



Déclaration sur l'accès des
pouvoirs publics aux données à
caractère personnel détenues
par des entités du secteur
privé



**Instruments
juridiques de l'OCDE**

Ce document est publié sous la responsabilité du Secrétaire général de l'OCDE. Il reproduit un instrument juridique de l'OCDE et peut contenir des informations complémentaires. Les opinions ou arguments exprimés dans ces informations complémentaires ne reflètent pas nécessairement les vues officielles des pays Membres de l'OCDE.

Ce document, ainsi que les données et cartes qu'il peut comprendre, sont sans préjudice du statut de tout territoire, de la souveraineté s'exerçant sur ce dernier, du tracé des frontières et limites internationales, et du nom de tout territoire, ville ou région.

Pour accéder aux textes officiels à jour des instruments juridiques de l'OCDE, ainsi qu'aux informations s'y rapportant, veuillez consulter le Recueil des instruments juridiques de l'OCDE <http://legalinstruments.oecd.org>.

Merci de citer cet ouvrage comme suit :

OCDE, *Déclaration sur l'accès des pouvoirs publics aux données à caractère personnel détenues par des entités du secteur privé*, OECD/LEGAL/0487

Collection : Instruments juridiques de l'OCDE

Crédits photo : © SOMKID THONGDEE/Shutterstock

© OECD 2022

Ce document est mis à disposition à titre gratuit. Il peut être reproduit et distribué gratuitement sans autorisation préalable à condition qu'il ne soit modifié d'aucune façon. Il ne peut être vendu.

Ce document est disponible dans les deux langues officielles de l'OCDE (anglais et français). Il peut être traduit dans d'autres langues à condition que la traduction comporte la mention "traduction non officielle" et qu'elle inclut l'avertissement suivant : "Cette traduction a été préparée par [NOM DE L'AUTEUR DE LA TRADUCTION] à des fins d'information seulement et son exactitude ne peut être garantie par l'OCDE. Les seules versions officielles sont les textes anglais et français disponibles sur le site Internet de l'OCDE <http://legalinstruments.oecd.org>".

Informations Générales

La Déclaration sur l'accès des pouvoirs publics aux données à caractère personnel détenues par des entités du secteur privé a été adoptée par les ministres et représentants de haut niveau des Membres de l'OCDE et de l'Union Européenne le 14 décembre 2022, à l'occasion de la réunion ministérielle du Comité de la politique de l'économie numérique de l'OCDE (CPEN) sur l'île de Grande Canarie en Espagne.

Premier accord intergouvernemental jamais conclu sur les approches communes relatives à la protection de la vie privée et autres droits et libertés des personnes dans le cas d'accès à des données personnelles aux fins de sécurité nationale et d'application de la loi, la Déclaration vise à promouvoir la confiance dans les flux transfrontières de données, qui sont aujourd'hui un moteur essentiel de l'économie globale.

Travaux de l'OCDE sur les flux transfrontières de données

L'évaluation de la mise en œuvre de la Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de 1980 [OECD/LEGAL/0188], achevée en 2021, a conduit à identifier des différences de politiques affectant de manière négative les flux transfrontières de données de caractère personnel, lesquels sont essentiels tant pour les transactions commerciales et les opérations des entreprises que pour les interactions sociales en ligne. Un manque fondamental a été identifié comme étant l'absence de formulation, au niveau international, des garanties mises en place par les pays pour protéger la vie privée ou les autres droits et libertés des personnes en cas d'accès des gouvernements aux données à caractère personnel détenues par des entités privées, dans le cadre de l'exercice de leurs obligations souveraines, liées à la sécurité nationale et à l'application de la loi.

La visée de la formulation de ces principes est double: i) accroître la confiance parmi les systèmes d'état de droit démocratiques qui, sans être identiques, ont cependant des éléments essentiels en commun, afin de faciliter les flux transfrontières de données de caractère personnel entre eux ; et ii) établir une norme quant à la manière dont les systèmes d'état de droit démocratiques limitent et contraignent la puissance gouvernementale, par opposition aux approches qui permettent un accès sans limite, déraisonnable, arbitraire ou disproportionné, en violation des droits humains et des obligations internationales.

Processus de développement de la Déclaration

Le CPEN a démarré ses travaux sur ce sujet en février 2021, sur la base des discussions s'étant tenues lors de sa réunion de novembre 2020, et en s'appuyant sur le travail et les discussions préalables du Groupe de Travail sur la Gouvernance des Données et de la Vie Privée (WPDGP) dans le contexte du rapport sur la mise en œuvre des Lignes Directrices sur la Vie Privée [C(2021)42].

