Les données

Willem, Pauline

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2024

Document Version
le PDF de l'éditeur

II. LES DONNÉES

A. Règlement (UE) 2022/868 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données – « Data Governance Act »)

Manon KNOCKAERT[61]

21. Introduction. Afin de concrétiser ses ambitions dans l'exploitation des données, l'Union européenne a récemment adopté le *Data Governance Act* (« DGA »)[62]. Ce nouveau règlement comporte quatre volets. Premièrement, le texte ambitionne d'accroître la réutilisation des informations du secteur public (« *open data* ») en visant un partage de données entre les organismes du secteur public et le secteur privé (G2B et G2C). Deuxièmement, le législateur européen entend réglementer les services de partage des données. Il veille ainsi à assurer la confiance dans le partage des données entre, d'une part, le citoyen et le secteur privé (C2B) et, d'autre part, entre les acteurs du secteur privé (B2B). Troisièmement, dans une optique d'altruisme, le DGA a pour objectif de permettre le partage des données du secteur privé vers le secteur public (B2G) et entre les acteurs du secteur privé (B2B). Quatrièmement et enfin, le texte créé un Comité européen de l'innovation dans le domaine des données[63].

22. Plan de la contribution. Au regard de la structure du DGA, la présente contribution propose, pour des raisons de clarté, une analyse du règlement « par pilier ». Dès lors, dans un premier temps, nous nous intéressons aux règles encadrant la réutilisation de certaines catégories particulières de données détenues par les organismes du secteur public, traditionnellement exclues de l'*open data* (voy. *infra*, n^os^ 24-37). Dans un deuxième temps, nous nous penchons sur les services d'intermédiation de données qui consacrent un véritable écosystème pour le partage des données (voy. *infra*, n^os^ 38-45). Enfin, nous analysons le cadre juridique donnant naissance à un altruisme en matière de données au sein de l'Union (voy. *infra*, n^os^ 46-53).

23. La notion de donnée. Soulignons d'ores et déjà que le législateur européen s'attelle à fournir une définition transversale de la notion de « données » en indiquant qu'elle recouvre « toute représentation numérique d'actes, de faits ou d'informations et toute compilation de

61 Chercheuse sénior et directrice de l'Unité de recherche « *Privacy & Data Protection* » au CRIDS/NaDI, Université de Namur.
Cette publication a été réalisée avec le soutien financier du projet d'excellence de la cybersécurité dans le cadre du plan de la Région wallonne (CyberWal) : Cyberexcellence financé par le Service Public de Wallonie sous la convention n° 2110186. La publication ne reflète que l'opinion de son auteure et la Région wallonne ne peut être tenue responsable de l'usage qui en serait fait.

62 Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), *J.O.*, L 152/1, 3 juin 2022 (ci-après « règlement (UE) 2022/868 sur la gouvernance des données »). Voy. également l'Exposé des motifs contenus dans la proposition législative (Proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données, 25 novembre 2020, COM(2020) 767 final).

63 Nous attirons l'attention du lecteur sur le fait que le Comité européen de l'innovation dans le domaine des données ne fera pas l'objet d'un commentaire dans le cadre de la présente contribution. Nous renvoyons aux articles 29 et suivants du DGA. Mentionnons toutefois que le Comité européen de l'innovation dans le domaine des données a notamment pour mission d'aider la Commission européenne dans l'élaboration de pratiques cohérentes au sein : i) des organismes du secteur public et des organismes compétents, ii) des autorités compétentes en matière de services d'intermédiation de données et iii) des autorités compétentes pour l'enregistrement des organisations altruistes. Pour la liste exhaustive des compétences du Comité, voy. l'article 30 du DGA.

ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels »[64].

1. Accroître la réutilisation des informations du secteur public

a. Contexte

24. La notion de réutilisation. Dans son premier volet, le DGA entend permettre la réutilisation de certaines catégories particulières de données détenues par les organismes du secteur public. Par réutilisation, il y a lieu de comprendre « l'utilisation, par des personnes physiques ou morales, de données détenues par des organismes du secteur public, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les données ont été produites, à l'exception de l'échange de données entre des organismes du secteur public aux seules fins de l'exercice de leur mission de service public »[65].

25. Un terme préexistant. En réalité, avec le DGA, le législateur européen renforce et complète une législation existante. En effet, dès 2003, l'Union européenne a publié son premier texte législatif ayant pour objectif d'encourager et de promouvoir la réutilisation des informations du secteur public, à savoir la directive 2003/98/CE[66]. Au lieu d'imposer l'ouverture, l'article 3 se contentait plutôt de l'encourager en laissant la mise à disposition effective des informations à la libre appréciation des organismes du secteur public[67]. Ce n'est que dix ans plus tard, par l'adoption de la directive modificative 2013/37/UE, que l'Union décide de durcir le ton en érigeant la réutilisation en une véritable obligation dans le chef des organismes du secteur public[68]. De surcroît, le principe d'ouverture est renforcé par des exigences techniques[69].

Le texte a fait l'objet d'une nouvelle refonte conséquente en 2019 avec l'adoption de la directive (UE) 2019/1024[70] dans l'objectif d'obliger les organismes du secteur public et, dans une

64 Règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 1.

65 Règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 2.

66 Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *J.O.C.E.*, L 345, 31 décembre 2003.

67 Directive 2003/98/CE, art. 3 : « les États membres veillent à ce que, lorsque la réutilisation de documents détenus par des organismes du secteur public est autorisée, ces documents puissent être réutilisés à des fins commerciales ou non commerciales ».

68 Directive (UE) 2013/37 du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public, *J.O.*, L 175, 27 juin 2013, art. 3. Pour une analyse du régime prévalant sous cette directive, voy. M. Knockaert, « La réutilisation des informations du secteur public : l'open data et les organismes publics », *J.T.*, 2018/27, n° 6739, pp. 613-621.

69 M. Knockaert, *op. cit.*, pp. 613 et s.

70 Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, *J.O.*, L 172, 16 juin 2019, (ci-après « directive (UE) 2019/1024 »). En droit belge, à l'exception du législateur fédéral, les textes de transposition ont été adoptés : Ordonnance du 10 décembre 2021 modifiant l'ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la directive 2019/1024/UE du Parlement européen et du Conseil du 20 juin 2019 (refonte) concernant les données ouvertes et la réutilisation des informations du secteur public, *M.B.*, 13 janvier 2022 ; Decreet van 2 juli 2021 tot wijziging van het Bestuursdecreet van 7 december 2018, *M.B.*, 8 juillet 2021 ; Dekret vom 28 Juni 2021 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, *M.B.*, 8 juillet 2021 ; décret de la Communauté française du 14 décembre 2022 relatif aux données ouvertes et à la réutilisation des informations du secteur public, *M.B.*, 17 février 2023, p. 23898 ; décret de la Région wallonne du 24 novembre 2022 relatif à la diffusion et à la réutilisation des informations du secteur public, *M.B.*, 29 décembre 2022.

moindre mesure, certaines entreprises publiques[71], à permettre la réutilisation de leurs informations tout en créant des régimes particuliers pour les données de la recherche, pour les données dynamiques et pour les ensembles de données de forte valeur[72].

b. Champ d'application

26. Champ d'application *rationae personae*. Le DGA vise les organismes du secteur public. Ils regroupent « l'État, les autorités régionales ou locales, les organismes de droit public ou les associations formées par une ou plusieurs de ces autorités ou un ou plusieurs de ces organismes de droit public »[73].

27. Champ d'application *rationae materiae*. En sus des informations soumises à la réutilisation par la directive (UE) 2019/1024, le DGA prévoit également une ouverture pour : i) les données protégées par une confidentialité commerciale, ii) les données protégées par un droit de propriété intellectuelle, iii) les données protégées par le secret statistique et iv) les données à caractère personnel[74]. Soulignons que ce nouveau texte n'a pas vocation à créer une véritable injonction, pour les organismes du secteur public, d'autoriser la réutilisation : le législateur a plutôt opté pour la mise en place d'un cadre légal afin d'inciter le partage des données[75]. Se calquant sur les obligations relatives à l'*open data*, le DGA rappelle que les conditions encadrant la réutilisation des données doivent être non discriminatoires, transparentes et proportionnées et qu'elles ne peuvent pas être utilisées pour restreindre la concurrence[76].

28. Exclusions. Le législateur européen exclut cinq catégories de données du champ d'application. Il s'agit : i) des données détenues par des entreprises publiques[77], ii) des données détenues

71 Voy. directive (UE) 2019/1024, art. 1, § 1, b). Sur le sujet de la directive (UE) 2019/1024 et son articulation avec le DGA, voy. M. Knockaert et A. Michel, « La Directive (UE) 2019/1024 et la réutilisation des informations du secteur public : un pas de plus vers un espace européen commun des données », *RTD eur.*, 2023/1, pp. 71 et s. ; M. Knockaert et A. Michel, « Le cadre européen de l'information environnementale : à la croisée des enjeux démocratiques, sociétaux et économiques », in H. Jacquemin et A. Lachapelle (dir.), *Numérique et développement durable : obstacles et opportunités pour le droit*, coll. du CRIDS, n° 54, Bruxelles, Larcier, 2023, pp. 369 et s.

72 Pour les ensembles de données de forte valeur, voy. le règlement d'exécution de la Commission européenne du 21 décembre 2022 établissant une liste d'ensembles de données de forte valeur spécifiques et les modalités de leur publication et de leur réutilisation, *J.O.*, L 19/43, 20 janvier 2023.

73 Règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 17. Les organismes de droit public sont définis comme étant « les organismes présentant les caractéristiques suivantes : a) ils ont été créés pour satisfaire spécifiquement des besoins d'intérêt général et n'ont pas de caractère industriel ou commercial ; b) ils sont dotés de la personnalité juridique ; c) ils sont financés majoritairement par l'État, les autorités régionales ou locales ou d'autres organismes de droit public, leur gestion est soumise à un contrôle de ces autorités ou organismes, ou leur organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les autorités régionales ou locales ou d'autres organismes de droit public » (voy. règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 18).

74 Règlement sur la gouvernance des données, art. 3, § 1.

75 En effet, l'article 5 précise que « les organismes du secteur public qui sont compétents en vertu du droit national pour *octroyer ou refuser* l'accès aux fins de la réutilisation […] ». Nous soulignons.

76 Règlement (UE) 2022/868 sur la gouvernance des données, art. 5, § 2.

77 Le législateur définit l'entreprise publique comme « toute entreprise sur laquelle les organismes du secteur public peuvent exercer directement ou indirectement une influence dominante du fait de la propriété de l'entreprise, de la participation financière qu'ils y détiennent ou des règles qui la régissent ; aux fins de la présente définition, une influence dominante des organismes du secteur public sur l'entreprise est présumée dans tous les cas suivants lorsque ces organismes, directement ou indirectement : a) détiennent la majorité du capital souscrit de l'entreprise ;

par des radiodiffuseurs de service public et leurs filiales et par d'autres organismes ou leurs filiales pour l'accomplissement d'une mission de radiodiffusion de service public, iii) des données détenues par des établissements culturels et des établissements d'enseignement, iv) des données détenues par des organismes du secteur public qui sont protégées pour des raisons de sécurité publique, de défense ou de sécurité nationale et v) des données dont la fourniture est une activité qui ne relève pas de la mission de service public dévolue aux organismes du secteur public[78].

c. Principales exigences

29. Le respect du principe de minimisation contenu dans le RGPD. Après avoir rappelé l'importance pour les organismes du secteur public de disposer des ressources nécessaires à l'effectivité de la réglementation[79], le législateur de l'Union impose certaines exigences de nature technique et juridique à la réutilisation des données, en raison de leur caractère « sensible »[80].

Il peut ainsi être requis que les données à caractère personnel ouvertes à la réutilisation aient préalablement fait l'objet d'une anonymisation ou d'une pseudonymisation[81] par l'organisme du secteur public ou par « l'organisme compétent »[82]. Le considérant 7 du DGA indique qu'« il existe des techniques permettant d'effectuer des analyses dans les bases de données contenant des données à caractère personnel, notamment l'anonymisation, la confidentialité différentielle, la généralisation, la suppression et la randomisation, l'utilisation de données synthétiques ou des méthodes similaires, et d'autres méthodes de préservation de la vie privée à la pointe de la technologie, qui pourraient contribuer à un traitement des données plus respectueux de la vie privée ». À cet égard, le DGA instaure une interdiction de principe visant à empêcher toute réidentification des personnes concernées en imposant la mise en place de mesures techniques et opérationnelles nécessaires à la préservation de l'identité et, le cas échéant, oblige le réutilisateur à avertir

b) disposent de la majorité des voix attachées aux parts émises par l'entreprise ; c) peuvent désigner plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance de l'entreprise » (règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 19).

78 Règlement (UE) 2022/868 sur la gouvernance des données, art. 3, § 2.

79 Règlement (UE) 2022/868 sur la gouvernance des données, art. 5, § 1, al. 2.

80 Voy. art. 2, § 17, et 2, § 18, pour les acteurs du secteur public entrant dans le champ d'application de la réutilisation.

81 Le législateur de l'Union souligne également qu'« avant leur transmission, les données à caractère personnel devraient être anonymisées, afin d'empêcher l'identification des personnes concernées, et les données contenant des informations commerciales confidentielles devraient être modifiées de telle sorte qu'aucune information confidentielle ne soit divulguée. Dans le cas où la fourniture de données anonymisées ou modifiées ne permettrait pas de répondre aux besoins du réutilisateur, sous réserve de satisfaire à toutes les exigences découlant des articles 35 et 36 du règlement (UE) 2016/679 qui imposent d'effectuer une analyse d'impact relative à la protection des données et de consulter l'autorité de contrôle, et lorsqu'il a été constaté que les risques pour les droits et les intérêts des personnes concernées sont minimes, la réutilisation des données dans un environnement de traitement sécurisé, sur place ou à distance, pourrait être autorisée » (règlement (UE) 2022/868 sur la gouvernance des données, cons. 15). Le RGPD définit la pseudonymisation comme « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable » (règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.*, L 119, 4 mai 2016, art. 4, § 5).

82 Règlement (UE) 2022/868 sur la gouvernance des données, art. 5, § 3, a), i). Sur l'organisme compétent, voy. *infra*, n° 36.

l'organisme du secteur public en cas de violation de données permettant la réidentification des personnes concernées[83].

30. Une réutilisation contrôlée. La réglementation prévoit la possibilité de modifier, d'agréger ou de traiter les informations afin de permettre le contrôle de la divulgation lorsque sont en jeu des informations confidentielles, des contenus protégés par un droit de propriété intellectuelle ou par un secret d'affaires[84].

31. Un environnement de traitement sécurisé. Le législateur européen permet aux organismes du secteur public d'imposer, s'ils le souhaitent, que l'accès et la réutilisation des données se fassent par le biais d'un environnement de traitement sécurisé dont ils ont la maîtrise[85]. Il s'agit d'un « environnement physique ou virtuel et les moyens organisationnels pour garantir le respect du droit de l'Union, tel que le règlement (UE) 2016/679, en particulier en ce qui concerne les droits des personnes concernées, les droits de propriété intellectuelle, la confidentialité commerciale et le secret statistique, l'intégrité et l'accessibilité, ainsi que le respect du droit national applicable, et pour permettre à l'entité fournissant l'environnement de traitement sécurisé de déterminer et de surveiller toutes les opérations de traitement de données, notamment l'affichage, le stockage, le téléchargement et l'exportation de données et le calcul de données dérivées au moyen d'algorithmes de calcul »[86].

Le DGA marque sa préférence pour un accès à distance mais permet également aux organismes du secteur public de faire en sorte que l'utilisation de l'environnement de traitement sécurisé ait lieu *in situ*, lorsque l'accès à distance ne peut être permis sans porter atteinte aux droits et aux intérêts de tiers[87].

32. Un droit de regard de la part de l'organisme du secteur public. En cas de recours à un environnement de traitement sécurisé, le législateur prévoit que « l'organisme du secteur public se réserve le droit de vérifier le processus, les moyens et tout résultat du traitement de données effectué par le réutilisateur afin de préserver l'intégrité de la protection des données et se réserve le droit d'interdire l'utilisation des résultats qui contiennent des informations portant atteinte aux droits et aux intérêts de tiers »[88].

33. La confidentialité. Le DGA impose aussi aux organismes du secteur public de s'assurer que le candidat réutilisateur respecte la confidentialité en cas de divulgation d'information qui compromettrait les droits et les intérêts des tiers, malgré les garanties mises en place[89].

34. Le consentement comme « filet de sécurité ». Relevons que le DGA prévoit la possibilité pour les candidats réutilisateurs – non sans avoir fait l'objet de vives critiques[90] – de demander

83 Règlement (UE) 2022/868 sur la gouvernance des données, art. 5, § 5.

84 Règlement (UE) 2022/868 sur la gouvernance des données, art. 5, § 3, a), ii).

85 Règlement (UE) 2022/868 sur la gouvernance des données, art. 5, § 3, b).

86 Règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 20.

87 Règlement (UE) 2022/868 sur la gouvernance des données, art. 5, § 3, c).

88 Règlement (UE) 2022/868 sur la gouvernance des données, art. 5, § 4. Le législateur précise que la décision d'interdiction d'utilisation des résultats doit être transparente et compréhensible pour le candidat réutilisateur.

89 Règlement (UE) 2022/868 sur la gouvernance des données, art. 5, § 5.

90 Dans leur avis conjoint, le Comité européen de la protection des données et le Contrôleur européen de la protection des données avaient alerté le législateur sur la qualité d'un tel consentement (voy. EDPB et CEPD, Avis conjoint 03/2021 sur la proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), version 1.1, pt 82).

aux organismes du secteur public leur aide dans l'obtention du consentement des personnes concernées à la réutilisation de leurs données à caractère personnel[91]. En effet, renvoyant à la définition du terme « consentement » consacrée par le RGPD[92], l'article 5, paragraphe 6, du DGA dispose que « lorsqu'il est impossible d'autoriser la réutilisation des données en respectant les obligations prévues aux paragraphes 3 et 4 du présent article et qu'il n'existe pas de base juridique pour la transmission des données au titre du règlement (UE) 2016/679, l'organisme du secteur public met tout en œuvre, conformément au droit de l'Union et au droit national, pour aider les réutilisateurs potentiels à demander le consentement des personnes concernées ou l'autorisation des détenteurs de données dont les droits et intérêts peuvent être affectés par cette réutilisation, lorsque cela est faisable sans charge disproportionnée pour l'organisme du secteur public »[93].

