OPPORTUNITÉS ▪ INNOVATION

Le règlement sur les marchés numériques (DMA)

Un guide concis pour les challengers technologiques

Qu'est-ce que le règlement sur les marchés numériques (DMA)?

Le règlement sur les marchés numériques (DMA, « Digital Markets Act ») est un règlement adopté par l'Union européenne en vue de créer des **opportunités en termes d'innovation** dans le secteur numérique en Europe. À cette fin, il impose diverses obligations aux grandes plateformes numériques connues sous le terme de « contrôleurs d'accès », au bénéfice des entreprises utilisatrices et des consommateurs.

Les obligations imposées par le DMA visent à :

- réduire les barrières à l'entrée et à l'expansion pour les challengers numériques, **augmentant ainsi la contestabilité du marché**. Le DMA encourage la concurrence directe entre les plateformes numériques (*concurrence interplateformes*), par exemple entre les différents moteurs de recherche ou entre les différents réseaux sociaux. Le DMA ouvre également les plateformes numériques existantes à la concurrence à différents niveaux de la chaîne de valeur (*concurrence intraplateforme*), par exemple en **facilitant l'accès des développeurs d'applications aux systèmes d'exploitation ou aux boutiques d'applications**.
- **améliorer l'équité** des droits et obligations respectifs des contrôleurs d'accès et de leurs utilisateurs et mieux partager la valeur créée dans les écosystèmes numériques des contrôleurs d'accès. Le DMA veille à ce que les utilisateurs puissent tirer profit de leurs innovations et de leurs efforts et promeut une relation équilibrée entre les plateformes numériques et leurs utilisateurs. Par exemple, le DMA vise à **permettre aux développeurs d'applications d'avoir accès aux boutiques d'applications à des conditions équitables et raisonnables** ou de pouvoir mettre fin à leur relation avec les plateformes numériques (et/ou d'en changer) sans difficultés excessives.

Le DMA fait partie d'un cadre réglementaire complet relatif aux droits et principes numériques, qui comprend également le règlement sur les services numériques (DSA, Digital Services Act), le règlement sur les données et le règlement sur l'intelligence artificielle, visant à promouvoir une vision européenne de la transformation numérique afin de garantir que la technologie est au service des personnes et contribue à encourager une société ouverte, compétitive, démocratique et durable, conformément aux valeurs et aux droits fondamentaux européens.

La mise en œuvre effective du DMA dépend de la volonté et de la capacité des entreprises utilisant les services de plateforme des contrôleurs d'accès, c'est-à-dire les « utilisateurs professionnels », à signaler les manquements des contrôleurs d'accès à leurs obligations telles qu'elles découlent du DMA.

Comment fonctionne le DMA en pratique ?

Le DMA impose aux grands acteurs du secteur numérique, connus sous le nom de « contrôleurs d'accès », diverses obligations qui s'appliquent aux « services de plateforme essentiels ». À leur tour, ces obligations créent des opportunités pour les concurrents et les entreprises utilisatrices des services en question.

Les contrôleurs d'accès : qui sont-ils ?

Les contrôleurs d'accès sont les plus grandes plateformes numériques actives en Europe (et au-delà). La Commission européenne désigne les contrôleurs d'accès sur la base de trois critères cumulatifs : (1) leur poids important sur le marché européen, (2) leur position en tant que point d'accès important pour atteindre les utilisateurs européens et (3) leur position solide et durable.

Pour faciliter la désignation, une plateforme est présumée rencontrer ces critères et être un contrôleur d'accès lorsqu'elle remplit trois critères :

- **Critère financier** : un chiffre d'affaires annuel dans l'Union européenne supérieur ou égal à 7,5 milliards d'euros au cours de chacun des trois derniers exercices ou une capitalisation boursière moyenne (ou juste valeur marchande équivalente) d'au moins 75 milliards d'euros au cours du dernier exercice ;
- **Critère géographique** : services fournis dans au moins trois États membres ;
- **Critère des utilisateurs** : service(s) de plateforme essentiel(s) utilisé(s) par au moins 45 millions d'utilisateurs finaux actifs par mois dans l'Union européenne (ce qui représente 10 % de la population européenne) et par au moins 10.000 entreprises utilisatrices actives par an dans l'Union européenne, au cours de chacun des trois derniers exercices.

La plateforme en question peut renverser ces présomptions de taille en démontrant que sa taille ne lui confère pas un pouvoir de contrôleur d'accès, car il existe d'autres voies pour atteindre les utilisateurs européens.

Inversement, à la suite d'une enquête de marché, la Commission européenne peut désigner comme contrôleurs d'accès des entreprises qui ne satisfont pas à chacun des seuils, mais qui satisfont néanmoins aux critères cumulatifs de présenter un poids important sur le marché, d'être un point d'accès majeur pour les utilisateurs et de jouir d'une position durable.

Qui sont les contrôleurs d'accès désignés ?

A ce jour, la Commission européenne a désigné sept grands opérateurs de plateformes numériques comme contrôleurs d'accès sur la base des seuils quantitatifs : Alphabet, Amazon, Apple, Booking, ByteDance, Meta et Microsoft.

Services de plateforme essentiels : de quoi s'agit-il ?

Le DMA réglemente certains services numériques qui ont « basculé » en faveur d'un nombre limité de fournisseurs en raison d'une combinaison de caractéristiques (économies d'échelle extrêmes, effets de réseau très importants, capacité de relier de nombreuses entreprises utilisatrices avec de nombreux utilisateurs finaux grâce au caractère multiface de ces services, degré considérable de dépendance des entreprises utilisatrices et des utilisateurs finaux, effets de verrouillage, absence de multihébergement par les utilisateurs finaux, intégration verticale et/ou avantages liés aux données, par exemple).

