Le Data Act, l'éléphant dans le couloir

Sébastien VIOU
Stratège Cybersécurité
Fortinet

Adopté officiellement en janvier 2024 et applicable à partir du 12 septembre 2025, le Data Act est présenté comme la grande réforme européenne nécessaire à la construction d'un marché unique de la donnée. Son objectif est clair : faciliter l'accès, la portabilité et l'utilisation des données générées par les utilisateurs de produits et services numériques, qu'il s'agisse d'objets connectés, de services cloud, ou de plateformes SaaS. En théorie, tout le monde devrait se réjouir : plus d'innovation, moins de dépendance, plus de concurrence. En pratique, le Data Act avance dans un silence assourdissant, éclipsé par NIS2 qui, dans les médias et les conférences, rafle toute l'attention. Pourtant, ce texte pourrait avoir des conséquences plus lourdes encore sur le quotidien des entreprises. Et à ce rythme, il faut le dire franchement : personne ne sera prêt.

Objectif : ouvrir le marché Européen du Cloud

Pour rappel, le Data Act impose que les données générées par un produit ou un service soient accessibles à son utilisateur et transférables vers un tiers de son choix. Conséquence directe : l'ère des écosystèmes fermés touche à sa fin. Prenons l'exemple d'une entreprise qui utilise des machines industrielles connectées : les données de performance ne pourront plus être verrouillées par le fabricant, elles devront être mises à disposition de l'entreprise utilisatrice et de tout prestataire tiers désigné. Même logique pour un particulier qui possède une voiture connectée : les données ne pourront plus être exclusivement réservées au constructeur, elles devront pouvoir être partagées avec un garagiste indépendant. Sur le papier, c'est une révolution. Mais combien d'acteurs sont techniquement prêts à fournir cette interopérabilité de manière sécurisée et documentée ?

Un impact sur l'ensemble des contrats

D'autant que le Data Act ne se limite pas à la technique. Il impose une véritable révolution contractuelle. Les clauses interdisant ou limitant l'accès et la portabilité des données deviennent clairement abusives, et même illégales. Les fournisseurs devront revoir leurs contrats de service en profondeur. Par exemple, un éditeur SaaS ne pourra plus imposer des frais prohibitifs pour exporter les données d'un client. De même, un fournisseur cloud ne pourra plus insérer dans ses CGU des clauses rendant la migration impossible ou dont le coût serait à définir au moment de réaliser l'action. Les juristes d'entreprise et les directions achats vont devoir se retrousser les manches pour réécrire leurs contrats. Et une fois le contrat rédigé, ce texte devient une gigantesque source de potentiels litiges, que le monde juridique se fera un plaisir de traiter.

Le tout, dans le respect de l'état de l'art Cybersécurité

Et puisque l'on parle de contractuel, il va de soi que partage et portabilité ne signifient pas abandon de la sécurité. Le Data Act insiste : les données doivent circuler en toute confiance. Cela implique chiffrement systématique, contrôle d'accès granulaire, journalisation exhaustive et traçabilité. Imaginez une entreprise de santé qui souhaite transférer ses données patients d'un cloud vers un autre : le fournisseur sera obligé de garantir un transfert chiffré de bout en bout, avec un suivi détaillé des accès. Même chose dans l'industrie aéronautique : si un sous-traitant transfère des données de maintenance, il devra démontrer que ces données sont protégées à chaque étape.

Et avec le maximum de simplicité

Que l'on se rassure cependant, le transfert est simple. Ou plutôt, il le sera forcément. Pourquoi ? Parce que le Data Act l'exige. Comment ? Avec l'utilisation d'API standard et documentées. Oubliez les formats propriétaires conçus pour dissuader les clients de migrer. Désormais, un fournisseur devra mettre en place des interfaces claires, normalisées et publiques. Prenons l'exemple d'une solution de gestion RH en SaaS : les données des salariés devront pouvoir être extraites via des API lisibles par des tiers, pas seulement par l'éditeur d'origine. Même contrainte pour un constructeur de capteurs IoT industriels : les données de télémétrie devront être accessibles par des standards ouverts. L'impact est colossal : cela implique de revoir les architectures techniques, de développer des passerelles fiables et d'investir dans l'interopérabilité. Un travail considérable qui, même s'il est aidé par de nombreux langages standardisé (REST API, JSON), reste largement sous-estimé.

Dans un délai acceptable et encadré

Pour finir sur le terrain des mesures applicable, la cerise sur le gâteau, le Data Act ne se contente pas de définir des principes : il impose des délais d'application stricts. Un client qui souhaite changer de fournisseur ne pourra pas être retenu captif indéfiniment. Le texte fixe deux contraintes claires : un préavis maximum de deux mois et un transfert des données devant être achevé en moins de trente jours. Prenons un exemple concret : une entreprise qui souhaite migrer d'un fournisseur cloud A vers un acteur G devra pouvoir le faire en respectant ce calendrier. Le fournisseur sortant n'aura pas le droit de ralentir volontairement le processus ou de facturer des frais excessifs. Dans l'absolu, c'est une bonne nouvelle pour les clients. Mais dans la réalité, combien d'opérateurs cloud sont capables de garantir un transfert complet, sécurisé et opérationnel en 30 jours ? Très peu. Et encore moins de clients ont anticipé ces obligations pour l'inclure dans leur gouvernance IT.

Avec des conséquences business et industrielles fortes

On le sent à travers ces paragraphes, les conséquences pour les entreprises sont importantes, surtout que le Data Act ne concerne pas uniquement les géants du cloud. Il touche aussi les PME, les startups et les industriels. Et ce quelque soit le pays d'origine de l'entreprise, à partir du moment où elle commercialise un produit au sein de l'Union Européenne. Un fabricant d'objets connectés devra revoir sa stratégie de données, un éditeur SaaS devra repenser son modèle économique, un prestataire de service SOC devra anticiper la traçabilité de ses échanges de données. À court terme, cela représente un coût de mise en conformité considérable : adaptation des systèmes, mise à jour des contrats, formation des équipes. À long terme, c'est un changement complet de paradigme : l'économie de la donnée ne sera plus fermée, mais ouverte et transparente.

En conclusion : serez-vous prêt ?

Pour conclure, le Data Act est, en théorie, une

avancée majeure pour l'économie numérique européenne. En pratique, il est invisible dans le débat public, éclipsé par NIS2 et le CRA. Or, entre l'ouverture des données, la mise à jour contractuelle, l'adoption d'API standard et le respect des délais de migration, les défis sont immenses. Et soyons honnêtes : à ce rythme, la majorité des entreprises concernées ne seront pas prêtes en septembre 2025. Le Data Act avance dans l'ombre, mais son impact n'en sera que plus brutal. Et cette fois, il ne suffira pas de lancer un plan d'action improvisé pour éviter les sanctions : la révolution des données est en marche, et elle ne laissera personne intact.

Il est très probable que ce dernier paragraphe vous ai interpelé, car oui, Septembre 2025, c'était bien il y a 2 mois…