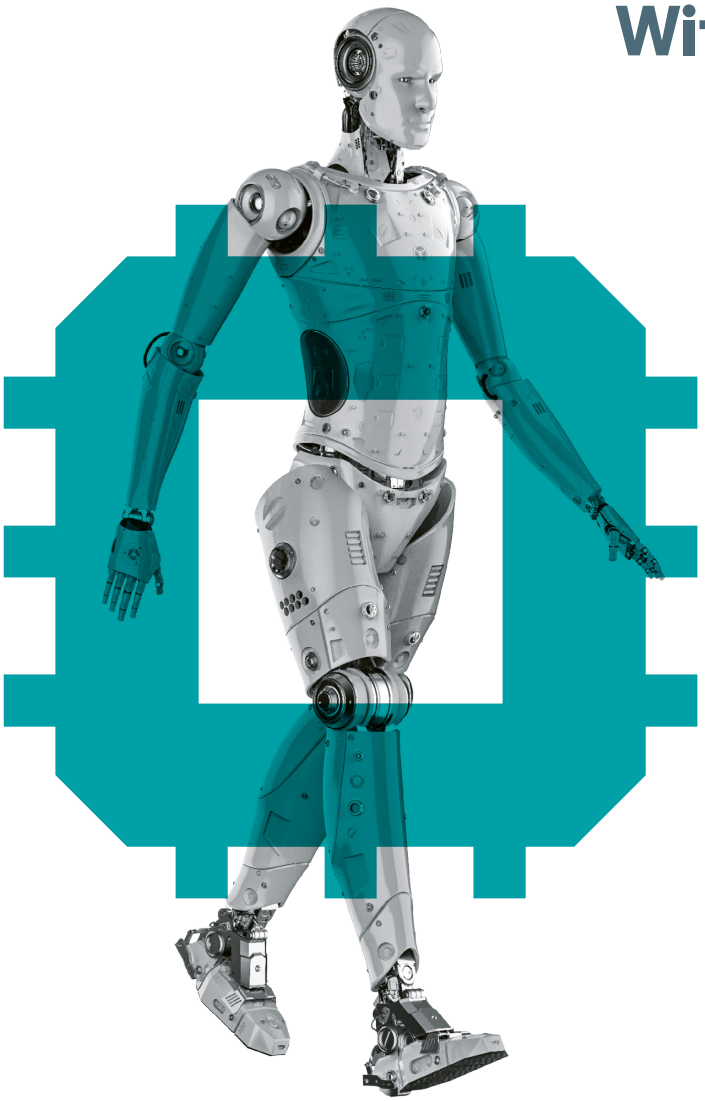
N

Monthly Newsletter March 2025

ICT

Schellenberg Wittmer



Pertinence pour les entreprises suisses des réglementations européennes dans le domaine du numérique

Roland Mathys, Jacqueline Brunner

Key Take-aways

1.
Les entreprises suisses actives dans l'UE et y offrant des produits ou services entrent souvent dans le champ d'application de diverses réglementations de l'UE dans le domaine du numérique, cela directement ou au travers de l'effet extraterritorial desdites réglementations.

2.
Les règlements de l'UE introduisent des règles de conduite étendues visant à renforcer la sécurité, la transparence et l'innovation, ainsi qu'à améliorer l'accès aux données.

3.
Les infractions peuvent entraîner des sanctions importantes, c'est pourquoi les entreprises suisses devraient évaluer en permanence la nécessité de prendre certaines mesures de mise en conformité.

1 Introduction

De nombreux textes législatifs ont été récemment adoptés dans l'Union européenne (**UE**) dans le domaine du numérique et des données. Cette lettre d'information propose un bref aperçu d'une sélection de textes législatifs (sans prétendre à l'exhaustivité) relatifs à l'environnement numérique et met en lumière leur pertinence pour les entreprises suisses.

2 Règlement sur les données (Data Act, DA), Règlement sur les services numériques (Digital Services Act, DSA) et Règlement sur les marchés numériques (Digital Markets Act, DMA)

Le DA est entré en vigueur le 11 janvier 2024 et sera applicable dans toute l'UE après une période de transition de 20 mois.

Le DA vise à garantir **un libre accès aux données** et à encourager l'innovation. Parmi les dispositions centrales de le DA figurent la garantie de l'accès aux données et de leur mise à disposition, ainsi que la garantie de l'interopérabilité et de la conformité aux contrats.