Dans ce but, un groupe de travail informel a été convoqué, composé d'experts issus à terme de 33 pays membres de l'OCDE et de l'Union Européenne. Le groupe de travail s'est réuni 18 fois en 2021 et 2022. Sur la base de ces sessions, des contributions d'experts et de parties prenantes, ainsi que de deux rapports d'études, l'OCDE a identifié sept principes communs issus des lois et pratiques existantes des membres de l'OCDE, qui forment le cœur de cette Déclaration.

Portée de la Déclaration

La Déclaration est constituée de trois sections principales :

1.« Accès légitime par le gouvernement sur la base de valeurs communes », qui reconnaît le rôle important des transferts de données dans l'économie globale et rappelle la raison qui motive l'accès des gouvernements aux données à caractère personnel, l'importance des garanties apportées à la protection de la vie privée et des autres droits et libertés des personnes, et l'existence de caractéristiques communes à cet effet parmi les membres de l'OCDE ;

2.« Promouvoir la confiance dans les flux transfrontière de données », qui réaffirme l'engagement des pays à permettre la libre circulation des données dans des conditions de confiance, considérant que les principes dans la Section 3 de cette Déclaration constituent une expression de leurs valeurs démocratiques, et qui reconnaît que la mise en œuvre effective de ces principes par un pays de destination est une contribution positive à la facilitation des flux de données transfrontières ;

3.« Principes pour l'accès des gouvernements aux données de caractère personnel détenues par des entités privées », énumérant sept principes qui reflètent les caractéristiques communes aux membres de l'OCDE sur la base de leurs lois et pratiques existants, et qui doivent être combinées entre elles pour protéger la vie privée et les autres droits et libertés des personnes : base légale ; finalités légitimes ; autorisation ; traitement des données ; transparence ; contrôle ; recours. Cette section inclut par ailleurs une définition et un champ d'application pour chaque principe.

Pour plus d'information veuillez consulter le site web de la réunion ministérielle du CPEN : <https://www.oecd-events.org/digital-ministerial/> ou contacter digitaleconomypolicy@oecd.org.

NOUS, MINISTRES ET REPRÉSENTANTS DE l'Allemagne, de l'Australie, de l'Autriche, de la Belgique, du Canada, du Chili, de la Colombie, de la Corée, du Costa Rica, du Danemark, de l'Espagne, de l'Estonie, des États-Unis, de la Finlande, de la France, de la Grèce, de la Hongrie, de l'Irlande, de l'Islande, d'Israël, de l'Italie, du Japon, de la Lettonie, de la Lituanie, du Luxembourg, du Mexique, de la Norvège, de la Nouvelle-Zélande, des Pays-Bas, de la Pologne, du Portugal, de la République slovaque, de la République tchèque, du Royaume-Uni, de la Slovénie, de la Suède, de la Suisse, de la Türkiye, et de l'Union européenne (UE), rassemblés sur l'île de la Grande Canarie, en Espagne, les 14 et 15 décembre 2022, sous la présidence de l'Espagne et la vice-présidence du Danemark, des États-Unis, du Japon, du Royaume-Uni et de la République de Türkiye, pour la réunion du Comité de la politique de l'économie numérique (CPEN) au niveau des Ministres, sur le thème « Impulser une relance et une croissance économique à long terme fondées sur un avenir numérique de confiance, durable et inclusif ».

Accès légitime des pouvoirs publics fondé sur des valeurs communes

NOUS RAPPELONS notre engagement conjoint à défendre la démocratie et l'état de droit, protéger la vie privée et les autres droits et libertés des personnes, promouvoir la libre circulation des données dans des conditions de confiance au sein de l'économie numérique, et veiller au maintien d'un internet mondial, ouvert, accessible, interconnecté, interopérable, fiable et sûr.

NOUS RECONNAISSONS que la transformation numérique à l'œuvre entraîne la création de volumes croissants de données, notamment de données à caractère personnel, dans la mesure où les technologies qui la sous-tendent sont utilisées dans tous les secteurs de l'économie mondiale.

NOUS RECONNAISSONS EN OUTRE que les données jouent un rôle central dans le fonctionnement de nos sociétés et nos économies, et que les flux transfrontières de données sous-tendent les échanges internationaux et le commerce mondial, ainsi que la coopération et le développement économiques, contribuent grandement à l'innovation, à la recherche et au développement dans les différents secteurs ; et sont essentiels à la conduite des entreprises et la réalisation des objectifs économiques et sociétaux.