35. Délai de traitement de la demande de réutilisation. Les organismes du secteur public disposent de deux mois pour répondre, favorablement ou défavorablement, à une demande de réutilisation. Ce délai peut être prolongé de trente jours en cas de demande de réutilisation détaillée et complexe. Cette éventuelle prolongation doit être motivée auprès du candidat réutilisateur[94].

d. Mise en œuvre, exécution et sanctions

i. Les organismes compétents

36. Un appui aux organismes du secteur public. Chaque État membre doit instituer un « organisme compétent » ayant pour fonction principale d'aider les organismes du secteur public à se conformer à la réglementation et à accorder ou à refuser l'accès aux données[95]. Cet organisme compétent reçoit notamment les missions de fournir une assistance technique en mettant à disposition un environnement de traitement sécurisé, à proposer des orientations techniques et le soutien nécessaire pour assurer la confidentialité, l'intégrité et l'accessibilité des données, en particulier lorsqu'il s'agit d'anonymiser ou de pseudonymiser des données à caractère personnel[96].

91 Règlement (UE) 2022/868 sur la gouvernance des données, art. 5, § 6, et cons. 15.

92 Règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 5.

93 Règlement (UE) 2022/868 sur la gouvernance des données, art. 5, § 6.

94 Règlement (UE) 2022/868 sur la gouvernance des données, art. 9. Le législateur donne la possibilité aux États membres de fixer un délai plus court dans leur droit national.

95 Règlement (UE) 2022/868 sur la gouvernance des données, art. 7, § 1. Le législateur de l'Union précise que l'organisme compétent devrait agir sur instruction des organismes du secteur public (cons. 26).

96 Règlement (UE) 2022/868 sur la gouvernance des données, art. 7, § 4. Par ailleurs, ils pourraient recevoir la compétence, en droit national, d'octroyer eux-mêmes l'accès aux données (art. 7, § 2). Le considérant 26 indique également que « [c]es organismes compétents devraient fournir une assistance aux organismes du secteur public en recourant à des techniques de pointe, notamment en ce qui concerne la meilleure manière de structurer et de stocker les données en vue de les rendre facilement accessibles, en particulier au moyen d'interfaces de programmation d'applications, et de rendre les données interopérables, transférables et interrogeables, en tenant compte des meilleures pratiques en matière de traitement des données et de toutes les normes réglementaires et techniques existantes ainsi que des environnements sécurisés pour le traitement des données, qui permettent l'analyse des données d'une manière qui préserve le caractère privé des informations ».

ii. Les points d'information unique

37. Un appui aux réutilisateurs potentiels. Le DGA prévoit également la mise en place d'un point d'information unique au sein de chaque État membre[97]. Le législateur de l'Union précise son rôle en indiquant que « […] les modalités pratiques existantes, telles que les portails des données ouvertes, pourraient être utilisées. Le point d'information unique devrait disposer d'une liste de ressources comprenant un aperçu de toutes les ressources en données disponibles, y compris, le cas échéant, les ressources en données qui sont disponibles dans les points d'information sectoriels, régionaux ou locaux, ainsi que les informations pertinentes décrivant les données disponibles »[98].

2. Le service de partage de données

a. Contexte

38. Une stratégie pour le marché unique numérique. Constatant les potentialités liées au partage des données dans notre société du numérique, le législateur de l'Union reconnaît le besoin de légiférer en la matière. En effet, il met en exergue que « les services d'intermédiation de données sont appelés à jouer un rôle essentiel dans l'économie des données, notamment en soutenant et en promouvant les pratiques volontaires de partage de données entre les entreprises, ou en facilitant le partage de données dans le cadre des obligations fixées par le droit de l'Union ou le droit national. Ils pourraient devenir un outil facilitant l'échange de quantités substantielles de données pertinentes. […] Cela revêtira une importance particulière dans la perspective de la création d'espaces européens communs de données […] »[99].

b. Champ d'application

39. Un « partage »… Après s'être attaqué à la réutilisation de certaines catégories de données provenant du secteur public par le secteur privé ou par le citoyen, le règlement se donne également pour objectif d'encadrer le partage des données. La relation vise cette fois, d'une part, le citoyen et le secteur privé (C2B) et, d'autre part, les acteurs du secteur privé entre eux (B2B).

La notion de partage est définie comme « la fourniture de données à un utilisateur de données par une personne concernée ou un détenteur de données, en vue de l'utilisation conjointe ou individuelle desdites données, sur la base d'accords volontaires ou du droit de l'Union ou du droit national, directement ou via un intermédiaire, par exemple dans le cadre de licences ouvertes ou commerciales, moyennant le paiement d'une redevance ou gratuitement »[100].

40. … par « les services d'intermédiation de données ». Les services d'intermédiation de données sont définis comme « [des] service[s] qui vise[nt] à établir des relations commerciales à des fins de partage de données entre un nombre indéterminé de personnes concernées et de détenteurs de données, d'une part, et d'utilisateurs de données, d'autre part, par des moyens

97 Règlement (UE) 2022/868 sur la gouvernance des données, art. 8.
98 Règlement (UE) 2022/868 sur la gouvernance des données, cons. 26.
99 Règlement (UE) 2022/868 sur la gouvernance des données, cons. 27.
100 Règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 10.

techniques, juridiques ou autres, y compris aux fins de l'exercice des droits des personnes concernées en ce qui concerne les données à caractère personnel »[101].

Le DGA vise trois services d'intermédiation. Il s'agit : i) des services d'intermédiation entre les détenteurs de données[102] et les utilisateurs de données potentiels[103], ii) des services d'intermédiation entre soit les personnes concernées qui cherchent à mettre à disposition leurs données à caractère personnel ou soit les personnes physiques qui cherchent à mettre à disposition des données à caractère non personnel et les utilisateurs de données potentiels[104] et iii) des services de coopératives de données[105].

41. Exclusions. Partant, le législateur exclut expressément quatre catégories de services. Sont exclus du DGA : i) les « services qui obtiennent des données auprès des détenteurs de données et les agrègent, les enrichissent ou les transforment afin d'en accroître substantiellement la valeur et concèdent une licence d'utilisation des données résultantes aux utilisateurs de données, sans établir de relation commerciale directe entre les détenteurs de données et les utilisateurs de données »[106], ii) les services portant sur l'intermédiation de contenus protégés par le droit d'auteur, iii) les services « qui sont utilisés exclusivement par un seul détenteur de données pour lui permettre d'utiliser les données qu'il détient, ou qui sont utilisés par des personnes morales

101 Règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 11.

102 Dans un souci de différenciation avec les autorisations données par les personnes concernées au sens du RGPD, la notion de « détenteurs de données » est entendue comme « une personne morale, y compris des organismes du secteur public et des organisations internationales, ou une personne physique qui n'est pas une personne concernée pour ce qui est des données spécifiques considérées, qui, conformément au droit de l'Union ou au droit national applicable, a le droit d'octroyer l'accès à certaines données à caractère personnel ou non personnel » (règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 8).

103 Pour sa part, la notion d'« utilisateur de données » vise la « personne physique ou morale qui dispose d'un accès licite à certaines données à caractère personnel ou non personnel et qui a le droit, y compris au titre du règlement (UE) 2016/679 lorsqu'il s'agit de données à caractère personnel, d'utiliser ces données à des fins commerciales ou non commerciales » (règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 9). Le législateur indique que « ces services peuvent comprendre des échanges bilatéraux ou multilatéraux de données ou la création de plateformes ou de bases de données permettant l'échange ou l'utilisation conjointe de données, ainsi que la mise en place d'une autre infrastructure spécifique pour l'interconnexion des détenteurs de données avec les utilisateurs de données » (règlement (UE) 2022/868 sur la gouvernance des données, art. 10, a)).

104 Règlement (UE) 2022/868 sur la gouvernance des données, art. 10, b). À cet égard, le législateur relève que « [l]es prestataires de services qui proposent leurs services à des personnes concernées constituent une catégorie spécifique de prestataires de services d'intermédiation de données. Ces prestataires de services d'intermédiation de données cherchent à renforcer la capacité d'action des personnes concernées, et plus particulièrement le contrôle qu'exercent les personnes physiques sur les données les concernant. Ces prestataires devraient aider les personnes physiques à exercer leurs droits au titre du règlement (UE) 2016/679 […]. Dans ce contexte, il importe que le modèle commercial de ces prestataires garantisse qu'il n'existe pas d'incitations inadaptées poussant les personnes physiques à recourir à de tels services pour mettre à disposition, en vue d'un traitement, davantage de données les concernant qu'elles ne devraient le faire dans leur intérêt […] » (règlement (UE) 2022/868 sur la gouvernance des données, cons. 30).

105 Il s'agit des « services d'intermédiation de données proposés par une structure organisationnelle constituée de personnes concernées, d'entreprises unipersonnelles ou de PME qui sont membres de cette structure dont les objectifs principaux consistent à aider ses membres à exercer leurs droits à l'égard de certaines données, y compris quant au fait d'opérer des choix en connaissance de cause avant qu'ils ne consentent au traitement de données, à mener des échanges de vues sur les finalités et les conditions du traitement de données qui représenteraient le mieux les intérêts de ses membres en ce qui concerne leurs données, et à négocier les conditions et modalités du traitement des données au nom de ses membres avant que ceux-ci ne donnent l'autorisation de traiter des données à caractère non personnel ou ne donnent leur consentement au traitement de données à caractère personnel » (règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 15).

106 Règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 11, a).

multiples au sein d'un groupe fermé »[107] et iv) les services de partage proposés par des organismes du secteur public ne cherchant pas à nouer des relations commerciales[108].

c. Principales exigences

i. Exigence de neutralité

42. Les conditions d'octroi de la qualification. Le DGA n'impose pas moins de quinze conditions pour être valablement reconnu comme un service d'intermédiation de données. Nous pouvons notamment relever le fait : i) de poursuivre la seule finalité de mettre à disposition des données à des utilisateurs, ii) de maintenir une neutralité par rapport aux données échangées, empêchant ainsi le service d'intermédiation de pouvoir traiter les données pour son propre compte, iii) de mettre en place une procédure d'accès équitable, transparent et non discriminatoire, iv) d'assurer la sécurité du partage effectué, ou encore v) de faciliter et de garantir l'interopérabilité dans les échanges de données[109].

ii. Exigence de notification

43. Une notification avant le début des activités. Tout prestataire de services d'intermédiation de données est tenu de soumettre préalablement au commencement de ses activités une notification auprès de « l'autorité compétente »[110]. La Commission européenne a adopté le logo à disposition des services d'intermédiation de données attestant de leur qualification et de leur conformité au cadre légal[111]. Par ailleurs, si un prestataire de services d'intermédiation de données dispose d'établissements dans différents États membres, il doit alors relever de la compétence de l'État dans lequel il a son établissement principal[112].

d. Mise en œuvre, exécution et sanctions

44. Les demandes d'informations. Outre la réception et la gestion des notifications envoyées par les services d'intermédiation de données, les autorités compétentes désignées par chaque État membre[113] reçoivent également la compétence de contrôler le respect des obligations imposées par

107 Le législateur poursuit en précisant « y compris dans le cadre de relations de fournisseur ou de client ou de collaborations établies par contrat, en particulier ceux qui ont pour principal objectif de garantir les fonctionnalités d'objets et de dispositifs connectés à l'internet des objets » (règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 11, c)).

108 Règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 11.

109 Règlement (UE) 2022/868 sur la gouvernance des données, art. 11.

110 Règlement (UE) 2022/868 sur la gouvernance des données, art. 11, § 1, et art. 11, § 4. Cette notification doit comprendre une information sur : i) le nom du prestataire, ii) le statut juridique et le cas échéant son numéro d'enregistrement, iii) l'adresse de l'éventuel établissement principal du prestataire de services d'intermédiation de données dans l'Union et, le cas échéant, de toute succursale dans un autre État membre, ou l'adresse du représentant légal, iv) un site internet rendu accessible au public comprenant au minimum les informations susmentionnées, v) les coordonnées des personnes de contact et du prestataire, vi) la description du service qui doit également être indiquée sur le site internet du prestataire et vii) une estimation de la date de lancement de l'activité dans l'hypothèse où elle serait différente de la date de notification (art. 11, § 6). La réglementation précise qu'« un prestataire de services d'intermédiation de données qui n'est pas établi dans l'Union mais qui propose les services d'intermédiation de données […] dans l'Union désigne un représentant légal dans l'un des États membres où il propose lesdits services » (art. 11, § 3).

111 Règlement d'exécution (UE) 2023/1622 de la Commission du 9 août 2023 relatif à la conception de logos communs permettant d'identifier les prestataires de services d'intermédiation de données et les organisations altruistes en matière de données reconnus dans l'Union, *J.O.*, L 200/1, 10 août 2023.

112 Règlement (UE) 2022/868 sur la gouvernance des données, art. 11, § 2.

113 Règlement (UE) 2022/868 sur la gouvernance des données, art. 13.

le DGA[114]. À cette fin, elles doivent pouvoir demander au prestataire toutes les informations nécessaires, la demande d'informations devant être proportionnée et motivée[115]. En cas de constatation de manquement aux obligations imposées par le DGA, l'autorité compétente doit en avertir le prestataire qui dispose d'un délai de trente jours, à compter de la réception de la notification, pour s'expliquer[116].

45. Une large gamme de sanctions envers les services d'intermédiation de données. De surcroît, l'autorité compétente se voit reconnaître un panel de sanctions. Premièrement, elle peut imposer des sanctions financières qualifiées de dissuasives[117]. Deuxièmement, il est possible d'exiger du service d'intermédiation de données un report du lancement de son activité ou une suspension le temps de sa mise en conformité[118]. Troisièmement, face à des infractions graves ou répétées, l'autorité compétente peut exiger la cessation des activités lorsque, malgré la notification reçue, le prestataire du service d'intermédiation de données ne s'est pas conformé aux obligations imposées par le DGA[119]. Dans un tel scénario, sur demande de l'autorité compétente, la Commission européenne peut radier le prestataire du registre[120].

Notons que lorsque le prestataire de services d'intermédiation de données possède son établissement principal dans un État membre mais fournit des services dans un autre État membre, les autorités compétentes respectives doivent coopérer entre elles et se prêter assistance[121].

3. L'altruisme en matière de données

a. Contexte

46. Les données au service de l'intérêt général. Dans un espace européen commun des données en plein essor, le législateur de l'Union défend le besoin d'un cadre légal entourant le partage des données à des fins altruistes. Il argue que « pour atteindre des objectifs d'intérêt général, nombreuses sont les possibilités offertes par l'utilisation de données mises à disposition volontairement par les personnes concernées sur le fondement de leur consentement éclairé ou, lorsqu'il s'agit de données à caractère non personnel, mises à disposition par des détenteurs de données. Ces objectifs auraient trait notamment aux soins de santé, à la lutte contre le changement climatique, à l'amélioration de la mobilité, à la facilitation du développement, de la production et de la diffusion de statistiques officielles, à l'amélioration de la prestation de services publics ou à l'élaboration des politiques publiques. Le soutien à la recherche scientifique devrait également être considéré comme un objectif d'intérêt général. Le présent règlement devrait viser à contribuer à l'émergence de réserves de données d'une taille suffisante mises à disposition sur le fondement de l'altruisme en matière de données […] »[122].

114 Règlement (UE) 2022/868 sur la gouvernance des données, art. 14.
115 Règlement (UE) 2022/868 sur la gouvernance des données, art. 14, § 2.
116 Règlement (UE) 2022/868 sur la gouvernance des données, art. 14, § 3.
117 Règlement (UE) 2022/868 sur la gouvernance des données, art. 14, § 4, a).
118 Règlement (UE) 2022/868 sur la gouvernance des données, art. 14, § 4, b).
119 Règlement (UE) 2022/868 sur la gouvernance des données, art. 14, § 4, c).
120 Règlement (UE) 2022/868 sur la gouvernance des données, art. 14, § 4, al. 3.
121 Règlement (UE) 2022/868 sur la gouvernance des données, art. 14, § 7.
122 Règlement (UE) 2022/868 sur la gouvernance des données, cons. 45. Voy. également le rapport réalisé par Human Technology Foundation, « Le data altruisme : les données au service de l'intérêt général », disponible sur : https://www.human-technology-foundation.org/fr-news/rapport-data-altruisme.

b. Champ d'application

47. Notion d'altruiste des données. L'altruisme des données est défini comme « le partage volontaire de données fondé sur le consentement donné par les personnes concernées au traitement de données à caractère personnel les concernant, ou l'autorisation accordée par des détenteurs de données pour l'utilisation de leurs données à caractère non personnel sans demander ni recevoir de contrepartie qui aille au-delà de la compensation des coûts qu'ils supportent lorsqu'ils mettent à disposition leurs données, pour des objectifs d'intérêt général prévus par le droit national […] »[123].

48. Les conditions de reconnaissance. L'entité doit remplir cinq conditions qui lui permettront d'être valablement reconnue comme « organisation altruiste en matière de données »[124]. Ainsi, l'entité doit : i) mener des activités altruistes en matière de données, ii) être une personne morale constituée en vertu du droit national pour poursuivre des objectifs d'intérêt général, iii) être juridiquement indépendante de toute activité à but lucratif, iv) disposer d'une structure fonctionnelle permettant la séparation entre les activités altruistes et les autres activités et v) respecter l'ensemble des exigences adoptées par la Commission dans ses actes délégués[125].

c. Principales exigences

49. La préservation des intérêts des tiers. Outre les conditions imposées pour permettre à l'entité de bénéficier de la qualification d'organisation altruiste en matière de données, la réglementation met en place des exigences particulières afin d'assurer la préservation des droits et des intérêts des personnes concernées et des détenteurs de données[126]. Premièrement, l'organisation altruiste ne peut faire usage des données pour accomplir des objectifs autres que ceux d'intérêt général ayant permis d'obtenir le consentement de la personne concernée ou l'autorisation du détenteur des données. Deuxièmement, l'organisation altruiste ne peut pas recourir à des pratiques commerciales trompeuses pour obtenir les données[127]. Troisièmement, elle doit proposer des outils afin d'obtenir le consentement de la personne concernée ou l'autorisation du détenteur de données, cet outil devant permettre également un retrait aisé du consentement ou de l'autorisation[128]. Quatrièmement, un niveau de sécurité approprié pour le stockage et le traitement des données doit être assuré[129]. Cinquièmement, l'organisation altruiste doit informer sans délai toute violation de données[130]. Sixièmement et enfin, si l'organisation altruiste facilite le traitement de données par des tiers, elle doit en préciser la juridiction du pays[131].

