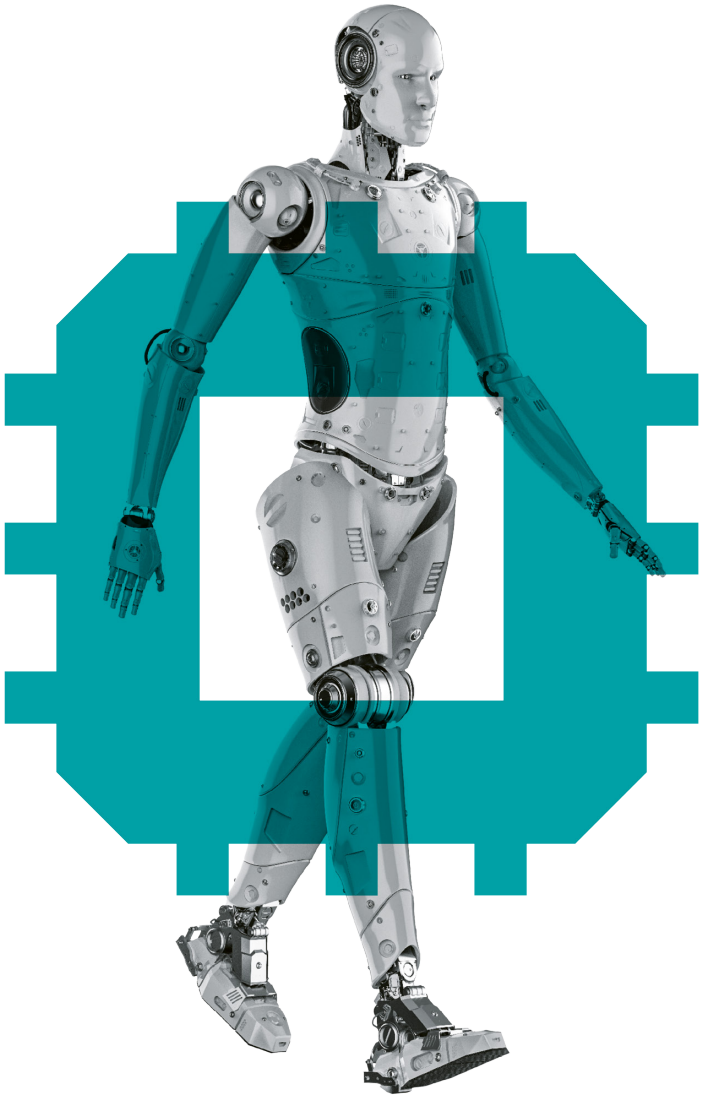
N

Monthly Newsletter March 2025

ICT

Schellenberg Wittmer



Relevanz von EU-Erlassen im digitalen Umfeld für Schweizer Unternehmen

Roland Mathys, Jacqueline Brunner

Key Take-aways

1.
Schweizer Unternehmen, die in der EU tätig sind und dort Produkte oder Dienstleistungen anbieten, fallen häufig in den Anwendungsbereich diverser EU-Erlasse im digitalen Umfeld, entweder direkt oder durch deren extraterritoriale Wirkung.

2.
Mit den EU-Erlassen werden umfangreiche Verhaltensregeln eingeführt, die für mehr Sicherheit, Transparenz und Innovation sowie einen besseren Datenzugang sorgen sollen.

3.
Zuwiderhandlungen können erhebliche Sanktionen nach sich ziehen, weshalb Schweizer Unternehmen ihren Handlungsbedarf laufend prüfen sollten.

1 Einleitung

In jüngerer Vergangenheit wurden in der Europäischen Union (**EU**) zahlreiche Gesetze im Bereich Digital und Data erlassen. Dieser Newsletter bietet eine Kurzübersicht über ausgewählte Erlasse (ohne Anspruch auf Vollständigkeit) im digitalen Umfeld und beleuchtet deren Relevanz für Schweizer Unternehmen.

2 Data Act (DA), Digital Services Act (DSA) und Digital Markets Act (DMA)

Der DA ist am 11. Januar 2024 in Kraft getreten und nach einer Übergangsfrist von 20 Monaten in der gesamten EU anwendbar.

Der DA zielt auf einen **freien Datenzugang** und die Förderung von Innovation ab. Zu den zentralen Bestimmungen des DA gehören die Gewährleistung des Datenzugangs und der Datenbereitstellung sowie die Sicherstellung der Interoperabilität und der Vertragskonformität.

Der DA betrifft **Personen- und Sachdaten**, die im Rahmen der Nutzung von "vernetzten Produkten" (Gegenstände, die Daten über ihre Nutzung oder Umgebung erlangen, generieren oder erheben und diese Daten über eine kabelgebundene oder kabellose Verbindung übermitteln können) und "verbundenen Diensten" (digitale Dienste, die mit einem vernetzten Produkt verbunden sind und dessen Funktionen unterstützen) generiert werden.

