



## DONNÉES

# Protection du patrimoine des entreprises dans le cadre des DGA DA EHDS



Dans cet article rédigé en l'état des projets de règlements européens au 20 janvier 2023, les auteures nous présentent le nouveau cadre juridique européen en cours de construction destiné à faciliter l'accès, le partage et la réutilisation responsable des données. La première partie porte sur le périmètre de la notion de donnée dans le règlement sur la gouvernance des données (DGA), le règlement sur les données (DA) et dans la proposition de règlement européen relatif à l'Espace européen des données de santé (EHDS) et la seconde partie est consacrée aux obligations relatives à la mise à disposition des données.

Dans cet article rédigé en l'état des projets de règlements européens au 20 janvier 2023, les auteures nous présentent le nouveau cadre juridique européen en cours de construction destiné à faciliter l'accès, le partage et la réutilisation responsable des données. La première partie publiée dans ce numéro porte sur le périmètre de la notion de donnée dans le règlement sur la gouvernance des données (DGA), Règlement (ou « loi ») sur les données (DA) et dans la proposition de règlement européen relatif à l'Espace européen des données de santé (EHDS). Le mois prochain paraîtra la seconde partie consacrée aux obligations relatives à la mise à disposition des données.

Présentée par la Commission européenne en février 2020, la stratégie européenne du marché unique numérique vise à faire de l'Europe un leader mondial de l'économie fondée sur les données. Dans ce but, le nouveau cadre juridique européen en cours de construction entend faciliter l'accès, le partage

et la réutilisation responsable des données dans le respect des valeurs de l'Union, notamment la protection des données personnelles. C'est à ce prix que les acteurs européens pourront rester engagés dans la course du commerce mondial, face à leurs concurrents américains ou chinois et développer des applications innovantes dans des secteurs stratégiques comme la santé, le spatial, les transports, l'énergie ou la banque. Au-delà, c'est bien la souveraineté numérique de l'Europe qui est en jeu, dans le cadre du plan d'actions annoncé par l'Union à l'horizon 2030.

La proposition de règlement sur la gouvernance des données (en anglais, « *Data Governance Act* » ou « *DGA* ») publiée en novembre 2020 par la Commission européenne, constitue le premier pilier de ce véritable arsenal en matière de données. Après un accord politique sur son contenu atteint en novembre 2021 entre le Conseil et le Parlement européens, le DGA a été définitivement adopté en mai 2022 et entrera en application en septembre 2023<sup>1</sup>.

## Quels objectifs pour le DGA ?

Selon la Commission européenne, les mesures envisagées par le *Data Governance Act* génèreraient 7 à 11 milliards d'euros de valeur par an au titre du seul échange de données, et 120 milliards d'économies par an dans le seul secteur de la santé.

Le DGA aura ainsi pour but de garantir l'accès à de grands volumes de données tout en garantissant un meilleur contrôle sur les données, le tout dans le but de la souveraineté numérique de l'UE<sup>2</sup>. Le DGA contient :

- des conseils et une assistance technique et juridique pour faciliter la réutilisation de certaines catégories de données protégées du secteur public (informations commerciales confidentielles, propriété intellectuelle, données personnelles) ;
- les modalités de fourniture et une certification obligatoire pour les prestataires de services d'intermédiation de données ;

## DOCTRINE

- le cadre dans lequel des acteurs pourront collecter et traiter des données à des fins altruistes et une certification facultative pour la réalisation de telles activités ;
- et prévoit la création d'un Comité européen de l'innovation dans le domaine des données.

Si le DGA vise à la fois les données personnelles et non personnelles, il exclut certaines catégories de données de son périmètre, notamment les données détenues par des entreprises publiques, les données détenues par des établissements culturels ou d'enseignement, les données protégées pour des raisons de sécurité publique, de défense ou de sécurité nationale ou les données dont la fourniture est une activité ne relevant pas d'une mission de service public.

