Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Interdepartementale Koordinationsgruppe EU-Digitalpolitik**
**IK-EUDP**

Bern, 13.02.2025

# Die Schweiz und die Digitalpolitik der Europäischen Union

Analyse der Interdepartementalen Koordinationsgruppe IK-EUDP

Stand der Analyse: 18.12.2024

# Über dieses Dokument

Dieses Analysedokument ist ein Produkt der *Interdepartementalen Koordinationsgruppe EU-Digitalpolitik* (IK-EUDP) des Bundes. Die IK-EUDP wurde vom Bundesrat beauftragt, ein Monitoring der EU-Digitalpolitik sicherzustellen und den Bundesrat regelmässig über relevante Entwicklungen zu informieren. Zu diesem Zweck erarbeitet die IK-EUDP unter Koordination von BAKOM und EDA Staatssekretariat Abteilung Europa alle zwei Jahre eine ausführliche Analyse der regulatorischen Entwicklungen im Zusammenhang mit der EU-Digitalpolitik.

Mittlerweile lassen sich 33 relevante Massnahmen für die Schweiz verorten. Dieses Analysedokument bietet eine Übersicht dieser Massnahmen und analysiert deren mögliche Auswirkungen auf die Schweiz. Einige dieser Massnahmen wurden bereits zu Beginn des Mandates der neuen Kommission unter Ursula von der Leyen kommuniziert und sind mittlerweile abgeschlossen, andere sind später dazugekommen und noch in der Umsetzung. Mit 33 Massnahmen ist die Strategie sowohl umfangreich als auch heterogen.

Es gilt **unbedingt zu beachten**, dass dieses Dokument eine Momentaufnahme darstellt. Die dokumentierten Massnahmen befinden sich in unterschiedlichen Stadien und können je nach Umsetzungs- und Anwendungspraxis unterschiedliche Auswirkungen entwickeln. Dieses Dokument und die darin enthaltenen Einschätzungen sollten deshalb mit der entsprechenden Vorsicht konsultiert werden.

# Inhaltsverzeichnis

# Executive Summary

Die Kommission von der Leyen I war in der vergangenen Legislatur (2019-2024) im Bereich der Digitalpolitik ausserordentlich aktiv. Gemäss dem Think-Tank Bruegel hat die Europäische Kommission seit 2020 59 legislative Massnahmen initiiert und Stand heute 44 erfolgreich abgeschlossen.

Die Attraktivität des EU-Binnenmarkts, das Timing der Regulierungsmassnahmen und der Einfluss der Europäischen Kommission als Regulierungs- und Umsetzungsbehörde, erlauben es der EU als **Standardsetzerin zu agieren und weltweiten regulatorischen Einfluss auszuüben**. Entsprechend hat die Digitalpolitik der EU auch Auswirkungen auf die Schweiz.

Die Effekte vieler digitalpolitischer Massnahmen sind über die Grenzen der EU hinaus spürbar und wirken sich auf die Schweiz und die Schweizer Unternehmen aus, die auf dem EU-Markt tätig sind. Dies ist eine direkte Konsequenz der EU-Bestrebungen die Integrität und Rechtsordnung des europäischen Binnenmarktes auch im grenzüberschreitenden digitalen Raum zu wahren. Konkret macht sich das insbesondere auch durch den **Einsatz von Regulierungsinstrumenten zur Durchsetzung von EU-Standards in Drittländern** bemerkbar, z.B. Äquivalenzverfahren und die Ernennung eines Rechtsvertreters in der EU.

Gleichzeitig verändern die Massnahmen vielfach auch das institutionelle Gefüge in der EU. Ein nicht unerheblicher Anteil der neuen Gesetzgebungen sind horizontale, sektorübergreifende Rechtsakte, womit oftmals auch eine (zumindest teilweise) **Verschiebung von Kompetenzen** weg von den Mitgliedstaaten und hin zur Europäischen Kommission einhergeht. In gewissen Bereichen birgt dies auch für die Schweiz Herausforderungen, da etablierte Kanäle der regulatorischen Kooperation oder des Informationsaustausches wegfallen und ersetzt werden müssen.

Die vorliegende Analyse hat im digitalen Bereich **keine erheblichen Risiken für den Binnenmarktzugang** für Schweizer Unternehmen festgestellt. Es ist aber festzuhalten, dass gewisse Massnahmen wie bspw. die Verordnung über künstliche Intelligenz (Massnahme 1), die Verordnung über Cyberresilienz (Massnahme 16) oder die die Ökodesign-Verordnung (Massnahme 20) sich auch auf Bereiche auswirken werden, die unter das Abkommen zwischen der Schweiz und der EU über die gegenseitige Anerkennung von Konformitätsbewertungen (MRA) fallen. Zu den bestehenden werden auch neue Anforderungen hinzukommen und könnten, ohne eine Erweiterung des MRA auf die jeweiligen Bereiche, Schweizer Unternehmen mit **zusätzlichen Markthürden** konfrontieren.

Ein Grossteil der legislativen Massnahmen befindet sich momentan in der Umsetzungsphase. Die Umsetzungs- und Anwendungspraxis sowie allfällige Rechtsprechungen werden massgeblich beeinflussen, ob die digitalpolitischen Initiativen der Kommission von der Leyen I als Erfolg gewertet werden können. Unter Umständen kann dies auch weitere Auswirkungen auf die Schweiz haben.

Die Analyse der Massnahmen hat aufgezeigt, dass die Bundesverwaltung die digitalpolitischen Entwicklungen eng verfolgt und sich den möglichen Auswirkungen bewusst ist. In verschiedenen Bereichen hat der **Bundesrat bereits entsprechend gehandelt** und Massnahmen in der Schweiz ergriffen.

Die nächste umfassende Analyse ist für **Anfang 2027** vorgesehen.

Massnahme 1
# AI Act

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung (EU) 2024/1689 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 01.08.2024 |
| **Federführung in der Bundesverwaltung** | BAKOM |

## Beschrieb

Am 1. August 2024 trat die Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (nachfolgend «AI Act») in Kraft (Verordnung [EU] 2024/1689). Der AI Act deckt insbesondere die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen der künstlichen Intelligenz (KI) in der EU ab, die mit den Werten der Union im Einklang stehen müssen. Die Verordnung führt eine risikobasierte Klassifizierung von KI-Systemen ein und legt entsprechende Anforderungen und Pflichten fest. Die neuen Vorschriften gelten in erster Linie für Anbieter von KI-Systemen mit Sitz in der EU oder einem Drittland, die KI-Systeme auf dem EU-Markt in Verkehr bringen oder in der EU in Betrieb nehmen, sowie für Betreiber von KI-Systemen mit Sitz in der EU. Der AI Act findet auch auf Anbieter und Betreiber von KI-Systemen mit Sitz in einem Drittland Anwendung, wenn die von dem KI-System ausgegebenen Ergebnisse in der EU genutzt werden.

Der AI Act **verbietet besonders schädliche und missbräuchliche KI-Systeme oder KI-Praktiken**, die im Widerspruch zu den EU-Werten stehen, insbesondere:

- KI-Systeme, die Techniken der unterschwelligen Beeinflussung einsetzen;
- KI-Systeme, die die Schwächen einer spezifischen Gruppe von Einzelpersonen ausnutzen;
- Bewertung des sozialen Verhaltens durch öffentliche und private Akteure (in bestimmten Fällen);
- Systeme zur biometrischen Kategorisierung;
- biometrische Fernidentifizierung in Echtzeit in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, mit wenigen Ausnahmen.

Der AI Act sieht vor, dass **Hochrisiko-KI-Systeme** nur dann in Verkehr gebracht, in Betrieb genommen oder verwendet werden dürfen, wenn sie bestimmte Anforderungen erfüllen. Die Gesetzgebung unterscheidet zwischen zwei Kategorien von Hochrisiko-KI-Systemen:

a. KI-Systeme, die als Sicherheitskomponente eines Produkts verwendet werden sollen, das unter die in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der EU fällt (z. B. Maschinen, Spielzeug, Luftfahrt), oder bei denen es sich selbst um Produkte handelt;
b. Hochrisiko-KI-Systeme in acht spezifischen Bereichen, die in Anhang III der Verordnung definiert sind;
    - Biometrische Systeme;
    - Verwaltung und Betrieb kritischer Infrastruktur;
    - Allgemeine und berufliche Bildung;
    - Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit;
    - Zugänglichkeit und Inanspruchnahme bestimmter wesentlicher privater und öffentlicher Dienste und Leistungen;
    - KI-Systeme, die von Strafverfolgungsbehörden eingesetzt werden;
    - KI-Systeme, die im Rahmen von Migration, Asyl und Grenzkontrolle verwendet werden;
    - Bestimmte KI-Systeme für die Rechtspflege und für demokratische Prozesse.

Hochrisiko-KI-Systeme dürfen erst nach einer Konformitätsbewertung auf den Markt gebracht werden.

Die Verordnung sieht Pflichten für sämtliche **KI-Modelle mit allgemeinem Verwendungszweck** (General Purpose AI Models, GPAI) vor sowie zusätzliche Pflichten für GPAI-Modelle mit systemischen Risiken. Alle GPAI-Anbieter unterliegen – unabhängig vom Risiko, das sie darstellen – Transparenzmassnahmen hinsichtlich der Daten, die für das Vortraining und das Training von Modellen verwendet werden, einschliesslich urheberrechtlich

geschützter Texte und Daten. Für Modelle mit systemischen Risiken gelten zusätzliche Anforderungen, insbesondere die Verpflichtung zur Durchführung von Penetrationstests zur Ermittlung und Minderung systemischer Risiken, zur Verringerung systemischer Risiken, die sich aus der Entwicklung, dem Inverkehrbringen oder der Verwendung des Modells ergeben können, und zur Meldung von Vorfällen.

Die Anbieter von GPAI-Modellen können sich bis zur Veröffentlichung einer harmonisierten Norm auf Praxisleitfäden stützen, um nachzuweisen, dass sie die Anforderungen der Verordnung erfüllen. Das bei der Europäischen Kommission angesiedelte Büro für Künstliche Intelligenz wird die Erstellung solcher Leitfäden unterstützen.

**KI-Systeme mit geringem Risiko** werden Transparenzpflichten unterliegen. So müssen etwa KI-Systeme für die Interaktion mit natürlichen Personen so konzipiert und entwickelt werden, dass natürliche Personen darüber informiert sind, dass sie mit einem KI-System, wie z. B. einem Software-Roboter (Chatbot), interagieren.

Die Gesetzgebung sieht für Verstösse gegen die im AI Act festgelegten Pflichten erhebliche **finanzielle Sanktionen** vor. Beispielsweise können Verstösse gegen das Verbot von KI-Praktiken mit Geldbussen von bis zu 35 Millionen Euro oder bis zu 7 Prozent des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden. Die Nichteinhaltung der Vorschriften für Betreiber oder notifizierte Stellen kann mit Geldbussen von bis zu 15 Millionen Euro oder bis zu 3 Prozent des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres sanktioniert werden.

## Stand der Dinge

Der AI Act gilt zwei Jahre nach seinem Inkrafttreten, d. h. ab dem 2. August 2026, mit Ausnahme einiger spezifischer Bestimmungen:

- Die Bestimmungen über verbotene Praktiken im KI-Bereich sind ab dem 2. Februar 2025 anwendbar.
- Die Bestimmungen zu KI-Modellen mit allgemeinem Verwendungszweck finden ab dem 2. August 2025 Anwendung.
- Die Bestimmungen für Hochrisiko-KI-Systeme, die mit unter die Harmonisierungsrechtsvorschriften der EU fallenden Produkten in Verbindung stehen (Anhang I Abschnitt A), gelten ab dem 2. August 2027.

## Mögliche Auswirkungen auf die Schweiz

Der AI Act wirkt sich auch auf Schweizer Betreiber aus. Konkret bedeutet dies, dass Schweizer Akteure, die KI-Produkte oder Produkte mit KI-Systemen in die EU exportieren wollen, die Konformität ihrer Produkte gemäss dem AI Act bewerten (lassen) müssen, sofern diese in die Kategorie der Hochrisiko-KI-Systeme fallen. Für den Export in die EU werden dadurch neue Handelshemmnisse entstehen.

Die Schweiz hat heute mit der EU ein Abkommen über die gegenseitige Anerkennung von Konformitätsbewertungen (MRA) für Produkte in 20 Sektoren. Der AI Act wird sich auf die Sektoren, die von diesem Abkommen abgedeckt werden (insb. Maschinen), auswirken, da für Produkte mit KI-Komponenten die Verpflichtungen des AI Act zu den bestehenden Anforderungen für den Marktzugang hinzukommen werden. Die Frage, ob das MRA-Abkommen erweitert werden könnte, um auch die KI-Anforderungen zu umfassen und damit mögliche Handelshemmnisse abzubauen, muss geprüft werden. Voraussetzung hierfür ist, dass entsprechende äquivalente Bestimmungen im Schweizer Recht eingeführt würden. Dazu kommt, dass weiterhin unklar ist, ab wann die EU im Kontext der Beziehungen zwischen der Schweiz und der EU wieder zu einer Aktualisierung des MRA bereit sein wird.

Eine detaillierte Analyse des AI Act und dessen Auswirkungen auf die Schweiz wird derzeit im Rahmen einer Auslegeordnung zu möglichen Regulierungsansätzen für KI durchgeführt, die der Bundesrat am 22. November 2023 beim UVEK (BAKOM) und dem EDA (Abteilung Europa) in Auftrag gegeben hat. Die Auslegeordnung soll in der Form eines öffentlichen Berichts an den Bundesrat vorliegen.

## Bereits ergriffene Massnahmen in der Schweiz

Wie bereits in der vorstehenden Antwort erwähnt, führt die Schweiz zurzeit eine Bestandsaufnahme der Regulierungsansätze für KI durch, wobei unter anderem auch die Art und Weise untersucht wird, wie sich internationale Instrumente wie der AI Act auf die Schweiz auswirken. Das Mandat zur Erarbeitung der Auslegeordnung und der darin enthaltenen Analyse des AI Acts wurde aus Eigeninitiative der Schweiz erteilt.

Massnahme 2

# Gesetz über die digitalen Dienste (Digital Services Act)

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung über einen Binnenmarkt für Digitale Dienste |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung (EU) 2022/2065 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 16.11.2022 |
| **Federführung in der Bundesverwaltung** | BAKOM |

## Beschrieb

Der *Digital Services Act* (DSA) ist am 16. November 2022 in Kraft getreten. Damit wurde ein neues EU-Regelwerk für Online-Vermittlungsdienste geschaffen. Die Verordnung sieht einheitliche Regeln für die Rechte und Verantwortlichkeiten von digitalen Diensten, insbesondere auch Online-Plattformen, im Umgang mit illegalen und/oder schädlichen Online-Inhalten vor. Die DSA sieht gestaffelte Pflichten vor: Die Dienste mit dem höchsten Risikoprofil (namentlich sehr grosse Online-Plattformen) müssen allen Anforderungen entsprechen, während kleinere oder anders ausgerichtete Anbieter nur einen Teil der Pflichten zu erfüllen haben. Die verschiedenen Dienste unterliegen unter anderem den folgenden Verpflichtungen:

**Pflichten für alle Vermittlungsdienste:**

- Sämtliche Vermittlungsdienste müssen einen Vertreter benennen, der als zentrale Kontaktstelle fungiert.
- Alle Vermittlungsdienste, welche keine Niederlassung in der EU haben, müssen eine Rechtsvertretung innerhalb der EU ernennen. Diese kann explizit für Verstösse gegen die im DSA vorgesehenen Pflichten haftbar gemacht werden.
- Einmal jährlich müssen alle Vermittlungsdienste einen Transparenzbericht veröffentlichen, der die Moderationspraktiken beschreibt.
- Sie sind verpflichtet, die innerstaatlichen Justiz- oder Verwaltungsbehörden darüber zu informieren, welche Massnahmen sie nach Anordnungen zur Löschung eines Inhalts oder zur Erteilung von Auskünften ergriffen haben.

**Sorgfaltspflichten für Hosting-Anbieter, einschliesslich Online-Plattformen**

- Alle Hosting-Anbieter müssen über ein Meldesystem verfügen, über welches Nutzerinnen und Nutzer sowie Organisationen Inhalte melden können, die sie als illegal einstufen.
- Hosting-Anbieter müssen Einschränkungen ihrer Dienste gegenüber betroffenen Nutzerinnen und Nutzern spätestens ab Zeitpunkt der Einschränkung klar begründen.
- Bei Verdacht auf eine kriminelle Aktivität, welche Leben oder Sicherheit einer Person bedroht, muss der Hosting-Anbieter dies den zuständigen Behörden melden.

**Zusätzliche Sorgfaltspflichten für Online-Plattformen**

- Online-Plattformen müssen ein internes Beschwerdesystem betreiben, welches es Nutzerinnen und Nutzern erlaubt, Einschränkungsmassnahmen der Online-Plattform anzufechten.
- Online-Plattformen, welche Werbung schalten, müssen sicherstellen, dass Nutzerinnen und Nutzer diese auch als solche identifizieren können. Neben dem Umstand, dass es sich um Werbung handelt, müssen auch der Werbetreibende bzw. die Finanzierungsquelle der Werbung (wenn unterschiedlich) sowie die Parameter, welche für die Ausspielung der Werbung verantwortlich sind, klar ersichtlich sein. Zudem ist Werbung basierend auf dem Profiling von sensiblen Daten verboten.

**Bestimmungen für Anbieter von Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen**

- Die betroffenen Anbieter müssen sicherstellen, dass Unternehmen ihre Plattform nur nutzen können, wenn sie gewisse notwendige Informationen erhalten haben.