Le DMA a identifié **dix catégories de tels services numériques** qui sont désignés comme des « **services de plateforme essentiels** » soumis à diverses obligations et interdictions lorsqu'ils sont fournis par des plateformes désignées comme contrôleur d'accès. Ces services peuvent être regroupés au sein de quatre niveaux de la chaîne de valeur numérique : infrastructure, accès, applications et publicités en ligne.

Au niveau de l'infrastructure :

- **Systèmes d'exploitation** : « un logiciel système qui contrôle les fonctions de base du matériel informatique ou du logiciel et permet d'y faire fonctionner des applications logicielles ». **Exemples** : Google Android, Apple iOS ou Microsoft Windows.

- **Services d'informatique en nuage** : « services de la société de l'information qui permettent l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées ».

- **Assistants virtuels** : « un logiciel qui peut traiter des demandes, des tâches ou des questions, notamment celles fondées sur des données d'entrée sonores, visuelles ou écrites, de gestes ou de mouvements, et qui, sur la base de ces demandes, tâches ou questions, donne accès à d'autres services ou contrôle des appareils connectés physiques. »

Au niveau de l'accès :

- **Services d'intermédiation B2C en ligne** : « les services de la société de l'information qui permettent (i) aux entreprises utilisatrices d'offrir des biens ou services aux consommateurs, en vue de (ii) faciliter l'engagement de transactions directes entre ces entreprises utilisatrices et des consommateurs, que ces transactions soient finalement conclues hors ligne, en ligne ou pas du tout et (iii) qui sont fournis aux entreprises utilisatrices sur la base de relations contractuelles entre la plateforme et l'entreprise utilisatrice. » Il s'agit notamment de ce qui suit :

  - **boutiques d'applications** : « services d'intermédiation en ligne qui se concentrent sur les applications logicielles en tant que produit ou service intermédié ». **Exemples** : Apple App store ou Google Play store;

  - **places de marché** : « services de la société de l'information qui permettent aux consommateurs et/ou aux professionnels de conclure des contrats de vente ou de service en ligne avec des professionnels soit sur le site internet de la place de marché en ligne, soit sur le site internet d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne. » **Exemples** : Amazon Marketplace ou Meta Marketplace.

- **Navigateurs internet** : « applications logicielles qui permettent aux utilisateurs finaux d'accéder à des contenus internet hébergés sur des serveurs connectés à des réseaux tels que l'internet, y compris les navigateurs internet autonomes, ainsi que les navigateurs internet intégrés ou inclus dans un logiciel ou équivalent, et d'interagir avec ces contenus ». **Exemples** : Apple's Safari ou Google Chrome.

Au niveau de l'application :

- **Moteurs de recherche en ligne** : « services de la société de l'information qui permettent aux utilisateurs de formuler des requêtes afin d'effectuer des recherches sur, en principe, tous les sites internet ou les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot-clé, d'une demande vocale, d'une expression ou d'une autre entrée, et qui renvoie des résultats dans quelque format que ce soit dans lesquels il est possible de trouver des informations en rapport avec le contenu demandé ». **Exemples** : Google Search.

- **Réseaux sociaux en ligne** : « plateformes permettant aux utilisateurs finaux de se connecter ainsi que de communiquer entre eux, de partager des contenus et de découvrir d'autres utilisateurs et d'autres contenus, sur plusieurs appareils et, en particulier, au moyen de conversations en ligne (chats), de publications (posts), de vidéos et de recommandations »'. **Exemples** : Facebook et Instagram de Meta, TikTok de ByteDance ou LinkedIn de Microsoft.

- **Services de plateformes de partage de vidéos** : « services ou fonctionnalité essentielle des services dont l'objet principal est la fourniture au grand public de programmes, de vidéos créées par l'utilisateur, ou des deux, qui ne relèvent pas de la responsabilité éditoriale du fournisseur de la plateforme et dont l'organisation est déterminée par le fournisseur ». - **Exemples** : YouTube de Google.

- **Services de communications interpersonnelles non fondés sur la numérotation** : « services qui permettent l'échange interpersonnel et interactif d'informations, via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires, et qui ne permettent pas la connexion aux ressources de numérotation attribuées publiquement ». **Exemples** : WhatsApp ou Facebook Messenger de Meta.

Au niveau de la publicité :

- Les **services de publicité** fournis par une entreprise qui met à disposition n'importe lequel des neuf services de plateforme essentiels énumérés ci-dessus, y compris tout réseau publicitaire, échange publicitaire et autre service d'intermédiation publicitaire. **Exemples** : Google AdX, Amazon Ad Server ou Meta Audience Network.

Dans ses décisions de désignation des contrôleurs d'accès, la Commission européenne a également identifié et délimité les services de plateforme essentiels des contrôleurs d'accès auxquels s'appliquent les obligations du DMA.

Tableau 1 : **Services de plateforme essentiels par contrôleur d'accès**

	Système d'exploitation	Intermédiation	Navigateur	Recherche	Réseau social	Partage de vidéos	App. de com.	Publicités
Alphabet	Android	Google Play Google Shopping Google Maps	Chrome	Google Search		YouTube		Google
Amazon		Amazon Marketplace						Amazon
Apple	iOS iPadOS	Apple Store	Safari					
Booking		Booking.com						
Byte Dance					TikTok			
Meta		Meta Marketplace			Facebook Instagram		WhatsApp Messenger	Meta
Microsoft	Window				LinkedIn			

Quelles sont les opportunités créées par le DMA ?