### Le DA comme outil d'application du DGA

Alors que le DGA crée le cadre, les processus et les structures pour faciliter le partage des données, le Règlement (ou « loi ») sur les données (en anglais, « Data Act » ou « DA ») a pour vocation d'établir des règles harmonisées sur le partage et l'utilisation éthiques et responsables des données<sup>5</sup>. Plus particulièrement, le DA clarifie quels seront les acteurs pouvant accéder aux données et les utiliser – et donc les contrôler et en bénéficier – et quelles seront les conditions pour assurer une meilleure répartition de la valeur issue de leur utilisation.

### Quel est le périmètre du DA ?

La proposition DA harmonise les règles de partage et d'utilisation des données personnelles et non personnelles dans une série de situations<sup>6</sup> : entre entreprises, entreprises et organismes publics, par les individus, dans le contexte d'infrastructures de données telles que le cloud ou le edge computing, ou lorsque des données non personnelles sont transférées hors UE.

Ainsi, le DA s'appliquera et créera des obligations pour :

- les fabricants de produits connectés et les fournisseurs de services connexes commercialisés dans l'UE, ainsi que les utilisateurs de ces produits ou services ;

- les détenteurs de données qui mettent des données à la disposition de destinataires de données dans l'UE ;
- les destinataires de données dans l'UE auxquels les données sont mises à disposition ;
- les organismes du secteur public et les institutions, agences ou organes de l'UE qui demandent aux détenteurs de données de mettre des données à disposition en cas de besoin exceptionnel ;
- les fournisseurs de services de traitement des données (par exemple, le « cloud ») qui les proposent à leurs clients dans l'UE.

En principe, les micro et petites entreprises seraient exemptées des obligations liées à l'accès aux données et au partage des données en vertu de la proposition de Data Act. En pratique, ces obligations ne s'appliqueraient pas aux données générées par l'utilisation de produits fabriqués ou de services connexes fournis par ces micro ou petites entreprises<sup>5</sup>.

### Quels sont les objectifs spécifiques du DA ?

Le DA repose sur les principaux objectifs suivants :

- faciliter le partage entre entreprises (B2B) et avec le consommateur (B2C) des données, en rendant leur accès obligatoire lorsqu'elles proviennent d'objets connectés et services connexes, en contrepartie d'une compensation juste et équitable ;
- amener les entreprises privées à donner l'accès aux données aux organismes du secteur public en situation de besoin exceptionnel, pour l'exécution d'une mission de service public ;
- lutter contre l'imposition unilatérale aux PME de clauses contractuelles inéquitable sur le partage des données ;
- obliger les fournisseurs de services cloud et edge computing à garantir des conditions de changement de service (« switching ») simples pour leurs clients, notamment par la suppression progressive des frais liés à ce changement pour le consommateur ;
- mettre en place des garanties contre les accès illicites de gouvernements de pays tiers aux données

non-personnelles contenues dans le cloud ;

- prévoir l'élaboration de normes d'interopérabilité pour les données et leurs réutilisations entre les secteurs.

Publié par la Commission européenne le 23 février 2022, le DA est encore une proposition de règlement en cours d'examen par les colégislateurs de l'UE, le Conseil et le Parlement européens<sup>6</sup>.

### Vers un nouvel espace européen des données de santé

Dans la continuité de ces deux textes et au titre d'une première mise en œuvre sectorielle, la proposition de règlement européen relatif à l'Espace européen des données de santé (« European Health Data Space » ou « EHDS » en anglais) publiée le 3 mai 2022 est, elle aussi, en cours d'examen par les instances législatives européennes<sup>7</sup>. Il s'agit d'un premier espace de données en annonçant d'autres notamment dans la mobilité ou l'assurance.

L'EHDS permettra de créer un cadre pour le partage de données spécifiques à la santé en établissant des règles, normes et pratiques communes, une infrastructure et un cadre de gouvernance pour l'utilisation des données de santé électroniques des patients. L'objectif est, d'une part, d'améliorer la fourniture de soins de santé (usage primaire) et d'autre part, de soutenir la recherche, l'innovation, la sécurité des patients, l'élaboration de politiques, de statistiques ou de réglementations (usage secondaire).