123 Règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 16.

124 Règlement (UE) 2022/868 sur la gouvernance des données, art. 19.

125 Règlement (UE) 2022/868 sur la gouvernance des données, art. 18 et art. 22.

126 Règlement (UE) 2022/868 sur la gouvernance des données, art. 21. Pour rappel, la notion de « détenteur de données » est définie comme étant : « une personne morale, y compris des organismes du secteur public et des organisations internationales, ou une personne physique qui n'est pas une personne concernée pour ce qui est des données spécifiques considérées, qui, conformément au droit de l'Union ou au droit national applicable, a le droit d'octroyer l'accès à certaines données à caractère personnel ou non personnel » (règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 8).

127 Règlement (UE) 2022/868 sur la gouvernance des données, art. 21, § 2.

128 Règlement (UE) 2022/868 sur la gouvernance des données, art. 21, § 3.

129 Règlement (UE) 2022/868 sur la gouvernance des données, art. 21, § 4.

130 Règlement (UE) 2022/868 sur la gouvernance des données, art. 21, § 5. Le législateur indique en effet que « l'organisation altruiste en matière de données reconnue informe, sans retard, les détenteurs de données de tout transfert, de tout accès ou de toute utilisation non autorisés portant sur les données à caractère non personnel qu'elle a partagées ».

131 Règlement (UE) 2022/868 sur la gouvernance des données, art. 21, § 6.

50. Trois mécanismes de transparence. Premièrement, l'entité qualifiée d'organisation altruiste en matière de données doit tenir un registre complet et à jour reprenant les informations relatives aux personnes physiques ou morales ayant bénéficié du service fourni par l'organisation. Ces informations portent sur : i) leur identité, ii) la date ou la durée du traitement qu'elles ont effectué, iii) la finalité du traitement telle que définie par la personne physique ou morale ayant effectué le traitement et iv) les éventuelles redevances acquittées[132].

Deuxièmement, elle doit fournir annuellement à l'autorité compétente un rapport d'activité[133].

Troisièmement, une obligation d'information envers les détenteurs de données ou les personnes concernées doit être honorée avant le début de tout traitement de données. Le législateur de l'Union insiste sur l'importance d'un langage clair devant notamment permettre d'indiquer, les finalités d'intérêt général pour lesquelles le traitement des données a été autorisé et, le cas échéant, les traitements éventuels effectués en dehors de l'Union[134].

d. Mise en œuvre, exécution et sanctions

i. Un mécanisme d'enregistrement

51. Un enregistrement et des informations disponibles au public. Lorsque l'entité remplit les conditions pour être légalement qualifiée d'altruiste, elle bénéficie alors de la possibilité d'être enregistrée en tant qu'« organisation altruiste en matière de données » au sein de l'Union[135]. Le législateur européen énumère les informations devant être communiquées[136]. Soulignons que le nom de l'entité, son statut juridique, ses coordonnées ainsi que les personnes de contact et l'objectif d'intérêt général qu'elle poursuit sont des informations qui se retrouveront dans le registre public[137]. Le législateur prévoit en outre que le site internet de l'organisation altruiste doit informer sur les sources de revenus de l'entité[138]. Un mécanisme de reconnaissance mutuelle est mis en place, car le DGA prévoit que l'enregistrement, une fois effectué, est valable dans tous les États membres[139].

ii. L'autorité compétente

52. Le registre des organisations altruistes en matière de données. Chaque État membre doit désigner l'autorité compétente en matière d'altruisme de données[140]. À la compétence d'enregistrement s'ajoute la mission de tenir un registre des organisations altruistes qui, sur base

132 Règlement (UE) 2022/868 sur la gouvernance des données, art. 20, § 1.
133 Règlement (UE) 2022/868 sur la gouvernance des données, art. 20, § 2.
134 Règlement (UE) 2022/868 sur la gouvernance des données, art. 21, § 1.
135 Règlement (UE) 2022/868 sur la gouvernance des données, art. 19. Notons que le législateur prévoit que l'État membre compétent pour effectuer l'enregistrement d'une entité qui dispose de plusieurs établissements au sein de différents États membres, est celui du lieu de l'établissement principal (art. 19, § 2).
136 Règlement (UE) 2022/868 sur la gouvernance des données, art. 18.
137 Règlement (UE) 2022/868 sur la gouvernance des données, art. 19, § 6.
138 Règlement (UE) 2022/868 sur la gouvernance des données, art. 19, § 4, f).
139 Règlement (UE) 2022/868 sur la gouvernance des données, art. 19, § 5.
140 Sur les exigences relatives aux autorités compétentes, voy. l'article 26 de la réglementation. Relevons que le législateur de l'Union utilise le terme « autorité compétente » par distinction à la notion d'« organisme compétent » utilisée pour encadrer la réutilisation de certaines catégories particulières de données détenues par les organismes du secteur public.

volontaire, souhaitent être reconnues comme telle au sein de l'Union[141]. Ce registre est public et permet de recevoir le label « organisation altruiste en matière de données reconnue dans l'Union »[142]. La Commission européenne tient elle aussi un registre répertoriant l'ensemble des organisations altruistes reconnues au sein de l'Union[143].

53. Une autorité qui veille. De plus, les autorités compétentes reçoivent une mission de contrôle du respect de la réglementation[144]. À ce titre, elles disposent de la possibilité de demander les informations nécessaires et proportionnelles pour vérifier le respect par l'organisation altruiste des exigences imposées par le DGA[145]. Elles peuvent également signaler à l'organisation une infraction et exiger qu'elle y remédie dans un délai raisonnable[146]. Enfin, l'organisation peut également recevoir une interdiction, rendue publique, de continuer à utiliser le label « organisation altruiste en matière de données » et être radiée du registre public national et du registre européen[147].

4. Conclusion

54. Un constat de nécessité. Le législateur européen souligne que « la mise en place de règles et pratiques communes dans les États membres en ce qui concerne l'élaboration d'un cadre de gouvernance des données devrait contribuer à la réalisation [des] objectifs [de marché intérieur], dans le plein respect des droits fondamentaux. Elle devrait également garantir le renforcement de l'autonomie stratégique ouverte de l'Union tout en facilitant la libre circulation des données à l'échelle internationale »[148].

55. La place des données à caractère personnel dans la réutilisation et le partage. Force est de constater que tant les données à caractère personnel qu'à caractère non personnel sont au coeur de la stratégie européenne. En effet, le souhait de permettre une réutilisation des données à caractère personnel est désormais assumé. Si des garanties ont été mises en place dès la proposition législative, l'EDPB et le CEPD ont néanmoins appelé à une plus grande vigilance[149]. À cet

141 Règlement (UE) 2022/868 sur la gouvernance des données, art. 17, § 1. Voy. également le rapport réalisé par la Human Technology Foundation, « Le data altruisme : les données au service de l'intérêt général ». Disponible sur : https://www.human-technology-foundation.org/fr-news/rapport-data-altruisme.

142 Règlement (UE) 2022/868 sur la gouvernance des données, art. 17, § 2. Cette labellisation est accompagnée d'un logo conçu par la Commission. Voy. règlement d'exécution (UE) 2023/1622 de la Commission du 9 août 2023 relatif à la conception de logos communs permettant d'identifier les prestataires de services d'intermédiation de données et les organisations altruistes en matière de données reconnus dans l'Union, *J.O.*, L 200/1, 10 août 2023.

143 Règlement (UE) 2022/868 sur la gouvernance des données, art. 17, § 2.

144 Règlement (UE) 2022/868 sur la gouvernance des données, art. 24. Le législateur de l'Union prévoit également que ce contrôle peut être réalisé à la suite d'une demande formulée par une personne physique ou morale (art. 24, § 1). Sur le droit d'introduire une réclamation, voy. l'art. 27 de la réglementation.

145 Règlement (UE) 2022/868 sur la gouvernance des données, art. 24, § 2.

146 Règlement (UE) 2022/868 sur la gouvernance des données, art. 24, § 3, et art. 24, § 4.

147 Règlement (UE) 2022/868 sur la gouvernance des données, art. 24, § 5. Le législateur précise que « si une organisation altruiste en matière de données reconnue a son établissement principal ou son représentant légal dans un État membre mais qu'elle exerce des activités dans d'autres États membres, l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données de l'État membre où est situé l'établissement principal ou dans lequel se trouve le représentant légal et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données de ces autres États membres coopèrent et se prêtent assistance […] » (art. 24, § 6).

148 Règlement (UE) 2022/868 sur la gouvernance des données, cons. 1.

149 EDPB et CEPD, Avis conjoint 03/2021 sur la proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), version 1.1.

égard, les organismes du secteur public sont désormais amenés à une délicate articulation entre le RGPD, la réglementation relative à la réutilisation des informations du secteur public et le DGA. Les données à caractère personnel reçoivent également une attention particulière lorsqu'elles font l'objet du service de partage proposé par les services d'intermédiation de données. Ces derniers ont dorénavant la lourde responsabilité de remplir toutes les conditions nécessaires à l'obtention de la qualification de « services d'intermédiation de données » tout en assurant le respect des garanties offertes par le RGPD.

Enfin, les données à caractère personnel sont également au cœur des préoccupations du législateur de l'Union pour le partage des données à des fins altruistes. En témoigne la définition même de la notion d'« organisation altruiste en matière de données » qui vise notamment le « partage volontaire de données fondé sur le consentement donné par les personnes concernées au traitement de données à caractère personnel les concernant »[150].

56. Un pari pour l'avenir ? Dans leur avis conjoint, l'EDPB et le CEPD ont exprimé leurs réserves quant au DGA. Tout en « reconnaiss[ant] l'objectif légitime consistant à favoriser la disponibilité de données en vue de leur utilisation, en augmentant la confiance dans les intermédiaires de données et en renforçant les mécanismes de partage de données dans l'ensemble de l'Union », ils s'inquiètent d'une possible compatibilité entre les objectifs – certes louables – du législateur et la protection des données à caractère personnel[151].

B. Règlement (UE) 2023/2854 fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données – « *Data Act* »)

Chloé Antoine[152]

57. Introduction. Le règlement (UE) 2023/2854 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données)[153], plus connu sous son appellation en langue anglaise « *Data Act* », a été adopté le 13 décembre 2023.

1. Contexte, objectifs et articulation avec d'autres instruments

58. Contexte. À l'instar du *Data Governance Act*[154] (ci-après « DGA »), l'adoption du *Data Act* s'inscrit dans la stratégie européenne pour les données définie par la Commission européenne en 2020. Cette dernière a pour but d'établir « […] une approche globale de l'économie fondée sur les données qui vise à accroître l'utilisation et la demande de données et de produits et services fondés sur les données dans l'ensemble du marché unique […] »[155].

150 Règlement (UE) 2022/868 sur la gouvernance des données, art. 2, § 16.

151 EDPB et CEPD, Avis conjoint 03/2021 sur la proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), version 1.1, p. 9.

152 Chercheuse au CRIDS/NaDI (UNamur) et avocate au barreau de Namur.

153 Règlement (UE) 2023/2854 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données), *J.O.*, 22 décembre 2023.

154 Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), *J.O.*, L 152, 3 juin 2022.

155 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Une stratégie européenne pour les données », 19 février 2020, COM(2020) 66 final, p. 2.

59. Objectifs. Dans le cadre de cette stratégie européenne pour les données, le *Data Act* a pour objet d'établir des règles harmonisées relatives à :

(i) « […] la mise à disposition de données relatives au produit[156] [,] de données relatives au service connexe[157] [et de données relatives à l'assistant virtuel qui interagit avec un tel produit ou service[158] (ci-après « assistant virtuel »)] au profit de l'utilisateur du produit connecté ou du service connexe [ou de l'assistant virtuel] ;

(ii) […] la mise à disposition de données par les détenteurs de données au profit des destinataires de données ;

(iii) […] la mise à disposition de données par les détenteurs de données au profit d'organismes du secteur public, de la Commission, de la Banque centrale européenne [(ci-après « BCE »)] et d'organes de l'Union, lorsqu'il existe un besoin exceptionnel de disposer de ces données pour exécuter une mission spécifique d'intérêt public ;

(iv) […] la facilitation du changement de de [*sic*] service de traitement de données ;

(v) […] l'introduction de garanties contre l'accès illicite de tiers aux données à caractère non personnel ; et

(vi) […] le développement de normes d'interopérabilité pour les données auxquelles il doit être accédé, qui doivent être transférées et qui doivent être utilisées »[159].

Chacun de ces aspects fait l'objet d'une analyse au sein de la présente contribution, étant entendu qu'une attention particulière est portée aux exigences relatives au partage de données entre entreprises[160] et consommateurs[161] (« *business to consumer* » – *B2C*), entre entreprises (« *business to business* » – *B2B*) et entre entreprises et les organismes du secteur public[162], la Commission, la BCE et les organes de l'Union[163] (« *business to government* » – *B2G*). Ces exigences constituent

156 Les données relatives au produit sont définies comme « […] les données générées par l'utilisation d'un produit connecté que le fabricant a conçu pour qu'elles puissent être extraites, au moyen d'un service de communications électroniques, d'une connexion physique ou d'un dispositif d'accès intégré, par un utilisateur, un détenteur de données ou un tiers, y compris, le cas échéant, le fabricant » (règlement (UE) 2023/2854 sur les données, art. 2, 15)).

157 Les données relatives au service connexe sont définies comme « […] les données représentant la numérisation des actions de l'utilisateur ou des événements liés au produit connecté, enregistrées intentionnellement par l'utilisateur ou générées en tant que produit annexe de l'action de l'utilisateur lors de la fourniture d'un service connexe par le fournisseur » (règlement (UE) 2023/2854 sur les données, art. 2, 16)).

158 Il est important de souligner que toutes les références aux produits connectés et services connexes contenues dans le *Data Act* doivent s'entendre comme visant aussi les assistants virtuels qui interagissent avec un produit connecté ou un service connexe (règlement (UE) 2023/2854 sur les données, art. 1er, § 4). Nous adoptons la même approche au sein de la présente contribution.

159 Règlement (UE) 2023/2854 sur les données, art. 1er, § 1er.

160 Une entreprise est définie comme « […] une personne physique ou morale qui, en ce qui concerne les contrats et pratiques relevant du présent règlement, agit à des fins liées à son activité commerciale, industrielle, artisanale ou libérale » (règlement (UE) 2023/2854 sur les données, art. 2, 24)).

161 Un consommateur est défini comme « […] toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale » (règlement (UE) 2023/2854 sur les données, art. 2, 23)).

162 Les organismes du secteur public sont définis comme « […] les autorités nationales, régionales ou locales des États membres et les organismes de droit public des États membres ou les associations formées par une ou plusieurs de ces autorités ou un ou plusieurs de ces organismes » (règlement (UE) 2023/2854 sur les données, art. 2, 28)).

163 Les organes de l'Union sont définis comme « […] les organes et organismes de l'Union mis en place par ou en vertu des actes adoptés sur la base du traité sur l'Union européenne, du traité sur le fonctionnement de l'Union européenne ou du traité instituant la Communauté européenne de l'énergie atomique » (règlement (UE) 2023/2854 sur les données, art. 2, 27)).

selon nous l'apport majeur du *Data Act* eu égard à l'objectif poursuivi de développement d'une économie fondée sur les données.

60. Articulation avec la législation en matière de respect de la vie privée et de protection des données. Le *Data Act* prévoit expressément qu'il est sans préjudice de la législation nationale et de l'Union relative au respect de la vie privée, à la protection des données à caractère personnel, à la confidentialité des communications et à l'intégrité des équipements terminaux, et en particulier du règlement général sur la protection des données[164] (ci-après « RGPD »). Le *Data Act* précise encore que la législation de l'Union ou la législation nationale adoptée conformément au droit de l'Union en matière de protection de la vie privée ou des données à caractère personnel prévaut sur les dispositions du *Data Act* en cas de conflit[165].

61. Articulation avec le DGA et avec la directive *Open Data*[166]. Le DGA et la directive *Open Data* ne s'appliquent pas aux données mises à disposition des organismes du secteur public en cas de besoin exceptionnel conformément au chapitre V du *Data Act*[167].

62. Articulation avec la législation en matière de propriété intellectuelle. Le *Data Act* prévoit que, par principe, son application est sans préjudice de la législation de l'Union et nationale applicable en matière de propriété intellectuelle, en particulier les directives (UE) 2019/790, 2004/48/CE et 2001/29/CE[168]. Toutefois, en vue d'éliminer les potentiels obstacles à l'exercice, par les utilisateurs, de leurs droits d'accès et à la portabilité des données tels que consacrés par le *Data Act*[169], le règlement exclut expressément la protection du droit *sui generis* sur les bases de données[170] lorsque les données sont obtenues à partir de – ou générées par – un produit connecté, un service connexe ou un assistant virtuel relevant du champ d'application du *Data Act*[171]. Il convient par ailleurs de souligner qu'en ce qui concerne les demandes de mise à disposition de données formulées par les organismes du secteur public, la Commission, la BCE ou les organes de l'Union dans une situation de besoin exceptionnel[172], le considérant 71 du *Data Act* prévoit qu'en cas d'application du droit *sui generis* sur les bases de données aux jeux de données demandés, le détenteur de données devrait exercer son droit de manière à ne pas empêcher le demandeur d'obtenir les données ou de les partager.

63. Articulation avec la législation de l'Union en matière de protection des consommateurs. Le *Data Act* est un instrument qui a vocation à compléter la législation de l'Union en matière de protection des consommateurs et s'applique sans préjudice de cette législation[173].

---

164 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.*, L 119, 4 mai 2016.

165 Règlement (UE) 2023/2854 sur les données, art. 1er, § 5.

166 Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte), *J.O.*, L 172, 26 juin 2019.

167 Règlement (UE) 2023/2854 sur les données, art. 17, § 3.

168 Règlement (UE) 2023/2854 sur les données, art. 1er, § 8.

169 Voy. *infra*, nos 70 et s.

170 Voy. directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données, *J.O.C.E.*, L 77, 27 mars 1996, art. 7.

171 Règlement (UE) 2023/2854 sur les données, art. 43. Voy. ég. cons. 112.

172 Voy. *infra*, nos 92 et s.

173 Règlement (UE) 2023/2854 sur les données, art. 1er, § 9.

2. Champ d'application

64. Champ d'application personnel. Le *Data Act* s'applique : (i) aux fabricants de produits connectés, (ii) aux fournisseurs de services connexes et d'assistants virtuels, (iii) aux utilisateurs[174], (iv) aux détenteurs de données[175] qui mettent des données à disposition, (v) aux destinataires de données[176], (vi) aux organismes du secteur public, à la Commission, à la BCE et aux organes de l'Union, (vii) aux fournisseurs de services de traitement de données et (viii) « […] aux participants à des espaces de données et aux vendeurs d'applications utilisant des contrats intelligents et aux personnes dont l'activité commerciale, l'entreprise ou la profession implique le déploiement de contrats intelligents pour des tiers dans le cadre de l'exécution d'un accord »[177].

