEC-27000", publiées conjointement par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (IEC), bien que d'autres normes équivalentes soient également largement reconnues et suivies par des organisations dans le monde entier. Ces normes fournissent les meilleures pratiques en matière de gestion de la sécurité de l'information, de risques et de contrôles dans le contexte d'un système GSI global. Une administration fiscale doit être en mesure de démontrer qu'elle dispose d'un cadre de sécurité de l'information conforme à la série ISO 27000 ou à une autre norme équivalente, ou qu'elle dispose d'un cadre équivalent.

7. La Norme EAR précise que les normes internationalement reconnues ou les meilleures pratiques comprennent une série de contrôles GSI de base (c'est-à-dire minimaux) à mettre en place.[7] Ces références spécifiques aux contrôles de base doivent être complétées par la référence générale de la norme aux normes ou meilleures pratiques internationalement reconnues, afin de s'assurer que tous les éléments pertinents de ces normes ou meilleures pratiques sont couverts. Certains éléments supplémentaires devraient être en place, notamment la planification au niveau stratégique et les

[6] Le terme "autorité fiscale" comprend les administrations fiscales ainsi que d'autres autorités chargées de traiter les renseignements échangées dans le cadre d'une convention, par exemple les autorités des juridictions non réciproques en ce qui concerne la Norme EAR qui traitent les données relatives à la norme et n'administrent pas des impôts.

[7] Paragraphes 12 et 13-34 du commentaire sur la section 5 du Modèle d'AAC.

dispositions de gouvernance essentielles à un système GSI. Les autorités fiscales devraient également mettre en place des contrôles de sécurité adaptés à leur architecture EAR spécifique et aux risques liés à la sécurité de l'information.

8. Les autorités fiscales doivent satisfaire aux exigences de GSI dans leur système GSI global (SE 3.2.1), dans la mise en œuvre de divers contrôles de sécurité (SE 3.2.2 à 3.2.5) et dans leur cadre opérationnel pour tester l'efficacité de ces contrôles (SE 3.2.6), comme suit :

SE 3.2.1 : Les autorités fiscales doivent disposer d'un système global de gestion de la sécurité de l'information qui soit approprié

9. Les autorités fiscales doivent :

1. faire preuve d'une compréhension claire du cycle de vie des renseignements échangés dans le cadre des conventions au sein de l'organisation, s'engager à préserver leur confidentialité et leur utilisation appropriée conformément à l'instrument d'échange international applicable, et disposer de procédures appropriées pour traiter ces informations (y compris pour rester conscient de leur nature échangée dans le cadre d'une convention) ;

2. gérer la sécurité de l'information au moyen d'une politique écrite de sécurité de l'information et de dispositions opérationnelles et de gouvernance appropriées, dans le cadre d'une structure de sécurité globale qui définit clairement les rôles, les responsabilités et les voies hiérarchiques en matière de sécurité, qui appartient à la direction générale et qui est tenue à jour;

3. faire de la sécurité une partie intégrante de la gestion de l'environnement et des services informatiques, notamment en mettant en place un processus de gestion du changement intégrant la sécurité et en utilisant des accords de niveau de service ;

4. gérer systématiquement les risques liés à la sécurité de l'information, y compris les risques liés aux technologies de l'information, à la cybersécurité et aux renseignements échangés, en tenant compte des menaces, des vulnérabilités, des impacts et de la gestion des opérations de sécurité ; et

5. prendre des dispositions appropriées pour gérer et maintenir la continuité des activités et des services informatiques.

SE 3.2.2 : Les autorités fiscales doivent mettre en place des contrôles appropriés en matière de ressources humaines

10. Les autorités fiscales doivent :

1. procéder à des vérifications d'antécédents et à un contrôle approprié de tous les candidats à l'emploi, des employés et des prestataires, conformément aux meilleures pratiques acceptées et aux risques perçus ;

2. veiller à ce que les rôles et les responsabilités des employés et des prestataires en matière de sécurité soient définis, documentés, clairement communiqués et compris par eux, et régulièrement revus, à ce qu'ils reçoivent une formation et une sensibilisation à la sécurité régulières et actualisées (les personnes jouant un rôle sensible recevant des conseils supplémentaires concernant le traitement de documents plus sensibles), et à ce qu'ils appliquent les politiques et les procédures en matière de sécurité ; et

3. disposer de politiques et de procédures relatives à la fin de l'engagement (y compris le passage à d'autres fonctions) qui protègent les informations sensibles.