### Distinction entre usage primaire et usage secondaire des données

Grâce à l'EHDS et dans le cadre de l'usage primaire, les citoyens auront un accès immédiat, gratuit et simplifié à leurs données de santé sous forme électronique.

Ils pourront facilement les partager avec différents professionnels de santé dans et entre les États membres de l'Union, afin d'améliorer la prestation de soins de santé qui leur seront rendus. Ils exerceront le contrôle sur leurs données. Une infrastructure numérique transfrontière (MyHealth@



EU) sera mise en place pour aider les patients à partager leurs données par-delà les frontières.

Dans le cadre de l'usage secondaire, l'EHDS créera également un cadre juridique pour améliorer l'utilisation des données de santé à des fins de recherche, d'innovation et d'élaboration de nouvelles politiques. Dans des conditions strictes et sous réserve d'autorisation, les chercheurs, les innovateurs, les institutions publiques ou les entreprises auront accès à de grandes quantités de données de santé de qualité élevée pour mettre au point de nouveaux produits, services et traitements, améliorer l'accès aux soins et rendre les systèmes de santé plus résilients.

### Quelle articulation entre les textes européens sur la donnée ?

Rappelons que le DGA et le DA sont conçus pour s'articuler avec le Digital Services Act (DSA)<sup>8</sup> et le Digital Market Act (DMA)<sup>9</sup>, deux textes majeurs visant respectivement à mettre en place un espace numérique plus sûr en protégeant les droits fondamentaux des utilisateurs et à encadrer la responsabilité des intermédiaires, en établissant et en garantissant des conditions de concurrence équitables sur le marché numérique.

Si les développements du présent article n'y sont pas consacrés, il est important de les avoir identifiés compte tenu de l'ampleur des obligations qu'ils contiennent et de leurs effets sur la gestion des données personnelles et les articulations qui devront être trouvées entre les différentes législations.

La pandémie de Covid-19 a démontré l'importance de la disponibilité des données personnelles et particulièrement des données de santé pour l'élaboration de politiques en réponse aux crises. Alors même que leur accès est particulièrement protégé pour veiller au respect de la vie privée des personnes concernées, ce contexte sanitaire a mis en lumière qu'il était impératif d'avoir un accès rapide à ces données, pour le traitement, mais aussi pour la recherche.

Les textes visés ci-dessus, que l'on désignera ensemble sous la formule « DGA, DA, EHDS », composent une sorte de triptyque, dont le contenu est encore en cours d'écriture

et de stabilisation. Si leur objectif est clair et aisé à comprendre, les moyens et conditions proposés pour y parvenir le sont moins, tandis qu'ils pourront avoir des impacts opérationnels et commerciaux significatifs pour les acteurs de terrain. Il est donc essentiel d'anticiper leur arrivée dans notre corpus juridique.

Dans cet objectif, l'attention mérite d'être portée sur les nouvelles obligations de mise à disposition des données générées par les produits connectés et services des entreprises et ce, potentiellement au profit de concurrents. En miroir, la question se pose du respect et de la valorisation de l'investissement dans la construction de bases de données et des droits de propriété qu'il peut générer.

En d'autres termes, comment assurer la protection du patrimoine des entreprises dans le cadre du nouvel arsenal « DGA DA EHDS » ? Cette question est d'autant plus prégnante que le Data Act interdit désormais le recours au régime juridique du droit sui generis de producteur de bases de données s'agissant des données générées par des objets connectés couverts par le texte. Elle engendre immédiatement celle de savoir comment va être assurée la régulation des nouveaux espaces de circulation consacrés aux données ? Nous partageons avec vous les quelques éléments de réflexion ci-après.