NOUS RAPPELONS l'existence de la Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de 1980, révisée pour la dernière fois en 2013 [[OECD/LEGAL/0188](#)] (ci-après dénommée les « Lignes directrices de l'OCDE sur la protection de la vie privée »), qui constitue une référence commune fondamentale pour la protection des données à caractère personnel, dans les secteurs public comme privé, et a pour objet de promouvoir et faciliter les flux transfrontières de données à caractère personnel tout en défendant les valeurs démocratiques, l'état de droit et la protection de la vie privée et des autres droits et libertés des personnes.

NOUS RECONNAISSONS le devoir et la responsabilité souverains de chaque pays de protéger la sécurité de sa population en s'attachant à prévenir, détecter et gérer les activités criminelles et les menaces à l'ordre public et à la sécurité nationale, dans le respect des valeurs démocratiques, de l'état de droit, de la vie privée et des autres droits et libertés fondamentaux des personnes.

NOUS SOMMES CONSCIENTS que l'accès des pouvoirs publics aux données à caractère personnel détenues par des entités du secteur privé est reconnu dans nos cadres juridiques nationaux comme essentiel pour assumer lesdits devoirs et responsabilités souverains, et que les autorités chargées de faire respecter l'application des lois et de défendre la sécurité nationale sont par conséquent investies des pouvoirs d'accéder légalement à ces données.

NOUS REJETONS toute approche de l'accès des pouvoirs publics aux données à caractère personnel détenues par des entités du secteur privé qui, indépendamment du contexte, contrevient aux valeurs démocratiques et à l'état de droit, et est libre de contrainte, déraisonnable, arbitraire ou disproportionnée. De telles approches portent atteinte à la vie privée et aux autres des autres droits et libertés fondamentaux des personnes, enfreignent les obligations internationales, sapent la confiance et font obstacle aux flux de données, nuisant par là même à l'économie mondiale. À l'inverse, l'approche de nos pays en matière d'accès des pouvoirs publics s'inscrit dans le respect des valeurs démocratiques ; des garanties de

protection de la vie privée et des autres des autres droits et libertés fondamentaux des personnes ; et de l'état de droit, avec un pouvoir judiciaire indépendant. Ces protections contribuent en outre à favoriser la confiance des entités du secteur privé tenues d'assumer leurs responsabilités dans ce cadre.

NOUS INSISTONS, au vu des dérogations aux Lignes directrices de l'OCDE sur la protection de la vie privée pour des raisons liées au respect de l'application des lois et de la sécurité nationale, sur l'importance de renforcer la confiance au travers d'une compréhension commune des protections que nos pays mettent en œuvre lorsqu'ils accèdent à des données à caractère personnel détenues par des entités du secteur privé dans de telles circonstances.

NOUS RECONNAISSONS que nos pratiques et garanties existantes à cet égard sont, non pas identiques, mais fondées sur des principes similaires reflétant un engagement conjoint à protéger la vie privée et les autres des autres droits et libertés fondamentaux des personnes.

NOUS PRENONS ACTE des appels des parties prenantes à poursuivre les travaux et les efforts pour identifier les garanties communes en place dans les Membres de l'OCDE pour protéger la vie privée et la liberté d'expression, et par là même promouvoir la confiance, dans le cadre de l'acquisition de données à caractère personnel disponibles sur le marché, de l'accès à des données à caractère personnel rendues publiques, et de la communication volontaire de données à caractère personnel par les autorités chargées de l'application des lois et de la sécurité nationale.

NOUS RÉITÉRONS notre ambition de parvenir à une compréhension commune, entre démocraties partageant une communauté de vues, des protections de la vie privée et des autres droits et libertés fondamentaux des personnes prévues dans le cadre de l'accès aux données à caractère personnel détenues par des entités du secteur privé à des fins de respect de l'et de sécurité nationale, afin d'étayer les efforts déployés pour promouvoir la libre circulation des données dans des conditions de confiance.

Favoriser la confiance dans les flux transfrontières de données

NOUS RÉAFFIRMONS notre engagement en faveur de la libre circulation des données dans des conditions de confiance donnant des assurances aux individus et aux entreprises lors des transferts de données à caractère personnel à l'échelle internationale.