- Die betroffenen Anbieter stellen sicher, dass Unternehmen, die ihre Plattform nützen geltendes Recht in Bezug auf vorvertragliche Informationen, Konformität und Produktsicherheitsinformationen einhalten können. Sie müssen ebenfalls sicherstellen, dass die notwendigen Kontaktinformationen verfügbar sind.

**Zusätzliche Sorgfaltspflichten für sehr grosse Online-Plattformen** (mit durchschnittlich mehr als 45 Millionen aktiven Nutzerinnen und Nutzern in der EU)

- Sehr grosse Online-Plattformen (very large online platforms – VLOPs) müssen ein jährliches Risiko-Assessment durchführen und konkrete Massnahmen zur Risikominderung ergreifen. Dies umfasst systemische Risiken, darunter die Verbreitung illegaler Inhalte sowie Risiken im Zusammenhang mit Grundrechten und der öffentlichen Kommunikation.
- VLOPs können im Krisenfall durch einen Entscheid der Europäischen Kommission (KOM) dazu verpflichtet werden, spezifische Massnahmen zu treffen.
- VLOPs müssen jährlich ein unabhängiges Audit ihrer Prozesse und ihrer Pflichten durchlaufen.
- Sie müssen mindestens ein Empfehlungssystem anbieten, das nicht auf Profiling beruht.
- Im Bereich Online-Werbung sind VLOPs verpflichtet, eine öffentlich einsehbare Datenbank einzurichten, welche insbesondere den Inhalt der publizierten Werbung, Details der Werbetreibenden und der Werbefinanzierung, Profilingmuster der Werbung und die Anzahl der erreichten Personen enthält.
- VLOPs haben den zuständigen Aufsichtsbehörden auf Anfrage Zugriff auf Daten zu gewähren, die für die Durchsetzung des DSA nötig sind. Ebenfalls können Aufsichtsbehörden verlangen, dass anerkannte Wissenschaftlerinnen und Wissenschaftler Zugang zu Daten erhalten.
- Sie müssen alle sechs Monate einen Transparenzbericht vorlegen und zusätzliche Informationen bereitstellen, wie etwa die für die Inhaltsmoderation aufgewendeten personellen Ressourcen und die ergriffenen Massnahmen zur Risikominderung.

Die EU-Mitgliedstaaten bzw. ihre nationalen Aufsichtsbehörden sind für die **Aufsicht und Durchsetzung** des DSA bei den Vermittlungsdiensten, Hosting-Anbietern und Online-Plattformen zuständig. Die Aufsicht über VLOPs fällt ausschliesslich in die Kompetenz der KOM. Bei Nichteinhaltung der Verpflichtungen betragen diese Geldbussen maximal 6 Prozent des weltweiten Jahresumsatzes. Bei fehlerhaften, nicht kompletten oder irreführenden Informationen können Geldbussen von bis zu 1 Prozent des weltweiten Jahresumsatzes verhängt werden.

Bis Oktober 2024 hatte die KOM insgesamt 25 Dienste als sehr grosse Online-Plattformen und sehr grosse Online-Suchmaschinen bezeichnet. Dazu gehören AliExpress, Amazon, Apple Store, Booking, Google Search, Google Maps, LinkedIn, Facebook, Instagram, Microsoft Bing, Pinterest, Pornhub, Snapchat, Tik Tok, X, Youtube und Zalando.

## Stand der Dinge

Die Verordnung trat am 16. November 2022 in Kraft und ist seit dem 17. Februar 2024 uneingeschränkt anwendbar. Im Zuge der Umsetzung der Rechtsvorschriften hat die Kommission förmliche Vertragsverletzungsverfahren gegen TikTok, AliExpress, Facebook, Instagram und X eröffnet. Im April 2024 leitete die Kommission Vertragsverletzungsverfahren gegen sechs Mitgliedstaaten (Tschechien, Estland, Polen, Portugal, Slowakei, Zypern) ein, die bis zum 17. Februar 2024 ihre nationale Koordinatorin bzw. ihren nationalen Koordinator für digitale Dienste noch nicht benannt hatten.

## Mögliche Auswirkungen auf die Schweiz

Die Schweiz verfügt aktuell über keine eigene spezifische Gesetzgebung im Bereich der Online-Vermittlungsdienste. Der DSA wird jedoch sowohl direkte als auch indirekte Auswirkungen auf die Schweiz und in der Schweiz domizilierte Anbieter von Online-Vermittlungsdiensten haben.

Die wichtigste Direktauswirkung für Schweizer Unternehmen ist der Umstand, dass die Verordnung nicht nur für Anbieter innerhalb des EU-Territoriums Geltung hat, sondern für alle Anbieter, welche Dienste an Kunden in EU-Mitgliedstaaten anbieten – unabhängig vom Ort ihrer Niederlassung. Dies bedeutet, dass auch im EU-Binnenmarkt tätige Schweizer Online-Dienstanbieter Verpflichtungen des DSA grundsätzlich folgen müssen. Es ist zum aktuellen Zeitpunkt nicht zu erwarten, dass ein Schweizer Unternehmen gemäss den im Entwurf des DSA festgehaltenen Kriterien als «sehr grosse Online-Plattform» designiert wird. Entsprechend werden die strengsten Verpflichtungen keine direkte Anwendung auf Schweizer Anbieter finden.

Um die Durchsetzbarkeit der Vorschriften zu erleichtern, setzt die EU jedoch auf das Erfordernis eines Rechtsvertreters innerhalb des EU-Binnenmarktes. Die Verpflichtung zur Ernennung eines Rechtsvertreters mit geschäftlichem Sitz innerhalb der EU betrifft somit alle Schweizer Vermittlungsdienste, welche ihre Dienste in der EU anbieten. Dieser Rechtsvertreter kann bei Verstössen gegen die Verordnung direkt haftbar gemacht werden (insb. Zahlung allfälliger Bussen). Da dies de facto eine nicht erhebliche Marktzugangshürde für Schweizer Unternehmen darstellt, dürften sich die Kosten für einen solchen Rechtsvertreter im Normalfall in Grenzen halten. Dies ist in der Praxis insbesondere dann der Fall, wenn mehrere EU-Regularien mit demselben Rechtsvertreter abgedeckt werden können.

Bezüglich indirekter Auswirkungen ist es möglich, dass ausländische Plattformen einige EU-Standards auch auf die Schweiz anwenden, da diese bei international angebotenen Diensten eher oft demselben Markt wie die EU-Mitgliedstaaten zugeschrieben wird. Dies wird jedoch von Plattform zu Plattformen unterschiedlich gehandhabt. Plattformen sind durchaus in der Lage, länderspezifische Lösungen zu betreiben und tun dies auch, wenn es zu ihrem Nutzen ist. Auf jeden Fall können Schweizer Nutzerinnen und Nutzer die Schutzmechanismen des DSA, welche für EU-Bürgerinnen und -Bürger gelten, in der Schweiz nicht einklagen. Solche Schutzmechanismen würden in der Schweiz nur aufgrund eines freiwilligen Engagements der Intermediäre greifen. Schweizer Nutzerinnen und Nutzer sind deshalb gegenüber denjenigen der EU tendenziell schlechter gestellt, auch wenn die Intermediäre eventuell bestimmte technische Anpassungen, die der DSA verlangt, auch für die Schweiz umsetzen würden.

## Bereits ergriffene Massnahmen in der Schweiz

Der Bundesrat hat am 05. April 2023 das UVEK (BAKOM) damit beauftragt, eine Vernehmlassungsvorlage für die Regulierung von grossen Kommunikationsplattformen auszuarbeiten. Die Vernehmlassungsvorlage hat einen engeren Fokus als der DSA und konzentriert sich auf Aspekte, welche relevant für die öffentliche Kommunikation und Meinungsbildung sind. In diesen Bereichen sollen die Rechte von Nutzerinnen und Nutzern gestärkt und Transparenz von Seiten der Plattformen geschaffen werden. Die Vernehmlassungsvorlage wird sich, wo sinnvoll, an den Regeln des Digital Services Act orientieren, die Entscheidung in diesem Bereich regulatorisch aktiv zu werden, ist aber unabhängig vom DSA erfolgt. Die Vorlage ist für Anfang 2025 geplant.

In anderen Bereichen des DSA, wie beispielsweise dem Schutz vor illegalen, gefälschten oder unsicheren Produkten gibt es in der Schweiz aktuell keine Massnahmen.

Massnahme 3

# Gesetz über digitale Märkte (Digital Markets Act)

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung über bestreitbare und faire Märkte im digitalen Sektor |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung (EU) 2022/1925 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 01.11.2022 |
| **Federführung in der Bundesverwaltung** | SECO |

## Beschrieb

Am 1. November 2022 trat das Gesetz über digitale Märkte (Digital Markets Act; DMA) in Kraft. Der DMA stellt für bestimmte grosse Online-Plattformen, die als Torwächter («*Gatekeeper*») bezeichnet werden, eine Reihe neuer Ex-ante-Regeln auf. Ziel des DMA ist die Gewährleistung von Bestreitbarkeit und Fairness auf digitalen Märkten. Die neue Regulierung ergänzt das Wettbewerbsrecht.

Ein Unternehmen gilt als Gatekeeper, wenn es die folgenden Kriterien erfüllt:

- Es betreibt (in mindestens drei Mitgliedstaaten der EU) mindestens einen zentralen Plattformdienst wie eine Suchmaschine, ein soziales Netzwerk, eine Videosharing-Plattform, einen Messengerdienst, ein Betriebssystem, einen Webbrowser, eine Cloud-Computing-Dienstleistung, Online-Werbedienstleistungen oder Online-Vermittlungsdienste (z. B. App-Store).
- Es hat in den letzten drei Geschäftsjahren in der Union einen Jahresumsatz von mindestens 7,5 Milliarden Euro erzielt oder sein durchschnittlicher Börsenwert betrug im letzten Geschäftsjahr mindestens 75 Milliarden Euro.
- Es betreibt einen zentralen Plattformdienst mit mindestens 45 Millionen in der EU niedergelassenen oder aufhältigen monatlich aktiven Endnutzerinnen und Nutzern bzw. mindestens 10 000 in der EU niedergelassenen jährlich aktiven gewerblichen Nutzerinnen und Nutzern.

Die Gatekeeper müssen insbesondere:

- sicherstellen, dass die Abmeldung von zentralen Plattformdiensten genauso einfach ist wie die Anmeldung;
- dafür sorgen, dass die grundlegenden Funktionen von Sofortnachrichtendiensten interoperabel sind;
- gewerblichen Nutzerinnen und Nutzern Zugang zu ihren Marketing- oder Werbeleistungsdaten auf der Plattform geben;
- Daten ausschliesslich produktbezogen verwenden,
- die Europäische Kommission (KOM) über von ihnen durchgeführte Übernahmen und Fusionen unterrichten.

Den Gatekeepern soll es künftig u. a. nicht mehr möglich sein:

- die eigenen Produkte oder Dienste gegenüber jenen anderer Marktteilnehmenden durch Ranking besser zu positionieren (Selbstbevorzugung);
- bestimmte Apps oder Software vorzuinstallieren oder Nutzerinnen und Nutzer daran zu hindern, diese Apps oder Software einfach zu deinstallieren;
- die Installation von Software für die wichtigsten Programme (z. B. Web-Browser) bei der Installation des Betriebssystems standardmässig vorzuschreiben;
- die im Zuge der Bereitstellung eines Dienstes erhobenen personenbezogenen Daten für die Zwecke einer anderen Bereitstellung wiederzuverwenden.

Verstösst ein Gatekeeper gegen die Vorschriften des DMA, droht ihm eine Geldbusse von bis zu 10 Prozent seines weltweiten Gesamtumsatzes und im Wiederholungsfall von bis zu 20 Prozent dieses Umsatzes.

Die KOM ist für die Benennung der Unternehmen als Gatekeeper verantwortlich. Sobald ein Unternehmen den Schwellenwert für die Benennung als Gatekeeper erreicht, muss es dies der KOM spätestens innerhalb von zwei Monaten mitteilen. Wenn ein Unternehmen die entsprechenden Informationen nicht liefert, darf die KOM gestützt auf die ihr vorliegenden Informationen dieses Unternehmen einseitig als Gatekeeper bezeichnen. Die KOM darf als einzige Instanz die Regeln und Pflichten des DMA durchsetzen. Zur Unterstützung der KOM haben die Mitgliedstaaten die Möglichkeit, ihre für die Durchsetzung von Wettbewerbsvorschriften zuständigen nationalen Behörden zu ermächtigen, Untersuchungen zur möglichen Nichteinhaltung des DMA durchzuführen und deren Ergebnisse an die KOM zu berichten.

## Stand der Dinge

Die Rechtsvorschrift trat am 1. November 2022 in Kraft und ist seit dem 7. März 2024 uneingeschränkt anwendbar. Bis Oktober 2024 hatte die KOM total **7 Gatekeeper** benannt – **Alphabet, Amazon, Apple, Booking, ByteDance, Meta und Microsoft**. Insgesamt wurden 24 zentrale Plattformdienste benannt, die von Gatekeeper erbracht werden.

Am 25. März 2024 hat die KOM ein Verfahren gegen Alphabet, Apple und Meta eingeleitet, da der Verdacht auf diverse Verstösse gegen den DMA bestand. Die KOM möchte prüfen, ob die Anzeige der Google-Suchergebnisse durch Alphabet dazu führt, dass eigene nachgelagerte Suchdienste (z. B. für Waren, Flüge oder Hotels) gegenüber vergleichbaren Suchfunktionen konkurrierender Anbieter bevorzugt werden.

## Mögliche Auswirkungen auf die Schweiz

Der DMA gilt für alle Unternehmen, die in der EU tätig sind. Es existieren aber bislang keine Unternehmen mit Sitz in der Schweiz, die als Torwächter («Gatekeeper») im Sinne des DMA eingestuft werden könnten. Deshalb ist er aktuell nur für Unternehmen mit Sitz in der Schweiz relevant, die in der EU einen zentralen Plattformdienst eines Gatekeepers gewerblich nutzen.

Eine entscheidende Frage ist aber, inwieweit der DMA in der Schweiz indirekt Wirkung entfalten wird, weil die Gatekeeper die neuen Verhaltensregeln des DMA von sich aus auch in der Schweiz befolgen. Hier zeigt sich ein differenziertes Bild. Umgesetzt wird der DMA in der Schweiz gemäss Ankündigung von Meta (mit seinen Plattformdiensten Facebook, Instagram, Whatsapp, Messenger, Marketplace, Ads). Ebenfalls umgesetzt in der Schweiz wird der DMA gemäss Ankündigung auch von Microsoft für den zentralen Plattformdienst LinkedIn. Nicht vollständig umgesetzt wird er von Microsoft, zumindest vorerst, jedoch für den zentralen Plattformdienst Windows. In der Schweiz ebenfalls nicht vollständig umgesetzt (zumindest vorläufig) wird der DMA scheinbar von Apple (App Store, Safari, iOS), Bytedance (TikTok) und Alphabet (Google Search, Google Ads, Chrome, Google Maps, Google Play, Google Shopping, Youtube, Google Android). Bei Amazon (Marketplace, Ads) scheinen für Nutzende aus der Schweiz die Regeln des jeweiligen Markplatzes zu gelten. Noch keine Ankündigung gibt es von Booking.

## Bereits ergriffene Massnahmen in der Schweiz

Der DMA ist wesentlich vom EU-Wettbewerbsrecht inspiriert, so dass unterschiedliche ex ante-Regelungen des DMA potenziell auch ex-post durch das Wettbewerbsrecht durchgesetzt werden könnten. Analog dürften die Bestimmungen des DMA in der Schweiz durch die kartellrechtliche Missbrauchskontrolle (Art. 7 KG) grundsätzlich erfasst sein (vgl. auch Motion 23.3069 Digital Markets Act für die Schweiz). Im Einzelfall können von den Wettbewerbsbehörden zudem auch vorsorgliche Massnahmen angeordnet werden, etwa dort, wo irreversible Marktverschliessungen drohen.

Seit dem 1. Dezember 2022 sind Paritätsklauseln bezüglich Preises, Verfügbarkeit oder sonstige Konditionen in Verträgen zwischen Online-Buchungsplattformen und Beherbergungsbetrieben in der Schweiz verboten (Art. 8*a* UWG). Eine vergleichbare Regelung existiert ebenfalls im DMA (Art. 5 Abs. 3). Im DMA ist die Bestimmung aber nicht auf den Bereich Beherbergung beschränkt. Dafür gilt der DMA nur für sehr grosse Plattformen, während die Regelung im UWG für alle Online-Plattformen gilt. Die Regelung im UWG ist keine Reaktion auf den DMA, sondern eine Umsetzung der Mo. 16.3902 Bischof.

Massnahme 4

# Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern |
| **Art der Massnahme** | Verordnungsvorschlag |
| **Referenz (falls vorhanden)** | Vorschlag für eine Verordnung COM/2022/209 final |
| **Aktueller Stand** | Im Gesetzgebungsprozess |
| **Datum des Inkrafttretens** | Noch nicht verabschiedet |
| **Federführung in der Bundesverwaltung** | fedpol |

## Beschrieb

Am 11. Mai 2022 veröffentlichte die Europäische Kommission (KOM) einen Verordnungsvorschlag zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern im Internet (Child Sexual Abuse Proposal; CSA). Zusammen mit dem Vorschlag legte die KOM auch eine neue Europäische Strategie für ein besseres Internet für Kinder vor.