65. Champ d'application personnel : exclusions. L'application des obligations en matière de partage de données dans les relations entre entreprises (*B2B*) et entre entreprises et consommateurs (*B2C*) prévues au chapitre II du *Data Act* est exclue pour les microentreprises et les petites entreprises[178] sous certaines conditions[179] et pour les moyennes entreprises[180] qualifiées comme telles depuis moins d'un an[181]. Concernant le partage de données en cas de besoin exceptionnel (chap. V du *Data Act*), certaines obligations ne s'appliquent pas aux microentreprises et petites entreprises[182].

66. Champ d'application matériel. De manière générale, le *Data Act* a vocation à s'appliquer aux données, à savoir à « […] 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

174 L'utilisateur est défini comme : « […] une personne physique ou morale à laquelle appartient un produit connecté ou à laquelle des droits temporaires d'utilisation de ce produit connecté ont été cédés contractuellement, ou qui reçoit des services connexes » (règlement (UE) 2023/2854 sur les données, art. 2, 12)).

175 Le détenteur de données est défini comme « […] une personne physique ou morale qui, conformément au présent règlement, aux dispositions applicables du droit de l'Union ou à la législation nationale adoptée conformément au droit de l'Union, a le droit ou l'obligation d'utiliser et de mettre à disposition des données, y compris, lorsqu'il en a été convenu par contrat, des données relatives au produit ou des données relatives au service connexe qu'elle a extraites ou générées au cours de la fourniture d'un service connexe » (règlement (UE) 2023/2854 sur les données, art. 2, 13)).

176 Le destinataire de données est défini comme « […] une personne physique ou morale, autre que l'utilisateur d'un produit connecté ou d'un service connexe, agissant à des fins qui sont liées à son activité commerciale, industrielle, artisanale ou libérale, à la disposition duquel le détenteur de données met des données, y compris un tiers lorsque l'utilisateur a adressé une demande au détenteur de données ou conformément à une obligation légale découlant du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union » (règlement (UE) 2023/2854 sur les données, art. 2, 14)).

177 Règlement (UE) 2023/2854 sur les données, art. 1er, § 3.

178 Les microentreprises sont les entreprises occupant moins de 10 personnes et ayant un chiffre d'affaires annuel ou un bilan annuel de maximum 2 millions d'euros. Quant aux petites entreprises, il s'agit des entreprises occupant moins de 50 personnes et ayant un chiffre d'affaires annuel ou un total du bilan annuel n'excédant pas 10 millions d'euros (annexe à la recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises, C(2003) 1422, *J.O.*, L 124, 20 mai 2003, art. 2, §§ 2 et 3 – ci-après « recommandation de la Commission concernant la définition des PME »).

179 Les conditions sont les suivantes : les microentreprises et petites entreprises (i) n'ont, le cas échéant, que des entreprises partenaires ou des entreprises liées (au sens de l'article 3 de l'annexe à la recommandation de la Commission concernant la définition des PME) qui sont elles-mêmes considérées comme des microentreprises ou des petites entreprises et (ii) ne sont pas chargées en sous-traitance de la conception ou de la fabrication d'un produit connecté ou de la fourniture d'un service connexe (règlement (UE) 2023/2854 sur les données, art. 7, § 1er).

180 Les moyennes entreprises sont les entreprises qui occupent entre 50 et 249 personnes et qui ont soit un chiffre d'affaires annuel n'excédant pas 50 millions d'euros, soit un bilan annuel de maximum 43 millions d'euros (annexe à la recommandation de la Commission concernant la définition des PME, art. 2, §§ 1er et 2).

181 Par ailleurs, les obligations en matière de partage des données dans les relations *B2B* et *B2C* ne s'appliquent à l'égard des produits connectés qu'après un an suivant leur date de mise sur le marché s'ils sont mis sur le marché par une moyenne entreprise (règlement (UE) 2023/2854 sur les données, art. 7, § 1er, al. 2).

182 Voy. *infra*, n° 94.

sonores, visuels ou audiovisuels »[183]. Le règlement vise tant les données à caractère personnel[184] que les données à caractère non personnel[185].

Plus précisément, les données tombant dans le champ d'application du *Data Act* sont les suivantes :

(i) les données[186], à l'exclusion du contenu[187], concernant la performance, l'utilisation et l'environnement des produits connectés[188] (plus connus sous l'appellation d'« Internet des objets » ou d'« IoT »[189]) et services connexes[190] ainsi que des assistants virtuels[191] (chap. II du *Data Act*) ;

183 Règlement (UE) 2023/2854 sur les données, art. 2, 1).

184 Comme le précise l'article 2, 3), du *Data Act*, la notion de « données à caractère personnel » doit s'entendre par référence à l'article 4, 1), du RGPD comme « […] toute information se rapportant à une personne physique identifiée ou identifiable […] ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

185 Les données à caractère non personnel sont définies comme des « […] données autres que des données à caractère personnel » (règlement (UE) 2023/2854 sur les données, art. 2, 4)).

186 Il est important d'insister sur le fait que le considérant 15 du *Data Act* précise que « […] [r]elèvent du champ d'application du présent règlement les *données qui ne sont pas substantiellement modifiées*, c'est-à-dire les données sous forme brute, également appelées "données sources" ou "données primaires", désignant des points de données qui sont générés automatiquement sans autre forme de traitement, ainsi que les ***données qui ont été prétraitées*** dans le but de les rendre compréhensibles et utilisables avant leur traitement et leur analyse ultérieurs. Ces données comprennent les données collectées à partir d'un capteur unique ou d'un groupe de capteurs connecté dans le but de rendre les données collectées compréhensibles pour les cas d'utilisation plus larges en déterminant une grandeur ou une qualité physique ou la modification d'une grandeur physique, telle que la température, la pression, le débit, l'audio, la valeur de pH, le niveau de liquide, la position, l'accélération ou la vitesse. […] À l'inverse, *les informations dérivées ou déduites de ces données, qui sont le résultat d'investissements supplémentaires dans l'attribution de valeurs ou d'informations tirées des données, en particulier au moyen d'algorithmes complexes et propriétaires, y compris ceux qui font partie d'un logiciel propriétaire, ne devraient pas être considérées comme relevant du champ d'application du présent règlement* et ne devraient donc pas être soumises à l'obligation pour un détenteur de données de les mettre à la disposition d'un utilisateur ou d'un destinataire de données, sauf accord contraire entre l'utilisateur et le détenteur de données. Ces données pourraient comprendre en particulier les informations obtenues au moyen de la fusion de capteurs, qui infère ou déduit des données provenant de capteurs multiples, collectées dans le produit connecté, au moyen d'algorithmes complexes et propriétaires, et qui pourraient être soumises à des droits de propriété intellectuelle » (nous soulignons).

187 Le considérant 16 du *Data Act* apporte des précisions quant à cette exclusion : « […] les données que ces produits connectés équipés de capteurs génèrent lorsque l'utilisateur enregistre, transmet, affiche ou lit du contenu, ainsi que le contenu lui-même, qui est souvent couvert par des droits de propriété intellectuelle, entre autres pour une utilisation par un service en ligne, ne devraient pas être couvertes par le présent règlement […] ».

188 Le produit connecté est défini comme « […] un objet qui obtient, génère ou recueille des données concernant son utilisation ou son environnement, qui est en mesure de communiquer des données relatives au produit par l'intermédiaire d'un service de communications électroniques, d'une connexion physique ou d'un dispositif d'accès intégré et dont la fonction première n'est pas de stocker, de traiter ou de transmettre des données pour le compte de toute partie autre que l'utilisateur » (règlement (UE) 2023/2854 sur les données, art. 2, 5)). Sont par exemple visés les montres connectées, les véhicules connectés, les dispositifs médicaux connectés ou encore les machines agricoles connectées.

189 Règlement (UE) 2023/2854 sur les données, cons. 14.

190 Un service connexe est défini comme « […] un service numérique, autre qu'un service de communications électroniques, y compris un logiciel, qui est connecté au produit au moment de l'achat, ou de la mise en location ou en crédit-bail, de telle sorte que son absence empêcherait le produit connecté d'exécuter une ou plusieurs de ses fonctions, ou qui est ensuite connecté au produit par le fabricant ou un tiers pour ajouter, mettre à jour ou adapter les fonctions du produit connecté » (règlement (UE) 2023/2854 sur les données, art. 2, 6)). La notion de « service connexe » pourrait par exemple couvrir le logiciel qui serait utilisé pour traiter les données de géolocalisation et celles relatives à la fréquence cardiaque enregistrées par une montre connectée.

191 Les assistants virtuels sont définis comme « […] des logiciels capables de traiter des demandes, des tâches ou des questions, notamment celles fondées sur des données d'entrée sonores ou écrites, ou des gestes ou des mouvements, et qui, sur la base de ces demandes, tâches ou questions, donnent accès à d'autres services ou contrôlent les

(ii) les données du secteur privé[192] légalement soumises à des obligations de partage des données[193] (chap. III du *Data Act*) ;

(iii) les données du secteur privé dont l'accès et l'utilisation sont basés sur un contrat entre entreprises (chap. IV du *Data Act*) ;

(iv) les données du secteur privé, et principalement les données à caractère non personnel (chap. V du *Data Act*) ;

(v) les données et les services traités par les fournisseurs de services de traitement de données[194] (chap. VI du *Data Act*) ;

(vi) les données à caractère non personnel détenues dans l'Union par les fournisseurs de services de traitement de données (chap. VII du *Data Act*)[195].

Le *Data Act* s'applique en outre aux espaces de données[196], aux services de traitement de données et aux contrats intelligents portant sur l'exécution d'accords de partage de données (chap. VIII du *Data Act*)[197].

67. Champ d'application matériel : exclusions. Sont expressément exclus du champ d'application du *Data Act* : (i) les accords volontaires d'échange de données entre entités privées et publiques, (ii) la collecte, le partage, l'accès aux données et leur utilisation en vertu de la législation européenne relative aux informations accompagnant les transferts de fonds[198] et de celle relative au blanchiment de capitaux et au financement du terrorisme[199] et (iii) les matières ne relevant pas du droit de l'Union[200].

---

fonctions des produits connectés » (règlement (UE) 2023/2854 sur les données, art. 2, 31)). Il convient de préciser que, selon les termes du considérant 23 du *Data Act*, « […] seules les données résultant de l'interaction entre l'utilisateur et un produit connecté ou un service connexe *par l'intermédiaire de l'assistant virtuel* devraient être couvertes par le présent règlement. *Les données produites par l'assistant virtuel qui sont sans rapport avec l'utilisation d'un produit connecté ou d'un service connexe ne sont pas couvertes par le présent règlement* » (nous soulignons). Le logiciel traitant les demandes formulées oralement par un utilisateur en vue de permettre le fonctionnement du produit « Alexa », commercialisé par Amazon, devrait par exemple être considéré comme un assistant virtuel couvert par le *Data Act*.

192 Les données du secteur privé sont les données détenues par des entreprises.

193 Sont visées les données détenues par des entreprises qui, en vertu du droit de l'Union ou d'une législation nationale adoptée conformément au droit de l'Union, sont tenues de partager ces données avec d'autres entreprises. Il s'agit par exemple des données qui doivent être mises à disposition du tiers désigné par l'utilisateur conformément à l'article 5 du *Data Act* (voy. *infra*, n[os] 78 et s.).

194 Un service de traitement de données est défini comme « […] un service numérique qui est fourni à un client et qui permet un accès par réseau en tout lieu et à la demande à un ensemble partagé de ressources informatiques configurables, modulables et variables de nature centralisée, distribuée ou fortement distribuée, qui peuvent être rapidement mobilisées et libérées avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services » (règlement (UE) 2023/2854 sur les données, art. 2, 8)).

195 Règlement (UE) 2023/2854 sur les données, art. 1[er], § 2.

196 Parmi ces espaces de données, l'on retrouve par exemple l'espace européen des données de santé (EHDS) qui fait l'objet de la proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé du 3 mai 2022 (COM(2022) 197 final).

197 Règlement (UE) 2023/2854 sur les données, art. 33-36.

198 Règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) n° 1781/2006, *J.O.*, L 141, 5 juin 2015.

199 Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, *J.O.*, L 141, 5 juin 2015.

200 Règlement (UE) 2023/2854 sur les données, art. 1[er], § 6.

68. Champ d'application territorial. Le champ d'application territorial du *Data Act* est particulièrement large puisqu'il ne repose pas sur le lieu d'établissement des acteurs auxquels il impose des obligations. En effet, le *Data Act* a vocation à s'appliquer dès qu'un lien peut être établi entre les acteurs visés et le territoire de l'Union européenne. Il s'applique ainsi aux :

(i) fabricants de produits connectés *mis sur le marché dans l'Union* et fournisseurs de services connexes ;

(ii) utilisateurs *dans l'Union* de tels produits connectés ou services connexes ;

(iii) détenteurs de données mettant des données à la disposition : (a) de destinataires de données *dans l'Union* ou (b) d'un organisme du secteur public, de la Commission, de la BCE ou d'un organe de l'Union en réponse à une demande fondée sur un besoin exceptionnel ;

(iv) destinataires de données *dans l'Union* auxquels les données sont mises à disposition ;

(v) fournisseurs de services de traitement de données fournissant ces services à des clients[201] *dans l'Union*[202].

69. Champ d'application temporel. La plupart des dispositions du *Data Act* seront applicables à partir du 12 septembre 2025[203] afin d'octroyer aux acteurs concernés un délai pour se mettre en conformité, y compris pour qu'ils puissent mettre en place des mesures techniques nécessaires[204].

Par exception, l'exigence d'accessibilité des données dès la conception[205] sera applicable aux produits connectés et services connexes mis sur le marché après le 12 septembre 2026[206].

Le régime des clauses abusives relatives à l'accès et l'utilisation des données entre entreprises, prévu au chapitre IV du *Data Act*[207], sera quant à lui applicable :

(i) à compter du 12 septembre 2025 pour les contrats conclus après cette date ; et

(ii) à partir du 12 septembre 2027 pour les contrats conclus le 12 septembre 2025 ou avant cette date étant de durée indéterminée ou expirant dix ans ou plus à compter du 11 janvier 2024[208].

3. Principales exigences

a. Partage de données « B2C » et « B2B »

70. Plan. Le chapitre II du *Data Act* impose aux détenteurs de données l'obligation de rendre les données relatives aux produits connectés, aux services connexes et aux assistants

201 Un client est défini comme « […] une personne physique ou morale qui a noué une relation contractuelle avec un fournisseur de services de traitement de données dans le but d'utiliser un ou plusieurs services de traitement de données » (règlement (UE) 2023/2854 sur les données, art. 2, 30)).

202 Règlement (UE) 2023/2854 sur les données, art. 1er, § 3.

203 Règlement (UE) 2023/2854 sur les données, art. 50, al. 2. En particulier, les exigences du chapitre III du *Data Act* relatives aux obligations légales de partage de données s'appliqueront uniquement en ce qui concerne les obligations de partage prévues par le droit de l'Union ou la législation nationale adoptée conformément au droit de l'Union entrant vigueur après le 12 septembre 2025 (règlement (UE) 2023/2854 sur les données, art. 50, al. 4).

204 Règlement (UE) 2023/2854 sur les données, cons. 117.

205 Règlement (UE) 2023/2854 sur les données, art. 3, § 1er. Pour des précisions quant à cette disposition, voy. *infra*, n° 71.

206 Règlement (UE) 2023/2854 sur les données, art. 50, al. 3.

207 Voy. *infra*, nos 89 et s.

208 Règlement (UE) 2023/2854 sur les données, art. 50, al. 5-6.

virtuels[209] accessibles aux utilisateurs, d'une part, et aux tiers désignés par ces utilisateurs, d'autre part. Autrement dit, les utilisateurs se voient octroyer des droits à l'égard de ces données, lesquels pourraient, à l'instar des droits conférés par les articles 15 et 20 du RGPD aux personnes concernées, être qualifiés de « droit d'accès » et de « droit à la portabilité des données »[210]. Le contenu et les modalités d'exercice du droit d'accès (i) et du droit à la portabilité des données (ii) ainsi que les dérogations prévues à l'exercice de ces droits (iii) sont examinés ci-après. L'obligation d'information précontractuelle envers les utilisateurs (iv), le régime de clauses abusives *B2B* (v) et le mécanisme de règlement des litiges (vi) instaurés par le *Data Act* font ensuite l'objet d'une brève analyse.

i. Mise à disposition des données aux utilisateurs (« droit d'accès »)

71. Accessibilité des données dès la conception. En matière de mise à disposition des données aux utilisateurs, l'article 3, paragraphe 1er, du *Data Act* consacre tout d'abord un principe selon lequel « [l]es produits connectés sont *conçus et fabriqués*, et les services connexes *conçus et fournis*, de telle sorte que les données relatives auxdits produits et les données relatives aux services connexes, y compris les métadonnées[211] pertinentes nécessaires à l'interprétation et à l'utilisation de ces données, sont, par défaut, accessibles à l'utilisateur, de manière aisée, sécurisée, sans frais, *dans un format complet, structuré, couramment utilisé et lisible par machine, et sont, lorsque cela est pertinent et techniquement possible, directement accessibles à l'utilisateur* »[212]. Ce principe pourrait être qualifié d'« accessibilité des données dès la conception » dès lors qu'il impose, d'une part, des exigences relatives au format des données qui sont de nature à en faciliter l'accès et, d'autre part, une exigence d'accessibilité directe des données au bénéfice de l'utilisateur « *lorsque cela est pertinent et techniquement possible* ».

La portée de cette exigence d'accessibilité directe des données est toutefois particulièrement floue en raison de l'emploi des termes « *lorsque cela est pertinent* ». En effet, dans quelle mesure pourrait-on raisonnablement considérer qu'il n'est pas pertinent de concevoir un produit connecté, un service connexe ou un assistant virtuel de manière à rendre les données y afférentes

209 Pour rappel, aux termes de l'article 1er, paragraphe 4, du règlement (UE) 2023/2854 sur les données, « [l]orsque le présent règlement fait référence à des produits connectés ou à des services connexes, ces références s'entendent également comme incluant également les assistants virtuels, dans la mesure où ceux-ci interagissent avec un produit connecté ou un service connexe ».