Afin d'ouvrir de nouvelles opportunités aux entreprises utilisatrices européennes et de déverrouiller l'innovation numérique dans l'Union européenne, le DMA impose une liste de choses à faire et à ne pas faire aux contrôleurs d'accès désignés en ce qui concerne leurs services de plateforme essentiels.

Ces obligations et interdictions peuvent être regroupées en quatre catégories : (i) empêcher les pratiques d'effet de levier anticoncurrentiel au sein des écosystèmes numériques des contrôleurs d'accès, (ii) réduire les barrières à l'entrée du côté de l'offre et ouvrir les plateformes et les données des contrôleurs d'accès, (iii) réduire les barrières à l'entrée du côté de la demande et faciliter le changement de plateforme pour l'utilisateur et le multihébergement et (iv) accroître la transparence dans la chaîne de valeur de la publicité en ligne.

(i) Empêcher les pratiques d'effet de levier anticoncurrentiel par les contrôleurs d'accès

Le premier groupe d'obligations imposées par le DMA vise à empêcher les contrôleurs d'accès de tirer parti de leur position de force sur un marché numérique ou dans un service numérique par rapport à d'autres services de ce type au sein de leurs propres écosystèmes. À cet égard, le DMA contient cinq grandes interdictions liées aux services et aux données :

- Il est interdit aux contrôleurs d'accès de **combiner les données à caractère personnel provenant de leurs propres services de plateforme essentiels avec des données provenant de tout autre de leurs services**, ou de tout service fourni par des tiers, **à moins que** ce choix précis ait été présenté à l'utilisateur final et que ce dernier ait donné son **consentement** (*Article 5.2*).
- Il est interdit aux contrôleurs d'accès de **regrouper différents services de plateforme essentiels désignés**, par exemple un système d'exploitation et une boutique d'applications ou un moteur de recherche (*Article 5.8*).

- Il est interdit aux contrôleurs d'accès de **regrouper leurs services de plateforme essentiels désignés avec leurs services d'identification, leur navigateur internet ou leurs services de paiement**, par exemple en contraignant l'utilisateur d'un système d'exploitation ou d'une boutique d'applications à utiliser le service d'identification du contrôleur d'accès (*Article 5.7*).

- Il est interdit aux contrôleurs d'accès d'**accorder un traitement plus favorable** à ses propres produits et services qu'aux services et produits de tiers concurrents (*Article 6.5*).

- Il est interdit aux contrôleurs d'accès d'**utiliser, en concurrence avec les entreprises utilisatrices, les données** (qui ne sont pas accessibles au public), **quelles qu'elles soient, qui sont générées ou fournies par ces entreprises utilisatrices** ou par leurs clients dans le cadre de leur utilisation des services de plateforme essentiels des contrôleurs d'accès (*Article 6.2*).

(ii) Ouvrir les plateformes et les données des contrôleurs d'accès

Le deuxième groupe d'obligations imposées par le DMA vise à ouvrir les plateformes des contrôleurs d'accès afin que les nouveaux développeurs d'applications et plateformes innovantes puissent se baser sur elles pour déployer leurs propres produits. À cet égard, le DMA contient quatre grandes obligations :

- Les contrôleurs d'accès sont tenus de **permettre le parachargement** et l'utilisation d'applications ou de boutiques d'applications de tiers utilisant ou interopérant avec leur système d'exploitation. Cette obligation permet l'accès aux applications ou boutiques d'applications de tiers par des moyens autres que les services de plateforme essentiels du contrôleur d'accès (*Article 6.4*).

- Les contrôleurs d'accès sont tenus de permettre aux entreprises utilisatrices et aux fournisseurs de services auxiliaires d'**accéder** aux mêmes caractéristiques que celles qu'ils utilisent dans leurs services de plateforme essentiels afin de fournir des services auxiliaires et d'**interopérer verticalement** avec ces mêmes caractéristiques (*Article 6.7*).

- Les contrôleurs d'accès sont tenus de donner **accès à leurs boutiques d'applications, moteurs de recherche et assistants virtuels** à des conditions équitables, raisonnables et non discriminatoires (*Article 6.12*).

- Les contrôleurs d'accès sont tenus de permettre une **interopérabilité horizontale** avec les fonctionnalités de base de leurs applications de communication (*Article 7*).

Les données étant devenues un élément clé de l'innovation numérique, le DMA ouvre également les données des contrôleurs d'accès :

- Les contrôleurs d'accès sont tenus d'**assurer gratuitement aux entreprises utilisatrices un accès effectif, de haute qualité, continu et en temps réel aux données** générées par ou dans le cadre de l'utilisation des services de plateforme essentiels par ces entreprises utilisatrices et par les utilisateurs finaux (*Article 6.10*).
- Les contrôleurs d'accès sont tenus de procurer à toute entreprise tierce fournissant des moteurs de recherche en ligne, à des conditions équitables, raisonnables et non discriminatoires, un accès aux données concernant les classements, requêtes, clics et vues en lien avec les recherches générées par les utilisateurs finaux sur leurs moteurs de recherche en ligne (*Article 6.11*).