Le DA concerne **les données personnelles et non-personnelles** générées dans le cadre de l'utilisation de «produits connectés» (objets capables d'obtenir, de générer ou de collecter des données sur leur utilisation ou leur environnement et de transmettre ces données via une connexion câblée ou sans fil) et de «services connectés» (services numériques associés à un produit connecté et prenant en charge ses fonctionnalités).

Le DA **s'adresse** en particulier aux fabricants de produits en réseau et aux fournisseurs de services connectés, ainsi qu'à leurs utilisateurs, aux détenteurs de données et aux organismes publics. Les micro et petites entreprises (moins de 10 ou 50 employés et EUR 2 ou 10 millions de chiffre d'affaires/bilan) sont en grande partie exemptées des obligations (par ex. transfert de données personnelles). En raison de son effet extraterritorial, dont la portée exacte reste encore incertaine, le DA peut également concerner des **entreprises suisses**, à savoir:

- Les fabricants de produits connectés commercialisés dans l'UE et les fournisseurs de services connectés aux utilisateurs de l'UE;
- les détenteurs de données qui fournissent des données à des destinataires dans l'UE; et
- fournisseurs de services de traitement de données qui offrent leurs services à des clients dans l'UE.

Les infractions au DA **donnent lieu à des sanctions** importantes. Les États membres de l'UE sont tenus d'adopter des règles relatives aux sanctions, et le DA stipule que les sanctions doivent être efficaces, proportionnées et dissuasives. Dans ce cadre, les amendes peuvent atteindre EUR 20 millions ou 4% du chiffre d'affaires annuel mondial.

Le DMA (qui réglemente les *gatekeepers*) et le DSA (qui réglemente les fournisseurs de services numériques) contiennent des règles de conduite étendues pour une utilisation équitable et sûre des plateformes numériques. Les entreprises suisses peuvent également être concernées.

Vous trouverez des informations détaillées à ce sujet dans notre newsletter «Digital Markets Act et Digital Services Act: conséquences pour la Suisse».

3 L'intelligence artificielle (IA)

3.1 Règlement européen sur l'intelligence artificielle (AI Act)

L'AI Act est entré en vigueur le 1er août 2024, avec une mise en œuvre échelonnée dans le temps. L'objectif est de garantir la sécurité et la transparence des systèmes d'IA dans l'UE et de préserver les droits fondamentaux.

L'AI Act distingue entre les **systèmes d'IA et les modèles d'IA**: Le terme système d'IA désigne un système assisté par machine qui peut fonctionner de manière autonome et s'adapter à de nouvelles situations, et qui peut apprendre à partir des entrées qu'il reçoit et faire des prédictions, du contenu, des recommandations ou prendre des décisions qui peuvent affecter des environnements physiques ou virtuels (par exemple, ChatGPT). Les modèles d'IA sont des éléments constitutifs des systèmes d'IA et se rapportent à des composants spécifiques au sein d'un système d'IA (par exemple, les modèles de grands langages, LLM).

De nombreux règlements de l'UE s'appliquent également aux entreprises suisses.

L'AI Act adopte une **approche basée sur le risque**: les systèmes d'IA sont classés en quatre catégories de risque (inacceptable, élevé, limité ou minimal) avec une réglementation décroissante. Alors que les systèmes d'IA à risque inacceptable sont généralement interdits, ceux à risque élevé sont soumis à des conditions strictes (par exemple, la gestion des risques, la gouvernance des données et la documentation technique). Les systèmes d'IA à risque limité sont soumis à des obligations moins strictes (par exemple, obligation d'information sur l'interaction avec un système d'IA) et ceux à risque minimal ne sont guère réglementés; la «compétence en matière d'IA» doit être garantie. La liste étendue des obligations s'adresse en premier lieu aux fournisseurs. Les déployeurs sont responsables de l'utilisation conforme du système d'IA (par exemple, supervision humaine et surveillance du fonctionnement de l'IA). En raison de son **effet extraterritorial**, dont la portée exacte reste encore incertaine, l'AI Act peut également s'appliquer aux **entreprises suisses**. En effet, il s'applique notamment aux:

- fournisseurs qui mettent sur le marché ou mettent en service des systèmes d'IA ou qui commercialisent des modèles d'IA d'usage général dans l'UE, que ces fournisseurs soient établis dans l'UE ou dans un pays tiers;
- fournisseurs et déployeurs de systèmes d'IA basés ou situés dans un pays tiers, lorsque la sortie générée par le système d'IA est utilisée dans l'UE.