210 Le *Data Act* précise d'ailleurs, en son article 1er, paragraphe 5, que « […] [d]ans la mesure où les utilisateurs sont des personnes concernées, les droits prévus au chapitre II du présent règlement complètent les droits d'accès des personnes concernées et les droits à la portabilité des données au sens des articles 15 et 20 du [RGPD] […] ». Le considérant 35 précise, concernant le droit à la portabilité des données, que : « […] [l']article 20 du [RGPD] indique qu'il porte sur les données fournies par la personne concernée, mais ne précise pas si cela nécessite un comportement actif de la part de la personne concernée ou s'il s'applique également aux situations dans lesquelles un produit connecté ou un service connexe, par sa conception, observe le comportement d'une personne concernée ou d'autres informations relatives à une personne concernée de manière passive. […] Le présent règlement accorde aux utilisateurs le droit d'accéder à toutes données relatives à un produit ou données relatives à un service connexe et de mettre celles-ci à la disposition d'un tiers, quelle que soit leur nature en tant que données à caractère personnel, *sans distinction entre les données fournies activement et les données observées passivement*, et quelle que soit la base juridique du traitement […] » (nous soulignons).

211 Les métadonnées sont définies comme « […] une description structurée du contenu ou de l'utilisation des données qui facilite la découverte ou l'utilisation de ces données » (règlement (UE) 2023/2854 sur les données, art. 2, 2)).

212 Nous soulignons.

directement accessibles aux utilisateurs ? Il est regrettable que le *Data Act* n'apporte pas de précisions à cet égard, créant ainsi une certaine insécurité juridique qui résultera probablement en un renvoi préjudiciel en interprétation devant la Cour de justice de l'Union européenne.

72. Demande d'accès. Si le produit connecté, le service connexe ou l'assistant virtuel ne permet pas à l'utilisateur d'accéder directement aux données, ce dernier peut adresser une demande d'accès au détenteur de données, et ce, par voie électronique lorsque c'est techniquement possible[213].

73. Demande d'accès : recours à un sous-traitant par le détenteur de données. Dans l'hypothèse où les données faisant l'objet de la demande seraient des données à caractère personnel traitées par un sous-traitant[214], l'utilisateur devrait directement pouvoir adresser sa demande d'accès au sous-traitant[215]. Ce dernier ne peut toutefois être qualifié de « détenteur de données »[216]. Dans cette logique, le considérant 22 indique que le responsable du traitement peut spécifiquement charger son sous-traitant de mettre les données à disposition. Le degré d'implication du sous-traitant dans le traitement des demandes d'accès qui lui seraient directement adressées par les utilisateurs variera donc en fonction des instructions qui lui ont été communiquées en amont par le responsable du traitement. Il convient à cet égard de souligner, conformément à l'article 28 du RGPD et aux lignes directrices du Comité européen de la protection des données (ci-après « EDPB »), que les instructions du responsable du traitement doivent être claires, documentées et communiquées au sous-traitant avant le traitement[217].

74. Demande d'accès : identification de l'utilisateur. Une fois saisi de la demande d'accès, le détenteur de données devrait s'assurer que la personne dont émane ladite demande a bien la qualité d'« utilisateur ». À cet égard, le *Data Act* prévoit, en son considérant 29, que le détenteur de données peut requérir de l'utilisateur une identification appropriée. Il ne peut cependant exiger de la personne qui a introduit la demande qu'elle fournisse des informations allant au-delà de ce qui est nécessaire aux fins de la vérification de sa qualité d'utilisateur[218]. Dans le cadre de la détermination de ce caractère « nécessaire », le détenteur de données devrait, dans la mesure où la personne qui a introduit la demande est une personne physique, avoir égard aux indications fournies par l'EDPB concernant la procédure d'identification et d'authentification des personnes qui introduisent une demande d'accès au sens du RGPD[219], et ce, même si la demande d'accès – cette

213 Règlement (UE) 2023/2854 sur les données art. 4, § 1er. Il y a lieu de préciser que, « […] [l]orsque plusieurs fabricants ou fournisseurs de services connexes ont vendu ou loué des produits connectés à un même utilisateur ou conclu un crédit-bail ayant pour objet de tels produits avec un même utilisateur, ou fourni des services connexes à un même utilisateur, ces produits et services étant intégrés ensemble, l'utilisateur devrait s'adresser à chacune des parties avec lesquelles il a conclu un contrat » (règlement (UE) 2023/2854 sur les données, cons. 21).

214 À savoir « […] la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement » (art. 4, 8), du RGPD).

215 En effet, le considérant 29 du *Data Act* prévoit ce qui suit : « […] les détenteurs de données devraient veiller à ce que la demande d'accès soit reçue et traitée par le sous-traitant ».

216 Règlement (UE) 2023/2854 sur les données, cons. 22.

217 EDPB, « Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD », version 2.0, 7 juillet 2021, pt 132.

218 Règlement (UE) 2023/2854 sur les données, art. 4, § 5. Cette exigence fait écho au principe de minimisation des données consacré par l'article 5, § 1er, c), du RGPD, selon lequel « [l]es données à caractère personnel doivent être […] adéquates, pertinentes et *limitées à ce qui est nécessaire* au regard des finalités pour lesquelles elles sont traitées […] » (nous soulignons).

219 Voy. EDPB, « Guidelines 01/2022 on data subject rights – Right of access », version 2.0, 28 mars 2023, pts 58-79.

fois au sens du *Data Act* – ne porte pas (exclusivement) sur des données à caractère personnel. En effet, le traitement des informations destinées à permettre la vérification de la qualité d'utilisateur de la personne physique qui a introduit la demande d'accès est un traitement de données à caractère personnel qui, par définition, est soumis aux exigences du RGPD, et en particulier au principe de minimisation des données[220].

75. Demande d'accès : données à caractère personnel relatives à un tiers. Si la demande d'accès introduite par l'utilisateur porte sur des données à caractère personnel qui ne le concernent pas, le détenteur de données devra vérifier si la mise à disposition desdites données à l'utilisateur se fonde sur l'une base de licéité prévue par l'article 6 du RGPD ou, s'il s'agit de données dites « sensibles », par l'article 9 du RGPD. Le cas échéant, il devra aussi vérifier si la mise à disposition des données répond aux conditions prévues par l'article 5, paragraphe 3, de la directive e-Privacy[221,222]. Comme le précise le considérant 7 du *Data Act*, le détenteur de données peut aussi répondre à une telle demande d'accès en anonymisant les données à caractère personnel concernant le tiers ou en communiquant à l'utilisateur uniquement les données à caractère personnel le concernant dans l'hypothèse où les données se rapportent à plusieurs personnes concernées, dont l'utilisateur.

76. Mise à disposition des données à l'utilisateur. Après avoir procédé à ces étapes de vérification, le cas échéant, le détenteur des données sera tenu de rendre accessibles à l'utilisateur sans retard injustifié les données facilement accessibles et les métadonnées pertinentes nécessaires pour interpréter et utiliser ces données. Les données et métadonnées concernées doivent avoir la même qualité que celles dont dispose le détenteur de données et être rendues accessibles gratuitement, aisément, de manière sécurisée et dans un format structuré, complet, lisible par machine et couramment utilisé. En outre, les données et métadonnées doivent être accessibles en continu et en temps réel lorsque c'est pertinent et techniquement possible[223]. Seules les données facilement accessibles (et les métadonnées pertinentes nécessaires pour les interpréter et les utiliser) doivent donc être mises à disposition de l'utilisateur. Il s'agit des « […] données relatives à un produit et les données relatives à un service connexe qu'un détenteur de données obtient légalement ou peut obtenir légalement à partir du produit connecté ou du service connexe, sans effort disproportionné allant au-delà d'une simple opération »[224]. Comme le précise le considérant 20 du *Data Act*, ne sont ainsi pas visées « […] les données générées par l'utilisation d'un produit connecté lorsque la conception du produit connecté ne prévoit pas que ces données sont stockées ou transmises en dehors du composant dans lequel elles sont générées ou du produit connecté dans son ensemble ».

220 Voy. RGPD, art. 5, § 1er, c).

221 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.*, L 201, 31 juillet 2022. L'article 5, paragraphe 3, de cette directive énonce les conditions dans lesquelles l'utilisation des réseaux de communications électroniques en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur est permise.

222 Règlement (UE) 2023/2854 sur les données, art. 4, § 12.

223 Règlement (UE) 2023/2854 sur les données, art. 4, § 1er.

224 Règlement (UE) 2023/2854 sur les données, art. 2, 17). Le considérant 20 du *Data Act* précise qu'il peut par exemple s'agir des données (qui peuvent être) obtenues légalement et sans effort disproportionné par le détenteur de données à travers la conception du produit connecté, les moyens techniques d'accès aux données dont il dispose ou encore au moyen du contrat conclu avec l'utilisateur concernant la fourniture de services connexes.

77. Limites d'utilisation imposées au détenteur de données. Le *Data Act* impose également des limites quant à l'utilisation des données à caractère non personnel[225]. Ainsi, le détenteur de données ne peut, d'une part, utiliser les données facilement accessibles que sur la base d'un contrat conclu avec l'utilisateur et, d'autre part, utiliser ces données en vue d'obtenir des informations relatives à la situation économique de l'utilisateur, à ses méthodes de production et actifs ou à leur utilisation, d'une façon qui pourrait porter atteinte à la position commerciale de l'utilisateur sur les marchés sur lesquels il est actif[226]. Le *Data Act* interdit en outre au détenteur de données de mettre à disposition de tiers les données à caractère non personnel relatives aux produits connectés à d'autres fins que l'exécution du contrat conclu avec l'utilisateur. Si toutefois cette mise à disposition se révélait nécessaire aux fins de l'exécution du contrat, le détenteur de données serait tenu d'interdire contractuellement au tiers concerné de partager les données reçues[227].

ii. Mise à disposition des données à des tiers (« droit à la portabilité des données »)

78. Droit à la portabilité des données. L'utilisateur dispose également d'un droit à la portabilité des données. En vertu de ce droit, il peut demander au détenteur de données de mettre à la disposition d'un tiers sans retard injustifié les données facilement accessibles et les métadonnées pertinentes nécessaires pour interpréter et utiliser ces données. Les données et métadonnées concernées doivent être de même qualité que celles dont dispose le détenteur de données et être mises à disposition au tiers aisément, de manière sécurisée, gratuitement pour l'utilisateur et dans un format structuré, complet, lisible par machine et couramment utilisé. Par ailleurs, les données et métadonnées doivent être accessibles en continu et en temps réel lorsque c'est pertinent et techniquement possible[228]. En pratique, cette demande pourrait directement émaner du tiers désigné par l'utilisateur dès lors que l'article 5, paragraphe 1er, du *Data Act* prévoit expressément que la demande peut être formulée par « une partie agissant pour le compte d'un utilisateur ».

79. Droit à la portabilité des données : exclusions. L'application du droit à la portabilité des données est exclue dans deux situations[229]. La première est la situation dans laquelle les données facilement accessibles portent sur de nouveaux produits connectés, substances ou procédés qui n'ont pas encore été mis sur le marché et qui font l'objet d'essais, hormis dans l'hypothèse où l'utilisation de ces données par un tiers est permise contractuellement[230]. La seconde est la situation dans laquelle le tiers auquel l'utilisateur souhaiterait mettre les données à disposition est un contrôleur d'accès (*gatekeeper*) au sens du règlement (UE) 2022/1925 sur les marchés numériques (*Digital Markets Act*)[231], le *Data Act* prévoyant qu'un contrôleur d'accès ne peut avoir

225 En ce qui concerne les données à caractère personnel, ce sont les exigences imposées par la législation en matière de protection des données à caractère personnel, en particulier le RGPD, qui trouvera à s'appliquer (règlement (UE) 2023/2854 sur les données, art. 1, § 5).

226 Règlement (UE) 2023/2854 sur les données, art. 4, § 13.

227 Règlement (UE) 2023/2854 sur les données, art. 4, § 14.

228 Règlement (UE) 2023/2854 sur les données, art. 5, § 1er.

229 En sus de ces exclusions, certaines dérogations à l'exercice du droit à la portabilité des données sont prévues (voy. *infra*, nos 83 et s.).

230 Règlement (UE) 2023/2854 sur les données, art. 5, § 2.

231 Règlement (UE) 2022/1925 du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques), *J.O.*, L 265, 12 octobre 2022.

la qualité de tiers éligible à la mise à disposition des données[232]. Afin de garantir l'effet utile de cette disposition, le *Data Act* entend également interdire une mise à disposition « détournée » des données aux contrôleurs d'accès, c'est-à-dire une mise à disposition des données directement par l'utilisateur qui aurait exercé son droit d'accès[233] ou encore par le tiers au bénéfice duquel l'utilisateur aurait exercé son droit à la portabilité des données[234].

80. Demande de portabilité des données : identification de l'utilisateur et du tiers et données à caractère personnel relatives à un tiers (renvoi). Plusieurs exigences sont imposées au détenteur de données lorsque ce dernier procède à la vérification de la qualité d'utilisateur du demandeur et de celle de tiers[235] et lorsque la demande de portabilité porte sur des données relatives à un tiers à l'utilisateur[236], à l'instar de ce qui est prévu concernant les demandes d'accès[237].

81. Obligations imposées au détenteur de données aux fins de la mise à disposition des données au tiers. Lorsqu'il est saisi d'une demande de portabilité des données et sous réserve des dérogations à l'exercice du droit à la portabilité des données examinées ci-après[238], le détenteur de données est tenu, dans les relations *B2B*, de convenir des modalités de mise à disposition des données avec le destinataire des données[239], étant entendu que cette mise à disposition doit être réalisée de manière transparente et reposer sur des conditions équitables, raisonnables et non discriminatoires[240]. Cette exigence implique par exemple qu'une compensation convenue

232 Règlement (UE) 2023/2854 sur les données, art. 5, § 3. Le considérant 40 du *Data Act* apporte des éclaircissements quant à la raison d'être de cette exclusion : « […] [c]onformément au [*Digital Markets Act*], et compte tenu de la capacité sans égale [des contrôleurs d'accès] en matière d'acquisition de données, il n'est pas nécessaire, pour atteindre l'objectif du présent règlement, et il serait donc disproportionné à l'égard des détenteurs de données soumis à de telles obligations, d'inclure ces contrôleurs d'accès parmi les bénéficiaires du droit d'accès aux données. Il est probable qu'une telle inclusion limiterait également les avantages du présent règlement pour les PME, liés à l'équité de la répartition de la valeur des données entre les acteurs du marché. […] Les droits d'accès prévus par le présent règlement contribuent à élargir le choix des services offerts aux consommateurs. Étant donné que les accords volontaires entre les contrôleurs d'accès et les détenteurs de données ne sont pas affectés, limiter le droit d'accès pour les contrôleurs d'accès ne les exclurait pas du marché ni ne les empêcherait de proposer leurs services ».

233 Il est ainsi expressément prévu qu'un contrôleur d'accès ne peut : « a) inviter un utilisateur, par une sollicitation ou par une incitation commerciale, quelles qu'elles soient, y compris en fournissant une compensation pécuniaire ou de toute autre nature, à mettre à la disposition de l'un de ses services des données que l'utilisateur a obtenues à la suite d'une demande [d'accès] ; b) inviter un utilisateur, par une sollicitation ou par une incitation commerciale, à demander au détenteur de données de mettre des données à la disposition de l'un de ses services [en vertu du droit à la portabilité des données de cet utilisateur] ; c) recevoir d'un utilisateur des données que ce dernier a obtenues à la suite d'une demande [d'accès] » (règlement (UE) 2023/2854 sur les données, art. 5, § 3).

234 Règlement (UE) 2023/2854 sur les données, art. 6, § 2, d). Le considérant 40 du *Data Act* indique à cet égard que « […] [p]ar exemple, le tiers ne peut pas sous-traiter la fourniture d'un service à un contrôleur d'accès. Cela n'empêche toutefois pas que des tiers puissent recourir aux services de traitement de données offerts par un contrôleur d'accès. Cela n'empêche pas non plus [les contrôleurs d'accès] d'obtenir et d'utiliser les mêmes données par d'autres moyens licites ».

235 Règlement (UE) 2023/2854 sur les données, art. 5, § 4.

236 Règlement (UE) 2023/2854 sur les données, art. 5, § 7.

237 Voy. *supra*, n^os^ 74 et 77.

238 Voy. *infra*, n^os^ 83 et s.

239 Il convient toutefois de souligner que, si le détenteur de données et le tiers ne parviennent pas à s'accorder sur les modalités de mise à disposition des données, cela ne doit pas empêcher l'exercice des droits conférés à la personne concernée par le RGPD et, en particulier, de son droit à la portabilité des données au sens de l'article 20 du RGPD (règlement (UE) 2023/2854 sur les données, art. 5, § 8).

240 Règlement (UE) 2023/2854 sur les données, art. 8, § 1^er^. Cette obligation s'applique également lorsque le détenteur de données est tenu de mettre des données à disposition d'un destinataire de données en vertu d'une autre législation de l'Union ou d'une législation nationale adoptée conformément au droit de l'Union.

entre un destinataire et un détenteur de données dans une relation *B2B* doit être raisonnable et non discriminatoire[241], ou encore qu'une clause contractuelle relative à l'utilisation ou l'accès aux données qui serait considérée comme abusive[242] ou qui exclurait l'application, dérogerait ou modifierait les effets des droits des utilisateurs à leur détriment ne serait pas contraignante[243].

82. Limites d'utilisation imposées au détenteur de données. De manière similaire aux limites d'utilisation des données prévues au bénéfice de l'utilisateur dans les dispositions relatives droit d'accès[244], le *Data Act* prévoit, cette fois au bénéfice du tiers, que le détenteur de données ne peut, sauf en cas d'autorisation du tiers et si ce dernier dispose de la possibilité technique de retirer aisément cette autorisation à tout moment, utiliser les données facilement accessibles en vue d'obtenir des informations relatives à la situation économique du tiers, à ses méthodes de production et actifs ou à leur utilisation d'une façon qui pourrait porter atteinte à la position commerciale du tiers sur les marchés sur lesquels il est actif[245].

iii. Dérogations à l'exercice des droits d'accès et à la portabilité des données

83. Limitations contractuelles en cas de risque en matière de sécurité. Si l'utilisation, l'accès ou le partage ultérieur des données peut porter atteinte aux exigences légales de sécurité du produit connecté et nuire gravement à la sûreté, la sécurité ou la santé de personnes physiques, des restrictions ou interdictions quant au traitement des données peuvent être prévues contractuellement par les utilisateurs et détenteurs de données. Le détenteur de données qui refuse de partager les données pour cette raison est tenu d'en informer l'autorité compétente[246,247].