Der Schutz von Kindern (online und offline) ist eine Priorität der EU. In der Vergangenheit forderte die KOM Unternehmen auf, ihre Anstrengungen zur Erkennung, Meldung und Entfernung von illegalen Online-Inhalten zu verstärken. Diese freiwilligen Massnahmen haben sich als unzureichend erwiesen und mehrere Mitgliedstaaten haben nationale Vorschriften zur Bekämpfung des sexuellen Missbrauchs von Kindern im Internet erlassen. Dies führte zu einer zunehmenden Fragmentierung des digitalen Binnenmarkts für Dienstleistungen. Mit dem Vorschlag der KOM soll nun ein klarer und harmonisierter Rechtsrahmen zur Verhütung und Bekämpfung des sexuellen Missbrauchs von Kindern im Internet geschaffen werden.

Die vorgeschlagene Verordnung besteht aus zwei Hauptbausteinen:

1. Verpflichtungen für Anbieter in Bezug auf die Aufdeckung, Meldung, Entfernung und Sperrung von Material über sexuellen Kindesmissbrauch:
    - Anbieter müssen – unabhängig von ihrem Niederlassungsort – Material über sexuellen Kindesmissbrauch in ihren Diensten aufdecken, melden und entfernen. Die Meldung erfolgt an das neu zu schaffende EU-Zentrum.
    - App-Stores müssen sicherstellen, dass Kinder keine Apps herunterladen können, die eine erhöhte Gefahr bergen, dass Täter darüber Kontakt zu den Kindern suchen.
    - Anbieter von Hosting- oder Messenger-Diensten müssen zukünftig eine Risikobewertung lancieren, inwieweit ihre Dienste für die Verbreitung von Material über sexuellen Kindesmissbrauch oder für die Kontaktanbahnung («Grooming») missbraucht werden könnten.
    - Die Mitgliedstaaten sollen nationale Behörden benennen, die für die Überprüfung der Risikobewertungen zuständig sind.
2. Die Schaffung einer EU-Zentralstelle als dezentrale Agentur, um die Umsetzung der neuen Verordnung zu ermöglichen.

Die Dienstanbieter sind bei ihren Massnahmen dem Schutz der Privatsphäre ihrer Nutzerinnen und Nutzer verpflichtet. Jede erforderliche Überprüfung muss anonym erfolgen. Massnahmen zur Identifizierung der Nutzerinnen und Nutzer dürfen nur im Falle eines potenziellen sexuellen Kindesmissbrauchs im Internet ergriffen werden. Die verwendete Technologie soll ausschliesslich Informationen extrahieren, die zur Aufdeckung des Missbrauchs unbedingt notwendig sind. **Eine kontinuierliche, anlasslose staatliche Überwachung jeglicher**

**interpersonellen digitalen Kommunikation ist im aktuellen Vorschlag der KOM nicht vorgesehen.** Trotzdem hat die Veröffentlichung des Vorschlags für die Verordnung heftige Reaktionen ausgelöst. Besonders die Aufdeckungsanordnung und auch die Ende-zu-Ende-Verschlüsselung sind stark umstritten.

## Stand der Dinge

Aktuell wird der CSA-Verordnungsvorschlag im Rat der EU und parallel dazu im Parlament der EU beraten. Besonders die Aufdeckungsanordnung und auch die Aufdeckung des verschlüsselten Materials bei der Ende-zu-Ende-Verschlüsselung sind umstritten. Inzwischen wurde der Verordnungsentwurf mehrfach überarbeitet und es wurden alternative Vorschläge vorgelegt. Bis heute konnte allerdings noch keine Einigung erzielt werden. Die ungarische Ratspräsidentschaft nahm das Geschäft wieder auf und brachte einen neuen Kompromissvorschlag ein, welcher jedoch letztlich nicht zur Abstimmung gebracht wurde. Aktuell gibt es nach wie vor eine blockierende Minderheit (DE, AT, LUX, IT, NL, PL, SK, EE), wobei davon bloss ein Mitgliedstaat zustimmen oder sich enthalten müsste, damit ein Kompromissvorschlag zustande käme.

Ob und wann der CSA-Verordnungsvorschlag umgesetzt und ob die Aufdeckungsanordnung darin enthalten sein wird, ist somit zurzeit noch unklar.

## Mögliche Auswirkungen auf die Schweiz

Die CSA-Verordnung stellt keine Weiterentwicklung des Schengen-Besitzstands dar. Dennoch kann nicht ausgeschlossen werden, dass Personen mit Sitz oder Wohnsitz in der Schweiz von den vorgeschlagenen Regelungen und damit auch von den Aufdeckungsanordnungen betroffen sein könnten.

Solche Aufdeckungsanordnungen stünden wohl in einem Konflikt mit dem schweizerischen Recht: gemäss Art. 271 StGB macht sich strafbar, wer auf schweizerischem Gebiet ohne Bewilligung für einen fremden Staat Handlungen vornimmt, die einer Behörde oder einem Beamten zukommen oder wer solche Handlungen für eine ausländische Behörde oder eine andere Organisation des Auslands vornimmt oder aber solchen Handlungen Vorschub leistet. Dem Schweizerischen Recht ist auch unterworfen, wer im Ausland ein solches Vergehen begeht (Art. 4 Abs. 1 StGB).

## Bereits ergriffene Massnahmen in der Schweiz

In der Schweiz gab der CSA-Verordnungsvorschlag im Jahr 2022 im Nationalrat Anlass zu einer Interpellation (Interpellation 22.3404 Bellaiche vom 9. Mai 2022, Chat-Kontrolle) und einer Motion (Motion 22.4113 Bellaiche vom 29. September 2022, Chat-Kontrolle. Schutz vor anlassloser dauernder Massenüberwachung). Der Bundesrat wurde damit beauftragt, das von Art. 8 EMRK und Art. 13 BV garantierte Recht auf Schutz der Privatsphäre durchzusetzen und die Einwohnerinnen und Einwohner der Schweiz vor der im CSA-Verordnungsvorschlag vorgesehenen Chatkontrolle zu schützen.

In seiner Stellungnahme vom 23. November 2022 hat der Bundesrat festgehalten, dass sich die Auswirkungen auf die Schweiz zum jetzigen Zeitpunkt nicht abschliessend beurteilen lassen. Deshalb hat er eine Analyse zum Handlungsbedarf beim Kindes- und Jugendschutz im Internet sowie zu den Auswirkungen des CSA-Verordnungsvorschlags angekündigt, um so allfälligen Handlungsbedarf frühzeitig erkennen zu können.

Die RK-N hat nach Anhörung des EDÖB am 27. April 2023 kommuniziert, dass sie ein besonderes Augenmerk darauf richten werde, wie sich die Kontrolle von Chatnachrichten in der EU entwickelt und was für Folgen dies für die Schweizer Bevölkerung haben könnte. Der Nationalrat hat die Motion am 25. September 2023 deutlich angenommen.

Der vom Bundesrat angekündigte Bericht des EJPD wurde am 27. September 2024 veröffentlicht.

Massnahme 5

# European Digital Identity Regulation (eID)

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung (EU) 2024/1183 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 20.05.2024 |
| **Federführung in der Bundesverwaltung** | BJ |

## Beschrieb

Am 20. Mai 2024 trat die Verordnung über die europäische digitale Identität (eID) in Kraft. Die Verordnung ändert die eIDAS-Verordnung (EU) Nr. 910/2014 aus dem Jahr 2014 und schafft den notwendigen Rahmen für eine europäische digitale Identität. Mit der Verordnung werden die Lücken des eIDAS-Systems geschlossen, die Wirksamkeit des Rechtsrahmens verbessert und die Vorteile auf den Privatsektor ausgeweitet. Die Mitgliedstaaten stellen ihren Bürgerinnen und Bürgern und den Unternehmen digitale Brieftaschen (e-wallets) zur Verfügung, in denen sie verschiedene Aspekte ihrer nationalen digitalen Identität verknüpfen. Diese Brieftaschen werden von Behörden oder privaten Einrichtungen bereitgestellt, sofern sie von den Mitgliedstaaten anerkannt sind. Die Konsumentinnen und Konsumenten können auch online auf Dienste zugreifen, ohne private Plattformen zu nutzen oder unnötig personenbezogene Daten weitergeben zu müssen.

Die wichtigsten Elemente der überarbeiteten Rechtsvorschrift können wie folgt zusammengefasst werden:

- Bis 2026 muss jeder Mitgliedstaat seinen Bürgerinnen und Bürgern eine Brieftasche für die europäische digitale Identität (EUid-Wallet) zur Verfügung stellen und solche aus anderen Mitgliedstaaten gemäss der überarbeiteten Verordnung akzeptieren.
- Ausreichende Garantien zur Verhinderung jeglicher Diskriminierung von Personen, die die Brieftasche nicht in Anspruch nehmen; die Nutzung der Brieftasche erfolgt stets auf freiwilliger Basis.
- Das Geschäftsmodell der Brieftasche: Ausstellung, Nutzung und Widerruf sind für alle natürlichen Personen unentgeltlich.
- Die Validierung der elektronischen Attributsbescheinigungen: Die Mitgliedstaaten sind verpflichtet, kostenlose Validierungsmechanismen zur Verfügung zu stellen, die ausschliesslich dazu dienen, die Echtheit und Gültigkeit der Brieftasche und die Identität der Nutzerinnen und Nutzer zu überprüfen.
- Der Code für Brieftaschen: Für die Softwarekomponenten der Anwendungen wird ein offener Quellcode verwendet, wobei die Mitgliedstaaten über einen gewissen Spielraum verfügen, um in begründeten Fällen spezifische Komponenten, die nicht auf Benutzergeräten installiert sind, nicht offenzulegen.
- Die Kohärenz zwischen der Brieftasche als Form der elektronischen Identifikation und dem System, in dessen Rahmen sie ausgestellt wird, wurde sichergestellt.

Schliesslich wird in der überarbeiteten Verordnung der Anwendungsbereich von qualifizierten Zertifikaten für die Authentifizierung von Websites geklärt, wodurch sichergestellt wird, dass die Nutzerinnen und Nutzer überprüfen können, wer die Seite betreibt, während die etablierten aktuellen Sicherheitsvorschriften und -standards der Branche gewahrt bleiben.

## Stand der Dinge

Die Verordnung wurde am 30. April 2024 im Amtsblatt der EU veröffentlicht. Die eID-Verordnung zur Änderung der eIDAS-Verordnung trat am 20. Mai 2024 in Kraft und muss bis 2026 vollständig umgesetzt werden.

## Mögliche Auswirkungen auf die Schweiz

Die Schweiz ist rechtlich nicht verpflichtet, die eIDAS-Verordnung und die damit zusammenhängenden Änderungen zu übernehmen. Angesichts der engen geschäftlichen und gesellschaftlichen Verflechtungen mit den meisten EU-Mitgliedstaaten hat die Schweiz jedoch ein Interesse daran, ihr E-ID-System so zu gestalten, dass es mit jenem der EU interoperabel funktioniert.

Um in den Mitgliedstaaten anerkannt zu werden, muss die schweizerische E-ID im Rahmen des Notifizierungsverfahrens akzeptiert werden, wozu ein völkerrechtlicher Vertrag erforderlich wäre. Die einseitige Übernahme der eIDAS-Verordnung in das schweizerische Recht erscheint uns wenig vorteilhaft, da es um die gegenseitige Anerkennung der schweizerischen und europäischen Systeme (und nicht nur um die Anerkennung des schweizerischen Systems in der EU) geht.

Der Entwurf zum E-ID-Gesetz sieht vor, dass der Bundesrat internationale Abkommen abschliessen kann, um eine internationale Anerkennung der E-ID zu erreichen und ausländische E-ID anzuerkennen (Art. 31). Damit wird eine gegenseitige Anerkennung namentlich mit der EU möglich.

Die Einführung der E-ID und die Schaffung der Vertrauensinfrastruktur ist nicht Gegenstand der Verhandlungen mit der EU über die bilateralen Abkommen des neuen Pakets.

## Bereits ergriffene Massnahmen in der Schweiz

Nach der Ablehnung des Bundesgesetzes über elektronische Identifizierungsdienste durch das Volk am 7. März 2021 hat der Bundesrat das Eidgenössische Justiz- und Polizeidepartement beauftragt, zusammen mit der Bundeskanzlei und dem Eidgenössischen Finanzdepartement eine staatliche E-ID-Lösung zu erarbeiten. Zwischenzeitlich haben National- und Ständerat sechs gleichlautende Motionen aller Fraktionen angenommen, die ein staatlich verwaltetes System zum elektronischen Identitätsnachweis verlangen.

Am 22. November 2023 hat der Bundesrat die Botschaft und den neuen Entwurf des E-ID-Gesetzes verabschiedet. Die parlamentarische Beratung hat im Januar 2024 begonnen. Die Kommission für Rechtsfragen des Nationalrates (RK-N) stimmte der Vorlage mit 21 zu 0 Stimmen bei 3 Enthaltungen zu, der Nationalrat (Plenum) mit 175 zu 12 Stimmen bei 2 Enthaltungen. Die Beratungen im Zweitrat wurden im März 2024 aufgenommen und haben bis zur Herbstsession 2024 gedauert. Da es noch Differenzen zwischen den Bundesräten gibt, werden diese derzeit im Bereinigungsverfahren bearbeitet.

Der neue Entwurf zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) sieht die Einführung eines kostenlosen und freiwilligen staatlichen elektronischen Identitätsnachweises für Inhaberinnen und Inhaber eines von den Schweizer Behörden ausgestellten Ausweises vor. Der Staat nimmt dabei weiterhin seine Kernaufgabe wahr, die darin besteht, die Identität einer Person zu prüfen und den entsprechenden elektronischen Nachweis auszustellen. Wie in den im Nationalrat eingereichten Motionen gefordert, verfolgt der neue Entwurf einen Ansatz, der auf den Grundsätzen des Schutzes der Privatsphäre durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, der Datensparsamkeit und der dezentralen Datenspeicherung beruht.

Zudem soll mit dem Gesetzesentwurf eine staatliche Vertrauensinfrastruktur geschaffen werden, die es Akteurinnen des öffentlichen und privaten Sektors ermöglicht, elektronische Nachweise auszustellen und zu verwenden. Der Staat wird das erforderliche Basissystem betreiben (Basisregister, Vertrauensregister) und eine staatliche elektronische Brieftasche in Form einer mobilen Anwendung zur Verfügung stellen, die die E-ID und weitere elektronische Nachweise enthalten kann. Die Inhaberinnen und Inhaber der elektronischen Brieftasche können ihre E-ID und andere elektronische Nachweise sicher und transparent vorweisen.

Massnahme 6

# Data Governance Act

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung über die europäische Daten-Governance |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung (EU) 2022/868 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 23.06.2022 |
| **Federführung in der Bundesverwaltung** | BAKOM/BJ |

## Beschrieb

Am 23. Juni 2022 ist die Verordnung (EU) 2022/868 über europäische Daten-Governance in Kraft getreten. Mit dieser Verordnung soll der Datenverkehr im Binnenmarkt gefördert werden. Damit sollen Anreize für die Weiterverwendung von sensiblen Daten öffentlicher Stellen geschaffen werden, die unter das Geschäftsgeheimnis, die statistische Geheimhaltung, den Schutz der Rechte am geistigen Eigentum oder den Schutz von personenbezogenen Daten fallen (wie z. B. Energie-, Verkehrs- oder Gesundheitsdaten). Bisher ermöglichte die PSI-Richtlinie 2019/1024 die Weiterverwendung von Daten des öffentlichen Sektors; für sogenannte «sensible» Daten galt sie jedoch explizit nicht.

Die Verordnung enthält drei Prioritäten:

1. Festlegung **spezifischer Bedingungen für die Förderung und Erlaubnis der Weiterverwendung** gewisser Daten des öffentlichen Sektors, die durch Rechte am geistigen Eigentum geschützt sind oder unter die statistische Geheimhaltung, den Datenschutz oder das Geschäftsgeheimnis fallen
2. Einführung gemeinsamer Grundsätze für Datenmittler, insbesondere einen **Anmelde- und Aufsichtsrahmen für die Erbringung von Diensten für die gemeinsame Datennutzung**
3. Förderung des Datenaltruismus durch die Einführung eines Rahmens für **die freiwillige Eintragung** von Einrichtungen, die solche Daten sammeln und verarbeiten.

Daten, die im Besitz öffentlicher Unternehmen sind (wie öffentlich-rechtliche Rundfunkanstalten, Kultur- und Bildungseinrichtungen) sowie Daten, die aus Gründen der öffentlichen Sicherheit geschützt sind, fallen nicht in den Anwendungsbereich der Verordnung (Art. 3).

Die Verordnung beinhaltet weder eine Verpflichtung zur Verarbeitung oder Speicherung der Daten in der EU noch eine Pflicht zur Niederlassung in der EU für Drittstaaten. Die KOM sieht vor, in Durchführungsrechtsakten festzuhalten, dass die Durchsetzungsmechanismen eines Drittstaats für den Schutz des geistigen Eigentums und von Geschäftsgeheimnissen einen Schutz gewährleisten, der im Wesentlichen gleichwertig mit demjenigen der EU ist.

## Stand der Dinge

Die Verordnung ist am 23. Juni 2022 in Kraft getreten. Die neuen Regeln gelten seit September 2023. Im August 2023 hat die KOM mittels einer Durchführungsverordnung gemeinsame Logos zur einfachen Identifizierung von vertrauenswürdigen Datenvermittlungsdiensten und altruistischen Datenorganisationen in der EU eingeführt.

Im Mai 2024 leitete die KOM Vertragsverletzungsverfahren ein, indem sie ein Aufforderungsschreiben an 18 Mitgliedstaaten versandte, die keine für die Umsetzung der Verordnung über die Daten-Governance zuständigen Behörden benannt oder nicht nachgewiesen haben, dass diese Behörden zur Ausführung der in der Verordnung vorgesehenen Aufgaben befugt sind.