Les infractions à l'AI Act peuvent donner lieu à de lourdes **sanctions**, l'AI Act prévoyant des amendes pouvant atteindre EUR 35 millions ou, dans le cas d'une entreprise, 7% du chiffre d'affaires annuel mondial de l'exercice précédent (le montant le plus élevé étant retenu).

Les entreprises concernées peuvent s'attendre à un effort de conformité élevé.

3.2 Point d'actualité: La réglementation de l'IA en Suisse

Le Conseil fédéral a récemment publié un document de position concernant la régulation de l'IA en Suisse (communiqué de presse du 12 février 2025): Selon ce document de position. la Convention sur l'IA du Conseil de l'Europe doit être transposée dans le droit suisse, et les ajustements législatifs nécessaires doivent être apportés de manière sectorielle et spécifique. Une régulation spécifique, exhaustive et détaillée, à l'instar de l'AI Act de l'UE, n'est ainsi pas à l'ordre du jour, la réglementation des activités touchant les droits fondamentaux étant réservée. Les entreprises opérant uniquement en Suisse et ne relevant pas l'AI Act bénéficieront ainsi d'assouplissements, contrairement à celles soumises également à l'AI Act. En effet, la future régulation suisse de l'IA ne mettra pas en œuvre les prescriptions de l'AI Act, ou ne le fera qu'en partie.

4 Règlement sur la cyber-résilience (Cyber Resilience Act, CRA)

Le CRA est entré en vigueur le 10 décembre 2024 et sera pleinement applicable à partir du 11 décembre 2027, après une période de mise en œuvre de trois ans. Toutefois, certaines dispositions (telles que l'obligation de signaler les vulnérabilités informatiques et les incidents de sécurité) peuvent être appliquées plus tôt.

Le CRA vise à améliorer de manière significative la **cybersécurité** des produits en réseau. Le CRA définit des exigences minimales en matière de cybersécurité et couvre les produits contenant des «éléments numériques» qui sont commercialisés dans l'UE et peuvent être connectés à Internet, à d'autres appareils ou à des réseaux, tels que les produits matériels et logiciels, les appareils de l'Internet des objets, les appareils ménagers intelligents, les véhicules connectés et les machines industrielles.

Les dispositions importantes du CRA concernent la garantie de la cybersécurité tout au long du cycle de vie, le respect des obligations de notification, de documentation et de transparence, les évaluations de conformité et la fourniture de mises à jour de sécurité. Les obligations concrètes découlent du rôle du destinataire ainsi que de la qualification du produit. Les fabricants sont les premiers responsables de la sécurité des produits et doivent, par exemple, préparer une documentation technique et des supports d'information sur la cybersécurité. Les importateurs et les distributeurs doivent s'assurer que les produits sont conformes à la réglementation (par exemple, vérifier le marquage CE/la déclaration de conformité). Les obligations de notification des risques de sécurité et des vulnérabilités concernent tous les acteurs.

Le CRA s'adresse aux fabricants, importateurs et distributeurs de l'UE. En raison de son **effet extraterritorial**, dont la portée exacte reste encore incertaine, il s'applique également aux fabricants, importateurs et distributeurs suisses qui fournissent de tels produits à des acheteurs dans l'UE.

Les infractions au CRA peuvent donner lieu à de lourdes **sanctions**, à savoir des amendes pouvant atteindre EUR 15 millions ou 2,5% du chiffre d'affaires mondial du groupe (le montant le plus élevé étant retenu). En outre, des mesures de surveillance du marché - telles que des rappels obligatoires de produits - sont possibles.

Les contrevenants s'exposent à des sanctions importantes.

5 Règlement sur la résilience opérationnelle numérique (Digital Operational Resilience Act, DORA)

Le DORA est entré en vigueur le 17 janvier 2025. Il **se concentre** sur les risques liés aux technologies de l'information et de la communication (**TIC**) et vise à renforcer la résilience opérationnelle numérique du secteur financier européen.