### Périmètre de la notion de données dans le triptyque DGA/DA/EHDS : de quoi parle-t-on ?

Les définitions sont déterminantes pour comprendre le champ d'application des nouveaux textes européens. Nous nous concentrons sur les notions de données et de données générées. D'autres définitions sont bien entendu également cruciales pour déterminer le champ d'application telles que celles relatives au « détenteur de données » et à « les utilisateurs des données » ou encore à la « réutilisation » et au « partage » de données.

#### La notion de données

Le DGA et le DA définissent ainsi le terme de « donnée » comme « toute représentation numérique d'actes, de faits ou d'informations et toute

compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels ».

Les « données à caractère personnel » désignent les données à caractère personnel au sens de l'article 4, point 1), du RGPD. Les « données à caractère non personnel » sont toutes les données autres que les données à caractère personnel.

Il est intéressant de noter que, de façon logique, le projet de règlement EHDS renvoie à la définition des données du RGPD pour la notion de « données de santé électroniques à caractère personnel » : il s'agit des « données concernant la santé et les données génétiques telles que définies dans le règlement (UE) 2016/679, ainsi que les données se rapportant aux déterminants de la santé, ou les données traitées dans le cadre de la prestation de services de soins de santé, qui existent sous forme électronique » ; les « données de santé électroniques à caractère non personnel » désignent « les données concernant la santé et les données génétiques sous forme électronique qui ne répondent pas à la définition des données à caractère personnel énoncée à l'article 4, point 1, du règlement (UE) 2016/679 [RGPD] ». La notion de « données de santé électroniques » permettra d'englober les données de santé électroniques à caractère personnel ou non personnel. Il faudra donc à l'avenir être prudent dans l'emploi de ces différentes notions qui ne recouvriront pas le même champ d'application.

En tout état de cause, la simple analyse des définitions montre l'importance de ces textes européens, qui vont avoir pour effet d'imposer le respect et la veille des règles concernant tout type de données, tout en tenant compte des règles spécifiques aux données personnelles et en leur sein, aux données personnelles de santé.

#### La notion de données générées

Une autre notion est largement employée par le DA mais insuffisamment définie ou tout au moins source de difficulté potentielle d'interprétation : celle de « données générées ».



## DOCTRINE

Le texte l'emploie pour désigner les données produites par l'utilisation de « produit » et « service connexe »<sup>10</sup>. Au stade de son élaboration, le Data Act ne donne pas de définition de ce que recouvre le terme. Il précise que les « données générées » par l'utilisation d'un produit ou d'un service connexe incluent les données enregistrées intentionnellement par l'utilisateur (considérant 17). Il ne s'agit pas de toutes les données circulant sur le marché. Il s'agirait des données enregistrées intentionnellement par l'utilisateur et les données générées en tant que sous-produit de l'action de l'utilisateur, telles que les données de diagnostic. Les données découlant de l'interaction entre l'utilisateur et le produit par l'intermédiaire d'un assistant virtuel entrent dans le champ d'application du projet de DA, tandis que les données produites par un assistant virtuel sans lien avec l'utilisation d'un produit n'en font pas partie<sup>11</sup>.

Pour autant et comme le soulignent les auteurs du rapport de la mission sur la réforme européenne du droit sui generis des bases de données du Conseil supérieur de la propriété littéraire et artistique (CSPLA)<sup>12</sup>, le même considérant 17 inclut, en dépit de l'absence d'intentionnalité, les données générées lorsque le produit est en « veille » ou éteint :

« Les données générées par l'utilisation d'un produit ou d'un service lié incluent les données enregistrées intentionnellement par l'utilisateur. De telles données comprennent également les données générées en tant que sous-produit de l'action de l'utilisateur, telles que les données de diagnostic, celles générées sans aucune action de la part de l'utilisateur, comme lorsque le produit est en "mode veille", et les données enregistrées pendant les périodes au cours desquelles le produit est éteint. (...) ».