## Mögliche Auswirkungen auf die Schweiz

Die Verordnung ist für die Schweiz nicht verbindlich. Die Vorgaben für die Weitergabe von vertraulichen Daten öffentlicher Stellen sowie die gesetzlichen Anforderungen für Datenintermediäre gelten also nicht für die Schweiz.

Die Verordnung entbindet die betreffenden EU-Stellen nicht von einschlägigen Geheimhaltungspflichten und internationale Abkommen sind vorbehalten (vgl. Art. 3 Abs. 3 der Verordnung). Entsprechend sollten Daten, welche eine EU-Stelle mittels Amtshilfe aus dem Ausland (bspw. der Schweiz) erhalten hat, von der Anwendung nicht betroffen sein, da Amtshilfevereinbarungen typischerweise Spezialitäts- und Vertraulichkeitsvorbehalte enthalten.

Schweizer Unternehmen werden jedoch insofern betroffen sein, als Datenintermediäre, welche ihre Dienstleistungen in der EU anbieten, aber nicht in der EU niedergelassen sind (sondern bspw. in der Schweiz), gewisse Regeln befolgen müssen. So müssen sie zum Beispiel einen gesetzlichen Vertreter in einem Mitgliedstaat ernennen (siehe Art. 11 Abs. 3).

Zudem ist die Verordnung im Zusammenhang mit dem Transfer von vertraulichen, nicht-personenbezogenen Daten von öffentlichen Stellen aus der EU in die Schweiz relevant. So dürfen Weiterverwender dieser Daten nur Transfers in Drittstaaten (bspw. die Schweiz) veranlassen, wenn in diesen Drittstaaten angemessene Schutzvorkehrungen für diese nicht-personenbezogenen Daten bestehen. Angemessene Schutzvorkehrungen gelten dann als vorhanden, wenn in einem Drittland im Hinblick auf den Schutz von Geschäftsgeheimnissen und des geistigen Eigentums ein im Wesentlichen gleichwertiges Schutzniveau wie in der EU gilt. Hierzu kann die KOM Durchführungsrechtsakte erlassen, in denen sie erklärt, dass ein Drittland ein im Wesentlichen gleichwertiges Schutzniveau bietet. Dieses Angemessenheitsbeschlussverfahren zum Transfer von vertraulichen Daten von öffentlichen Stellen ist zu unterscheiden vom Angemessenheitsbeschlussverfahren, welches in der DSGVO festgehalten ist und für den Transfer von allen personenbezogenen Daten in Drittländer gilt. Es ist davon auszugehen, dass die Schweiz solche angemessenen Schutzvorkehrungen geltend machen kann, da Geschäftsgeheimnisse und geistiges Eigentum in der Schweiz und der EU ähnlich geschützt sind. Konkret wird dieser Fall wohl nur sehr wenige Unternehmen oder Stellen (bspw. Forschungseinrichtungen oder Hochschulen) in der Schweiz betreffen – nämlich solche, die auf von öffentlichen Stellen in der EU veröffentlichte, vertrauliche Daten zugreifen und diese in die Schweiz transferieren möchten.

Die Schweiz ist zudem als Mitglied des European Statistical System (ESS) (Statistikabkommen bei den Bilateralen II) indirekt betroffen. Die Verordnung hat direkten Einfluss auf die Statistikproduktion der EU-Mitgliedstaaten. Dies wird früher oder später auch in den Regulierungen der Europäischen Statistikproduktion sichtbar werden und möglicherweise in das bilaterale Statistikabkommen EU-CH einfliessen.

## Bereits ergriffene Massnahmen in der Schweiz

Im Rahmen der ständerätlichen Motion 22.3890 «Rahmengesetz für die Sekundärnutzung von Daten» wurde der Bundesrat damit beauftragt, Grundlagen zu schaffen, damit spezifische Infrastrukturen für die Sekundärnutzung von Daten in strategisch relevanten Bereichen rasch initialisiert und aufgebaut werden können. Das BJ hat den Data Governance Act im Rahmen seiner üblichen legistischen Arbeiten zur Kenntnis genommen. Es ist momentan noch nicht entschieden, ob und wie weit diese EU-Massnahme in die Vorlage Eingang finden wird.

Massnahme 7

# Data Act

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung (EU) 2023/2854 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 11.01.2024 |
| **Federführung in der Bundesverwaltung** | BAKOM/BJ |

## Beschrieb

Im Januar 2024 trat die Datenverordnung (EU) 2023/2854 (Data Act) in Kraft. Die Verordnung regelt, wer in der EU generierte personenbezogene und nicht personenbezogene Daten verwenden und wer unter welchen Bedingungen darauf zugreifen darf.

Die Verordnung soll einen horizontalen Rechtsakt für die gemeinsame Nutzung von Industriedaten schaffen: Sie beinhaltet die Pflicht, Nutzerinnen und Nutzern Zugang zu gemeinsam erzeugten Daten zu gewähren und öffentlichen Stellen unter ausserordentlichen Umständen Zugang zu Daten im Besitz von Privatpersonen zu geben. Hersteller von vernetzten Produkten und Anbieter von damit verbundenen Diensten, die sogenannten «Data Holders», müssen den Nutzerinnen und Nutzern leichten, unmittelbaren und kostenlosen Zugang zu den Daten gewähren, zu deren Erzeugung sie beigetragen haben. Die Nutzerinnen und Nutzer könnten beschliessen, die Daten mit Dritten zu teilen. Letztere dürften sie allerdings nicht für die Entwicklung von Konkurrenzprodukten nutzen. Gezielte Massnahmen sollen vermeiden, dass Dritte die Zustimmung zur gemeinsamen Datennutzung erpressen oder manipulieren. Die gemäss dem Gesetz über digitale Märkte (DMA) als «Torwächter» benannten grossen Online-Plattformen kommen als Dritte hier nicht in Betracht.

Die Verordnung hält fest, dass die Bereitstellung der Daten durch die Inhaberinnen und Inhaber an die Empfängerinnern und Empfänger unter fairen, angemessenen und nichtdiskriminierenden Bedingungen und in transparenter Weise zu erfolgen hat. Ein Fairness-Test soll verhindern, dass kleinen und mittleren Unternehmen missbräuchliche Vertragsbedingungen aufgezwungen werden.

Die Verordnung erlaubt den öffentlichen Einrichtungen, Zugang zu Daten zu verlangen, die für eine Reaktion auf öffentliche Notlagen wie z. B. Terroranschläge und Naturkatastrophen als wesentlich gelten. Solche Datenanfragen müssen verhältnismässig sein und sich auf die Krise beschränken, zu deren Bewältigung sie dienen sollen. Kleinst- und Kleinunternehmen sind von den Pflichten in Bezug auf die gemeinsame Datennutzung ausgenommen.

Die Verordnung beinhaltet zudem Regeln über die Interoperabilität und die Möglichkeit, den Anbieter von Cloud-Datenverarbeitungsdiensten zu wechseln («Cloud Switching»). Zudem ist darin vorgesehen, dass die Verträge den Wechsel zu einem anderen Dienst innerhalb von 30 Tagen mit umfassender Unterstützung und Betriebskontinuität während des Umstellungsprozesses erlauben müssen. Nach drei Jahren muss der «Ausstiegsdienst» unentgeltlich angeboten werden. Die Cloud-Dienste müssen die Kompatibilität mit offenen Schnittstellen oder in der EU etablierten Interoperabilitätsstandards gewährleisten.

Die Verordnung sieht ein ähnliches System wie jenes für personenbezogene Daten vor: Cloud-Anbieter werden verpflichtet, geeignete Schutzmassnahmen zu treffen, um mit der europäischen oder nationalen Gesetzgebung nicht vereinbare internationale Übermittlungen von Industriedaten bzw. den Zugang durch Drittstaaten zu verhindern.

## Stand der Dinge

Die Verordnung trat am 11. Januar 2024 in Kraft. Die Regelungen kommen ab dem 12. September 2025 zur Anwendung.

## Mögliche Auswirkungen auf die Schweiz

Die Verordnung ist nicht direkt auf die Schweiz anwendbar, Der Data Act gilt aber nicht nur für Datenhalter, Datenempfänger und Anbieter von Produkten und Dienstleistungen welche innerhalb des EU-Territoriums niedergelassen sind, sondern für alle Anbieter, welche relevante Produkte und Dienste oder Daten an Kundinnen und Kunden in EU-Mitgliedstaaten anbieten bzw. Daten empfangen – völlig unabhängig vom Ort ihrer Niederlassung.

Es sind also auch gewisse Schweizer Unternehmen betroffen, insbesondere solche, die:

- vernetzte Produkte oder mit diesen Produkten verbundene Dienstleistungen in der EU anbieten und in den Verkehr bringen;
- relevante Daten halten und diese Datenempfängern in der EU bereitstellen;
- Datenverarbeitungsdienste an Kunden in der EU anbieten.

Diese Unternehmen müssen den relevanten Bestimmungen des Data Acts Folge leisten.

## Bereits ergriffene Massnahmen in der Schweiz

In der Schweiz bestehen aktuell keine horizontalen Regeln oder Gesetze für den Austausch von nicht-personenbezogenen Daten unter Privatpersonen. Im Bereich des öffentlichen Rechts existiert das Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG, SR 172.019), das Vorschriften zu Open Government Data enthält. Diese gelten jedoch nur für die Bundesverwaltung. Im Rahmen der ständerätlichen Motion 22.3890 «Rahmengesetz für die Sekundärnutzung von Daten» wurde der Bundesrat damit beauftragt, Grundlagen zu schaffen, damit spezifische Infrastrukturen für die Sekundärnutzung von Daten in strategisch relevanten Bereichen rasch initialisiert und aufgebaut werden können. Das BJ hat den Data Act im Rahmen seiner üblichen legistischen Arbeiten zur Kenntnis genommen. Es ist momentan noch nicht entschieden, ob und wie weit diese EU-Massnahme in die Vorlage Eingang finden wird.

Massnahme 8

# Gemeinsame Europäische Datenräume

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Gemeinsame Europäische Datenräume |
| **Art der Massnahme** | Strategie |
| **Referenz (falls vorhanden)** | - |
| **Aktueller Stand** | In Umsetzung |
| **Federführung in der Bundesverwaltung** | BAKOM/BK |

## Beschrieb

Die Europäische Datenstrategie (2020) zeigt den Weg für die Schaffung eines echten Binnenmarkts für Daten auf, in dem personenbezogene und nicht personenbezogene Daten, einschliesslich sensibler Unternehmensdaten, transparent von Land zu Land und zwischen verschiedenen Branchen ausgetauscht werden können.

Um diese Vision zu konkretisieren, werden Datenräume eingerichtet, die die gemeinsame Nutzung und den Austausch zuverlässiger und sicherer Daten in strategischen Wirtschaftszweigen und öffentlichen Bereichen erleichtern sollen. Die europäischen Datenräume werden schrittweise verbunden und bilden eine Säule des Datenbinnenmarkts.

Wichtige Fortschritte wurden beim **Rechtsrahmen der EU für Datenräume** erzielt, insbesondere mit dem Inkrafttreten des Daten-Governance-Gesetzes (siehe Massnahme 6), der Verabschiedung des Datengesetzes (siehe Massnahme 7) und dem Durchführungsrechtsakt zu hochwertigen Datensätzen gemäss der Richtlinie über offene Daten._Massnahme_6_–_Massnahme_7_–

Seit Lancierung der Strategie hat die Europäische Kommission (KOM) 14 Datenräume in verschiedenen Sektoren und Bereichen von öffentlichem Interesse angekündigt. Einen Überblick über den aktuellen Stand der gemeinsamen europäischen Datenräume gibt die KOM in einer im Januar 2024 veröffentlichten Arbeitsunterlage. Die EU finanziert mehrere Initiativen im Zusammenhang mit gemeinsamen europäischen Datenräumen. Koordinierungs- und Unterstützungsmassnahmen sowie Einführungsmassnahmen werden hauptsächlich im Rahmen des Programms Digital Europe finanziert, Innovations- und Forschungsinitiativen über das Programm Horizon Europe.

Nachfolgend eine Liste der bestehenden europäischen Datenräume:

1) **Der europäische Agrardatenraum** wird die Nachhaltigkeit und Wettbewerbsfähigkeit der EU-Landwirtschaft stärken, indem Daten zu Produktion, Bodennutzung, Umwelt sowie andere Daten verfügbar gemacht und gemeinsam genutzt werden.
2) **Der europäische Datenraum für das kulturelle Erbe** gilt als Leitinitiative der Kommission, um den digitalen Wandel im europäischen Kulturbereich voranzutreiben und die Erstellung und Wiederverwendung von Inhalten des digitalen Kulturerbes zu fördern.
3) **Der europäische Energiedatenraum** soll einen umfassenden und kohärenten europäischen Rahmen für den Datenaustausch zur Unterstützung innovativer Energiedienstleistungen schaffen. Dies wird der EU helfen, ihre übergeordneten Ziele in Bezug auf Energieversorgungssicherheit, Nachhaltigkeit und Integration der Energiemärkte zu erreichen (siehe Massnahme 8b)._Massnahme_8b_–
4) **Der europäische Finanzdatenraum** wird zur digitalen Transformation im EU-Finanzsektor beitragen und den digitalen Finanzsektor in Europa ankurbeln.
5) **Der Datenraum zum europäischen Grünen Deal** wird die Umsetzung der Politik des Grünen Deals anhand einschlägiger Daten (z. B. zur Luft-, Wasser- und Bodenqualität im Rahmen der Null-Schadstoff-Strategie) unterstützen und zu einem höheren Umweltschutzniveau beitragen.
6) **Der europäische Gesundheitsdatenraum** würde es natürlichen Personen ermöglichen, ihre elektronischen Gesundheitsdaten zu kontrollieren. Gleichzeitig könnten Forschung, Innovation und Politik diese Daten anonymisiert, sicher und zuverlässig nutzen (siehe Massnahme 8a)._Massnahme_8a_–

7) **Der europäische Industriedatenraum** (Fertigung) wird der verarbeitenden Industrie in Europa dabei helfen, Industriedaten besser zu nutzen und flexiblere und widerstandsfähigere Lieferketten zu schaffen.
8) **Der europäische Sprachdatenraum** soll ein Ökosystem schaffen, das die Sammlung, Erstellung, gemeinsame Nutzung und Weiterverwendung multimodaler Sprachmodelle und -daten in allen Branchen ermöglicht.
9) **Der europäische Mediendatenraum** soll Medienorganisationen dabei unterstützen, durch datengestützte Zusammenarbeit erfolgreich zu sein und die Herausforderungen der digitalen Wirtschaft zu meistern, insbesondere im Hinblick auf ihre Wettbewerbsfähigkeit in einem von Online-Plattformen dominierten Markt.
10) **Der europäische Mobilitätsdatenraum** unterstützt die Ziele der Strategie für nachhaltige und intelligente Mobilität und wird den Zugang zu sowie die Zusammenführung und die gemeinsame Nutzung von Daten aus bestehenden und künftigen Verkehrs- und Mobilitätsdatenquellen erleichtern.
11) **Der Datenraum für europäische öffentliche Verwaltungen** soll den sicheren Datenaustausch für europäische öffentliche Verwaltungen fördern.
12) **Der gemeinsame europäische Datenraum für Forschung und Innovation** soll die Praxis der offenen Wissenschaft in Europa weiter stärken.
13) **Der europäische Kompetenzdatenraum** wird eine Infrastruktur für den Zugang zu sowie den Austausch und die Weiterverwendung von Qualifikations- und Bildungsdaten für eine Vielzahl von Zwecken wie die Entwicklung innovativer Anwendungen und Lösungen, die Modernisierung des Lernangebots, die Erforschung und Analyse von Arbeitsmarkttrends bieten.
14) **Der europäische Tourismusdatenraum** wird den Datenbedarf des öffentlichen und privaten Sektors decken und die gemeinsame Nutzung, Verarbeitung und Analyse von Daten innerhalb der Branche erleichtern. Für die Konsumentinnen und Konsumenten bedeutet der Zugang zu Daten eine bessere Auswahl. Für die Entscheidungstragenden wird er ein Instrument zur Vorhersage von Touristenströmen sein, um die öffentlichen Dienstleistungen entsprechend anzupassen. Und für Unternehmen ergibt sich die Möglichkeit, ihre Dienstleistungen besser zu planen und zielgerichteter zu gestalten.

## Stand der Dinge

Die gemeinsamen branchenspezifischen Datenräume werden nach einem eigenen Zeitplan implementiert.

## Mögliche Auswirkungen auf die Schweiz

Die verschiedenen Datenraumprojekte werden die Schweiz nicht direkt betreffen. Datenräume in allen Bereichen könnten jedoch zur Innovations- und Effizienzsteigerungen in der EU beitragen. Je nach Bereich könnte es auch für die Schweiz wünschenswert sein vom Zugang zu europäischen Datenräumen zu profitieren. Entsprechend muss in diesen Bereich frühzeitig die Interoperabilität von schweizerischen Datenraumprojekte mit europäischen Datenraumprojekten sichergestellt werden. Diese Arbeiten sollen ab 2025 auch im Rahmen der Anlaufstelle für Datenräume (verantwortet von BK; BAKOM, BFS und EDA DV) vorangetrieben werden.

Die Schweiz als Mitglied des European Statistical System (ESS) (Statistikabkommen bei den Bilateralen II) ist indirekt betroffen. Die Diskussion zu den Datenräumen, insbesondere einem Datenraum für Statistik, wird das ESS in der Zukunft sicher verschiedene Chancen und Risiken ermöglichen.