(iii) Faciliter le changement de plateforme pour l'utilisateur et favoriser la mobilité

L'accès aux plateformes et aux données existantes ne suffit pas à déverrouiller l'innovation numérique. Les innovateurs numériques doivent également avoir accès à des utilisateurs qui ne sont pas liés aux contrôleurs d'accès existants. Le troisième groupe d'obligations imposées par le DMA augmente dès lors les possibilités pour les utilisateurs de passer d'une plateforme à l'autre ou de recourir au multihébergement sur plusieurs plateformes. Ces obligations augmentent en outre le choix et l'autonomie des utilisateurs européens. À cet égard, le DMA contient sept interdictions et obligations :

- Il est interdit aux contrôleurs d'accès d'**utiliser des clauses de parité de prix ou des mesures ayant un effet équivalent à parité**. Ils doivent donc permettre aux entreprises utilisatrices de proposer les mêmes services aux utilisateurs finaux à des conditions différentes de celles qui sont proposées par les services de plateforme essentiels (*Article 5.3*).
- Il est interdit aux contrôleurs d'accès d'utiliser des **clauses « anti-steering »**. Les contrôleurs d'accès doivent donc permettre aux entreprises utilisatrices de promouvoir des offres auprès des utilisateurs finaux acquis grâce aux services de plateforme essentiels et de conclure des contrats avec ces utilisateurs finaux, en utilisant ou non à cette fin les services de plateforme essentiels du contrôleur d'accès (*Article 5.4*).
- Il est interdit aux contrôleurs d'accès de recourir à des pratiques anti-désintermédiation. Les contrôleurs d'accès doivent donc permettre aux utilisateurs finaux, par l'intermédiaire de leurs services de plateforme essentiels, d'accéder à des contenus, abonnements, fonctionnalités ou autres éléments et de les utiliser en se servant des applications d'une entreprise utilisatrice, y compris lorsque les utilisateurs finaux ont acquis de tels éléments auprès de l'entreprise utilisatrice sans avoir recours aux services de plateforme essentiels du contrôleur d'accès (*Article 5.5*).
- Les contrôleurs d'accès sont tenus de **permettre aux utilisateurs finaux de désinstaller facilement** les applications préinstallées sur leurs services de plateforme essentiels et de modifier facilement les paramètres par défaut relatifs à des services de

plateforme essentiels spécifiques, notamment via l'utilisation d'écrans de choix (*Article 6.3*).

- Il est interdit aux contrôleurs d'accès de **restreindre techniquement** la capacité des utilisateurs finaux de **changer** d'applications logicielles et de services accessibles en utilisant leurs systèmes d'exploitation (*Article 6.6*).

- Il est interdit aux contrôleurs d'accès de **restreindre la possibilité des entreprises utilisatrices de se plaindre** et de faire part à toute autorité publique de tout problème lié aux pratiques des contrôleurs d'accès (*Article 5.6*).

- Il est interdit aux contrôleurs d'accès d'imposer des **conditions** ou des procédures **disproportionnées** de **résiliation** des services de plateforme essentiels (*Article 6.13*).

Compte tenu de l'importance des données, le DMA prévoit également que :

- Les contrôleurs d'accès sont tenus d'assurer la **portabilité** effective, continue et en temps réel **des données** générées par l'activité de l'entreprise utilisatrice ou de son utilisateur final, en particulier en facilitant l'exercice de cette portabilité des données par les utilisateurs finaux (*Article 6.9*).

(iv) Accroître la transparence dans la publicité en ligne

Le dernier groupe d'obligations imposées par le DMA accroît la transparence dans la chaîne de valeur de la publicité en ligne. La transparence peut réduire les pratiques anticoncurrentielles sur les marchés de la publicité en ligne et permettre aux autorités publiques de mieux lutter contre de telles pratiques. Le DMA impose deux grandes obligations en matière de transparence :

- Les contrôleurs d'accès sont tenus de communiquer aux annonceurs en ligne et aux éditeurs des informations concernant le **prix payé par l'annonceur et la rémunération** perçue par l'éditeur (*Article 5.9 et 5.10*).

- Les contrôleurs d'accès sont tenus de fournir gratuitement aux annonceurs en ligne et aux éditeurs en ligne un accès à leurs outils de mesure de performance et aux données qui leur sont nécessaires pour effectuer leur propre vérification indépendante de l'inventaire publicitaire (*Article 6.8*).

Comment le DMA aide-t-il les entreprises utilisatrices à introduire des innovations sur le marché ?

Les obligations imposées par le DMA entraîneront des modifications des services de plateforme essentiels des contrôleurs d'accès, ce qui créera de nombreuses opportunités pour les entreprises utilisatrices de lancer des innovations sur les marchés numériques en Europe. Par exemple :

- L'obligation d'écrans de choix neutres facilite le déploiement de navigateurs et de moteurs de recherche innovants sur les smartphones, les tablettes et les ordinateurs.
- Les obligations de désintermédiation et d'interopérabilité facilitent la distribution de boutiques d'applications alternatives sur les smartphones Android et Apple ainsi que sur les ordinateurs Windows.
- Les dispositions relatives aux clauses anti-steering et au parachargement facilitent le déploiement d'applications, car elles réduisent la dépendance vis-à-vis des conditions des boutiques d'applications d'Apple et de Google.
- L'interdiction d'accorder un traitement plus favorable à ses propres produits et l'obligation de permettre aux entreprises utilisatrices d'accéder aux données facilitent le développement de places de marché alternatives.
- L'obligation de donner accès aux données générées par les clients sur les plateformes des contrôleurs d'accès (y compris aux mesures de performance et aux comportements des utilisateurs) permet aux entreprises en ligne de prendre des décisions plus éclairées.
- Les nombreuses obligations en matière d'accès aux données et de portabilité de celles-ci facilitent le développement de nouveaux services basés sur les données et de services de publicité en ligne.
- L'interopérabilité entre les applications de communication facilite la création de nouveaux services de messagerie.
- Le navigateur est le point d'accès vers le web. Les challengers technologiques doivent être en mesure d'exercer librement leurs activités sur la base d'une interopérabilité d'accès aux logiciels, produits et services, à la fois au sein et entre sites web, et d'accéder aux données lorsqu'il existe un déficit de données, comme par exemple en ce qui concerne les identifiants publicitaires, et ce afin de garantir l'équité des conditions de concurrence dans les services publicitaires.