Le critère de l'intentionnalité n'est pas repris dans le projet de règlement EHDS. Selon la proposition de règlement sur l'EHDS (Extrait du considérant 5) :

« Les données de santé électroniques concernent toutes les catégories de ces données, indépendamment du fait que ces données sont fournies par la personne concernée ou par d'autres

personnes physiques ou morales, telles que des professionnels de la santé, ou sont traitées en relation avec la santé ou le bien-être d'une personne physique, et devraient également inclure les données déduites et dérivées, telles que les diagnostics, les analyses et les examens médicaux, ainsi que les données observées et enregistrées par des moyens automatiques. »

Enfin, on peut s'interroger conjointement avec les auteurs du rapport précité sur l'absence de distinction faite entre données brutes et données valorisées au regard de la suppression, par le projet DA, de la protection par le droit sui generis des bases de données. Celui-ci ne pourrait plus trouver à s'appliquer selon l'article 35 du DA, aux bases de données contenant des données obtenues ou générées par l'utilisation d'un produit ou d'un service connexe. L'on pourrait dès lors imaginer que la donnée brute est bien celle générée automatiquement, sans « enrichissement », tandis que la donnée valorisée a fait l'objet d'un investissement, à condition de préciser cette notion discutable d'investissement, en tenant compte des pratiques et des enjeux des acteurs de l'innovation. Il est certain que ces notions mériteraient d'être plus approfondies au regard de la complexité et de la mixité des données présentes dans les bases de données constituées pour le fonctionnement des produits et services visés par le DA. Cette distinction serait déterminante pour veiller à la protection des intérêts des acteurs de l'innovation.

### Obligations relatives à la mise à disposition des données

Le chapitre II du DA définit les droits et obligations concernant l'accès et l'utilisation des données générées par l'utilisateur des produits ou de services connexes, qu'il soit ou non un consommateur. Ces règles ne s'appliquent pas aux données générées par l'utilisation de produits ou de services connexes fabriqués/fournis par des micros et petites entreprises (Article 7). Les articles 4 et 5 sont au cœur du DA pour faciliter l'accès et l'utilisation des données. D'autres articles viennent régir la mise à disposition des données au profit des organismes du secteur public

et institutions, agences ou organes de l'Union basés sur les besoins exceptionnels mais ils ne seront pas approfondis ici.

### Droits des utilisateurs à accéder aux données générées par l'utilisation de produits ou de services connexes et à les utiliser

L'obligation de mise à disposition des données dans le cadre d'une relation d'entreprise à entreprise (« B-to-B ») et d'entreprise à consommateur (« B-to-C »), est organisée à l'article 4 qui est consacré aux « Droits des utilisateurs à accéder aux données générées par l'utilisation de produits ou de services connexes et à les utiliser », notamment :

- l'utilisateur qui ne peut pas accéder directement à des données à partir du produit, peut exiger du détenteur de données de mettre à sa disposition les données générées par l'utilisation que cet utilisateur fait d'un produit ou d'un service connexe ;
- le détenteur de données ne peut utiliser les données à caractère non personnel générées par l'utilisation d'un produit ou d'un service connexe que dans le cadre d'un accord contractuel avec l'utilisateur.

D'autre part, l'article 5 vise à créer les conditions du « Droit de partager des données avec des tiers ». En particulier, le détenteur des données doit mettre à disposition d'un tiers les données générées par l'utilisation d'un produit ou d'un service connexe si l'utilisateur en fait la demande. Le détenteur de données ne conserve aucune information sur l'accès du tiers aux données demandées au-delà de ce qui est nécessaire à la bonne exécution de sa demande d'accès et à la sécurité et à la maintenance de l'infrastructure de données.

On notera que certaines conditions relèvent d'un rappel pédagogique à la loi existante. Leur efficacité dépendra vraisemblablement du contrôle qui sera mis en place. Par exemple, le projet de texte énonce que « le tiers s'abstient de déployer des moyens coercitifs ou d'abuser des lacunes manifestes de l'infrastructure technique du détenteur de données afin de protéger les données afin d'obtenir l'accès aux données ».