## Bereits ergriffene Massnahmen in der Schweiz

Auch die Schweiz arbeitet intensiv an Datenräumen. Im Dezember 2023 hat der Bundesrat beschlossen, ein Datenökosystem Schweiz zu fördern und ab 2025 eine Anlaufstelle für Datenräume zu betreiben. Gleichzeitig bestehen bereits oder entstehen aktuell auch in der Schweiz viele sektorspezifische Datenraumprojekte, beispielsweise zu Gesundheit (siehe Massnahme 8a), Energie (siehe Massnahme 8b), öffentlicher Verkehr, Geodaten oder Statistik. _Massnahme_8a_–_Massnahme_8b_–

Massnahme 8a

# Europäischer Gesundheitsdatenraum

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung über den europäischen Raum für Gesundheitsdaten |
| **Art der Massnahme** | Verordnungsvorschlag |
| **Referenz (falls vorhanden)** | Vorschlag für eine Verordnung COM/2022/197 final |
| **Aktueller Stand** | Kurz vor Inkrafttreten |
| **Datum des Inkrafttretens** | Anfang 2025 |
| **Federführung in der Bundesverwaltung** | BAG |

## Beschrieb

Der Europäische Raum für Gesundheitsdaten (European Health Data Space - EHDS) ist ein wichtiger Pfeiler der europäischen Gesundheitsunion und stellt den ersten gemeinsamen EU-Datenraum in einem spezifischen Bereich dar, der aus der EU-Datenstrategie hervorgeht. Die Europäische Kommission hatte am 3. Mai 2022 einen Verordnungsvorschlag für die Schaffung eines europäischen Raums für Gesundheitsdaten veröffentlicht. Die Vorlage wurde am 15. März vom Europäischen Rat und am 24. April 2024 vom Europäischen Parlament angenommen.

Der EHDS zielt darauf ab, die Gesundheitsversorgung in der EU zu verbessern und sie für die digitale Zukunft vorzubereiten. Ziel ist es, klare Regeln, gemeinsame Standards und digitale Infrastrukturen zu etablieren, um die Nutzung elektronischer Gesundheitsdaten zu erleichtern. Dies soll sowohl Patientinnen und Patienten als auch Forschung, Innovation, Politik, Patientensicherheit, Statistik und regulatorischen Zwecken dienen.

Der EHDS umfasst zwei digitale Infrastrukturen:

- **Primäre Nutzung von Gesundheitsdaten**: Diese Infrastruktur ermöglicht den Austausch von Gesundheitsdaten für die direkte Patientenversorgung, wie z.B. Patientenakten und e-Rezepte. Ziel ist es, Gesundheitsdaten grenzüberschreitend zugänglich zu machen, zum Zweck der Vereinfachung der Erbringung von Gesundheitsdienstleistungen in der gesamten EU.
- **Sekundäre Nutzung von Gesundheitsdaten**: Diese Infrastruktur dient der Wiederverwendung von Gesundheitsdaten für Forschung, Innovation, Politikgestaltung und regulatorische Zwecke. Es soll ein kohärentes Umfeld für Forschung, Innovation sowie Politikgestaltung und Regulierungstätigkeiten geschaffen werden.

Als konkrete Beispiele der Funktionsweise können etwa genannt werden:

- Grenzüberschreitender Zugang zu Patientendaten ermöglicht eine effektivere Behandlung im Ausland
- Forschungsprojekte können auf umfangreiche Gesundheitsdaten zugreifen, um beispielsweise KI-basierte Tools zu entwickeln und innovative Produkte zu schaffen

Der EHDS baut dabei auf folgenden EU-Rechtsakten auf:

- Datenschutz-Grundverordnung (DSGVO)
- Daten-Governance-Rechtsakt (siehe Massnahme 6)_Massnahme_6_–
- Datengesetz (siehe Massnahme 7)_Massnahme_7_–
- Richtlinie über Netz- und Informationssysteme (siehe Massnahme 17)_Massnahme_17_–

Das Vertrauen ist ein grundlegender Faktor für den Erfolg des EHDS. Hierbei ist es entscheidend, dass Bürgerinnen und Bürger darauf vertrauen können, dass ihre sensiblen Gesundheitsdaten im EHDS angemessen geschützt und sinnvoll genutzt werden. Die Verordnung sieht folgende Opt-out-Regeln vor:

- Primärnutzung: Die Mitgliedstaaten können den Bürgerinnen und Bürgern ein Opt-out für die im Rahmen des EHDS zu errichtenden Infrastrukturen (beispielsweise Patientendossiers) anbieten.

- Sekundärnutzung: Opt-out-Regeln mit denen ein ausgewogenes Verhältnis zwischen der Achtung der Patientenwünsche und der Gewährleistung der Verfügbarkeit der richtigen Daten für die richtigen Personen im öffentlichen Interesse hergestellt wird.

Der Aufbau des EHDS wird für die Mitgliedstaaten umfangreiche Arbeiten, sowie finanzielle Investitionen erfordern. Die EU-KOM unterstützt dies durch die Kofinanzierung von Projekten wie dem Pilotprojekt HealthData@EU, direkte Finanzhilfen an die Mitgliedstaaten sowie dem Aufbau auf bestehenden Infrastrukturen.

## Stand der Dinge

Die Verordnung zum EHDS wurde im Frühling 2024 vom Rat und dem Europäischen Parlament angenommen. Momentan wird der Rechtstext von den Rechts- und Sprachverständigen überprüft und sollte Anfang 2025 im Amtsblatt der Europäischen Union veröffentlicht werden. Zwanzig Tage nach Veröffentlichung im Amtsblatt wird die Verordnung in Kraft treten.

In einem ersten Schritt soll die primäre Nutzung von Gesundheitsdaten vorangetrieben werden (Beginn des Datenaustauschs ab 2028, mit Erweiterungen um weitere Datenkategorien im 2030). Die Bestimmungen für die Sekundärnutzung von Gesundheitsdaten sollen ab 2028 in Kraft treten. Für bestimmte Datenkategorien (wie klinische Studiendaten und menschliche genetische Daten) ist eine zusätzliche Frist bis 2030 vorgesehen.

## Mögliche Auswirkungen auf die Schweiz

Die Möglichkeiten einer Anbindung von Drittstaaten wie der Schweiz an den EHDS sind momentan noch unklar. Die EU wünscht zuerst den Datenraum EU-intern zu vervollständigen, bevor Drittstaaten einbezogen werden. Aktuell bleibt es für die Schweiz wichtig, die Entwicklungen auf EU-Ebene in diesem Bereich eng mitzuverfolgen.

## Bereits ergriffene Massnahmen in der Schweiz

In der Schweiz verfolgt das nationale Programm zur Förderung der digitalen Transformation im Gesundheitswesen (DigiSanté) vergleichbare Ziele wie der EHDS. Im Fokus stehen eine flächendeckende digitale Vernetzung, Interoperabilität zwischen den Systemen und Akteuren sowie die Verbesserung der Datenverfügbarkeit, -nutzung und -qualität. Im Rahmen von vier Umsetzungspaketen werden von 2025 bis 2034 die Voraussetzungen für die digitale Transformation geschaffen, die notwendigen Infrastrukturen für einen sicheren und nahtlosen Datenaustausch etabliert, Behördenleistungen digitalisiert und die Möglichkeiten zur Sekundärnutzung von Gesundheitsdaten für Planung, Steuerung und Forschung weiter optimiert. Der im Zusammenhang mit dem Programm eingereichte Verpflichtungskredit im Rahmen von CHF 392 Millionen Franken wurde im Frühling 2024 von beiden Räten bewilligt, womit ab 2025 die Umsetzung von DigiSanté starten kann.

Seit 2017 existiert in der Schweiz zudem die gesetzliche Grundlage für das elektronische Patientendossier (EPDG). Mit dem elektronischen Patientendossier (EPD) sollen die Qualität der medizinischen Behandlung gestärkt, die Behandlungsprozesse verbessert, die Patientensicherheit erhöht und die Effizienz des Gesundheitssystems gesteigert sowie die Gesundheitskompetenz der Patientinnen und Patienten gefördert werden. Das EPDG regelt die Rahmenbedingungen für die Einführung und Verbreitung des EPD. Zurzeit läuft eine umfassende Revision dieser gesetzlichen Grundlage. Es soll damit unter anderem die Rollenverteilung zwischen Bund und Kantonen in Bezug auf das EPD klar geregelt und dessen Finanzierung sichergestellt werden. Bis zum Inkrafttreten der umfassenden Revision wird das EPD stetig weiterentwickelt mit dem Ziel, alle behandlungsrelevanten Daten darin ablegen zu können.

Im Rahmen einer Forschungsinfrastruktur-Initiative hat der Bund mit dem «Swiss Personalized Health Network» (SPHN) zudem von 2017-2024 CHF 135 Millionen in die verbesserte Nutzbarmachung von Gesundheitsdaten aus den fünf Schweizer Universitätsspitälern für die datengetriebene, biomedizinische Forschung investiert. Zudem wurde mit «BioMedIT» ein sogenanntes «Trusted Research Environment», also eine sichere IT-Umgebung für die Mobilisierung, Analyse und Speicherung von sensiblen Forschungsdaten aufgebaut, die von allen Schweizer Forschenden genutzt werden kann.

Im Rahmen der ständerätlichen Motion 22.3890 «Rahmengesetz für die Sekundärnutzung von Daten» wurde der Bundesrat damit beauftragt, Grundlagen zu schaffen, damit spezifische Infrastrukturen für die Sekundärnutzung von Daten in strategisch relevanten Bereichen rasch initialisiert und aufgebaut werden können. Das BJ hat die

Arbeiten zum EHDS im Rahmen seiner üblichen legislativen Arbeiten zur Kenntnis genommen. Es ist momentan noch nicht entschieden, ob und wie weit diese EU-Massnahme in die Vorlage Eingang finden wird.

Die beschriebenen Massnahmen wurden unabhängig von den Arbeiten zum EHDS (Vorstösse aus dem Parlament sowie Aufträge aus dem Bundesrat) lanciert. Die Schweiz verfolgt die Entwicklungen zum EHDS jedoch eng.

Massnahme 8b

# Europäischer Energiedatenraum

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Europäischer Energiedatenraum |
| **Art der Massnahme** | Aktionsplan/Kommunikation |
| **Referenz (falls vorhanden)** | - |
| **Aktueller Stand** | - |
| **Datum des Inkrafttretens** | - |
| **Federführung in der Bundesverwaltung** | BFE |

## Beschrieb

Es soll ein zuverlässiger und sicherer gemeinsamer europäischer Energiedatenraum (European Energy Data Space - EEDS) geschaffen werden. Ein solcher wurde in der europäischen Datenstrategie und dem EU-Aktionsplan zur Digitalisierung des Energiesystems angekündigt.

Dieser Datenraum soll den Zugang zu Daten erweitern, die zur Entwicklung innovativer Energiedienstleistungen erforderlich sind, um die Stromnetze auszugleichen und zu optimieren sowie die Energieeffizienz der gebauten Umwelt zu verbessern. Er wird eine Schlüsselrolle bei der Integration erneuerbarer Energiequellen spielen und somit die Ziele des „Fit for 55“-Pakets und des RePowerEU-Plans vorantreiben.

Der Energiedatenraum soll eng mit anderen sektorenspezifischen Datenräumen (z. B. Mobilität und intelligente Gemeinschaften) verknüpft sein und es Akteuren aus verschiedenen Sektoren wie Gebäudeautomation und Elektromobilität ermöglichen, aktiv am Energiemarkt teilzunehmen, Energiedienstleistungen zu erbringen und die Sektorintegration (Verbindung der verschiedenen Energieträger - Strom, Wärme, Kälte, Gas, feste und flüssige Brennstoffe - untereinander und mit den Endverbrauchssektoren wie Gebäude, Verkehr oder Industrie) zu fördern. Dies soll ihnen ermöglichen, zur effizienten Energienutzung beizutragen, die Nutzung erneuerbarer Energien zu steigern und die Integration, Zusammenarbeit und den Informationsaustausch zwischen verschiedenen Sektoren zu unterstützen sowie neue Geschäftsmöglichkeiten zu schaffen. Betroffen davon sind mehrere Sektoren wie der Stromsektor, Gebäudeautomation, Elektromobilität oder Energiegemeinschaften.

## Stand der Dinge

Bis am 29. Mai 2024 lief eine Ausschreibung zur Erstellung eines EU-weiten Energiedatenraums. Ziel dieser Ausschreibung ist die Einführung einer ersten Version eines gemeinsamen europäischen Energiedatenraums in mindestens 10 Mitgliedstaaten, Identifizierung von fünf Anwendungsfällen (z.B. DER-Management, Flexibilitätsdienste für Stromnetze, intelligentes EV-Laden) und Verwendung einer gemeinsamen Referenzarchitektur mit offenen Standards für Dateninteroperabilität. Sowie die Entwicklung von Geschäftsmodellen und Implementierung eines Governance-Systems zur Überwachung des Betriebs. Das Projekt wurde vergeben. Allerdings wird das Grant Agreement erst am 28. Februar 2025 unterzeichnet werden. Deswegen ist noch nicht bekannt, wer das Projekt durchführen wird.

## Mögliche Auswirkungen auf die Schweiz

Die Grundidee eines Datenraums ist es, eine interoperable Dateninfrastruktur für eine Vielzahl von Akteuren und Dienstleistungen innerhalb und ausserhalb eines Sektors zu schaffen, welche auf klaren Regeln und Standards beruht. Dies schliesst die Definition von Datenprodukten und Datenaustauschprozessen mit ein (vgl. Studie “Common European Energy Data Space”). Als Teil des Energiesystems soll ein Datenraum, durch erhöhte Interoperabilität und verbesserten Datenzugang, zusätzliche Transparenz, Effizienz und Geschäftsmöglichkeiten schaffen, wovon sowohl die Gesellschaft, Wirtschaft als auch die Behörden profitieren können. Ob es möglich ist, dass Drittstaaten wie die Schweiz an den europäischen Energiedatenraum angebunden werden können ist derzeit unklar. Aktuell bleibt es für die Schweiz wichtig, die Entwicklungen auf EU-Ebene in diesem Bereich eng mitzuverfolgen.

Die Umsetzung eines Energiedatenraums in der Schweiz sowie eine mögliche Anbindung an den europäischen Energiedatenraum wird jedoch vor dem Hintergrund der diversen und kleinteiligen Struktur der Schweizer Energiewirtschaft auch einige Herausforderungen schaffen, die es zu berücksichtigen gilt. So sind beispielsweise ein sehr heterogener Digitalisierungsgrad der Schweizer Energieversorgungsunternehmen (EVU) und bei sehr kleinen EVU geringeres Know-How/Kapazitäten für Datenstandardisierung bestehende Hürden für die Etablierung eines Energiedatenraums in der Schweiz.

Aus regulatorischer Sicht wurden jedoch mit dem revidierten Stromversorgungsgesetzes (Teil des «Mantelerlasses») bereits wichtige, gesetzliche Anforderungen formuliert, welche die Grundlage eines Schweizer Energiedatenraums legen können. So sind Datenharmonisierung und verbesserte Interoperabilität ein Kernanliegen der sogenannten «Datenplattform», welche eine Anbindung und somit Vernetzung aller Marktteilnehmer der Schweizer Stromwirtschaft (und absehbar auch der Gaswirtschaft) vorsieht. Zudem wurden im gleichen Gesetz bereits detaillierte Regelungen zur Nutzung von Flexibilität geschaffen (eingeschlossen sind auch Ladevorgänge von Elektromobilen), unter dem Abschnitt zum Einsatz von intelligenten Steuer- und Regelsystemen. Diese Gesetzesergänzungen sind jedoch zunächst ein erster Schritt hinsichtlich der Umsetzung von Anforderungen und Massnahmen, welche eine Übernahme oder Anbindung an einen europäischen Energiedatenraum mit sich bringen würde.

## Bereits ergriffene Massnahmen in der Schweiz

Der Hintergrundreport der Europäischen Kommission («Common European Energy Data Space») nennt mehrere Anwendungsfälle, die der Europäische Energiedatenraum abdecken solle. Unter anderem sind virtuelle Kraftwerke und Aggregation, preissensitive Lade- und Entladevorgänge von elektrischen Fahrzeugen und Optimierung im Gebäudeenergiebereich genannt.

Studien haben solchen Anwendungsfälle auch in der Schweiz identifiziert und untersucht. Zu nennende, geförderte oder begleitete Studien sind beispielsweise «Smart Interoperability Architecture (SINA): the Decentralized Data Space in the Building Industry» (abgeschlossen 04/2024) und «Digitalisierung im Gebäude - Interoperabilität und Informationssicherheit» (abgeschlossen 10/2022).

Erstere Studie analysierte auch mögliche Anforderungen eines europäischen Energiedatenraums aus der Sicht der Schweizer Energiewirtschaft. So wurde beispielsweise im Hinblick auf eine Anbindung des Schweizer an den Europäischen Datenraum in der Studie konstatiert, dass: «bei der Implementierung von Datenräumen (…) verschiedene Gesetze eingehalten werden, insbesondere bezüglich datenrechtlicher Belange, wie die General Data Protection Regulation (GDPR) der EU, oder das Eidgenössische Datenschutzgesetz (DSG). Das Framework der IDSA bietet hier Lösungen, da es mit den Datenschutzbestimmungen der Europäischen Union konform ist und fortlaufend an die Änderungen des rechtlichen Rahmens angepasst wird. Damit vereinfacht es den Aufbau und Betrieb eines Datenraumes in der Schweiz wesentlich. Dennoch muss in der Schweiz auf Spezifika des DSG geachtet werden.» (S.8).

Zudem wurde bereits intern die Machbarkeit spezifischer, technischer Regelungen im Bereich Smart Meter Daten («Commission Implementing Regulation (EU) 2023/1162») und Zugang und Austausch von Daten zu Flexibilität («Network Code Demand Response») analysiert. Hinsichtlich der Implementierung wurde jedoch noch kaum etwas unternommen.