Le DORA contient **des exigences relatives à la gestion des risques TIC** et aux contrats avec les fournisseurs de services TIC. Les destinataires sont ainsi tenus de mettre en place des mesures de cybersécurité robustes, de réaliser des audits de sécurité et d'assurer la continuité des opérations. Les objectifs clés comprennent: La gestion des risques liés aux TIC, la gestion des tiers en matière de TIC, la gestion des incidents liés aux TIC, les tests et le partage d'informations.

Le DORA s'adresse aux **entreprises financières** de l'UE (par exemple les établissements de crédit, les entreprises d'investissement et les entreprises d'assurance) et aux fournisseurs de TIC qui fournissent des services à ces entreprises financières. Les entreprises suisses qui agissent en tant que **fournisseurs de services TIC** pour des entreprises financières de l'UE ou qui font partie d'un groupe financier de l'UE sont également concernées par le DORA et doivent respecter ses dispositions.

Le DORA ne prévoit pas d'amendes directes ou de **sanctions** pénales. Il appartient plutôt aux États membres de l'UE de prévoir des sanctions dans leur droit national en cas d'infraction. Les autorités compétentes peuvent également prendre des sanctions administratives et des mesures correctives et publier sur leur site web les sanctions administratives imposées et les entreprises concernées.

6 Directive sur la sécurité des réseaux et de l'information (NIS2)

La NIS2 (qui succède à la NIS1) est entrée en vigueur le 16 janvier 2023 et devait être transposée en droit national par les États membres de l'UE avant le 17 octobre 2024. La NIS2 vise à renforcer la cybersécurité dans toute l'UE en établissant des normes plus élevées pour les **infrastructures critiques** et en étendant son champ d'application à d'autres secteurs et types d'organisations.

Les principales **dispositions** de la NIS2 concernent: La gouvernance, les mesures de gestion des risques en matière de cybersécurité, l'évaluation des risques liés à la sécurité des chaînes d'approvisionnement critiques dans l'UE, les obligations de déclaration, la représentation dans l'UE et l'enregistrement des opérateurs d'infrastructures critiques.

Le **champ d'application** de la NIS2 couvre les entités essentielles et importantes, avec différentes obligations liées à leur qualification. La NIS2 s'applique aux entités publiques et privées qualifiées de moyennes ou grandes entreprises (au moins 50 employés et EUR 10 millions de chiffre d'affaires/ total du bilan ou 250 employés et EUR 50 millions de chiffre d'affaires ou EUR 43 millions de total du bilan). Certaines installations (par exemple les réseaux de communication) sont couvertes par le champ d'application indépendamment de cela. Les **entreprises suisses** peuvent également être concernées par la NIS2, à savoir si elles fournissent leurs services ou exercent leurs activités dans l'UE.

Les infractions à la NIS2 peuvent faire l'objet de **sanctions**: Les autorités compétentes peuvent prendre diverses mesures de surveillance et d'application, telles que des inspections sur place. Les contrevenants s'exposent à des amendes pouvant aller jusqu'à EUR 10 millions ou 2% du chiffre d'affaires annuel mondial (le montant le plus élevé étant retenu) dans le cas d'installations importantes.

7 Conclusion

Les réglementations européennes susmentionnées relative à l'environnement numérique (ainsi que d'autres réglementations topiques) ne s'arrêtent pas aux frontières de l'UE (ou de l'EEE) - les entreprises suisses peuvent également être concernées et tenues de les appliquer. Il convient donc de procéder aux vérifications nécessaires aux fins d'identifier si ces réglementations sont à prendre en compte dans le cadre des activités des entreprises suisses et, cas échéant, d'agir de manière ciblée!

Roland Mathys
Associé
roland.mathys@swlegal.ch

Lorenza Ferrari Hofer
Associée
lorenza.ferrari@swlegal.ch

Stéphanie Chuffart-Finsterwald
Associée
stéphanie.chuffart@swlegal.ch

Grégoire Tribolet
Associé
gregoire.tribolet@swlegal.ch

Schellenberg Wittmer Ltd
Avocats

Zurich
Löwenstrasse 19
Case postale 2201
8021 Zurich / Suisse
T +41 44 215 5252
www.swlegal.com

Genève
15bis, rue des Alpes
Case postale 2088
1211 Genève 1 / Suisse
T +41 22 707 8000
www.swlegal.com

Singapour
Schellenberg Wittmer Pte Ltd
50 Raffles Place, #40-05
Singapore Land Tower
Singapore 048623
www.swlegal.sg