NOUS CONSIDÉRONS les principes énoncés ci-après comme une expression importante de nos valeurs démocratiques communes et de notre engagement conjoint en faveur de l'état de droit, qui distinguent nos pays de ceux dans lesquels l'accès aux données à caractère personnel à des fins de respect de l'application des lois et de sécurité nationale contrevient aux valeurs démocratiques et à l'état de droit, est libre de contrainte, déraisonnable, arbitraire ou disproportionné, ou constitue une atteinte aux droits humains.

NOUS RECONNAISSONS que, lorsque nos cadres juridiques imposent d'assortir les flux transfrontières de données de garanties, nos pays considèrent la mise en œuvre effective de ces principes dans le pays de destination comme une contribution positive à la facilitation des flux transfrontières de données en application de ces règles.

Principes relatifs à l'accès des pouvoirs publics aux données à caractère personnel détenues par des entités du secteur privé

NOUS DÉCLARONS que les principes partagés suivants reflètent les points communs observés entre les législations et les pratiques existantes des Membres de l'OCDE. Ces principes :

- se complètent mutuellement dans la protection de la vie privée et des autres droits et libertés fondamentaux ;
- s'appliquent à l'accès des pouvoirs publics aux données à caractère personnel détenues ou contrôlées par des entités du secteur privé et au traitement de ces données par les pouvoirs

publics, à des fins de respect de l'application des lois et de défense de la sécurité nationale sur leurs territoires respectifs, dans le respect de leurs cadres juridiques nationaux, y compris dans les cas où les pays ont autorité, au titre de leurs cadres juridiques nationaux, pour obliger les entités du secteur privé à leur fournir les données lorsque lesdites entités ou les données ne sont pas localisées sur leur territoire national (ci-après dénommé l'« accès des pouvoirs publics ») ;

- sont à interpréter à la lumière des cadres juridiques nationaux et pourraient être appliqués de diverses manières par les pays, selon le contexte et les conditions particulières, tels que le type d'accès visé ;
- doivent être interprétés au regard des définitions suivantes :
 - a) Les « données à caractère personnel » désignent toute information relative à une personne physique identifiée ou identifiable.
 - b) Le « cadre juridique » régissant l'accès des pouvoirs publics aux données à caractère personnel désigne les lois, les ordonnances ou décisions de justice, les règlements administratifs, la jurisprudence et les autres instruments juridiquement contraignants ou exigences à l'échelle nationale, y compris les obligations juridiques découlant du droit international et supranational applicables dans le pays.
 - c) Les « entités du secteur privé » désignent les personnes physiques et toute organisation non gouvernementale avec ou sans but lucratif.

Ces principes sont les suivants :

I. Base légale

L'accès des pouvoirs publics aux données à caractère personnel détenues par des entités du secteur privé est prévu et régi par le cadre juridique du pays, qui s'impose aux autorités publiques et est adopté et mis en œuvre par des institutions établies démocratiquement et fonctionnant dans le respect de l'état de droit. Le cadre juridique énonce les finalités, les conditions, les limites et les garanties applicables à l'accès des pouvoirs publics, de sorte que les individus bénéficient d'une protection suffisante contre le risque d'utilisation impropre et abusive.

II. Finalités légitimes

L'accès des pouvoirs publics sert des finalités spécifiques et légitimes. Les pouvoirs publics accèdent aux données uniquement dans l'optique de ces finalités, dans le respect de l'état de droit. L'accès des pouvoirs publics se fait dans des conditions qui ne sont pas excessives au regard des finalités légitimes et obéit aux normes juridiques de nécessité, de proportionnalité, de caractère raisonnable et aux autres normes relatives à la protection contre le risque d'utilisation impropre et abusive, conformément aux dispositions du cadre juridique du pays et à l'interprétation qui en est faite.

Les pouvoirs publics ne cherchent pas à accéder aux données à caractère personnel dans le but de supprimer les critiques ou contestations ou d'y faire obstacle ; ou pour désavantager des personnes ou des groupes sur la seule base de caractéristiques comprenant, entre autres : l'âge, le handicap mental ou physique, l'origine ethnique, le statut d'autochtone, l'identité ou l'expression de genre, l'orientation sexuelle, ou l'appartenance politique ou religieuse.

III. Autorisations

L'accès des pouvoirs publics est soumis à des obligations d'autorisation préalable (« autorisation ») prévues dans le cadre juridique afin de garantir que cet accès se fait dans le respect des normes, règles et procédures applicables. Ces obligations sont proportionnées au degré d'interférence avec la vie privée et les autres droits et libertés fondamentaux des personnes découlant dudit accès. Les dispositions afférentes énoncent les critères de demande et d'obtention de l'autorisation, la procédure à suivre et l'entité chargée de l'autorisation.