La mise en œuvre du DMA est un processus dynamique : **des opportunités plus nombreuses et plus intéressantes émergeront** à l'avenir. Pour l'instant, les contrôleurs d'accès désignés en septembre 2023 ont fait part des modifications apportées à leurs services dans leurs rapports de conformité. Les principales modifications, présentées dans le tableau en annexe, concernent ce qui suit :

- Mécanismes de consentement des utilisateurs de lier les données et les services au sein des écosystèmes des contrôleurs d'accès ;
- Possibilité pour les développeurs de boutiques d'applications et d'applications d'accéder plus facilement aux plateformes et aux utilisateurs de smartphones Apple et Android ;
- Nouvelles possibilités d'accès des entreprises utilisatrices aux données qu'elles ont générées sur les plateformes des contrôleurs d'accès ;
- Nouveaux écrans de choix du navigateur et du moteur de recherche proposés aux utilisateurs finaux ;
- Nouvelles possibilités pour les utilisateurs finaux de transférer leurs données en dehors des écosystèmes des contrôleurs ;
- Nouvelles informations pour les annonceurs en ligne afin de comprendre le prix et la performance de leurs campagnes.

Ces modifications font actuellement l'objet d'une évaluation par la Commission européenne afin de déterminer si elles sont suffisantes afin de garantir de façon effective la contestabilité et l'équité des marchés numériques européens. Si la Commission détermine que les changements en question ne sont pas suffisants, elle a la possibilité d'engager des **actions en non-conformité**. A ce jour, la Commission européenne a initié de telles actions à l'encontre de certains contrôleurs d'accès (par exemple, contre Alphabet concernant l'interdiction des dispositions anti-steering et du traitement plus favorable accordé à ses propres produits, Apple concernant l'obligation de choix de l'utilisateur et l'interdiction des dispositions anti-steering ou Meta concernant son nouveau modèle « payer ou consentir », par exemple) et a en outre pris des **mesures d'investigation** pour s'enquérir des problèmes rencontrés par les entreprises utilisatrices (Amazon concernant l'interdiction du traitement plus favorable accordé à ses propres produits et Apple concernant la nouvelle structure tarifaire pour accéder à son App Store).

Il est donc possible que certains contrôleurs d'accès soient amenés à modifier davantage leurs offres de services pour se conformer de façon effective au DMA.

Comment le DMA est-il mis en œuvre et appliqué ?

Le succès du DMA dans le déverrouillage des opportunités et des innovations sur les marchés numériques dépendra de l'efficacité de son application et de sa mise en œuvre. À cette fin, le DMA a mis en place un système sophistiqué de **conformité et d'application**, dirigé par la Commission européenne avec le soutien des autorités nationales (de la concurrence), des tribunaux nationaux, des contrôleurs d'accès eux-mêmes, de leurs entreprises et de leurs utilisateurs finaux, ainsi que des organisations de la société civile.

Commission européenne

Comme le DMA régit des entreprises internationales qui sont généralement actives dans tous les États membres de l'Union européenne, la Commission européenne est le principal régulateur chargé de son application. Elle peut adopter des décisions afin de :

- **Désigner** des contrôleurs d'accès en ce qui concerne les services de plateforme essentiels, qui sont alors soumis aux obligations du DMA ;
- **Spécifier** et clarifier le contenu des obligations imposées par le DMA ;
- **Surveiller** de près le respect du DMA par les contrôleurs d'accès ;
- En cas de suspicion de non-respect, **ouvrir une enquête** à l'encontre du contrôleur d'accès en question, qui doit faire l'objet d'une décision dans un délai de 12 mois en principe ;
- Imposer des **mesures provisoires** en cas de risque de préjudice grave et irréparable pour les utilisateurs des contrôleurs d'accès ;
- Accepter les **engagements** des contrôleurs d'accès **en matière de conformité** ;
- **Sanctionner la non-conformité** par l'imposition d'amendes, par la modification des pratiques ou même, en cas de non-respect systématique, par des mesures correctives structurelles (cession ou scission d'actifs/de systèmes, par exemple).

Compte tenu de la grande asymétrie du partage d'informations par les contrôleurs d'accès, la Commission européenne dispose de **pouvoirs étendus pour recueillir des informations** en envoyant des demandes d'informations, en imposant des obligations de conservation, en menant des inspections dans les locaux des contrôleurs d'accès, en auditionnant les entreprises des contrôleurs d'accès et les utilisateurs finaux ou les organisations de la société civile, ainsi que les lanceurs d'alerte, de manière confidentielle.

Pour mener à bien ces tâches multiples et complexes, la Commission européenne a constitué une vaste équipe d'experts juridiques, économiques et techniques, mais compte également sur l'expertise externe des entreprises utilisatrices (et des utilisateurs finaux), de la société civile et du milieu universitaire.