84. Préservation des secrets d'affaires : mesures de protection. Dès lors que l'exercice par l'utilisateur de son droit d'accès ou de son droit à la portabilité des données est susceptible de porter atteinte aux secrets d'affaires du détenteur de données ou d'un tiers, le *Data Act* établit certaines garanties. Ainsi, si l'utilisateur entend exercer son droit d'accès, la divulgation des secrets d'affaires est uniquement permise si l'utilisateur et le détenteur de données prennent toutes les mesures nécessaires avant la divulgation pour préserver la confidentialité des secrets, en particulier à l'égard des tiers[248]. Si l'utilisateur souhaite exercer son droit à la portabilité des données, la divulgation des secrets d'affaires au tiers concerné n'est quant à elle permise que dans la mesure strictement nécessaire à l'atteinte de la finalité convenue entre le tiers et l'utilisateur[249].

Dans ces deux hypothèses, le détenteur de secrets d'affaires doit, d'une part, identifier les données protégées en tant que secrets d'affaires et, d'autre part, convenir avec l'utilisateur ou,

241 Règlement (UE) 2023/2854 sur les données, art. 9, § 1er. Pour plus de détails concernant la fixation d'une compensation raisonnable et non discriminatoire, voy. le règlement (UE) 2023/2854 sur les données, art. 9, lequel prévoit notamment que la Commission adoptera des lignes directrices relatives au calcul d'une compensation raisonnable.

242 À propos du régime de clauses abusives *B2B* instauré par le *Data Act*, voy. *infra*, nos 89 et s.

243 Règlement (UE) 2023/2854 sur les données, art. 8, § 2.

244 Voy. *supra*, n° 75.

245 Règlement (UE) 2023/2854 sur les données, art. 5, § 6.

246 Sur les autorités compétentes, voy. *infra*, nos 107 et s.

247 Règlement (UE) 2023/2854 sur les données, art. 4, § 2.

248 Règlement (UE) 2023/2854 sur les données, art. 4, § 6.

249 Règlement (UE) 2023/2854 sur les données, art. 5, § 9.

selon le cas, le tiers auquel les données seront partagées, des mesures organisationnelles et techniques proportionnées nécessaires pour garantir la confidentialité des données, par exemple des accords de confidentialité, des clauses contractuelles types, des normes techniques, des protocoles d'accès stricts et l'application de codes de conduite[250].

85. Préservation des secrets d'affaires : blocage ou suspension du partage de données. Le *Data Act* permet au détenteur de données de bloquer ou de suspendre le partage des données dans trois hypothèses : (i) s'il ne parvient pas à s'accorder sur des mesures de préservation de la confidentialité des données partagées avec l'utilisateur ou, selon le cas, le tiers, (ii) si lesdites mesures ne sont pas mises en œuvre par l'utilisateur ou le tiers ou (iii) si ces derniers portent atteinte à la confidentialité des secrets d'affaires[251]. La décision de blocage ou de suspension du partage des données doit être dûment motivée et communiquée dans les plus brefs délais par écrit à l'utilisateur ou au tiers. Elle doit également être notifiée à l'autorité compétente[252].

Le *Data Act* permet en outre au détenteur de données de refuser, au cas par cas, de faire droit à une demande d'accès ou de portabilité portant sur des données spécifiques lorsque, dans des circonstances exceptionnelles, il est en mesure de démontrer qu'il est fort probable qu'il subisse un préjudice économique grave en raison de la divulgation de secrets d'affaires, et ce, malgré les mesures organisationnelles et techniques mises en place[253]. Dans ce cas, le détenteur de données est tenu de communiquer sa décision de refus à l'utilisateur ou au tiers par écrit et dans les plus brefs délais et de motiver dûment cette décision sur base d'éléments objectifs tels que le niveau de confidentialité et la nature des données concernées ou encore la nouveauté et le caractère unique du produit connecté concerné. Une notification à l'autorité compétente est par ailleurs requise[254].

86. Interdiction de développer un produit connecté concurrent. Dans une optique de protection des efforts d'innovation déployés par le détenteur de données, le *Data Act* prévoit que les droits d'accès et à la portabilité des données ne peuvent être exercés par l'utilisateur pour développer ou permettre à un tiers de développer un produit connecté concurrent[255]. En outre, les données obtenues ne peuvent être utilisées en vue d'obtenir des informations relatives à la

250 Règlement (UE) 2023/2854 sur les données, art. 4, § 6, et art. 5, § 9.
251 Règlement (UE) 2023/2854 sur les données, art. 4, § 7, et art. 5, § 10.
252 Règlement (UE) 2023/2854 sur les données, art. 4, § 7, et art. 5, § 10.
253 Règlement (UE) 2023/2854 sur les données, art. 4, § 8, et art. 5, § 11.
254 Règlement (UE) 2023/2854 sur les données, art. 4, § 8, et art. 5, § 11.
255 Règlement (UE) 2023/2854 sur les données, art. 4, § 10, et cons. 32. Le considérant 32 du *Data Act* donne des indications quant à la manière d'apprécier cette interdiction : « […] [l]e présent règlement vise dans le même temps à éviter que les incitations à l'investissement soient fragilisées pour le type de produit connecté à partir duquel les données sont obtenues, par exemple du fait de l'utilisation des données pour développer un *produit connecté concurrent considéré comme interchangeable ou substituable par les utilisateurs, en particulier sur la base des caractéristiques du produit connecté, de son prix et de son usage prévu*. Le présent règlement ne prévoit *aucune interdiction de développer un service connexe* utilisant des données obtenues en vertu du présent règlement, car cela aurait un effet dissuasif indésirable sur l'innovation. La question de savoir si un produit connecté est en concurrence avec le produit connecté dont proviennent les données dépend de la question de savoir si les deux produits connectés sont *en concurrence sur le même marché de produits*. Cela doit être déterminé sur la base des principes établis du *droit de la concurrence de l'Union* pour définir le marché de produits en cause. Cependant, des finalités licites de l'utilisation des données pourraient inclure l'ingénierie inverse, pour autant qu'elle respecte les exigences prévues par le présent règlement ainsi que par le droit de l'Union ou le droit national. Cela peut être le cas aux fins de la réparation ou de la prolongation de la durée de vie d'un produit connecté ou de la fourniture de services après-vente pour des produits connectés » (nous soulignons).

situation économique du fabricant ou, le cas échéant, du détenteur de données, à ses méthodes de production et à ses actifs[256].

87. Interdiction de recourir à la coercition et de tirer avantage des lacunes de l'infrastructure technique. En toute logique, le *Data Act* précise que l'utilisateur et, le cas échéant, le tiers ne peuvent, en vue d'accéder aux données, ni recourir à la coercition ni tirer avantage des éventuelles lacunes présentes dans l'infrastructure technique mise en place par le détenteur de données pour protéger ces données[257].

iv. Obligation d'information précontractuelle

88. Informations précontractuelles. Pour que les utilisateurs puissent exercer leurs droits d'accès et à la portabilité des données de manière informée, le *Data Act* impose aux vendeurs, aux bailleurs (en cas de crédit-bail ou « *lease* », en anglais) et aux loueurs de produits connectés ainsi qu'aux fournisseurs de services connexes de communiquer certaines informations précontractuelles[258].

v. Régime de clauses abusives *B2B*

89. Régime de clauses abusives *B2B*. L'article 13 du *Data Act* prévoit un régime spécifique de clauses abusives relatives à l'accès et à l'utilisation des données entre entreprises. Plus précisément, sur base de ce régime, une clause contractuelle considérée comme abusive[259] ne lie pas l'entreprise à laquelle elle a été unilatéralement imposée[260] si cette clause concerne l'utilisation et l'accès aux données ou la responsabilité et les voies de recours dans l'hypothèse d'une violation ou de l'extinction d'obligations relatives aux données[261]. Ne sont toutefois pas concernées par ce

256 Règlement (UE) 2023/2854 sur les données, art. 4, § 10. Concernant les tiers, il est spécifiquement prévu ce qui suit : « […] les tiers n'utilisent pas non plus de données à caractère non personnel relatives au produit ou relatives au service connexe mises à leur disposition pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production du détenteur de données ou sur l'utilisation que ce dernier en fait » (règlement (UE) 2023/2854 sur les données, art. 6, § 2, e)).

257 Règlement (UE) 2023/2854 sur les données, art. 4, § 11, et art. 5, § 5.

258 En ce qui concerne les produits connectés, il s'agit des suivantes : « […] a) le type, le format et le volume estimé des données relatives au produit que le produit connecté est capable de générer ; b) si le produit connecté est capable de générer des données en continu et en temps réel ; c) si le produit connecté est capable de stocker des données sur un dispositif intégré ou sur un serveur distant, y compris, le cas échéant, la durée de conservation prévue ; d) la manière dont l'utilisateur peut accéder aux données, extraire les données ou, le cas échéant, les effacer, y compris les moyens techniques nécessaires pour ce faire, ainsi que leurs conditions d'utilisation et leur qualité de service » (règlement (UE) 2023/2854 sur les données, art. 3, § 2). Les informations précontractuelles à fournir concernant un service connexe portent quant à elles notamment sur les finalités pour lesquelles le détenteur potentiel des données utilisera les données facilement accessibles, le cas échéant, sur l'existence de secrets d'affaires et l'identité du détenteur de ceux-ci ou encore sur les modalités de demande de partage – et, le cas échéant, de fin du partage – des données avec un tiers (pour une liste exhaustive, voy. règlement (UE) 2023/2854 sur les données, art. 3, § 3).

259 Voy. *infra*, n° 90.

260 « […] Il s'agit des situations du type "à prendre ou à laisser" dans lesquelles une partie prévoit une certaine clause contractuelle et où l'autre entreprise ne peut pas influencer le contenu de cette clause malgré une tentative de négociation. Une clause contractuelle qui est simplement prévue par une partie et acceptée par l'autre entreprise, ou une clause négociée puis convenue sous une forme modifiée entre les parties contractantes, ne devrait pas être considérée comme ayant été imposée unilatéralement » (règlement (UE) 2023/2854 sur les données, cons. 59).

261 Règlement (UE) 2023/2854 sur les données, art. 13, § 1er.

régime les clauses définissant l'objet principal du contrat et la question de l'adéquation du prix par rapport aux données fournies[262].

90. Détermination du caractère abusif d'une clause. Le régime de clauses abusives instauré par le *Data Act* suit la même logique que le régime de clauses abusives *B2C* encadré par la directive 93/13/CEE[263], transposée en droit belge par les articles VI.82 à VI.87 du Code de droit économique[264]. Le régime établi par le *Data Act* contient ainsi une norme générale[265] à la lumière de laquelle il convient d'évaluer le caractère abusif d'une clause, mais aussi une liste noire de clauses abusives (à savoir les clauses considérées abusives en toutes circonstances[266]) et une liste grise de clauses abusives (à savoir les clauses qui sont présumées abusives[267]).

vi. Règlement des litiges

91. Organes de règlement des litiges. Le *Data Act* prévoit la possibilité pour les utilisateurs, les détenteurs de données et les destinataires de données de recourir à un organe de règlement des litiges en vue de régler certains différends. Sont notamment visés les différends portant sur les restrictions ou interdictions, posées par le détenteur de données, d'accéder aux données, de les utiliser ou de les partager en vue de garantir la sécurité du produit connecté ou encore les différends portant sur la décision du détenteur de données de bloquer ou de suspendre le partage de données pour des raisons liées à la protection de secrets d'affaires[268]. Les organes de règlement des litiges doivent être certifiés sur base de certains critères tels que leur indépendance et leur impartialité[269].

b. Partage de données « B2G » en cas de besoin exceptionnel

92. Partage de données *B2G*. L'article 14 du *Data Act* impose aux détenteurs de données personnes morales qui ne sont pas des organismes du secteur public de mettre à disposition des organismes du secteur public ou, selon le cas, de la Commission, de la BCE ou des organes de l'Union les données que ces entités réclament. Pour que cette obligation s'applique, une demande motivée doit être formulée par l'entité concernée et cette dernière doit démontrer un besoin exceptionnel d'utiliser les données réclamées pour remplir ses obligations légales dans l'intérêt public.

---

262 Règlement (UE) 2023/2854 sur les données, art. 13, § 8.

263 Directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs, *J.O.*, L 95, 21 avril 1993.

264 Il y a lieu de noter que, depuis 2019, le Code de droit économique prévoit un régime général de clauses abusives *B2B* (art. VI.91/1 à VI.91/6) qui suit également la même logique que le régime *B2C*. Dans le cadre de l'évaluation du caractère abusif d'une clause contractuelle relative à l'accès et à l'utilisation de données, il conviendra donc, en ce qui concerne les contrats *B2B* régis par le droit belge, d'avoir égard à la fois au régime général de clauses abusives *B2B* (art. VI.91/1 à VI.91/6 du Code de droit économique) et au régime instauré par le *Data Act*.

265 Au sens de cette norme générale, « [u]ne clause contractuelle est abusive si elle est d'une nature telle que son utilisation s'écarte manifestement des bonnes pratiques commerciales en matière d'accès aux données et d'utilisation des données, contrairement à la bonne foi et à un usage loyal » (règlement (UE) 2023/2854 sur les données, art. 13, § 3).

266 Voy. règlement (UE) 2023/2854 sur les données, art. 13, § 4.

267 Voy. règlement (UE) 2023/2854 sur les données, art. 13, § 5.

268 Voy. *supra*, n^os^ 83 et 85.

269 Règlement (UE) 2023/2854 sur les données, art. 10.

93. Besoin exceptionnel. Selon l'article 15, paragraphe 1er, du *Data Act*, « [u]n besoin exceptionnel d'utiliser certaines données […] a *une durée et une portée limitées* et est réputé exister uniquement dans les cas suivants :

a) lorsque les données demandées sont nécessaires pour réagir à une situation d'urgence[270] et que l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union n'est pas en mesure d'obtenir ces données par d'autres moyens en temps utile et de manière efficace et dans des conditions équivalentes[271] ;

b) dans des circonstances non couvertes par le point a) et *uniquement en ce qui concerne les données à caractère non personnel*, lorsque :

(i) un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union agit sur la base du droit de l'Union ou du droit national et a déterminé des données spécifiques, dont l'absence l'empêche d'exécuter une mission spécifique d'intérêt public, qui a été explicitement prévue par la loi, telle que la production de statistiques officielles[272], l'atténuation d'une situation d'urgence ou le rétablissement à la suite d'une situation d'urgence ; *et*
(ii) l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union a épuisé tous les autres moyens à sa disposition pour obtenir ces données, y compris l'achat de données à caractère non personnel sur le marché aux prix du marché ou le recours aux obligations existantes de mise à disposition des données ou l'adoption de nouvelles mesures législatives pouvant garantir la disponibilité des données en temps utile »[273].

94. Cas particulier des microentreprises et petites entreprises. Les microentreprises et petites entreprises disposent d'une dérogation à l'obligation de mise à disposition des données si la demande qui leur est adressée se fonde sur le point b) ci-dessus[274].

95. Demande de mise à disposition de données : exigences. Lors de l'introduction d'une demande, plusieurs exigences doivent être rencontrées. Parmi ces exigences, l'on retrouve notamment : (i) l'obligation de formuler la demande par écrit et de manière concise, claire, simple et compréhensible pour le détenteur de données, (ii) l'obligation de formuler une demande proportionnée au besoin exceptionnel, (iii) l'obligation d'expliquer la finalité de la demande, (iv) l'obligation d'identifier les entités auxquelles les données pourraient être partagées, le cas échéant[275], et

---

270 La situation d'urgence est définie comme « une situation exceptionnelle, d'une durée limitée, telle qu'une urgence de santé publique, une urgence résultant d'une catastrophe naturelle ou d'une catastrophe majeure d'origine humaine, y compris un incident majeur de cybersécurité, ayant une incidence négative sur la population de l'Union ou sur l'ensemble ou une partie d'un État membre, entraînant un risque de répercussions graves et durables sur les conditions de vie ou la stabilité économique, la stabilité financière, ou la détérioration substantielle et immédiate d'actifs économiques dans l'Union ou l'État membre concerné, et qui est déterminée ou officiellement déclarée conformément aux procédures pertinentes prévues par le droit de l'Union ou le droit national » (règlement (UE) 2023/2854 sur les données, art. 2, 29)). Voy. ég. cons. 64.

271 Par exemple via la consultation d'une base de données publique ou la fourniture volontaire de données par une autre entreprise (règlement (UE) 2023/2854 sur les données, cons. 64).

272 Le considérant 65 du *Data Act* précise que, dans ce cas, « […] l'organisme du secteur public demandeur devrait également démontrer si le droit national l'autorise à acheter des données à caractère non-personnel sur le marché ».

273 Nous soulignons.

274 Règlement (UE) 2023/2854 sur les données, art. 15, § 2.

275 En ce qui concerne le partage des données, voy. règlement (UE) 2023/2854 sur les données, art. 17, § 4.

(v) l'obligation de fournir une justification à propos du détenteur de données choisi pour mettre à disposition les données[276]. Il y a lieu de souligner que la Commission est chargée de publier un modèle de demande répondant à ces exigences[277], ce qui devrait, selon nous, en permettre une meilleure application.

96. Demande de mise à disposition portant sur des données à caractère personnel. En principe, la demande de mise à disposition des données ne peut porter que sur des données à caractère non personnel[278]. Il en découle que, lorsque la demande de mise à disposition concerne des données à caractère personnel, le détenteur de données est soumis à une obligation d'anonymisation[279]. Par exception, la mise à disposition de données à caractère personnel peut être demandée en cas de besoin exceptionnel tel que défini à l'article 15, paragraphe 1er, a), du *Data Act*, à savoir « […] lorsque les données demandées sont nécessaires pour réagir à une situation d'urgence et [lorsque] l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union n'est pas en mesure d'obtenir ces données par d'autres moyens en temps utile et de manière efficace et dans des conditions équivalentes ». Dans ce cas, le demandeur ne pourra obtenir la mise à disposition des données à caractère personnel demandées que sous forme pseudonymisée et seulement si, d'une part, il démontre que les données à caractère non personnel sont insuffisantes pour répondre au besoin exceptionnel susvisé et, d'autre part, sa demande établit les mesures organisationnelles et techniques de protection des données à mettre en place[280]. Par ailleurs, le demandeur devra, dans sa demande, expliquer comment le traitement des données à caractère personnel est de nature à répondre au besoin exceptionnel, indiquer toutes les mesures organisationnelles et techniques nécessaires et proportionnées visant à mettre en œuvre les garanties nécessaires ainsi que les principes de protection des données (par exemple, la pseudonymisation) et préciser si le détenteur de données peut procéder à l'anonymisation avant de mettre les données à disposition[281]. La demande de mise à disposition des données devra, en outre, sans retard injustifié, faire l'objet d'une notification à l'autorité de protection des données de l'État membre où est établi l'organisme du secteur public[282].