Les obligations sont d'autant plus strictes que l'interférence est élevée et peuvent aller jusqu'à l'exigence d'obtenir l'autorisation d'autorités judiciaires ou d'organismes extra-judiciaires impartiaux. Des dérogations d'urgence aux obligations d'autorisation sont prévues par le cadre juridique et clairement définies, assorties des motifs de d'octroi de l'autorisation, des conditions d'application, et de leur durée de validité.

Les décisions relatives aux autorisations sont dûment documentées. Elles sont prises de manière objective, sur la base d'éléments factuels, dans un but précis et légitime, avec l'assurance que les conditions requises sont effectivement remplies.

Si l'autorisation n'est pas requise, d'autres garanties prévues dans le cadre juridique s'appliquent pour prévenir tout risque d'utilisation inappropriée ou abusive, notamment des règles claires énonçant des conditions ou des restrictions d'accès, ainsi qu'une surveillance effective.

IV. Traitement des données

Les données à caractère personnel acquises dans le cadre de l'accès des pouvoirs publics ne peuvent être traitées et gérées que par le personnel autorisé. Ces activités de traitement et de gestion sont soumises à des obligations prévues dans le cadre juridique, y incluses la mise en place de mesures physiques, techniques et administratives permettant de préserver la vie privée, la sécurité, la confidentialité et l'intégrité des données. Elles sont également assorties de mécanismes garantissant que le traitement des données à caractère personnel est légitime, que leur durée de conservation ne dépasse pas celle autorisée dans le cadre juridique au regard de la finalité visée et du caractère plus ou moins sensible qu'elles revêtent, et qu'elles restent exactes et tenues à jour de manière appropriée au vu du contexte du traitement.

Des contrôles internes sont mis en place afin de détecter, prévenir et gérer les pertes de données, ou l'accès aux données, la destruction, l'utilisation, la modification ou la divulgation de données non autorisés ou accidentels, et d'en rendre compte aux organes de surveillance.

V. Transparence

Le cadre juridique général régissant l'accès des pouvoirs publics aux données est clair et facilement accessible, de manière à ce que les individus soient en mesure d'évaluer les incidences qu'il peut avoir sur leur vie privée et leurs autres droits et libertés.

Des mécanismes garantissent la transparence sur l'accès des pouvoirs publics aux données à caractère personnel ; ils concilient l'intérêt des individus et le droit du public à être informé, et la nécessité d'éviter la divulgation d'informations susceptibles de nuire aux activités liées à la sécurité nationale ou à l'application des lois.

Ces mécanismes incluent des rapports publics des organes de surveillance sur le respect, par les administrations, des obligations légales, ainsi que des procédures de demande d'accès aux enregistrements publics. À cela s'ajoutent d'autres mesures telles que des rapports réguliers par les pouvoirs publics et, le cas échéant, des notifications individuelles.

Les entités du secteur privé sont autorisées à publier des rapports statistiques agrégés sur les demandes d'accès des pouvoirs publics en conformité avec le cadre juridique.

VI. Mécanismes de contrôle

Des mécanismes de contrôle effectifs et impartiaux sont mis en place aux fins de garantir que l'accès des pouvoirs publics est conforme aux dispositions du cadre juridique.

Le contrôle est assuré par des organes tels que des bureaux de conformité internes, des tribunaux, des commissions parlementaires ou législatives, ou des autorités administratives indépendantes.

Les dispositifs de contrôle des pays comprennent des organes, qui agissent selon leur mandat et sont notamment habilités à obtenir et examiner les informations pertinentes, mener des enquêtes ou des recherches, réaliser des audits, dialoguer avec les entités publiques sur la conformité et les mesures d'atténuation, et traiter les cas de non-conformité. Par ailleurs, ces organes reçoivent des rapports de non-conformité et y répondent, de manière à veiller à ce que les entités publiques en soient responsables ; ils peuvent également assumer des fonctions de gestion des plaintes des individus.

Dans l'exercice de leurs fonctions, les organes de contrôle sont protégés contre toute ingérence et disposent des ressources financières, humaines et techniques nécessaires pour mener à bien leur mission. Ils documentent leurs conclusions, établissent des rapports et formulent des recommandations, qui sont rendus publics dans toute la mesure du possible.