SE 3.2.3 : Les autorités fiscales doivent prendre des dispositions appropriées en matière de sécurité physique

11. Les autorités fiscales doivent :

    1. disposer de plans, de politiques ou d'autres documents appropriés en matière de sécurité physique ; et protéger les locaux physiques, notamment au moyen de périmètres sécurisés internes et externes et de contrôles d'accès en ce qui concerne les employés, les visiteurs et les prestataires.

SE 3.2.4 : Les autorités fiscales doivent disposer d'un système de sécurité informatique approprié

12. Les autorités fiscales doivent :

    1. gérer de manière adéquate leurs actifs informatiques tout au long de leur cycle de vie ;

    2. déployer une gamme appropriée de contrôles de la sécurité informatique, y compris des contrôles relatifs aux terminaux (postes de travail et autres dispositifs), aux serveurs, à l'infrastructure, aux applications, aux logiciels et à l'accès à l'internet ; et

    3. mettre en œuvre des contrôles d'accès logiques conformes aux principes du "besoin d'en connaitre" et du '"moindre privilège" et fondés sur une politique d'accès logique définie par l'encadrement supérieur.

SE 3.2.5 : Les autorités fiscales doivent protéger les informations de manière appropriée

13. Les autorités fiscales doivent :

    1. gérer efficacement les informations, y compris les renseignements échangés dans le cadre d'une convention conformément à un ensemble de politiques et de procédures tout au long du cycle de vie de la gestion de l'information, y compris la dénomination, la classification, le traitement, le partage, le stockage, la conservation et la destruction des documents.

SE 3.2.6 : Les autorités fiscales doivent disposer d'un cadre approprié de gestion des opérations, comprenant la surveillance, l'alerte et la journalisation, la gestion de la vulnérabilité, la gestion des incidents et l'audit

14. Les autorités fiscales doivent :

    1. mettre en place des dispositifs appropriés de surveillance, d'alerte et de journalisation, notamment pour détecter les accès, utilisations ou divulgations non autorisés d'informations ;

    2. disposer de processus et de procédures pour l'identification et la gestion des menaces et des vulnérabilités ;

    3. disposer d'un système de gestion des incidents qui couvre tous les types d'incidents de sécurité ; et

    4. disposer de fonctions d'audit interne/externe appropriées en ce qui concerne la sécurité de l'information.

Exigence fondamentale 3.3 : Les juridictions doivent disposer de dispositions et de procédures d'application pour traiter les violations de la confidentialité

SE 3.3.1 : Les juridictions doivent imposer des pénalités et/ou des sanctions appropriées en cas d'accès, d'utilisation ou de divulgation inappropriés d'informations

15. Le cadre juridique interne des juridictions doit permettre d'imposer des pénalités et/ou des sanctions significatives en cas d'accès, de divulgation ou d'utilisation inappropriés des informations relatives aux contribuables, y compris des renseignements échangés dans le cadre d'une, en tenant compte de manière appropriée des pénalités ou sanctions administratives, civiles et pénales.

SE 3.3.2 : Les juridictions doivent appliquer des processus appropriés pour traiter les cas de non-conformité suspectés ou avérés, y compris l'application effective de pénalités ou de sanctions

16. Les juridictions doivent :

1. disposer de procédures à suivre en cas d'accès, d'utilisation ou de divulgation non autorisés, réels ou suspectés (par exemple, identifiés par le biais de la gestion des incidents ou d'autres canaux), qui devraient garantir que ces problèmes sont signalés et examinés et que des mesures correctives appropriées, y compris des pénalités ou des sanctions et des mesures visant à prévenir des violations similaires à l'avenir, sont mises en œuvre ; et

2. appliquer des procédures pour notifier aux autres Autorités compétentes les violations de la confidentialité ou les défaillances des sauvegardes, ainsi que les sanctions et les mesures correctives imposées en conséquence.