Massnahme 9

# Europäischer Chips Act

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung zur Schaffung eines Rahmens für Massnahmen zur Stärkung des europäischen Halbleiter-Ökosystems und zur Änderung der Verordnung (EU) 2021/694 (Chip-Gesetz) |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung (EU) 2023/1781 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 21.09.2023 |
| **Federführung in der Bundesverwaltung** | SBFI/SECO |

## Beschrieb

Der European Chips Act ist am 21. September 2023 in Kraft getreten (Verordnung (EU) 2023/1781). Damit möchte die EU ihre Wettbewerbsfähigkeit bei Halbleitertechnologien stärken und die Lieferabhängigkeiten reduzieren. Fünf Ziele werden genannt:

- Erhöhung der Produktionskapazitäten bis 2030 von heute 10% auf 20%
- Stärkung der Forschungs- und Technologieführerschaft Europas
- Kapazitätsbildung und Leadership in Design, Produktion und Vermarktung
- Wissen zu globalen Lieferketten aufbauen
- Mangel an Fachkräften beheben, Talente anziehen und fördern

Die Verordnung wurde im Rahmen eines breiteren Pakets mit drei Hauptpfeilern veröffentlicht:

- «Chips for Europe»-Initiative (Säule1): Aufbau technologischer Kapazitäten und Innovationen durch Schliessung der Lücke zwischen den fortschrittlichen Forschungs- und Innovationskapazitäten und der industriellen Nutzung.
- Rahmen für die Versorgungssicherheit (Säule 2): Schaffung eines Rahmens, der die Versorgungssicherheit und Resilienz des Halbleitersektors gewährleisten soll, indem Investitionen angezogen und die Produktionskapazitäten in den Bereichen Fertigung, Verpackung, Test und Montage ausgebaut werden. Für Produktionsstandorte, welche den Status einer «integrierten Produktionsanlage und offener EU-Giesserei» erhalten, soll für die EU-Mitgliedsstaaten einfacher sein, Beihilfen sprechen zu können.[1] Deutschland hat bspw. angekündigt u.a. Intel, SMC, Wolfsspeed und Bosch mit rund 4,8 Milliarden Euro fördern zu wollen.[2]
- European Semiconductor Board (ESB) (Säule 3): Schaffung eines Koordinationsmechanismus zwischen den EU-Mitgliedstaaten und der Kommission zur Stärkung des Monitorings und des Krisenmanagements. Das ESB übernimmt auch die Aufsicht über den European Chips Act.

Der European Chips Act plant, bis 2030 mehr als 43 Milliarden Euro an öffentlichen und privaten Investitionen zu mobilisieren. Die vorgeschlagenen Ausgaben im Rahmen der «Chips for Europe»-Initiative sollen aus bereits vorhandenen Budgets aus Horizon Europe und dem DEP gespiesen werden. Die Mittel werden durch nationale Investitionen und durch langfristige private Investitionen ergänzt.

Der European Chips Act ergänzt andere Halbleiterinitiativen wie die Halbleiterindustrieallianz, Programmaktivitäten in diesem Bereich (z.B. Joint Undertaking oder im Rahmen von Horizon Europe oder DEP, das «wichtige Vorhaben von gemeinsamem europäischem Interesse» (IPCEI) in der Mikroelektronik und Kommunikationstechnologie, oder staatliche Beihilfen im Rahmen der Aufbau- und Resilienzfazilität (RRF).

## Stand der Dinge

[1] Siehe Draft guidance document S.9 (European Chips Act: Commission publishes guidance on the application process for the status of integrated production facility and open EU foundry | Shaping Europe's digital future)
[2] BMWK - Der Klima- und Transformationsfonds 2024: Entlastung schaffen, Zukunftsinvestitionen sichern, Transformation gestalten

Die Verordnung wurde am 18. September 2023 im Amtsblatt der EU veröffentlicht und ist seit dem 21. September 2023 in Kraft.

## Mögliche Auswirkungen auf die Schweiz

Der European Chips Act ist vorwiegend im Kontext der Spannungen zwischen China und Taiwan zu sehen und weitgehend mit geopolitischen Ambitionen begründet. Wie bei weiteren aktuellen industriepolitischen Initiativen der EU sind sowohl positive als auch negative wirtschaftliche Auswirkungen möglich. So eröffnen die Programme auch für Zulieferer und Produzenten aus der Schweiz teilweise neue Absatzchancen. Zudem könnten sich für die Industrie diversifiziertere Beschaffungsmöglichkeiten ergeben. Anderseits können Subventionen den Wettbewerb zum Nachteil von Produzenten verzerren. Dies gilt auch für die weltweit tätige Schweizer Halbleiterindustrie, die in Bezug auf Grösse und Spezialisierung sehr vielfältig entlang der gesamten Wertschöpfungskette aufgestellt ist.

Zur Umsetzung der «Chips for Europe Initiative» sieht der European Chips Act u.a. die Gründung eines gemeinsamen Unternehmens für Halbleiter (Chips JU) mit einem Budget von 4.2 Milliarden (2021-2027) vor, dass aus Horizon Europe und DEP finanziert wird. Das erklärte Ziel des Bundesrates bleibt die schnellstmögliche Assoziierung an das Horizon-Paket, um den Forschungsakteuren in der Schweiz die besten Bedingungen für die Teilnahme an europäischen Aktivitäten zu bieten. Grundsätzlich setzt sich die Schweiz dafür ein, dass die Initiativen im Ausland keine protektionistischen Elemente enthalten und die Förder- und Forschungsprogramme, wenn immer möglich, Drittländern gegenüber offenstehen. Im Oktober 2023 stellte die Kommission eine Liste von Technologiebereichen vor, die als «kritisch» für die wirtschaftliche Sicherheit der Europäischen Union eingestuft werden, darunter auch Halbleitertechnologien. Eine unmittelbare Folge davon ist, dass Schweizer Forscher, selbst bei einer eventuellen Assoziierung an Horizon-Europe und DEP, in ihrer Zusammenarbeit mit Europa wahrscheinlich von Einschränkungen betroffen sein werden.

## Bereits ergriffene Massnahmen in der Schweiz

Um die Auswirkungen des Ausschlusses von Schweizer Akteuren aus den von Europa als strategisch eingestuften Bereichen zu mildern, hat der Bundesrat am 24. Mai 2023 Übergangsmassnahmen beschlossen. Das SBFI hat auf dieser Basis eine Übergangsmassnahme im Halbleitersektor lanciert, die sich primär an die Schweizer Hochschulforschungsstätten richtet. Die entsprechende «SwissChips»-Initiative mit einer maximalen Fördersumme von 26 Mio. CHF wird auf die geplanten europäischen Aktivitäten abgestimmt und baut gleichzeitig auf den Stärken der Schweiz in der Halbleiterforschung auf.

Am 13. Juni 2024 hat der Nationalrat das Postulat Cottier 23.3866 angenommen, welches eine schweizerische Halbleiterstrategie fordert. Der Bundesrat wird in Erfüllung des Postulats die Auswirkungen ausländischer industriepolitischer Massnahmen im Bereich Halbleiter (inkl. jener der EU) analysieren und auch Möglichkeiten zur Verbesserung der Rahmenbedingungen prüfen.

Massnahme 10

# Europäische Strategie für Quantentechnologie

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Europäische Quantum-Strategie |
| **Art der Massnahme** | Strategie |
| **Referenz (falls vorhanden)** | - |
| **Aktueller Stand** | In Umsetzung |
| **Datum des Inkrafttretens** | 29.10.2018 |
| **Federführung in der Bundesverwaltung** | SBFI |

## Beschrieb

Im Oktober 2018 lancierte die Europäische Kommission die «Quantum Technologies Flagship»-Initiative. Die Initiative führt Forschungsinstitutionen, die Privatwirtschaft und Fördermittel aus der öffentlichen Hand zusammen, um Quantentechnologien für Europa zu fördern. Sie wird bis 2028 laufen und Projekte im Bereich Quantum mit insgesamt einer Milliarde Euro unterstützen. Die strategische Forschungsagenda (Strategic Research Agenda, SRA) des *Flagship* wurde am 3. März 2021 veröffentlicht. Sie gibt eine klare Richtung für die Entwicklung von Forschung und Innovation im Bereich Quantum vor. Forschung und Innovation unter dem *Quantum Flagship* werden sich auf vier Bereiche konzentrieren:

i. **Quantenkommunikation** für die Entwicklung von Netzwerken, die wachsende Mengen von Daten sicher übermitteln können;
ii. **Quantenrechner**, um riesige Rechenkapazitäten zur Lösung komplexer Probleme zur Verfügung stellen zu können;
iii. **Quantensimulation** komplexer nichtlinearer Phänomene oder mikroskopischer Prozesse auf molekularer/atomarer Ebene (z.B. Wetter, chemische/atomare Prozesse) sowie
iv. **Quantensensoren und -vermessung** für exakte Messergebnisse. Die SRA des *Quantum Flagship* soll diese vier Prioritäten mit folgenden Massnahmen umsetzen:
    1. Einbezug aller wichtiger Akteure auf dem Gebiet, Schaffung eines innovativen Ökosystems
    2. Förderung des **Zugangs zu Finanzierung,** Aufbau einer nachhaltigen Quantenindustrie in Europa
    3. Aufbau der **Infrastruktur und Wertschöpfungsketten**, Erarbeitung von Industriestandards mit internationalen Partnern
    4. Erarbeitung einer europäischen Strategie für **geistiges Eigentum und Definition von Standards** (zusammen mit dem europäischen Patentamt)
    5. **Bildung und Öffentlichkeitsarbeit**, Förderung von Quantenphysik als Teil der Bildung, Ausbildung und Förderung von Spezialistinnen und Spezialisten

## Stand der Dinge

Die Massnahme ist seit dem 29.Oktober 2018 in Kraft. Die ersten Projekte auf den oben genannten Gebieten wurden gemäss der SRA lanciert. Die zweite Phase der Quantum-Flagship-Initiative wurde mit Ausschreibungen im Rahmenprogramm Horizon Europe eingeleitet. Ziel ist es, die Führungsrolle der EU in der Forschung im Bereich Quantentechnologien zu stärken und die Forschungsergebnisse einer industriellen Nutzung anzunähern. Das DEP wird zusätzliche Fördermittel für Quantentechnologien zur Entwicklung und zum Ausbau der strategischen digitalen Kapazitäten Europas bieten.

## Mögliche Auswirkungen auf die Schweiz

Forschende in der Schweiz haben sich in den letzten Jahren erfolgreich an Quantentechnologieprojekten im Rahmen von Horizon 2020/Quantum Technologies Flagship und der europäischen QuantERA-Initiative beteiligt. Die Schweiz ist daran interessiert, die langjährige Kooperation mit Europa in diesem Bereich fortzusetzen. Weil jedoch die Assoziierung an die Programme Horizon Europe sowie DEP eine Voraussetzung für die weitere

Teilnahme der Schweiz an den verschiedenen Aktivitäten im Bereich der Quantentechnologien bildet, bleibt die Schweiz zurzeit noch ausgeschlossen. Mit den laufenden Verhandlungen für eine Assoziierung an Horizon Europe und DEP könnte auch eine Rückkehr in die Quantentechnologieprojekte erfolgen. Die Schweiz blieb bis zum Ende des Jahres 2024 ausgeschlossen. Da die Verhandlungen über eine Assoziierung am 20. Dezember 2024 abgeschlossen wurden, wurde eine Übergangsregelung aktiviert, die es Schweizer Forschern und Innovatoren ermöglicht, an den meisten Ausschreibungen unter Horizon Europe und Digital Europe teilzunehmen. Die Teilnahme an einigen Ausschreibungen mit hohem TRL im Quantenbereich unterliegt zusätzlichen Bedingungen.

Da die «technologische Souveränität» zu den Prioritäten der digitalen Strategie der EU gehört, ist es aber wahrscheinlich, dass an den Programmen Horizon Europe und Digital Europe Programme (DEP) assoziierte Drittstaaten trotz der Assoziierungsabkommen aus bestimmten sensiblen Technologiebereichen wie der Quantentechnologie ausgeschlossen werden. So arbeitet die EU derzeit an der Entwicklung und dem Aufbau einer Quantenkommunikationsinfrastruktur (EuroQCI), um Quantentechnologien in konventionelle Kommunikationsinfrastrukturen zu integrieren und dadurch eine ultrasichere Datenübertragung zu ermöglichen. Die EU hat jedoch die Beteiligung von Drittstaaten wie der Schweiz an EuroQCI aus Gründen der «technologischen Souveränität» ausgeschlossen. Selbst wenn die Schweiz an Horizon Europe und DEP assoziiert wäre, könnte sie trotzdem von gewissen Aktivitäten (z.B. Bau und Beschaffung von Quantenrechnern oder Quantenkommunikationsinfrastruktur) ausgeschlossen werden.

## Bereits ergriffene Massnahmen in der Schweiz

Der Bundesrat hat beschlossen mit Übergangsmassnahmen den Forschungsstandort Schweiz zu stärken.

Zudem sieht der Bundesrat in Forschungsbereichen mit strategischer Bedeutung für die Schweiz wie der Quantenforschung zusätzliche Massnahmen vor. Ziel ist es, die Forschung in der Schweiz strukturell und nachhaltig zu stärken. Diese Massnahmen dienen als Ergänzung zum EU-Rahmenprogramm und zu einer Assoziierung der Schweiz. So hat der Bundesrat im Mai 2022 die Swiss Quantum Initiative (SQI) beschlossen.

Die Schweiz intensiviert auch ihre Strategie der internationalen Zusammenarbeit im Bereich der Quantentechnologie (z.B. Mitwirkung am neuen internationalen Round Table über gemeinsame Forschung zu Quanteninformationen) sowie bilaterale Abkommen mit prioritären Partnern.

Massnahme 11

# Verordung für europäisches Hochleistungsrechnen

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung über das gemeinsame Unternehmen für europäisches Hochleistungsrechnen |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung (EU) 2021/1173 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 13.07.2021 |
| **Federführung in der Bundesverwaltung** | SBFI |

## Beschrieb

Mit dem neuen mehrjährigen Finanzrahmen (MFR) für die Periode 2021–2027 hat die Europäische Kommission (KOM) beschlossen, die künftig als institutionelle Partnerschaft fortgesetzte Verordnung Gemeinsames Unternehmen für europäisches Hochleistungsrechnen (GU EuroHPC) (Verordnung EU 2021/1173) zu überarbeiten. Teilnehmende des Gemeinsamen Unternehmens EuroHPC sind die EU-Mitgliedstaaten, die bei Horizon Europe, DEP und/oder dem EU-Förderinstrument Connecting Europe Facility (CEF) assoziierten Staaten sowie die privaten Vereinigungen European Technology Platform for High Performance Computing (ETP4HPC) und Big Data Value Association (BDVA). Die am 18. September 2020 vorgeschlagene Verordnung sieht im Wesentlichen eine Fortsetzung der bestehenden Initiative mit den folgenden Kernaufgaben beauftragt vor:

1. **Infrastruktur:** Beschaffung von Hochleistungsrechen- und Dateninfrastrukturen von Weltrang (inkl. zukünftige Quantenrechner) sowie Modernisierung der aktuellen Infrastruktur. Mehrere Hochleistungsrechner wurden bereits beschafft (z.B. die LUMI-Infrastruktur in Finnland, an der sich die Schweiz beteiligt).
2. **Föderierung von Hochleistungsrechendiensten:** Sicherstellung eines unionsweiten und Cloud-gestützten Zugangs zu gebündelten und sicheren Hochleistungsrechen-, Quanteninformatik- und Datenressourcen für öffentliche und private Nutzerinnen und Nutzer in ganz Europa.
3. **Technologie:** Unterstützung einer Forschungs- und Innovationsagenda zur Entwicklung eines europäischen Supercomputing-Ökosystems von Weltrang.
4. **Anwendung:** Unterstützung von Aktivitäten zur Erhaltung der Führungsposition Europas bei der Entwicklung wichtiger Rechen- und Datenanwendungen und Softwarecodes für die Wissenschaft, die Industrie (einschliesslich KMU) und den öffentlichen Sektor.
5. **Ausbau der Nutzung und der Kompetenzen:** Aufbau und Vernetzung von nationalen HPC-Kompetenzzentren, um die wissenschaftliche und industrielle Nutzung von Supercomputing-Ressourcen und Datenanwendungen zu fördern.

Im Juli 2021 verabschiedete die Verordnung GU EuroHPC. Die Verordnung definiert einen ehrgeizigen Auftrag und ist für den Zeitraum 2021–2027 mit einem deutlich höheren Budget dotiert, nämlich 7 Milliarden Euro, davon 1,9 Milliarden aus dem Digital Europe Programme (DEP), 900 Millionen von Horizon Europe und 200 Millionen aus der Fazilität Connecting Europe. Ebenso viel investieren die teilnehmenden Staaten, während sich der Beitrag der privaten Mitglieder auf 900 Millionen Euro (als Sach- und Barbeiträge) beläuft. Heute sind sechs von EuroHPC kofinanzierte Supercomputer voll funktionsfähig: LUMI in Finnland (Platz 5 weltweit[3]), LEONARDO in Italien (Platz 7 weltweit), MareNostrum 5 in Spanien (Platz 9 weltweit), Vega in Slowenien, MeluXina in Luxemburg, Discoverer in Bulgarien, Karolina in der Tschechischen Republik und Deucalion in Portugal. EuroHPC hat ausserdem fünf neue Hosting-Standorte für eine neue Generation europäischer Supercomputer in Deutschland, Griechenland, Ungarn, Irland und Polen angekündigt.