VII. Recours

Le cadre juridique garantit aux individus des possibilités de recours judiciaires et extrajudiciaires effectifs afin de déterminer les atteintes au cadre juridique national et le cas échéant d'y remédier.

Ces mécanismes tiennent compte de la nécessité de préserver la confidentialité des activités liées à la sécurité nationale et au respect de l'application des lois. Ils peuvent ainsi prévoir des restrictions quant à la possibilité d'informer les personnes physiques de l'accès aux données qui les concernent ou d'une éventuelle violation.

Les mesures correctrices peuvent aller, selon les conditions applicables, de la suspension de l'accès à la suppression des données indûment consultées ou conservées, en passant par le rétablissement de l'intégrité des données ou l'arrêt du traitement illégitime. Dans certains cas, les individus concernés peuvent également recevoir une indemnisation pour les préjudices subis.

NOUS SALUONS les travaux de l'OCDE sur la libre circulation des données dans des conditions de confiance et **NOUS APPELONS** l'Organisation à soutenir les pays dans la promotion de la présente Déclaration.

À propos de l'OCDE

L'OCDE est un forum unique en son genre où les gouvernements œuvrent ensemble pour relever les défis économiques, sociaux et environnementaux que pose la mondialisation. L'OCDE est aussi à l'avant-garde des efforts entrepris pour comprendre les évolutions du monde actuel et les préoccupations qu'elles font naître. Elle aide les gouvernements à faire face à des situations nouvelles en examinant des thèmes tels que le gouvernement d'entreprise, l'économie de l'information et les défis posés par le vieillissement de la population. L'Organisation offre aux gouvernements un cadre leur permettant de comparer leurs expériences en matière de politiques, de chercher des réponses à des problèmes communs, d'identifier les bonnes pratiques et de travailler à la coordination des politiques nationales et internationales.

Les pays Membres de l'OCDE sont : l'Allemagne, l'Australie, l'Autriche, la Belgique, le Canada, le Chili, la Colombie, la Corée, le Costa Rica, le Danemark, l'Espagne, l'Estonie, les États Unis, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Islande, Israël, l'Italie, le Japon, la Lettonie, la Lituanie, le Luxembourg, le Mexique, la Norvège, la Nouvelle Zélande, les Pays Bas, la Pologne, le Portugal, la République slovaque, la République tchèque, le Royaume-Uni, la Slovénie, la Suède, la Suisse et la Türkiye. L'Union européenne participe aux travaux de l'OCDE.

Instruments juridiques de l'OCDE

Environ 460 instruments juridiques de substance ont été développés dans le cadre de l'OCDE depuis sa création en 1961. Ces instruments comprennent les Actes de l'OCDE (les Décisions et Recommandations adoptées par le Conseil de l'OCDE conformément à la Convention relative à l'OCDE) et d'autres instruments juridiques développés dans le cadre de l'OCDE (notamment les Déclarations et les accords internationaux).

L'ensemble des instruments juridiques de substance de l'OCDE, qu'ils soient en vigueur ou abrogés, est répertorié dans le Recueil des instruments juridiques de l'OCDE. Ils sont présentés selon cinq catégories :

- Les **Décisions** sont adoptées par le Conseil et sont juridiquement contraignantes pour tous les Membres, à l'exception de ceux qui se sont abstenus au moment de leur adoption. Elles définissent des droits et des obligations spécifiques et peuvent prévoir des mécanismes de suivi de la mise en œuvre.
- Les **Recommandations** sont adoptées par le Conseil et n'ont pas une portée juridique obligatoire. Elles représentent un engagement politique vis-à-vis des principes qu'elles contiennent, il est attendu que les Adhérents feront tout leur possible pour les mettre en œuvre.
- Les **Documents finaux de substance** sont adoptés individuellement par les Adhérents indiqués plutôt que par un organe de l'OCDE et sont le résultat d'une réunion ministérielle, à haut niveau ou autre, tenue dans le cadre de l'Organisation. Ils énoncent habituellement des principes généraux ou des objectifs à long terme et ont un caractère solennel.
- Les **accords internationaux** sont négociés et conclus dans le cadre de l'Organisation. Ils sont juridiquement contraignants pour les parties.
- **Arrangement, accord/arrangement et autres** : plusieurs autres types d'instruments juridiques de substance ont été développés dans le cadre de l'OCDE au fil du temps, comme l'Arrangement sur les crédits à l'exportation bénéficiant d'un soutien public, l'Arrangement international sur les Principes à suivre dans les transports maritimes et les Recommandations du Comité d'aide au développement (CAD).