Der DA **adressiert** insb. Hersteller von vernetzten Produkten und Anbieter verbundener Dienste sowie deren Nutzer, Dateninhaber und öffentliche Stellen. Kleinst- und Kleinunternehmen (weniger als 10 bzw. 50 Mitarbeitende und EUR 2 bzw. 10 Mio. Umsatz/Bilanz) sind von den Pflichten (z.B. Weitergabe personenbezogener Daten) weitgehend ausgenommen. Aufgrund seiner extraterritorialen Wirkung, dessen genaue Reichweite noch unklar ist, kann der DA **auch Schweizer Unternehmen** betreffen, nämlich:

- Hersteller vernetzter Produkte, die in der EU in Verkehr gebracht werden, sowie Anbieter verbundener Dienste an Nutzer in der EU;
- Dateninhaber, die Daten Empfängern in der EU bereitstellen; und
- Anbieter von Datenverarbeitungsdiensten, die ihre Dienste Kunden in der EU anbieten.

Zuwiderhandlungen gegen den DA haben erhebliche **Sanktionen** zur Folge. Die EU-Mitgliedstaaten erlassen Vorschriften über Sanktionen, wobei der DA vorschreibt, dass die Sanktionen wirksam, verhältnismässig und abschreckend sein müssen. Hierbei sind Bussgelder bis zu EUR 20 Mio. oder 4% des weltweiten Jahresumsatzes möglich.

Der DMA (reguliert Gatekeeper) und der DSA (reguliert Anbieter digitaler Dienste) enthalten umfangreiche Verhaltensregeln für eine faire, sichere Nutzung digitaler Plattformen. Auch Schweizer Unternehmen können davon betroffen sein. In unserem Newsletter "Digital Markets Act und Digital Services Act: Auswirkungen für die Schweiz" finden Sie ausführliche Informationen hierzu.

3 Künstliche Intelligenz (KI)

3.1 EU Artificial Intelligence Act (AI Act)

Der AI Act ist am 1. August 2024 in Kraft getreten, wobei die Umsetzung zeitlich gestaffelt erfolgt. Ziel ist es, die Sicherheit und Transparenz von KI-Systemen in der EU zu gewährleisten und die Grundrechte zu wahren.

Im AI Act wird zwischen **KI-Systemen und KI-Modellen** differenziert: Der Begriff KI-System bezeichnet ein maschinengestütztes System, das eigenständig funktionieren und sich an neue Situationen anpassen kann, und das aus den erhaltenen Eingaben lernen und Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen treffen kann, die physische oder virtuelle Umgebungen beeinflussen können (z.B. ChatGPT). KI-Modelle sind Bestandteile von KI-Systemen und beziehen sich auf bestimmte Komponenten innerhalb eines KI-Systems (z.B. Large Language Modelle; LLM).

Zahlreiche EU-Erlasse gelten auch für Schweizer Unternehmen.

Der AI Act verfolgt einen **risikobasierten Ansatz**: KI-Systeme werden in vier Risikokategorien (unannehmbares, hohes, begrenztes oder minimales Risiko) mit abnehmender Regulierung eingeteilt. Während KI-Systeme mit unannehmbarem Risiko generell verboten sind, bestehen für solche mit hohem Risiko strenge Voraussetzungen (z.B. Risikomanagement, Data Governance und technische Dokumentation). Für KI-Systeme mit begrenztem Risiko gelten weniger strenge Pflichten (z.B. Informationspflicht über Interaktion mit einem KI-System), und solche mit minimalem Risiko sind kaum reguliert; die sog. KI-Kompetenz muss sichergestellt sein. Der umfangreiche Pflichtenkatalog richtet sich primär an Anbieter. Betreiber verantworten den regelkonformen Gebrauch des KI-Systems (z.B. menschliche Aufsicht und Überwachung des KI-Betriebs). Aufgrund seiner extraterritorialen Wirkung, dessen genaue Reichweite noch unklar ist, kann der AI Act auch auf **Schweizer Unternehmen** Anwendung finden. Denn er gilt unter anderem für:

- Anbieter, die in der EU KI Systeme in Verkehr bringen oder in Betrieb nehmen oder KI Modelle mit allgemeinem Verwendungszweck in Verkehr bringen, unabhängig davon, ob diese Anbieter in der EU oder in einem Drittland niedergelassen sind;
- Anbieter und Betreiber von KI Systemen, die ihren Sitz in einem Drittland haben oder sich in einem Drittland befinden, wenn die vom KI System hervorgebrachte Ausgabe in der EU verwendet wird.