Ateliers de la Commission européenne visant à renforcer le dialogue avec les utilisateurs des contrôleurs d'accès et les experts en vue d'une conformité effective au DMA

Pour atteindre les utilisateurs des contrôleurs d'accès, la société civile et le milieu universitaire, la Commission européenne a organisé deux séries d'ateliers ouverts. La première série, qui s'est tenue en 2023 alors que les contrôleurs d'accès préparaient leurs plans de conformité, a exploré les questions relatives à la mise en œuvre soulevées par certaines obligations du DMA. La deuxième série, qui a eu lieu en mars 2024 après les changements annoncés par les contrôleurs d'accès, s'est penchée sur l'efficacité de ces changements pour atteindre les objectifs du DMA.

Autorités nationales (de la concurrence)

Les autorités nationales ont un rôle important à jouer dans le soutien des efforts de la Commission européenne afin d'appliquer le règlement, car elles sont plus proches des innovateurs numériques locaux, qui sont les principaux bénéficiaires du DMA.

Les autorités nationales de la concurrence des États membres de l'Union européenne peuvent, selon des modalités différentes en fonction de la législation nationale, **recevoir des signaux** d'innovateurs locaux ou d'utilisateurs finaux faisant état de problèmes concernant d'éventuels cas de non-conformité au DMA. A l'issue d'une évaluation préliminaire ou après enquête plus poussée, l'autorité nationale de la concurrence peut transmettre les informations pertinentes à la Commission européenne pour suite à donner. Les autorités nationales de la concurrence peuvent également assister la Commission européenne dans le contrôle de conformité et la conduite d'enquêtes de marché en conduisant des inspections ou des entretiens, en recueillant et communiquant des informations en sa possession ou obtenues auprès de tiers, ainsi qu'en initiant ses propres mesures d'exécution qui seraient ensuite référées à la Commission européenne pour décision finale en vertu du DMA.

Tribunaux nationaux

Les tribunaux nationaux sont compétents pour faire appliquer le DMA dans une certaine mesure et peuvent entendre et juger les **actions en justice intentées contre les contrôleurs d'accès en cas de non-respect des obligations imposées par le DMA**. De telles actions en justice peuvent, par exemple, être intentées par une entreprise utilisatrice qui a constaté que l'interopérabilité offerte par les contrôleurs d'accès n'est pas suffisamment efficace pour atteindre les objectifs du DMA. Elles peuvent également être intentées par un utilisateur final ou même par un groupe d'utilisateurs finaux dans le cadre d'une action collective. Afin d'aider les tribunaux nationaux à trancher dans des affaires qui peuvent être complexes, la Commission européenne peut intervenir dans la procédure nationale en soumettant un avis d'expert (« amicus curiae ») aux juges nationaux.

Respect du règlement par les contrôleurs d'accès

Parallèlement aux autorités publiques, les contrôleurs d'accès et leurs utilisateurs ont aussi un rôle important à jouer dans l'application effective du DMA.

En vertu du DMA, **il incombe aux contrôleurs d'accès de démontrer qu'ils respectent** toutes les obligations applicables à leurs services. S'ils ne le font pas, ils peuvent faire l'objet d'une investigation et de sanctions pour non-conformité. C'est donc principalement aux contrôleurs d'accès qu'il revient de démontrer leur respect du règlement. Les contrôleurs d'accès doivent en outre désigner un responsable de la conformité spécifiquement chargé de veiller à l'application du DMA et à la coopération avec la Commission européenne. Ce **responsable de la conformité** doit être indépendant du personnel en charge des produits et rendre compte directement à la direction de son contrôleur d'accès.

Les contrôleurs d'accès doivent par ailleurs fournir à la Commission européenne des **rapports de conformité annuels** expliquant en détail les mesures contractuelles et techniques adoptées et envisagées en vue de la conformité au DMA, ainsi que des rapports sur la consultation des utilisateurs lors de la prise de décision concernant ces mesures et le suivi de leurs effets. Des versions non confidentielles de ces rapports de conformité sont disponibles sur le site internet de la Commission européenne afin de permettre aux utilisateurs, à la société civile et au grand public de contrôler la conformité au DMA.

Partenariat avec les entreprises et les utilisateurs finaux

Le DMA ne pourrait pas être appliqué efficacement sans l'avis et le soutien des entreprises et des utilisateurs finaux, qui interagissent directement avec les contrôleurs d'accès et sont les principaux bénéficiaires du DMA. Le DMA crée donc un **« partenariat » entre les autorités publiques et les utilisateurs existants ou potentiels** des contrôleurs d'accès, comme suit :

- Les utilisateurs ont accès aux rapports de conformité non confidentiels des contrôleurs d'accès, ce qui leur permet de comprendre ce qui a changé dans les services numériques concernés, pourquoi ces changements ont été apportés et quels en sont les effets.
- Si un utilisateur estime qu'un contrôleur d'accès ne respecte pas les obligations du DMA, il peut **soulever la question (également de manière anonyme) auprès de la Commission européenne ou de toute autorité nationale de la concurrence**. L'utilisateur peut également intenter une action en justice contre le contrôleur d'accès devant les tribunaux nationaux.
- Si la Commission européenne ou une autorité nationale suspecte un manquement à la conformité, elle peut ouvrir une enquête et **entendre les plaignants et d'autres utilisateurs**.
- La Commission européenne peut toujours entendre les utilisateurs avant de prendre une décision concernant l'application du DMA.