Am 24. Januar 2024 hat die Kommission eine Änderung der aktuellen EuroHPC-Verordnung (EU 2021/1173) des Rates von 2018 vorgeschlagen, um eine weitere Kernaufgabe aufzunehmen: Die Entwicklung und den Betrieb

[3] TOP500 ist die Liste der schnellsten Supercomputer weltweit (https://top500.org/lists/top500/list/2024/06/)

von «KI-Fabriken» zur Unterstützung der Weiterentwicklung eines hochgradig wettbewerbsfähigen und innovativen KI-Ökosystems in der Union. Dadurch sollen die Hochleistungsrechenkapazitäten der Union innovativen europäischen Start-ups für das Training und die Feinabstimmung von fortschrittlichsten KI-(Sprach-)Modelle zur Verfügung gestellt werden. Die vorgeschlagene Änderung ist Teil der KI-Initiative der Union, die Kommissionspräsidentin Ursula von der Leyen in ihrer Rede zur Lage der Union 2023 angekündigt hatte. Die Verordnung zur Änderung wurde im Rat COMPET Forschung am 23. Mai 2024 angenommen.

## Stand der Dinge

Die Anpassung zu KI ist seit dem 9. Juli 2024 in Kraft. Projektaufrufe werden von EuroHPC veröffentlicht werden.

## Mögliche Auswirkungen auf die Schweiz

Die Schweiz spielt in Europa eine Pionierrolle auf dem Gebiet des Hochleistungsrechnens. Der Supercomputer «Piz Daint» des Schweizerischen Zentrums für Wissenschaftliches Rechnen (CSCS) in Lugano zählte bereits 2013 zu den leistungsstärksten der Welt und sein Nachfolger «Alps» ist seit Juni 2024 auf Platz 6 weltweit gelistet.

Die Schweiz, die ab März 2019 Vollmitglied des gemeinsamen Unternehmens «EuroHPC» war, wollte die hervorragende Zusammenarbeit mit der EU auf dem Gebiet des Hochleistungsrechnens fortsetzen. Da EuroHPC in DEP integriert wurde und eine Assoziierung an Horizon Europe oder DEP eine Vorbedingung für die Teilnahme an den verschiedenen Aktivitäten von EuroHPC ist, bleibt die Schweiz Stand heute ausgeschlossen.

Für die Schweizer Strategie sind die jüngsten Entwicklungen problematisch, weil

a. Die Schweiz nicht mehr an der Entwicklung grosser, gemeinsamer, europaweiter HPC-Infrastrukturprojekte teilnehmen kann. Die Teilnahme an der LUMI-Infrastruktur in Finnland war für die Schweiz sowohl aus wissenschaftlicher als auch aus wirtschaftlicher Sicht (Problem der explodierenden Strompreise) von entscheidender Bedeutung.
b. Eine Zusammenarbeit im Bereich der Anwendungen, z.B. im Bereich der Wetter-/Klimasimulation oder der Beteiligung an den verschiedenen europäischen Exzellenzzentren im HPC-Bereich, ist nun nicht mehr möglich. Mit dem Ausschluss aus den entsprechenden Communities können somit notwendige technologische Weiterentwicklungen nicht vollzogen werden.

Aufgrund des kurzen Lebenszyklus der HPC-Systeme und in Anbetracht der neuen KI-zentrischen Anpassung der Verordnung, die die Bereitstellung zusätzlicher KI-Ressourcen vorsieht, ist eine schweizerische EuroHPC-Mitgliedschaft in naher Zukunft wünschenswert. Dies wird nach der Unterzeichnung des Abkommens über die Assoziierung mit EU-Programmen mit der vorläufigen Anwendung des Abkommens möglich sein. Die Übergangsvereinbarung ermöglicht bereits die Teilnahme an Projektaufrufen und einen Beobachterstatus in der Partnerschaft.

## Bereits ergriffene Massnahmen in der Schweiz

Nach der Nicht-Assoziierung der Schweiz an Horizon Europe und DEP hat das SBFI erste Massnahmen getroffen. So wurde Ende 2022 unter der Leitung der ETH Zürich die SwissTwins-Initiative ins Leben gerufen mit dem Ziel, eine integrierte Plattform für die Simulation von Wetter/Klima auf dem neuen alps Supercomputer in Lugano bereitzustellen. Unabhängig davon hat der ETH-Bereich die SWISS AI Initiative ins Leben gerufen, die ähnliche Ziele wie die europäische Verordnung verfolgt.

Massnahme 12

# Elektronischer Austausch von Sozialversicherungsdaten

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Elektronischer Austausch von Sozialversicherungsdaten (EESSI) |
| **Art der Massnahme** | Digitalisierungsprojekt |
| **Referenz (falls vorhanden)** | EESI |
| **Aktueller Stand** | In Umsetzung |
| **Datum der Veröffentlichung** | 05.07.2019 |
| **Federführung in der Bundesverwaltung** | BSV |

## Beschrieb

Der Elektronische Austausch von Sozialversicherungsdaten (*Electronic Exchange of Social Security Information* – EESSI) ist das Ergebnis zweier EU-Verordnungen zur Koordinierung der nationalen Systeme der sozialen Sicherheit (Verordnung (EG) Nr. 883/2004 und Verordnung (EG) Nr. 987/2009), welche die Schweiz im Kontext des Personenfreizügigkeitsabkommens zwischen der Schweiz und der EU sowie im Rahmen der Konvention der Europäischen Freihandelsassoziation (EFTA) übernommen hat..

Das EESSI ist ein dezentrales IT-System, das rund 3400 Träger der sozialen Sicherheit in den 32 teilnehmenden Ländern, d. h. den 27 EU-Mitgliedstaaten, Island, Liechtenstein, Norwegen, dem Vereinigten Königreich und der Schweiz, miteinander verbindet. Die Systemkomponenten wurden von der Europäischen Kommission (KOM) finanziert, entwickelt und geliefert.

Mithilfe des EESSI können die Sozialversicherungsträger in diesen Ländern über nationale Zugangspunkte rasch und sicher Informationen über die verschiedenen Zweige der sozialen Sicherheit austauschen (Arbeitslosigkeit, Familie, Rente, Leistungen bei Krankheit und Mutterschaft/Vaterschaft, Arbeitsunfälle, Betreibung und geltende Rechtsvorschriften). Ein solcher Informationsaustausch trägt dazu bei, dass die Sozialversicherungsansprüche der Bürgerinnen und Bürger über die Grenzen hinweg besser geschützt werden. Das EESSI ist somit ein wichtiger Pfeiler der Freizügigkeit in Europa.

## Stand der Dinge

Ursprünglich war vorgesehen, das EESSI 2012 in Betrieb zu nehmen. Aufgrund der Komplexität des Systems verzögerte sich das Projekt jedoch so stark, dass die Einführung erst im Juli 2019 beginnen konnte. Die Rolloutphase startete am 5. Juli 2019 und dürfte bis 2025 dauern.

Von den 32 Staaten, die sich am EESSI beteiligen, haben 19 (AT, BG, DE, EE, HU, IS, LV, MT, SE, UK, CY, DK, NO, PT, FR, IE, LI, FI, LT) die Systemintegration vollständig abgeschlossen. Das Projekt EESSI kann finalisiert werden, sobald die übrigen Länder, darunter die Schweiz, ihre Einführungsarbeiten beendet haben, was grundsätzlich im Laufe des Jahres 2025 der Fall sein sollte. Das Projekt EESSI umfasst daher sowohl die Einführungsphase als auch die Wartung und Weiterentwicklung des Systems, was zu einem hohen Ressourcenaufwand führt. Dies gilt für alle betroffenen Länder.

Ende 2020 hat die KOM einseitig und ohne vorherige Konsultation die Verantwortung für die Wartung und Weiterentwicklung bestimmter Komponenten an die am EESSI beteiligten Länder übertragen (HandOver). Seither stellen das Bundesamt für Sozialversicherungen (BSV) und das Bundesamt für Informatik und Telekommunikation (BIT) gemeinsam den ordnungsgemässen Betrieb des Systems in der Schweiz sicher.

## Mögliche Auswirkungen auf die Schweiz

Die EU-Verordnungen zur Koordinierung der Systeme der sozialen Sicherheit sind direkt auf die Schweiz anwendbar. Sämtliche schweizerischen Sozialversicherungseinrichtungen sind heute direkt oder indirekt an das EESSI angeschlossen und tauschen Informationen mit anderen Einrichtungen in Europa aus.

Zur Finanzierung des schweizerischen Teils des EESSI-Systems werden in der Schweiz Gebühren von jenen schweizerischen Institutionen erhoben, die das System nutzen.

Künftige Entwicklungen wie insbesondere die Initiative ESSPASS (siehe Massnahme 13), die eng mit der digitalen Identität und der europäischen elektronischen Brieftasche (EUID-Wallet), also mit eIDAS, verbunden ist (siehe Massnahme 5), werden erhebliche Auswirkungen auf das EESSI und seine Funktionsweise haben, d. h. auch auf die Bürgerinnen und Bürger und die schweizerischen Einrichtungen der sozialen Sicherheit. Massnahme 5 –

## Bereits ergriffene Massnahmen in der Schweiz

Für die Übertragung grosser Datenmengen müssen Ad-hoc-Anwendungen entwickelt werden. Dies war im Bereich der Altersvorsorge der ersten Säule (Entwicklung und Wartung bei der Zentralen Ausgleichsstelle), bei der Festlegung der auf Personen anwendbaren Sozialversicherungsgesetzgebung (Entwicklung und Wartung beim BSV), wie auch für die Krankenversicherung (Entwicklung und Wartung bei der Gemeinsamen Einrichtung KVG) der Fall.

Massnahme 13

# Europäischer Sozialversicherungsausweis

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Europäischer Sozialversicherungsausweis (ESSPASS) |
| **Art der Massnahme** | Initiative |
| **Referenz (falls vorhanden)** | ESSPASS |
| **Aktueller Stand** | Pilotphase |
| **Datum der Veröffentlichung** | - |
| **Federführung in der Bundesverwaltung** | BSV |

## Beschrieb

Im Aktionsplan zur europäischen Säule sozialer Rechte wurde die Initiative für einen Europäischen Sozialversicherungsausweis (*European Social Security Pass* – ESSPASS) angekündigt, um im Rahmen von Pilotmassnahmen eine digitale Lösung für die grenzüberschreitende Ausstellung und Überprüfung von Sozialversicherungsdokumenten zu testen. Dabei geht es um portable Dokumente – wie etwa die Europäische Krankenversicherungskarte (*European Health Insurance Card*) –, die den Bürgerinnen und Bürgern zur Geltendmachung ihrer Sozialversicherungsansprüche in Europa ausgestellt werden.

ESSPASS ist Teil der europäischen Verordnungen zur Koordinierung der nationalen Systeme der sozialen Sicherheit (Verordnung [EG] Nr. 883/2004 und Verordnung [EG] Nr. 987/2009) und betrifft alle 32 Länder, die diese Verordnungen anwenden (einschliesslich der Schweiz).https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32004R0883

Während EESSI (siehe Massnahme 12) lediglich einen digitalen Austausch zwischen Sozialversicherungsträgern ermöglicht, soll ESSPASS Personen, die in ein anderes Land reisen oder umziehen, oder Unternehmen, die im Ausland tätig sind, bei Bedarf dabei unterstützen, auf digitalem Wege mit Sozialversicherungsträgern, anderen öffentlichen Stellen wie Arbeitsinspektorinnen und Arbeitsinspektoren oder Gesundheitsdienstleistern zu interagieren. Massnahme 12 –

Ziel ist die Erstellung und der Austausch digitaler Dokumente, die für die Koordinierung der Systeme der sozialen Sicherheit notwendig sind. Dies steht in engem Zusammenhang mit der digitalen Identität. ESSPASS soll daher die Ausstellung, die Überprüfung der Echtheit und Gültigkeit in Echtzeit sowie die Rückverfolgbarkeit dieser Dokumente ermöglichen und gleichzeitig administrative Hürden abbauen und das Betrugs- und Fehlerrisiko verringern.

ESSPASS ist technologieunabhängig und zielt darauf ab, unter Berücksichtigung aller nationalen Erfordernisse und Besonderheiten die beste Lösung zu ermitteln und zu erproben. Dabei stützt ESSPASS sich auf andere EU-Initiativen, insbesondere auf:

- Die Verordnung über das **einheitliche digitale Zugangstor** (Verordnung [EU] 2018/1724). Die Website Your Europe wird eine einheitliche Anlaufstelle für Bürgerinnen und Bürger sowie Unternehmen bieten, die die Digitalisierung von Sozialversicherungsdokumenten entsprechend der Verordnung über das einheitliche digitale Zugangstor beantragen möchten.
- Den Rahmen für **die digitale Identität der EU** (EUID, vgl. Massnahme 5), der es Einzelpersonen und Unternehmen ermöglicht, sich zu identifizieren und Dokumente über Sozialversicherungsansprüche in ihrer elektronischen Brieftasche (EUID-Wallet) zu speichern. Massnahme 5 –
- Die europäische Blockchain-Service-Infrastruktur (*European Blockchain Services Infrastructure* – EBSI, vgl. Massnahme 23), die darauf abzielt, die Blockchain-Technologie zur Schaffung grenzüberschreitender Dienste für öffentliche Verwaltungen, Bürgerinnen und Bürger und deren Ökosysteme zu nutzen, um Informationen zu verifizieren und Dienste vertrauenswürdig zu gestalten. Massnahme 23 –

## Stand der Dinge

Die ESSPASS-Initiative startete 2021 mit einer ersten Pilotphase, die von der GD EMPL (Generaldirektion Beschäftigung, Soziales und Integration) gemeinsam mit der italienischen Sozialversicherungsbehörde (*Istituto Nazionale della Previdenza Sociale – INPS*) eingeleitet wurde und sich auf die Digitalisierung der Verfahren für das portable Dokument A1 (Bescheinigung über die auf eine Person anzuwendenden Rechtsvorschriften) und den Einsatz von Blockchain-Technologien konzentrierte. Dreizehn weitere EU-Mitgliedstaaten verfolgten die Entwicklungen, zumeist als Beobachter.

Als Follow-up zur ersten Phase der ESSPASS-Pilotmassnahmen führen zwei Konsortien, DC4EU und EBSI Vector, die Tests zur Ausstellung und Verifizierung des portablen Dokuments A1 und der europäischen Krankenversicherungskarte fort. Die beiden Konsortien werden voraussichtlich bis Ende des ersten Halbjahres 2025 ihre Berichte vorlegen und ihre Arbeiten präsentieren.

Gemäss der Mitteilung der Europäischen Kommission (KOM) vom September 2023 zur Digitalisierung der Koordinierung der sozialen Sicherheit (COM [2023] 501 final) soll unter Berücksichtigung der Ergebnisse der Pilotmassnahmen der Konsortien über die weiteren Schritte entschieden werden. Dabei geht es insbesondere um die Frage, ob in allen EU-Ländern eine ESSPASS-Lösung eingeführt werden kann und ob dazu allenfalls ein Rechtsrahmen geschaffen werden muss.

## Mögliche Auswirkungen auf die Schweiz

Bürgerinnen und Bürger der EU, die über portable digitalisierte Dokumente verfügen, können ihre Sozialversicherungsansprüche während eines vorübergehenden Aufenthalts in der Schweiz geltend machen. Die zuständigen Schweizer Behörden und Stellen müssen diese neuen Dokumententypen lesen können und können nicht verlangen, dass ihnen ein physisches Dokument vorgelegt wird. Dies wird für die Gesundheitsdienstleister zweifellos eine Herausforderung darstellen.

Sobald die Vertrauensinfrastruktur gemäss dem Gesetzesentwurf zur E-ID in der Schweiz verfügbar und mit derjenigen der EU kompatibel ist, können Schweizer Institutionen parallel zu den physischen auch digitalisierte, portable Dokumente ausstellen. Dadurch wird es Schweizer Bürgerinnen und Bürgern möglich sein, während ihres Aufenthalts in Europa ihre Sozialversicherungsansprüche wahrzunehmen.

In der Schweiz ist die europäische Krankenversicherungskarte auf der Rückseite der schweizerischen Versichertenkarte abgebildet; Letztere muss an die digitale Version der europäischen Karte angepasst werden.

## Bereits ergriffene Massnahmen in der Schweiz

Das BJ, fedpol und das BIT arbeiten bereits am Aufbau der Vertrauensinfrastruktur, wie sie im Gesetzesentwurf zur E-ID in der Schweiz vorgesehen ist (eID, Wallet, Register usw.). Diese muss mit der Vertrauensinfrastruktur der EU kompatibel sein.

Das BSV beteiligt sich aktiv an den Arbeiten des Konsortiums DC4EU (Konsortium für digitale Zertifikate für Europa) und koordiniert die Durchführung eines breit angelegten Pilotprojekts mit den potenziellen Akteuren in der Schweiz. Dazu zählen auf der einen Seite das BAG und santésuisse via Sasis AG im Hinblick auf die Ausstellung der europäischen Krankenversicherungskarte und auf der anderen Seite das SECO, die Eidgenössische Ausgleichskasse (AHV) und das Arbeitsinspektorat des Kantons Tessin für die Ausstellung des Nachweises der Unterstellung (Dokument A1). Das BSV bereitet sich zudem auf die Einführung der Lesesysteme für die neuen Dokumente vor.