Verstösse gegen den AI Act können mit empfindlichen **Sanktionen** geahndet werden, wobei der AI Act Geldbussen von

bis zu EUR 35 Millionen oder – im Falle eines Unternehmens – 7% des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres als Obergrenze vorsieht (je nachdem, welcher Betrag höher ist).

3.2 Aktueller Exkurs: KI-Regulierung in der Schweiz

Eben erst veröffentlichte der Bundesrat **für die Schweiz** eine Auslegeordnung zur Regulierung von KI (Medienmitteilung vom 12. Februar 2025): Danach sollen die KI-Konvention des Europarates ins Schweizer Recht übernommen und etwaige notwendige Gesetzesanpassungen möglichst sektoriell und punktuell vorgenommen werden. Es ist somit keine umfassende und detaillierte Regulierung wie im AI Act der EU vorgesehen – zentrale, grundrechtsrelevante Bereiche vorbehalten. Unternehmen, die nur in der Schweiz tätig sind und nicht dem AI Act unterliegen, profitieren somit von Erleichterungen – dies im Gegensatz zu solchen Unternehmen, die zusätzlich den AI Act einhalten müssen. Denn die künftige Schweizer KI-Regulierung wird die Vorgaben des AI Acts voraussichtlich nicht oder nur teilweise umsetzen.

4 Cyber Resilience Act (CRA)

Der CRA ist am 10. Dezember 2024 in Kraft getreten und wird ab dem 11. Dezember 2027 – nach einer dreijährigen Umsetzungsfrist – vollständig anwendbar sein. Einige Bestimmungen (wie etwa die Meldepflicht von IT-Schwachstellen und Sicherheitsvorfällen) sind jedoch bereits früher durchsetzbar.

Mit dem CRA soll die **Cybersicherheit** vernetzter Produkte massgeblich verbessert werden. Der CRA legt Mindestanforderungen an die Cybersicherheit fest und erfasst Produkte mit “digitalen Elementen”, die in der EU in Verkehr gebracht werden und mit dem Internet, anderen Geräten oder Netzwerken verbunden werden können, wie beispielsweise Hardware- und Softwareprodukte, Geräte des Internet-of-Things, smarte Haushaltsgeräte, vernetzte Fahrzeuge und industrielle Maschinen.

Betroffene Unternehmen erwartet ein potenziell hoher Compliance-Aufwand.

Wichtige Bestimmungen des CRA betreffen die Gewährleistung der Cybersicherheit während des gesamten Lebenszyklus, die Einhaltung von Melde-, Dokumentations- und Transparenzpflichten, Konformitätsbewertungen sowie die Bereitstellung von Sicherheitsupdates. Die konkreten Pflichten ergeben sich aus der Rolle des Adressaten sowie der Produktqualifikation. Hersteller tragen die Hauptverantwortung für die Produktesicherheit und müssen z.B. eine technische Dokumentation und Informationsmaterialien zur Cybersicherheit erstellen. Importeure und Händler müssen sicherstellen, dass die Produkte den Vorschriften entsprechen (z.B. CE-Kennzeichnung/Konformitätserklärung überprüfen). Die Meldepflichten zu Sicherheitsrisiken und Schwachstellen treffen alle Akteure.

Der CRA richtet sich an Hersteller, Importeure und Händler in der EU. Aufgrund seiner **extraterritorialen Wirkung**, dessen genaue Reichweite noch unklar ist, gilt er auch für Schweizer Hersteller, Importeure und Händler, die solche Produkte für Abnehmer in der EU bereitstellen.

Verstösse gegen den CRA können mit empfindlichen **Sanktionen** geahndet werden, nämlich mit Strafen von bis zu EUR 15 Millionen oder 2.5% des weltweiten Konzernumsatzes (je nachdem, welcher Betrag höher ist). Darüber hinaus sind Marktüberwachungsmassnahmen – wie etwa verpflichtende Produktrückrufe – möglich.

5 Digital Operational Resilience Act (DORA)

Der DORA ist am 17. Januar 2025 in Kraft getreten. Der **Fokus** liegt auf Risiken der Informations- und Kommunikationstechnologie (**IKT**), und es wird die Stärkung der digitalen operationalen Resilienz des europäischen Finanzsektors bezweckt.

Der DORA beinhaltet **Anforderungen an das IKT-Risikomanagement** sowie an die Verträge mit IKT-Dienstleistern. Dadurch werden die Adressaten zur Einführung robuster Cybersicherheitsmassnahmen, Durchführung von Sicherheitsprüfungen sowie Sicherstellung der Betriebskontinuität verpflichtet. Zu den zentralen Bereichen gehören: IKT-Risikomanagement, IKT-Drittparteienmanagement, Management von IKT-Vorfällen, Testen und Informationsaustausch.

Bei Zuwiderhandlungen drohen erhebliche Sanktionen.