97. Rejet ou demande de modification de la demande de mise à disposition des données. Sans préjudice des possibilités de contestation dont dispose le demandeur[283], le détenteur de données peut rejeter ou demander la modification d'une demande de mise à disposition des données lorsqu'il se trouve dans l'une des situations suivantes :

(i) il n'a pas le contrôle sur les données demandées ;

(ii) une demande similaire pour la même finalité a été formulée précédemment par la Commission, la BCE, un autre organisme du secteur public ou un organe de l'Union et le détenteur de données n'a pas été informé de l'effacement des données communiquées ;

276 Règlement (UE) 2023/2854 sur les données, art. 17, § 1er, c), e) et f), et § 2, a) et c). Pour la liste complète des exigences imposées, voy. art. 17. Voy. ég. cons. 69.
277 Règlement (UE) 2023/2854 sur les données, art. 17, § 6.
278 Règlement (UE) 2023/2854 sur les données, art. 17, § 2, e).
279 Règlement (UE) 2023/2854 sur les données, art. 17, § 4.
280 Règlement (UE) 2023/2854 sur les données, art. 17, § 2, e).
281 Règlement (UE) 2023/2854 sur les données, art. 17, § 1er, c) et g).
282 Règlement (UE) 2023/2854 sur les données, art. 17, § 2, i).
283 Voy. *infra*, n° 112.

(iii) la demande ne remplit pas les conditions auxquelles doit satisfaire toute demande de mise à disposition de données telles que prévues à l'article 17, paragraphes 1 et 2[284,285].

Ce refus ou cette demande de modification doit être communiqué sans retard injustifié et au plus tard cinq jours ouvrables après la réception d'une demande portant sur les données nécessaires pour réagir à une situation d'urgence et au plus tard trente jours ouvrables après la réception d'une demande concernant un autre cas de besoin exceptionnel[286].

98. Préservation des secrets d'affaires. Comme dans le cadre du partage de données *B2C* et *B2B*[287], le *Data Act* encadre la divulgation des secrets d'affaires résultant d'une mise à disposition de données à un organisme du secteur public, à la Commission, à la BCE ou à un organe de l'Union. Ainsi, une telle divulgation « […] n'est exigée que dans la mesure où elle est strictement nécessaire pour atteindre la finalité d'une demande [de mise à disposition des données en cas de besoin exceptionnel]. Dans ce cas, le détenteur de données ou, s'il ne s'agit pas de la même personne, le détenteur de secrets d'affaires détermine les données qui sont protégées en tant que secrets d'affaires, y compris dans les métadonnées pertinentes. L'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union prend, avant la divulgation de secrets d'affaires, toutes les mesures techniques et organisationnelles nécessaires et appropriées pour préserver la confidentialité des secrets d'affaires, y compris, le cas échéant, l'utilisation de clauses contractuelles types et de normes techniques et l'application de codes de conduite »[288].

99. Interdiction de mise à disposition des données en vue de leur réutilisation. Les organismes du secteur public, la BCE, la Commission et les organes de l'Union ne peuvent mettre à disposition les données qu'ils ont obtenues en vue de leur réutilisation[289].

100. Compensation. Le détenteur de données ne bénéficie pas systématiquement d'une compensation du fait qu'il ait mis des données à disposition d'un organisme du secteur public, de la Commission, de la BCE ou d'un organe de l'Union. Ainsi, seuls les détenteurs de données ayant mis à disposition des données sur la base d'un besoin exceptionnel tel que défini à l'article 15, paragraphe 1er, b), du *Data Act*[290], d'une part, et les détenteurs de données qui sont des microentreprises ou petites entreprises et qui réclament une compensation pour la mise à disposition des données[291], d'autre part, peuvent obtenir une compensation équitable[292]. Ladite compensation a vocation à couvrir les coûts organisationnels et techniques encourus pour faire suite à la demande (tels que, le cas échéant, les coûts liés à la pseudonymisation,

284 Voy. règlement (UE) 2023/2854 sur les données, art. 17, §§ 1-2. Voy. ég. *supra*, n° 95.

285 Règlement (UE) 2023/2854 sur les données, art. 18, § 2.

286 Règlement (UE) 2023/2854 sur les données, art. 18, § 2.

287 Voy. *supra*, nos 84-85.

288 Règlement (UE) 2023/2854 sur les données, art. 19, § 3.

289 Règlement (UE) 2023/2854 sur les données, art. 17, § 3. La notion de « réutilisation » est à entendre au sens de l'article 2, 2), du DGA et de l'article 2, 11), de la directive *Open Data*.

290 Voy. *supra*, n° 93. Il convient toutefois de souligner que ne sont pas visés les détenteurs de données qui ont mis des données à disposition dans le cadre d'une demande justifiée par une mission spécifique réalisée dans l'intérêt public consistant en l'établissement de statistiques officielles et lorsque le droit national n'autorise pas l'achat de données (règlement (UE) 2023/2854 sur les données, art. 20, § 4).

291 Pour rappel, les microentreprises et petites entreprises sont uniquement tenues de mettre des données à disposition lorsque la demande porte sur un besoin exceptionnel lié à une situation d'urgence (voy. *supra*, n° 94).

292 Règlement (UE) 2023/2854 sur les données, art. 20, §§ 2-3.

l'anonymisation et l'agrégation des données et les coûts d'adaptation technique) ainsi qu'une marge raisonnable[293].

101. Partage ultérieur des données à des fins de recherche scientifique, d'analyse ou statistiques. Le *Data Act* permet à l'organisme du secteur public, la Commission, la BCE ou l'organe de l'Union auxquels les données ont été mises à disposition, de partager celles-ci, après en avoir notifié le détenteur de données[294], (i) avec des organismes ou des particuliers en vue d'effectuer des recherches scientifiques ou des analyses, dans la mesure où elles sont compatibles avec la finalité poursuivie lorsque les données ont été demandées ou (ii) avec Eurostat et les instituts nationaux de statistique pour la production de statistiques officielles[295].

c. Changement de services de traitement de données

102. Mesures permettant le changement de services de traitement de données. Le chapitre VI du *Data Act* impose aux fournisseurs de services de traitement de données de prendre différentes mesures[296], notamment d'ordre contractuel, « […] afin de permettre aux clients de changer de fournisseur pour passer à un service de traitement de données, couvrant le même type de service, qui est fourni par un fournisseur de services de traitement de données différent, ou passer à une infrastructure TIC sur site[297], ou, le cas échéant, recourir simultanément à plusieurs fournisseurs de services de traitement de données […] »[298].

d. Accès et transfert internationaux illicites de données à caractère non personnel par les autorités publiques

103. Garanties contre l'accès et le transfert internationaux illicites de données à caractère non personnel par les autorités publiques. Le chapitre VII du *Data Act* impose aux fournisseurs de services de traitement de données l'obligation de prendre « […] toutes les mesures techniques, organisationnelles et juridiques adéquates, y compris des contrats, afin d'empêcher l'accès international des autorités publiques et l'accès des autorités publiques des pays tiers aux données à caractère non personnel détenues dans l'Union et le transfert de ces données lorsque ce transfert ou cet accès risque d'être en conflit avec le droit de l'Union ou le droit national de l'État membre concerné […] »[299]. Le *Data Act* prévoit par ailleurs les conditions dans lesquelles des données peuvent être divulguées par les fournisseurs de services de traitement de données sur la base d'une décision ou d'un jugement émanant d'une juridiction d'un pays tiers ou d'une décision

293 Règlement (UE) 2023/2854 sur les données, art. 20, § 2.

294 Règlement (UE) 2023/2854 sur les données, art. 21, § 5.

295 Règlement (UE) 2023/2854 sur les données, art. 21, § 1er, a) et b). Il y a lieu de préciser que « [l]es particuliers ou les organismes qui reçoivent les données en vertu du paragraphe 1 [doivent agir] dans un but non lucratif ou dans le cadre d'une mission d'intérêt public reconnue par le droit de l'Union ou le droit national. Sont exclus les organismes sur lesquels des entreprises commerciales ont une influence significative, ce qui est susceptible de conduire à un accès préférentiel aux résultats des recherches » (règlement (UE) 2023/2854 sur les données, art. 21, § 2).

296 Voy. règlement (UE) 2023/2854 sur les données, spéc. art. 23, 25, 26, 27, 29 et 30.

297 L'infrastructure TIC sur site est définie comme « […] une infrastructure TIC et des ressources informatiques qui appartiennent au client, qu'il loue ou qu'il utilise en crédit-bail, situées dans le centre de données du client lui-même et exploitées par le client ou par un tiers » (règlement (UE) 2023/2854 sur les données, art. 2, 33)).

298 Règlement (UE) 2023/2854 sur les données, art. 23.

299 Règlement (UE) 2023/2854 sur les données, art. 32, § 1er.

rendue par une autorité administrative d'un pays tiers leur enjoignant de transférer des données à caractère non personnel[300].

e. Interopérabilité

104. Exigences essentielles en matière d'interopérabilité. Le chapitre VIII du *Data Act* a principalement pour objet de définir les exigences essentielles en matière d'interopérabilité[301] des données, des mécanismes et services de partage de données et des espaces européens communs de données. Ces exigences sont imposées aux participants aux espaces de données qui offrent des données ou des services de données à d'autres participants[302]. Des normes harmonisées qui répondent auxdites exigences devront être élaborées par une ou plusieurs organisations européennes de normalisation désignées par la Commission[303]. Dans certaines circonstances, la Commission pourra elle-même définir, au moyen d'actes d'exécution, des spécifications communes couvrant tout ou partie des exigences susvisées[304].

105. Exigences essentielles relatives aux contrats intelligents. L'article 36 du *Data Act* prévoit, en outre, plusieurs exigences applicables aux contrats intelligents dans le cadre de l'exécution d'accords de partage de données. Le respect de ces exigences incombe « [au] vendeur d'une application utilisant des contrats intelligents ou, à défaut, la personne dont l'activité commerciale, l'entreprise ou la profession nécessite le déploiement de contrats intelligents pour des tiers dans le cadre de l'exécution d'un accord ou d'une partie d'un accord de mise à disposition des données […] »[305]. L'établissement de normes harmonisées ou, le cas échéant, de spécifications communes est prévu[306], tout comme en matière d'interopérabilité.

4. Mise en œuvre, exécution et sanctions

106. Clauses contractuelles types et standard. L'article 41 du *Data Act* prévoit qu'avant le 12 septembre 2025, la Commission devra élaborer et recommander (i) des clauses contractuelles types de nature non contraignante relatives à l'accès aux données et à leur utilisation – dont des clauses relatives à la protection des secrets d'affaires et à une compensation raisonnable – et (ii) des clauses contractuelles standard, également non contraignantes, portant sur les contrats d'informatique en nuage en vue d'aider les parties à prévoir et à négocier des contrats prévoyant des droits et obligations raisonnables, non discriminatoires et équitables.

107. Autorités compétentes. Le *Data Act* impose la désignation, par chaque État membre, d'une ou plusieurs autorités compétentes chargées de son exécution et de son application. Il peut s'agir d'une ou plusieurs nouvelles autorités spécialement établies à cet effet ou d'autorités déjà existantes[307].

300 Voy. règlement (UE) 2023/2854 sur les données, art. 32, §§ 2-5.

301 L'interopérabilité est définie comme « […] la capacité d'au moins deux espaces de données ou réseaux de communication, systèmes, produits connectés, applications, services de traitement de données ou composants d'échanger et d'utiliser des données afin de remplir leurs fonctions » (règlement (UE) 2023/2854 sur les données, art. 2, 40)).

302 Règlement (UE) 2023/2854 sur les données, art. 33, § 1er.

303 Règlement (UE) 2023/2854 sur les données, art. 33, § 4.

304 Règlement (UE) 2023/2854 sur les données, art. 33, § 5.

305 Règlement (UE) 2023/2854 sur les données, art. 36, § 1er.

306 Règlement (UE) 2023/2854 sur les données, art. 36, §§ 5-6.

307 Règlement (UE) 2023/2854 sur les données, art. 37, § 1er.

108. Autorités compétentes : missions et pouvoirs. Les autorités compétentes sont notamment chargées de traiter les réclamations résultant d'infractions alléguées au *Data Act* et d'examiner, dans la mesure nécessaire, l'objet de ces réclamations, ou encore d'imposer des sanctions financières proportionnées, effectives et dissuasives[308]. Elles ont en outre notamment le pouvoir de demander aux utilisateurs, aux destinataires et détenteurs de données, ou à leurs représentants légaux, relevant de la compétence de leur État membre, toutes les informations nécessaires à la vérification du respect du *Data Act*[309].

109. Autorités compétentes : coordinateur des données. Si plusieurs autorités compétentes sont désignées au sein d'un même État membre, un coordinateur des données doit en outre être désigné parmi ces autorités compétentes. Son rôle consiste principalement à faciliter la coopération entre les autorités compétentes désignées dans l'État membre concerné[310].

110. Autorités compétentes : relations avec les autorités de protection des données et le Contrôleur européen de la protection des données. Dans la mesure où la protection des données à caractère personnel est concernée, la mission de contrôle de l'application du *Data Act* est déléguée aux autorités de protection des données (au sens du RGPD) et, en ce qui concerne la Commission, la BCE et les organes de l'Union, au Contrôleur européen de la protection des données (ci-après « CEPD »)[311].

111. Comité européen de l'innovation dans le domaine des données. Les autorités compétentes seront représentées au sein du Comité européen de l'innovation dans le domaine des données, lequel consiste en un groupe d'experts établi par la Commission conformément à l'article 29 du DGA. Ledit Comité sera chargé de contribuer à l'application cohérente du *Data Act*, principalement à travers son rôle consultatif vis-à-vis de la Commission[312].

112. Voies de recours. Si une personne physique ou morale estime qu'une atteinte a été portée aux droits que lui confère le *Data Act*, elle peut, sans préjudice de tout autre recours juridictionnel ou administratif, introduire une réclamation – individuellement ou, le cas échéant, collectivement avec d'autres personnes lésées – auprès de l'autorité compétente qui se situe dans l'État membre dans lequel elle a sa résidence habituelle, son lieu d'établissement ou son lieu de travail[313]. Elle dispose également d'un droit à un recours juridictionnel effectif contre les décisions juridiquement contraignantes adoptées par les autorités compétentes[314].

113. Sanctions. Les sanctions applicables en cas de violation du *Data Act* devront être déterminées par les États membres[315]. Elles devront, en tout état de cause, être proportionnées, effectives

308 Règlement (UE) 2023/2854 sur les données, art. 37, § 5.

309 Règlement (UE) 2023/2854 sur les données, art. 37, § 14.

310 Règlement (UE) 2023/2854 sur les données, art. 37, § 2. Pour plus de détails concernant les missions du coordinateur de données, voy. art. 37, § 6.

311 Règlement (UE) 2023/2854 sur les données, art. 37, § 3.

312 Règlement (UE) 2023/2854 sur les données, art. 42.

313 Règlement (UE) 2023/2854 sur les données, art. 37, § 2.

314 Règlement (UE) 2023/2854 sur les données, art. 39, § 1er.

315 Comme l'indique le considérant 109 du *Data Act*, « […] [c]es sanctions pourraient revêtir la forme, entre autres, de sanctions pécuniaires, d'avertissements, de blâmes ou d'injonctions de mettre des pratiques commerciales en conformité avec les obligations instaurées par le présent règlement […] ».

et dissuasives. Les États membres seront par ailleurs tenus de mettre en place les mesures nécessaires à la mise en œuvre de ces sanctions[316].

Dans la mesure où les violations des dispositions contenues aux chapitres II, III et V du *Data Act* concernent la protection des données à caractère personnel, les autorités de protection des données et le CEPD pourront, en respectant les limites de leurs compétences, imposer les amendes administratives conformément au RGPD et au règlement 2018/1725[317] et dont le montant maximal correspond au montant maximal des amendes administratives pouvant être imposées en cas de violation de ces instruments[318].

5. Conclusion et réflexions prospectives

114. Apports du *Data Act*. Grâce aux obligations de partage de données ainsi qu'aux exigences en matière d'interopérabilité et de changement de services de traitement de données, le *Data Act* devrait favoriser le développement d'une économie fondée sur les données au sein de l'Union. En particulier, les dispositions relatives à la mise à disposition de données qu'il instaure devraient encourager les acteurs économiques à développer et mettre sur le marché des produits et services innovants, notamment en matière d'intelligence artificielle.

115. Potentielles difficultés de mise en application. La mise en application pratique du *Data Act* risque toutefois de se révéler complexe à divers égards, et notamment en ce qui concerne l'interprétation et l'articulation du texte avec d'autres instruments. Premièrement, en raison du caractère (délibérément ?) flou de certaines dispositions du *Data Act*, des difficultés d'interprétation risquent d'apparaître, ouvrant ainsi la porte à des discussions quant à la portée des exigences applicables. Pensons notamment aux notions de « besoin exceptionnel » conditionnant la mise à disposition de données *B2G*, et de « données qui ne sont pas substantiellement modifiées » (données sous forme brute et données prétraitées), soumises aux obligations de partage *B2C* et *B2B*[319], à la détermination de la pertinence de rendre les données relatives à un produit connecté ou à un service connexe directement accessibles à l'utilisateur, ou encore à l'évaluation du caractère « strictement nécessaire » de la divulgation d'un secret d'affaires à un tiers pour atteindre l'objectif convenu entre l'utilisateur qui exerce son droit à la portabilité des données et ce tiers. En conséquence, les renvois préjudiciels en interprétation devant la Cour de justice risquent de se multiplier, à l'instar des renvois préjudiciels relatifs à l'interprétation des dispositions du RGPD. Deuxièmement, l'articulation des exigences du *Data Act* avec les obligations imposées par la législation applicable en matière de protection des données à caractère personnel, en particulier le RGPD, pourrait s'avérer complexe pour le détenteur de données

316 Règlement (UE) 2023/2854 sur les données, art. 40, § 1er.

317 Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE, *J.O.*, L 295, 21 novembre 2018.

318 Règlement (UE) 2023/2854 sur les données, art. 40, §§ 4-5.

319 Contrairement aux «[…] informations dérivées ou déduites de ces données, qui sont le résultat d'investissements supplémentaires dans l'attribution de valeurs ou d'informations tirées des données, en particulier au moyen d'algorithmes complexes et propriétaires, y compris ceux qui font partie d'un logiciel propriétaire […]» (règlement (UE) 2023/2854 sur les données, cons. 15).

tenu de mettre des données à disposition d'un utilisateur ou d'un destinataire de données. Même l'identification, d'apparence élémentaire, du caractère « personnel » ou « non personnel » d'une donnée n'est pas si évidente à effectuer[320]. Cette distinction, qui conditionne l'application du RGPD, a pourtant des conséquences importantes aux fins de l'application du *Data Act*. À titre d'exemple, le détenteur de données qui ne souhaiterait pas partager des données avec un tiers pourrait faire en sorte que les négociations portant sur les termes du partage des données n'aboutissent pas et prétexter que les données sur lesquelles portent la demande de portabilité de l'utilisateur ne sont pas des données à caractère personnel, ce qui lui permettrait d'échapper à son obligation de mettre à disposition du tiers les données demandées.