Où introduire une plainte en cas de non-conformité au règlement, et comment ?

Si vous êtes un utilisateur existant ou potentiel d'un service de plateforme essentiel d'un contrôleur d'accès et que vous suspectez le non-respect d'une ou de plusieurs obligations imposées par le DMA, vous disposez de différents moyens d'action :

- Signaler le problème auprès de la Commission européenne : EC-DMA@ec.europa.eu
- Signaler le problème ou déposer une plainte auprès de votre national competition authority
- Saisir les tribunaux nationaux

Sanctions en cas de non-conformité au règlement

Les manquements aux obligations imposées par le DMA peuvent donner lieu à d'**importantes sanctions financières, comportementales et structurelles**. En cas de non-conformité, la Commission européenne peut imposer ce qui suit :

- **Amendes** pouvant aller jusqu'à 10 % du chiffre d'affaires annuel mondial total du contrôleur d'accès ou jusqu'à 20 % en cas d'infractions répétées ;
- En cas d'infractions systématiques aux obligations imposées par le DMA, des **mesures correctives supplémentaires** peuvent être imposées aux contrôleurs d'accès après une enquête de marché. Ces mesures correctives doivent être proportionnelles, mais, si nécessaire et en dernier recours, des mesures non financières peuvent être imposées, notamment des mesures comportementales et structurelles, par exemple la cession de (parties de) l'entreprise.

En outre, lorsqu'un utilisateur (entreprise utilisatrice ou utilisateur final) subit une perte financière parce qu'un contrôleur d'accès n'a pas respecté les obligations imposées par le DMA, des **dommages et intérêts** peuvent être demandés devant un tribunal national.

Ressources pratiques supplémentaires

- Site internet de la Commission européenne sur le DMA : https://digital-markets-act.ec.europa.eu/index_en
- Décisions de la Commission européenne concernant la désignation des contrôleurs d'accès : https://digital-markets-act-cases.ec.europa.eu/search
- Rapports de conformité des contrôleurs d'accès : https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports
- Procédures de la Commission européenne en cas de non-conformité au DMA : https://digital-markets-act-cases.ec.europa.eu/search
- Outil d'alerte de la Commission européenne pour signaler un cas de non-conformité au DMA : https://digital-markets-act.ec.europa.eu/whistleblower-tool_en

Annexe : exemples de la manière dont la conformité au DMA a entraîné des modifications des services numériques en Europe

(sur la base des rapports de conformité originaux des contrôleurs d'accès et sujet à évaluation supplémentaire par la Commission européenne)

	Prévention de l'effet de levier anticoncurrentiel	Ouverture des plateformes et des données	Facilitation du changement de plateforme pour l'utilisateur et du multihébergement	Meilleure transparence des publicités en ligne
Alphabet	▸ Nouveaux paramètres pour l'obtention de consentements supplémentaires pour la liaison des services et des données de Google ▸ Nouvelles unités et nouveaux chips dédiés pour aider les utilisateurs à trouver des sites de comparaison dans des domaines tels que les vols, les hôtels et l'achat de produits	▸ Nouveaux outils pour les développeurs en vue du **parachargement** d'applications et de boutiques d'applications de tiers, de la facturation alternative et au choix de l'utilisateur et de programmes d'offres externes ▸ **Transparence** accrue **des données et des analyses** dans Play Console et Search Console, Merchant Center, Google Analytics, Google Ads et d'autres tableaux de bord et API	▸ Écrans de choix sur téléphone Android afin de changer de moteur de recherche et de navigateur ▸ Possibilités accrues de **partage** et de **portabilité** des données avec Google Takeout, l'Initiative de transfert des données et l'API de portabilité des données pour les développeurs	▸ Plus de **données pour les annonceurs**
Amazon	▸ Nouvelles **demandes de consentement pour le partage de données** entre les services d'Amazon ou pour l'utilisation des données à caractère personnel obtenues à partir de n'importe quel service d'Amazon ou de tiers afin de montrer des publicités personnalisées ▸ Nouveaux critères non discriminatoires qui déterminent l'« offre vedette » sur la page de détail du produit	▸ Nouveaux outils pour les développeurs en vue du **parachargement** d'applications et de boutiques d'applications de tiers, de la facturation alternative et au choix de l'utilisateur et de programmes d'offres externes ▸ **Transparence** accrue des données et des analyses dans Play Console et Search Console, Merchant Center, Google Analytics, Google Ads et d'autres tableaux de bord et API	▸ Nouveaux outils pour la **portabilité des données**	▸ Nouvelles données relatives aux prix et à la performance pour les clients publicitaires dans un environnement de données sécurisé dédié (salle blanche)