Der DORA richtet sich an EU **Finanzunternehmen** (z.B. Kreditinstitute, Wertpapierfirmen und Versicherungsunternehmen) und IKT-Anbieter, die Dienstleistungen für diese Finanzunternehmen erbringen. Auch Schweizer Unternehmen, die als **IKT-Dienstleister** für EU-Finanzunternehmen tätig sind oder Teil eines EU-Finanzkonzerns bilden, sind vom DORA betroffen und müssen die Bestimmungen beachten.

Der DORA sieht keine unmittelbaren Geldbussen oder strafrechtlichen **Sanktionen** vor. Es liegt vielmehr im Ermessen der EU-Mitgliedstaaten, in ihrem nationalen Recht Sanktionen für Verstösse vorzusehen. Die zuständigen Behörden können zudem verwaltungsrechtliche Sanktionen sowie Abhilfemassnahmen treffen und die verhängten Verwaltungsstrafen sowie davon betroffene Unternehmen auf ihrer Webseite veröffentlichen.

6 Netzwerk- und Informationssicherheit-Richtlinie (NIS-2)

Die NIS-2 (Nachfolgerin der NIS-1) ist am 16. Januar 2023 in Kraft getreten und musste bis zum 17. Oktober 2024 durch die EU-Mitgliedstaaten in nationales Recht umgesetzt werden. Die NIS-2 bezweckt die Stärkung der Cybersicherheit in der gesamten EU, indem höhere Standards für **kritische Infrastrukturen** festgelegt werden und der Geltungsbereich auf weitere Sektoren und Arten von Organisationen ausgeweitet wurde.

Zentrale **Bestimmungen** der NIS-2 betreffen: Governance, Risikomanagementmassnahmen im Bereich Cybersecurity, Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten in der EU, Berichtspflichten, Vertretung in der EU sowie Registrierung von Betreibern kritischer Infrastrukturen.

Der **Anwendungsbereich** der NIS-2 umfasst wesentliche und wichtige Einrichtungen, wobei an die jeweilige Qualifikation unterschiedliche Pflichten geknüpft werden. Die NIS-2 gilt für öffentliche und private Einrichtungen, die als mittlere oder grosse Unternehmen (mind. 50 Mitarbeitende und EUR 10 Mio. Umsatz/Bilanzsumme bzw. 250 Mitarbeitende und EUR 50 Mio. Umsatz oder EUR 43 Mio. Bilanzsumme) eingestuft werden. Bestimmte Einrichtungen (z.B. Kommunikationsnetze) werden unabhängig davon vom Anwendungsbereich erfasst. Auch **Schweizer Unternehmen** können von der NIS-2 betroffen sein, nämlich wenn sie ihre Dienste in der EU erbringen oder ihre Tätigkeiten dort ausüben.

Verstösse gegen die NIS-2 können mit **Sanktionen** geahndet werden: Die zuständigen Behörden können verschiedene Aufsichts- und Durchsetzungsmassnahmen, wie bspw. Vor-Ort-Kontrollen, vornehmen. Bei Zuwiderhandlungen drohen Bussgelder, im Falle von wesentlichen Einrichtungen bis zu EUR 10 Millionen oder 2% des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist).

7 Fazit

Die genannten (und weitere) EU-Regulierungen im digitalen Umfeld machen an der EU- (bzw. EWR-) Aussengrenze nicht halt – vielmehr können auch Schweizer Unternehmen davon betroffen und zu deren Umsetzung gehalten sein. Daher gilt: Rechtzeitig prüfen und gezielt handeln!

Roland Mathys
Partner
roland.mathys@swlegal.ch

Lorenza Ferrari Hofer
Partnerin
lorenza.ferrari@swlegal.ch

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

Grégoire Tribolet
Partner
gregoire.tribolet@swlegal.ch

Der Inhalt dieses Newsletters stellt keine Rechts- oder Steuerauskunft dar und darf nicht als solche verwendet werden. Sollten Sie eine auf Ihre persönlichen Umstände bezogene Beratung wünschen, wenden Sie sich bitte an Ihre Kontaktperson bei Schellenberg Wittmer oder an eine der oben genannten Personen.

Schellenberg Wittmer AG ist Ihre führende Schweizer Wirtschaftskanzlei mit mehr als 150 Juristinnen und Juristen in Zürich und Genf sowie einem Büro in Singapur. Wir kümmern uns um alle Ihre rechtlichen Belange – Transaktionen, Beratung, Prozesse.

Schellenberg Wittmer Ltd
Rechtsanwälte

Zürich
Löwenstrasse 19
Postfach 2201
8021 Zürich / Schweiz
T +41 44 215 5252
www.swlegal.com

Genf
15bis, rue des Alpes
Postfach 2088
1211 Genf 1 / Schweiz
T +41 22 707 8000
www.swlegal.com

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