En conclusion, de nombreuses zones d'ombre quant à l'application du *Data Act* peuvent à ce stade être identifiées. Elles devraient toutefois s'éclaircir au fil de la mise en application du texte et des précisions qui seront, le cas échéant, apportées par la Cour de justice.

C. Proposition de règlement du Parlement européen et du Conseil relatif à la transparence et au ciblage de la publicité à caractère politique[321]

Alix Gobert[322] et Martin Rappe[323]

116. Contextualisation. Cette proposition de règlement s'inscrit dans le cadre du paquet législatif sur « le renforcement de la démocratie et l'intégrité des élections européennes »[324]. La publicité en ligne étant en outre une activité de service, la proposition vient compléter le règlement sur les services numériques pour ce qui concerne le secteur spécifique de la publicité à caractère politique[325].

117. Objet de la proposition. La proposition s'articule autour de deux objectifs principaux[326]. Premièrement, elle tend à définir des règles harmonisées au niveau européen pour un niveau élevé de transparence de la publicité à caractère politique et des services connexes[327]. Elle entend notamment atteindre cet objectif à travers l'imposition d'une obligation, pour les parraineurs, de déclarer l'éventuelle nature politique de la publicité qu'ils souhaitent confier à un service de

320 Voy. à cet égard : C.J., arrêt *Gesamtverband Autoteile-Handel eV c. Scania CV AB*, 9 novembre 2023, C-319/22, EU:C:2023:837, pts 45-46 ; C.J., arrêt *Patrick Breyer c. Bundesrepublik Deutschland*, 19 octobre 2016, C-582/14, EU:C:2016:779, pts 42-46 ; T.U.E., arrêt *Conseil de résolution unique (CRU) c. Contrôleur européen de la protection des données (CEPD)*, 26 avril 2023, T-557/20, EU:T:2023:219, pt 93 ; A. Gobert, M. Knockaert, M. Rappe et J.-M. Van Gyseghem, « La donnée à caractère personnel et sa réutilisation », *J.T.*, 2024, n° 8, pp. 124-127.

321 Proposition de règlement du Parlement européen et du Conseil du 25 novembre 2021 relatif à la transparence et au ciblage de la publicité à caractère politique, COM(2021) 731 final (ci-après : « Proposition relative à la transparence et au ciblage de la publicité à caractère politique »). Dans l'intervalle de la rédaction de cette chronique, cette proposition a été adoptée par le Parlement européen le 13 mars 2024.

322 Alix Gobert est chercheuse au CRIDS/NaDI.

323 Martin Rappe est chercheur au CRIDS/NaDI et consultant en protection des données et en sécurité de l'information (www.keystone-solutions.be).

324 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions relative au plan d'action pour la démocratie européenne, Bruxelles, le 3 décembre 2020.

325 Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques). Proposition relative à la transparence et au ciblage de la publicité à caractère politique, Exposé des motifs, p. 4.

326 Proposition relative à la transparence et au ciblage de la publicité à caractère politique, art. 1.1.

327 Proposition relative à la transparence et au ciblage de la publicité à caractère politique, chap. II.

publicité[328]. Elle poursuit aussi cet objectif en rendant obligatoire l'apposition d'une mention faisant référence au caractère politique de la publicité sur l'annonce concernée[329]. Deuxièmement, la proposition a également pour objectif la protection des personnes physiques en matière de traitement des données à caractère personnel les concernant[330]. À cette fin, la proposition pose le principe selon lequel le traitement de catégories particulières de données à caractère personnel à des fins de ciblage ou d'annonce publicitaire à caractère politique est interdit[331], sauf si le responsable du traitement peut faire valoir une exemption spécifique, notamment en cas d'obtention du consentement de la personne concernée[332]. En outre, la proposition entend imposer des obligations complémentaires et spécifiques au traitement de données à caractère personnel à des fins de ciblage publicitaire en imposant notamment aux responsables du traitement de mettre en place une politique interne, de tenir des registres dont le contenu est spécifique à cette activité et d'étendre l'obligation de transparence vis-à-vis des personnes concernées en ajoutant une obligation d'information sur la logique et les aspects techniques du ciblage utilisé[333].

Notons, finalement, que la proposition de règlement prévoit une définition de ce qu'il convient d'entendre par « publicité à caractère politique », afin de garantir un encadrement harmonisé et transfrontière au sein de l'Union européenne[334].

D. Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »)

Antoine Delforge[335]

118. Introduction et contexte. En vue de remplacer la directive 2002/58/CE « vie privée et communications électroniques »[336] visant à protéger spécifiquement la vie privée des utilisateurs dans le secteur des communications électroniques, la Commission a adopté une proposition de règlement (portant le même nom)[337] en 2017. Celle-ci tendait à mettre à jour la directive compte tenu notamment de l'adoption du RGPD. Près de six ans plus tard, ce futur règlement n'a toujours

328 Proposition relative à la transparence et au ciblage de la publicité à caractère politique, art. 5.
329 Proposition relative à la transparence et au ciblage de la publicité à caractère politique, art. 7.1, (a).
330 Proposition relative à la transparence et au ciblage de la publicité à caractère politique, chap. III.
331 Proposition relative à la transparence et au ciblage de la publicité à caractère politique, art. 12.1.
332 Proposition relative à la transparence et au ciblage de la publicité à caractère politique, art. 12.2.
333 Proposition relative à la transparence et au ciblage de la publicité à caractère politique, art. 12.3. Concernant ce point, notons que l'exposé des motifs de la proposition indique qu'elle vise à compléter et à développer les dispositions applicables au traitement des données à caractère personnel dans le contexte de la publicité à caractère politique, contenues dans le règlement (UE) 2016/679 et le règlement (UE) 2018/675 (Proposition relative à la transparence et au ciblage de la publicité à caractère politique, Exposé des motifs, p. 5).
334 Proposition relative à la transparence et au ciblage de la publicité à caractère politique, art. 2.2.
335 Assistant-doctorant à la Faculté de droit de l'UNamur et chercheur au CRIDS/NaDI.
336 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.*, L 201, 31 juillet 2002. On parle également de « directive ePrivacy ».
337 Proposition du 10 janvier 2017 de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »).

pas été adopté et la dernière version du texte date de février 2021[338]. Le texte ayant fort changé sur des points importants entre ces deux versions, il est probable que le texte évolue encore.

119. Traitements des données par les fournisseurs de réseaux et services de communication électronique (art. 5-7). La proposition précise que les communications électroniques (contenu et metadata) sont confidentielles. Toutefois, ce texte permet dans des cas particuliers aux fournisseurs de réseaux et de services de communications électroniques de traiter certaines données de communications électroniques, notamment si cela est techniquement nécessaire ou en cas de consentement de l'utilisateur.

120. Règles spécifiques en matière cookies et autres techniques de traçage (art. 4a, 8 et 11). La directive prévoit qu'il est interdit de déposer un quelconque fichier sur l'équipement terminal de l'utilisateur ou d'utiliser des informations sur cet équipement, sauf si l'utilisateur l'a autorisé ou si cela est nécessaire pour la fourniture du service. Cela visait notamment à encadrer certaines techniques de traçage des utilisateurs au moyen de cookies (fichiers déposés sur l'équipement terminal), ou d'autres techniques basées sur l'analyse des caractéristiques techniques de l'équipement (*digital fingerprinting*). Le futur règlement ne changerait pas le principe. Toutefois, il prévoirait d'autres hypothèses où le consentement de l'utilisateur ne serait pas requis, notamment pour des raisons de mesure d'audience, ou raisons de sécurité, ou lutte contre la fraude. S'il est clairement précisé que la validité du consentement obtenu s'appréciera au regard des règles prévues dans le RGPD à ce sujet, plusieurs précisions sont apportées. Initialement, il était envisagé que les navigateurs web doivent prévoir un blocage par défaut des cookies et proposer aux utilisateurs un moyen de paramétrer quels types de cookies ils autoriseraient. Dans la dernière version du texte, cette méthode resterait valable pour exprimer un consentement. Cependant, cette méthode, bien qu'apparemment encouragée, ne devrait plus obligatoirement être prévue dans les navigateurs web.

Dans la dernière version du texte, une autre précision mérite d'être mentionnée. Le considérant 20aaa prévoit explicitement de légaliser la pratique consistant à bloquer l'accès à un site web se finançant par de la publicité ciblée, utilisant des cookies par exemple, si l'utilisateur refuse ce type de traitement de données, pour autant qu'une « offre équivalente » sans traitement de données soit proposée[339,340].

121. Autres droits de l'utilisateur en matière de communications électroniques (art. 12-16). La proposition prévoit également différents droits pour l'utilisateur. Elle encadre ainsi la possibilité pour l'utilisateur de masquer son numéro lors d'appels. Elle impose aux fournisseurs de services de communications certaines obligations en vue de prévenir les appels indésirables et adapte légèrement les règles en matière de prospection directe non sollicitée.

338 Nous nous baserons sur cette version du texte et cette numérotation des articles (version du 10 février 2021, doc. 6087/21).

339 La Cour de justice a rendu le 4 juillet 2023 un arrêt *Meta c. Bundeskartellamt* (C-252/21) portant sur cette question.

340 Il est fort à parier que ces deux points spécifiques ont été l'une des raisons ayant retardé l'adoption du texte. De fait, depuis plusieurs années, et l'adoption du RGPD n'a pas répondu à la question, il existe un débat sur la possibilité de bloquer l'accès à un site si l'utilisateur « refuse les cookies publicitaires ». À ce sujet, nous renvoyons notamment à lettre du 13 décembre 2023 de l'EDPB répondant à l'« Initiative de la Commission pour un engagement volontaire des entreprises visant à simplifier la gestion par les consommateurs des cookies et des choix publicitaires personnalisés – Projet de principes ».

E. Proposition de règlement européen relatif à l'espace européen des données de santé (« European Health Data Space »)[341]

Jean-Marc Van Gyseghem[342]

122. Contexte. À titre de préambule, il est utile de rappeler que l'ambition de l'Union européenne est de créer divers espaces de données liés à des domaines spécifiques. L'EHDS constitue donc le premier maillon. L'objectif de cet espace de données de santé est de répondre « aux particularités du secteur de la santé concernant l'accès et le partage des données de santé électroniques »[343] et « fera partie intégrante de la création d'une union européenne de la santé »[344] dans la foulée de la pandémie Covid-19. Pour atteindre cet objectif, il met en place deux niveaux d'utilisation, à savoir les utilisations primaire et secondaire des données de santé électroniques.

1. L'utilisation primaire

123. Notion. L'utilisation primaire est définie comme « le traitement de données de santé électroniques à caractère personnel pour la fourniture de services de santé visant à évaluer, maintenir ou rétablir l'état de santé de la personne physique à laquelle ces données se rapportent, y compris la prescription, la dispensation et la fourniture de médicaments et de dispositifs médicaux, ainsi que pour les services de sécurité sociale, administratifs ou de remboursement pertinents »[345].

124. Accès aux données. Dans le cadre d'un tel traitement, les professionnels de la santé peuvent consulter les données de santé électroniques de leurs patients, quels que soient l'État membre d'affiliation et l'État membre de traitement, dans le respect du principe de minimisation conformément au RGPD. En complément à ceci, le patient peut tant consentir à l'accès à ses données de santé électroniques par tout autre destinataire du secteur de la santé ou sécurité sociale de son choix que demander leur transmission à ces mêmes acteurs. À noter que ce principe fait quelque peu écho à la section 12 de la loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé réglant l'accès aux données de santé[346].

125. Droits de la personne. Par ailleurs, les personnes physiques se voient attribuer, ou confirmer, des droits tels que ceux d'accès ou de rectification outre celui d'accès au log reprenant les personnes ayant eu accès au dossier médical électronique les concernant. Afin de permettre l'exercice de ces droits, les États membres doivent mettre en place, « à l'échelon national, régional ou local, un ou plusieurs services d'accès aux données de santé électroniques »[347]. De

341 Proposition de règlement du Parlement européen et du Conseil du 3 mai 2022 relatif à l'espace européen des données de santé, COM(2022) 197 final.

342 Directeur adjoint du CRIDS et avocat au barreau de Bruxelles. Cette publication a été réalisée avec le soutien financier du programme de recherche Digital Europe dans le cadre de la convention de subvention n° 101100700 (TEF-Health) et n° 101136379 (CERTAINTY). Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

343 EHDS, Exposé des motifs, Justification et objectifs de la proposition, p. 1.

344 *Ibid*.

345 EHDS, art. 2, 2., d).

346 Loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé, *M.B.*, 14 mai 2019.

347 EHDS, art. 3, 5., a).

plus et pour permettre une libre circulation des données de santé dans le cadre de cette utilisation primaire, une plateforme centrale pour la santé numérique est créée ; plateforme qui est reliée à des points de contact nationaux qui permettent l'échange des données de santé électroniques.

126. Situation en Belgique. La Belgique connaît déjà un système de *hubs*, que sont les réseaux santé régionaux et un *Metahub*, à savoir la plateforme *e-Health*, mettant en place des interconnections dans le cadre d'une telle utilisation primaire. Ce maillage permet, dans le respect de la section 12 de la loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé, de partager des données de santé entre professionnels de la santé moyennant le consentement de ces derniers et des patients concernés par les données ainsi partagées. Il conviendra dès lors d'analyser la manière avec laquelle ces réseaux existants pourront s'intégrer dans cette nouvelle structure européenne.

2. L'utilisation secondaire

127. Finalités. L'utilisation secondaire qui se fonde sur les données « produites » dans le cadre de l'utilisation primaire doit s'inscrire dans une des finalités reprises à l'article 34 de la proposition. Parmi ces finalités, l'on retrouve l'enseignement dans les secteurs de la santé ou des soins, la recherche scientifique en matière de santé ou la « protection contre les menaces transfrontières graves pour la santé »[348]. À n'en pas douter, cette dernière finalité est une réponse à la pandémie Covid-19. Par ailleurs, l'utilisation secondaire est interdite pour certaines finalités[349] telles des décisions préjudiciables à une personne physique ou encore des prises de décisions menant à une exclusion de personnes physiques d'un contrat d'assurance ou à une modification des cotisations ou des primes d'assurance.

128. Accès aux données. À l'instar des structures mises en place dans le cadre de l'utilisation primaire, les États membres devront désigner un ou plusieurs organismes chargés d'accorder l'accès aux données de santé électroniques à des fins d'utilisation secondaire.

129. La situation en Belgique. À noter que Sciensano est actuellement impliqué dans le projet EHDS2 PILOT qui « concevra, étudiera et analysera des cadres normatifs sur la gouvernance des données, la qualité des données et les infrastructures pour le partage des données entre différents pays participants à travers toute l'Europe »[350]. Par ailleurs, l'État belge a mis en place l'autorité des données santé (ADS) qui a pour mission principale « de soutenir la transition du système (de soins) de santé belge vers des soins axés sur les données. La mise à disposition de données de (soins de) santé pour le soutien aux politiques, l'innovation, la recherche et le développement de produits est essentielle à cet égard »[351]. Ces diverses institutions et, plus particulièrement, l'ADS serviront-elles d'organisme responsable de l'accès aux données dans le cadre de l'utilisation secondaire ? Il conviendra d'y répondre.

348 EHDS, art. 34, 1., a).

349 EHDS, art. 35.

350 https://www.sciensano.be/fr/projets/projet-pilote-sur-lespace-europeen-des-donnees-de-sante-pour-une-utilisation-secondaire-des-donnees.

351 https://news.belgium.be/fr/institution-dune-autorite-des-donnees-de-soins-de-sante.

F. Proposition de règlement établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union (règlement pour une Europe interopérable)

Pauline Willem[352]

130. Objectif de la proposition. La proposition de règlement pour une Europe interopérable[353] vise à ce que les services publics numériques dans l'Union européenne atteignent un haut degré d'interopérabilité. De la sorte, les échanges et la coopération entre ces services publics d'une part et avec les citoyens et entreprises d'autre part seront facilités. Les certificats Covid-19 européens ont démontré l'utilité de l'interopérabilité. Elle a en effet permis qu'ils puissent fonctionner au sein de toute l'Union européenne[354].

131. Cadre actuel de l'interopérabilité au niveau européen. Un instrument non contraignant connu sous le nom de *European interoperability framework* (« EIF »[355]) est déjà consacré à l'interopérabilité des services publics. Toutefois, l'analyse d'impact réalisée en amont de la proposition a montré que les recommandations de l'EIF ne sont plus suffisantes pour déployer des services publics numériques interopérables, de sorte qu'un instrument plus contraignant s'avère nécessaire.

132. Base juridique, éléments de la proposition et adoption. La Commission a donc adopté une proposition de règlement. Elle est basée sur l'article 172 TFUE (qui concerne l'établissement et le développement de réseaux transeuropéens dans les secteurs du transport, des télécommunications et de l'énergie). Diverses mesures sont prévues dont, le partage et la réutilisation de solutions d'interopérabilité entre les secteurs publics[356], une évaluation préalable de l'interopérabilité des solutions[357] ou encore la mise en place de systèmes de coopération sur la question de l'interopérabilité[358]. À l'heure d'écrire ces lignes, les négociations ont déjà bien avancé. Le trilogue a débuté et l'adoption du texte est prévue pour fin 2023 ou début 2024[359].

---

352 Pauline Willem est chercheuse au CRIDS/NaDI, avocate au barreau de Bruxelles et experte auprès de la Commission européenne.

353 Proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union (règlement pour une Europe interopérable), COM(2022) 720 final, 18 novembre 2022 (ci-après, « proposition interopérabilité »).

354 Voy. le règlement (UE) 2021/953 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats Covid-19 interopérables de vaccination, de test de rétablissements (certificat Covid numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de Covid-19, *J.O.U.E.*, L 211, 15 juin 2021.

355 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Cadre d'interopérabilité européen – Stratégie de mise en œuvre, COM(2017) 134 final.

356 Proposition interopérabilité, art. 4.

357 Proposition interopérabilité, art. 3.

358 Proposition interopérabilité, chap. 4.

359 Dans l'intervalle de la rédaction de la présente analyse, le règlement a été adopté (voy. règlement (UE) 2024/903 du Parlement européen et du Conseil du 13 mars 2024 établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union (règlement pour une Europe interopérable), *J.O.*, L, 22 mars 2024.