	Prévention de l'effet de levier anticoncurrentiel	Ouverture des plateformes et des données	Facilitation du changement de plateforme pour l'utilisateur et du multihébergement	Meilleure transparence des publicités en ligne
Apple		▸ **Modifications apportées à iOS** afin de permettre (i) de nouvelles options pour la distribution des applications iOS à partir de places de marché d'applications alternatives, (ii) **un nouveau cadre et de nouvelles API** pour la création de places de marché d'applications alternatives, (iii) de nouveaux cadres et nouvelles API pour des moteurs de navigateur alternatifs permettant aux développeurs d'utiliser d'autres moteurs de navigateur que WebKit, pour des applications de navigateur et des applications avec une expérience de navigation in-app, (iv) un **formulaire de demande d'interopérabilité** dans lequel les développeurs peuvent soumettre des demandes supplémentaires d'interopérabilité avec les caractéristiques matérielles et logicielles de l'iPhone et d'iOS. ▸ Nouvelles API permettant aux développeurs d'**utiliser la technologie NFC** dans leurs applications **bancaires et de porte-monnaie**. ▸ **Modifications dans les magasins d'applications** avec (i) de nouvelles options pour l'utilisation des fournisseurs de services de paiement dans l'application d'un développeur afin de **traiter les paiements** de biens et services numériques ; (ii) de nouvelles options de traitement des paiements via des liens permettant aux utilisateurs d'effectuer une transaction pour des biens et services numériques sur le site web externe du développeur et (iii) de nouveaux outils de planification d'entreprise permettant aux développeurs d'estimer les frais et de comprendre les mesures associées aux nouvelles conditions commerciales d'Apple pour les applications dans l'Union européenne. ▸ **Nouvelles conditions commerciales pour les applications iOS** avec (i) une commission réduite de 10 % ou 17 % sur les transactions relatives à des biens ou services numériques, (ii) 3 % supplémentaires de frais sur les frais de traitement des paiements et (iii) une Core Technology Fee de 0,50 € pour toute première installation d'une application par an au-delà d'un million de copies.	▸ **Nouvel écran de choix** dans Safari pour inviter les utilisateurs à choisir un navigateur par défaut parmi une liste d'options ▸ Extension de la **portabilité des données** sur le site « Données et confidentialité » d'Apple, où les utilisateurs de l'Union européenne peuvent récupérer de nouvelles données sur leur utilisation de l'App Store et les exporter vers un tiers autorisé.	

	Prévention de l'effet de levier anticoncurrentiel	Ouverture des plateformes et des données	Facilitation du changement de plateforme pour l'utilisateur et du multihébergement	Meilleure transparence des publicités en ligne
Byte Dance			▸ Nouvelle API de portabilité des données pour permettre aux développeurs enregistrés de demander aux utilisateurs l'autorisation de transférer une copie de leurs données TikTok, que ce soit une seule fois ou de manière récurrente. ▸ Amélioration de la vitesse et de la fonctionnalité de l'outil « Téléchargez vos données » qui permet aux comptes personnels et entreprises d'exporter et de télécharger des données de profil et des publications pertinentes ; ajout d'une fonctionnalité permettant aux utilisateurs de sélectionner les catégories de données qu'ils souhaitent exporter.	
Microsoft	▸ **Modifications du traitement des données dans Windows**, par exemple, les données collectées à partir de PC Windows relatives à des applications non-Microsoft fonctionnant sous Windows ne sont pas utilisées à des fins concurrentielles contre les fournisseurs de ces applications. ▸ Clarification des cas où Microsoft combine des données Windows avec des données provenant d'autres produits et services Microsoft et où le consentement des utilisateurs en vue de ces combinaisons de données est obtenu. ▸ Les utilisateurs de Windows **ne se connectent plus automatiquement** à d'autres produits Microsoft tels que Edge, Bing et le service « Start » de Microsoft	▸ Meilleure information des développeurs sur la manière de créer des fils d'actualité tiers sur le tableau des widgets Windows de la même manière que Microsoft Edge ▸ LinkedIn a déployé de nouveaux moyens pour les membres et les clients d'accéder à leurs données sur LinkedIn. Les membres de LinkedIn ont déjà la possibilité de télécharger une copie de leurs données via leurs paramètres ▸ Conception et mise en œuvre de nouvelles API pour les membres de LinkedIn et leurs développeurs tiers autorisés afin d'accéder, de manière continue, aux données qu'ils ont fournies sur LinkedIn ou qu'ils génèrent en exécutant des actions sur la plateforme.	▸ Remaniement du navigateur Edge et de la fonctionnalité de recherche en ligne Bing afin que les utilisateurs puissent **désinstaller** ces applications de Windows à l'aide des mécanismes standard de Windows disponibles pour la désinstallation ▸ Conception et mise en œuvre de nouvelles API permettant aux administrateurs de pages LinkedIn et à leurs développeurs tiers autorisés d'accéder : (1) aux données qu'ils ont fournies sur la plateforme LinkedIn ou générées lors de l'utilisation de LinkedIn et (2) aux données fournies ou générées par les membres de LinkedIn lors de leurs interactions avec les pages, sous réserve du consentement de ces membres.	▸ Permettre aux entreprises utilisatrices qui achètent des services de LinkedIn Marketing Solutions de travailler avec des partenaires de vérification publicitaire indépendants qui remplissent les conditions requises pour vérifier leur inventaire d'annonces à l'aide de l'API de vérification publicitaire.

	Prévention de l'effet de levier anticoncurrentiel	Opening platforms and data	Facilitation du changement de plateforme pour l'utilisateur et du multihébergement	Meilleure transparence des publicités en ligne
Meta			▸ **Options supplémentaires pour le partage de données sur les plateformes de Meta** (Facebook, Instagram, Messenger, Marketplace, Gaming) ▸ Nouveau choix pour les utilisateurs européens : utiliser Instagram et Facebook gratuitement avec des publicités ou s'abonner **pour ne plus voir de publicités** (modèle « payer ou consentir »).	

Une initiative de l'Autorité belge de la concurrence

Belgische Mededingingsautoriteit
Autorité belge de la Concurrence
Belgian Competition Authority

Avec les contributions du professeur **Alexandre de Streel** (UNamur) et de la professeure **Viktoria HSE Robertson** (WU Vienna)

Pour tout commentaire et demande de renseignements : DMA@bma-abc.be