Massnahme 14

# Gigabit Infrastructure Act

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Gigabit Infrastructure Act |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung (EU) 2024/1309 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum der Veröffentlichung** | 11.05.2024 |
| **Federführung in der Bundesverwaltung** | BAKOM |

## Beschrieb

Die Verordnung über Massnahmen zur Reduzierung der Kosten des Aufbaus von Gigabit-Netzen für die elektronische Kommunikation (Gigabit Infrastructure Act, GIA) ist am 11. Mai 2024 in Kraft getreten. Die Verordnung zielt darauf ab, den Ausbau von Hochgeschwindigkeitsnetzen wie Glasfaser- und 5G-Netzen zu beschleunigen und Investitionen in die digitale Infrastruktur anzukurbeln. Darüber hinaus wurde auf Vorschlag des Europäischen Parlaments die Abschaffung der Gebühren für intra-EU-Kommunikation in die Verordnung aufgenommen.

Für die Beschleunigung des Netzausbaus sollen insbesondere die Genehmigungsverfahren erleichtert werden. Die Verordnung verpflichtet die Mitgliedstaaten, eine nationale Streitbeilegungsstelle einzurichten, die bei bestimmten Streitfällen zwischen öffentlichen Stellen und Telekommunikationsbetreibern angerufen werden und verbindliche Entscheidungen zur Beilegung treffen kann. Zudem wird das tacit-approval-Prinzip eingeführt, welches besagt, dass ein Antrag für einen Netzausbau als stillschweigend genehmigt gilt, wenn die Antwort der zuständigen Behörde innerhalb einer bestimmten Frist ausbleibt. In einem Kompromiss zwischen dem Parlament und dem Rat wurde die Antwortfrist für die Genehmigung auf vier Monate festgelegt. Die Mitgliedstaaten können jedoch ganz vom tacit approval-Prinzip abweichen, wenn sie entweder ihre Behörden verpflichten, Antragsteller zu entschädigen, wenn sie nicht rechtzeitig antworten, oder den Antragstellern das Recht einräumen, vor Gericht zu klagen. Weiter wird die Verlegung von Glasfaserleitungen in allen neuen und renovierten Gebäuden, für die Baugenehmigungen nach dem 12. Februar 2026 beantragt wurden, verpflichtend. Ausnahmen gibt es für kritische nationale Infrastrukturen.

## Stand der Dinge

Die Gebühren für intra-EU Kommunikation werden bis 2029 abgeschafft. Aktuell bezahlen EU-BürgerInnen auf Reisen innerhalb der EU keine Roaminggebühren, es fallen jedoch Gebühren an, wenn sie von ihrem Heimatland aus in einen anderen Mitgliedstaat telefonieren oder eine SMS versenden. Die derzeit festgelegten Preisobergrenzen - 0.19€/min für Anrufe und 0.06€/SMS - für die intra-EU Kommunikation sind im Mai 2024 ausgelaufen und werden mit der neuen Verordnung vom 14. Mai 2024 bis zum 1. Januar 2032 verlängert. Bis zum 30. Juni 2027 muss die Kommission eine Folgenabschätzung für das Auslaufen der Preisobergrenze vorlegen. Bis im Juni 2028 muss die Kommission einen Durchführungsrechtsakt zur Abschaffung der intra-EU Kommunikationsgebühren erlassen, sodass ab dem 1. Januar 2029 die Endkundenpreise den nationalen Inlandspreisen entsprechen werden.

## Mögliche Auswirkungen auf die Schweiz

Es gibt keine direkten Auswirkungen auf die Schweiz.

## Bereits ergriffene Massnahmen in der Schweiz

Der Bundesrat hat unabhängig vom Gigabit Act das UVEK damit beauftragt, eine Vernehmlassungsvorlage für eine Gigabitstrategie in der Schweiz zu erarbeiten.

Massnahme 15

# Cybersicherheitsstrategie

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Europäische Cybersicherheits-Strategie |
| **Art der Massnahme** | Strategie |
| **Federführung in der Bundesverwaltung** | BACS/EDA ADIGI/EDA AIS |

## Beschrieb

In der Mitteilung über die Cybersicherheitsstrategie der EU für die digitale Dekade vom 16. Dezember 2020 wird vorgeschlagen, die Cybersicherheit entlang der gesamten Lieferkette zu integrieren und die Aktivitäten und Ressourcen der EU in den vier Cybersicherheitskreisen – Binnenmarkt, Strafverfolgung, Cyberdiplomatie und Cyberabwehr – zusammenzuführen. Die Strategie erstreckt sich auf die Sicherheit wesentlicher Dienste wie Krankenhäuser, Energienetze und Eisenbahnen sowie die ständig wachsende Zahl vernetzter Geräte in Haushalt, Büros und Industrie. Sie bezweckt den Aufbau kollektiver Kapazitäten, um grössere Cyberangriffe abwehren zu können. Im Hinblick auf die Gewährleistung der internationalen Sicherheit und Stabilität im Cyberspace enthält sie auch Pläne für die Zusammenarbeit mit Partnern aus der ganzen Welt. Die Strategie führt Massnahmen im Zusammenhang mit den drei Handlungsbereichen der EU auf: 1) Widerstandsfähigkeit, technologische Unabhängigkeit und Führungsrolle, 2) Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion und 3) Förderung eines globalen offenen Cyberraums durch Zusammenarbeit. In dieser Legislaturperiode wurden verschiedene Rechtsvorschriften zur Umsetzung der Strategie verabschiedet (siehe Massnahmen 16, 17, 18 und 19).

Auf der Tagung der für die Telekommunikation zuständigen Ministerinnen und Minister vom 21. Mai 2024 billigte der Europäische Rat Schlussfolgerungen zur Zukunft der Cybersicherheit, in denen gefordert wird, die Cybersicherheitsstrategie der EU von 2020 zu überarbeiten und ihre Ziele und ihr Konzept zu aktualisieren. So soll ein klarer Rahmen festgelegt werden, der die Aufgaben und Zuständigkeiten für alle Beteiligten definiert, einfache und wirksame Koordinierungsmechanismen schafft und die Zusammenarbeit mit dem Privatsektor und dem akademischen Bereich verstärkt. Der Rat ersucht daher die Kommission und den Hohen Vertreter der EU für Aussen- und Sicherheitspolitik, die Ergebnisse und Mängel der derzeitigen Strategie sowie ihre Auswirkungen zu bewerten und auf dieser Grundlage eine überarbeitete Strategie vorzulegen.

Die Umsetzung der Cybersicherheitsstrategie wird durch Ausschreibungen in den Programmen Horizon Europe und Digital Europe (DEP) gefördert.

## Stand der Dinge

Die am 16. Dezember 2020 veröffentlichte «Cybersicherheitsstrategie der EU für die digitale Dekade» ist kein Rechtsetzungsdokument, sondern vielmehr ein strategischer Rahmen. Als solcher tritt sie nicht zu einem bestimmten Zeitpunkt in Kraft, wie z. B. eine Richtlinie oder eine Verordnung. Sie dient jedoch als Richtschnur für die Massnahmen und Initiativen der EU im Bereich der Cybersicherheit für das kommende Jahrzehnt. Die Strategie dürfte in der nächsten Legislaturperiode überarbeitet werden.

## Mögliche Auswirkungen auf die Schweiz

Die Strategie ist nicht auf die Schweiz ausgerichtet, könnte aber indirekte Auswirkungen auf sie haben:

- **Harmonisierung von Standards und Vorschriften**: Die Schweiz muss möglicherweise ihre eigenen Normen und Regelungen in Bezug auf die Cybersicherheit an die von der EU geförderten Standards und Vorschriften angleichen, um die Zusammenarbeit und den Handel mit den EU-Mitgliedstaaten zu erleichtern. Dies könnte die Übernahme neuer Sicherheitstechnologien, verbesserter Verfahren und ähnlicher Compliance-Rahmen wie in der EU beinhalten.
- **Verstärkung der Zusammenarbeit**: Die Strategie fördert eine engere internationale Zusammenarbeit im Bereich der Cybersicherheit. Als wichtiger Partner der EU-Mitgliedstaaten könnte die Schweiz ihre Zusammenarbeit mit den EU-Institutionen für Cybersicherheit intensivieren, sich an gemeinsamen Übungen zur Reaktion auf Vorfälle beteiligen und Informationen über Bedrohungen und Schwachstellen austauschen.

- **Auswirkung auf Schweizer Unternehmen**: Schweizer Unternehmen – vor allem international tätige oder solche mit Partnerschaften mit EU-Institutionen – könnten von den neuen Cybersicherheitsstandards der EU betroffen sein. Sie müssen möglicherweise ihre Sicherheitsmassnahmen verbessern, um wettbewerbsfähig zu bleiben und den Erwartungen ihrer europäischen Partner gerecht zu werden.
- **Teilnahme an europäischen Initiativen**: Die Schweiz könnte sich an bestimmten europäischen Cybersicherheitsinitiativen wie Forschungs- und Entwicklungsprogrammen für Cybersicherheit, Kooperationsnetzwerken zur Bekämpfung von Cyberkrisen und anderen Projekten zur Stärkung der Cyberresilienz beteiligen. Dies könnte unter anderem über das Forschungsprogramm Horizon Europe erfolgen, für das die Schweiz derzeit mit der EU ein Assoziierungsabkommen aushandelt.

## Bereits ergriffene Massnahmen in der Schweiz

Die Schweiz hat keine besonderen Massnahmen ergriffen, um ihre Cybersicherheitsstrategie an jene der EU anzupassen. Allerdings zielen die Revision des Informationssicherheitsgesetzes (ISG) und die Nationale Cyberstrategie (NSC) grösstenteils in die gleiche Richtung.

Massnahme 16

# Cyberresilience Act

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung über horizontale Cybersicherheitsanforderungen an Produkte mit digitalen Elementen |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung (EU) 2024/2847 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 10.12.2024 |
| **Federführung in der Bundesverwaltung** | BACS/BAKOM |

## Beschrieb

Am 15. September 2022 legte die Europäische Kommission (KOM) einen Vorschlag für eine Verordnung über horizontale Cybersicherheitsanforderungen an Produkte mit digitalen Elementen (Cyber Resilience Act, CRA) vor. Der Rechtsakt baut auf der EU Cybersecurity Strategy 2020 und der EU Security Union Strategy 2020 auf und ergänzt die NIS-2 Richtlinie. Das Europäische Parlament und der Rat der EU erzielten im November 2023 eine vorläufige Einigung über den Verordnungstext.

Der CRA ist die erste gemeinsame europäische Gesetzgebung, die die Cybersicherheit von allen Produkten, die direkt oder indirekt über eine logische oder physische Datenverbindung mit einem anderen Gerät oder einem Netz verbunden sind, gewährleisten soll. Einige Ausnahmen gibt es für Produkte, für die in den geltenden EU-Vorschriften bereits Cybersicherheitsanforderungen festgelegt sind, z. B. Medizinprodukte, luftfahrttechnische Erzeugnisse oder Kraftfahrzeuge.

Die Verordnung unterscheidet zwischen kritischen und nicht-kritischen Produkten. 90% der Produkte werden auf dem Markt als nicht-kritisch eingestuft. Dies betrifft vor allem Produkte des Privatkonsums, deren Cybersicherheit einer Selbstbewertung der Hersteller unterliegen soll. Die **kritischen Produkte** betreffen zentrale staatliche Infrastrukturen und unter anderem VPNs, Firewalls oder Betriebssysteme. Sie werden in Klasse I und II gegliedert. Kritische Produkte der Klasse II müssen einer unabhängigen Konformitätsbewertung durch Dritte unterzogen werden. Für kritische Produkte der Klasse I braucht es eine unabhängige Bewertung durch Dritte, sofern nicht harmonisierte Normen angewendet werden. Mit dem Rechtsakt soll «Cybersecurity-by-Design» gewährleistet werden, d. h. Produkte müssen von Anfang an so konzipiert sein, dass sie cybersicher sind.

Darüber hinaus werden die neuen Vorschriften die **Verantwortung auf die Hersteller verlagern**, die die Konformität von Produkten mit digitalen Elementen, die auf dem EU-Markt bereitgestellt werden, mit den Sicherheitsanforderungen für die voraussichtliche Produktlebensdauer oder für einen Zeitraum von fünf Jahren gewährleisten müssen, ausser bei Produkten, die voraussichtlich für einen kürzeren Zeitraum genutzt werden.

Ausserdem müssen die Hersteller dem nationalen Computer Security Incident Response Team (CSIRT, verankert in NIS-2) sowie der EU-Agentur für Cybersicherheit (ENISA) **innerhalb von 24 Stunden melden**, wenn sie Kenntnis von einer aktiv ausgenutzten Schwachstelle in einem Produkt oder einem Vorfall mit schwerwiegenden Sicherheitsauswirkungen erhalten. Unter bestimmten Voraussetzungen kann das CSIRT beschliessen, die an die ENISA übermittelten Informationen aus Gründen der Cybersicherheit zu beschränken.

## Stand der Dinge

Am 12. März 2024 verabschiedete das Europäische Parlament die im November 2023 mit dem Rat der EU erzielte politische Einigung zum Cyber Resilience Act. Am 17. März 2024 veröffentlichte die Kommission einen Entwurf eines Normungsauftrags an das CENELEC, um die für den CRA erforderlichen harmonisierten Normen zu entwickeln. Am 10. Oktober 2024 wurde der Verordnungstext vom Rat der EU verabschiedet. Der endgültige Text wurde am 20. November 2024 im Amtsblatt der EU veröffentlicht und trat am 10. Dezember 2024 in Kraft. Daher wird die Umsetzung des CRA in verschiedenen Etappen von Ende 2024 bis 2027 erfolgen.

- 11. April 2026: Die Konformitätsbewertungsstellen (KBS) sind ermächtigt, die Konformität von Produkten mit den Anforderungen des CRA zu bewerten.
- 11. September 2026: Die Hersteller von vernetzten Produkten unterliegen der Meldepflicht für Schwachstellen und Vorfälle.
- 11 Dezember 2027: Alle CRA-Anforderungen gelten, einschliesslich der Einhaltung der grundlegenden Cybersicherheitsanforderungen vor dem Inverkehrbringen eines Produkts, der Behandlung von Schwachstellen während des gesamten Lebenszyklus des Produkts und der Transparenz gegenüber den Nutzern.

## Mögliche Auswirkungen auf die Schweiz

Der CRA wirkt sich in verschiedener Weise auf die Schweiz aus:

- **Harmonisierung der Standards**: Die Schweiz, respektive Unternehmen im Austausch mit der EU, könnten auf Handelshemmnisse stossen. Die Schweiz könnte daher beschliessen, ähnliche Sicherheitsstandards einzuführen, um die Kompatibilität mit der EU zu gewährleisten und Handelshemmnisse abzubauen. Dies würde zu einer Angleichung der Cybersicherheitsstandards zwischen der Schweiz und der EU führen.
- **Indirekte Auswirkungen**: Selbst ohne direkte Übernahme der neuen EU-Regelungen durch die Schweiz könnten Unternehmen und Behörden von strengeren Sicherheitsanforderungen profitieren, da das gesamte Cybersicherheitsniveau in Europa steigen würde. Dies speziell mit Blick auf EU-konforme Produkte von ausländischen Unternehmen, die in der Schweiz angeboten werden.
- **Abseitsstehen beim operativen Informationsaustausch auf EU-Ebene**: Die Schweiz ist nicht Teil des Netzwerkes der CSIRTs. Daraus können sich Nachteile für die Schweiz ergeben, wenn das Netzwerk zu einem koordinierten Vorgehen beiträgt oder koordinierte gemeinsame Aktionen durchgeführt werden (wie im EU Product Compliance Network [EUPCN]).
- **Auswirkungen auf die Wirtschaft**: Schweizer Unternehmen, die in die EU exportieren, müssen die oben genannten Pflichten (Bewertungs- und Dokumentationspflicht der Cyberrisiken, Meldepflicht für aktiv ausgenutzte Schwachstellen sowie Überwachungs- und Beseitigungspflicht von Schwachstellen und Sicherheitsupdates während der erwarteten Produktlebensdauer) erfüllen. Die Hersteller müssen nachweisen, dass die Cybersicherheitsanforderungen eingehalten wurden. Je nach Risikoeinstufung des betreffenden Produkts erfolgt dies durch eine Herstellererklärung oder eine Konformitätsbewertung durch Konformitätsbewertungsstellen in der EU nach EU-Recht (wichtige und kritische Produkte mit digitalen Elementen). Die EU-Importeure von Schweizer Produkten mit digitalen Elementen müssen ausserdem ihren Namen, Adresse, digitale Kontaktmöglichkeiten sowie gegebenenfalls ihre Website entweder auf dem Produkt, der Verpackung oder in den beigefügten Unterlagen angeben.

Die Schweiz hat heute mit der EU ein Abkommen über die gegenseitige Anerkennung von Konformitätsbewertungen (MRA) für Produkte in 20 Sektoren. Der CRA wird sich auf Sektoren, die von diesem Abkommen abgedeckt werden (insb. Maschinen), auswirken, da die Anforderungen gemäss CRA zu den bestehenden Anforderungen für den Marktzugang hinzukommen werden. Die Frage, ob das MRA-Abkommen erweitert werden könnte, um auch die Cybersicherheits-Anforderungen einzuschliessen und damit mögliche Handelshemmnisse abzubauen, muss geprüft werden. Es ist weiterhin unklar, ab wann die EU im Kontext der Beziehungen zwischen der Schweiz und der EU wieder zu einer Aktualisierung des MRA bereit sein wird.

## Bereits ergriffene Massnahmen in der Schweiz

Die Schweiz hat die folgenden Massnahmen aus Eigeninitiative bereits eingeleitet:

- Die Nationale Cyberstrategie (NSC)
- Schaffung und Verstärkung des BACS: So beispielsweise durch den Aufbau eines Strategischen Schwachstellenmanagements und der Etablierung von RVD-Prozessen zur verantwortungsvollen Offenlegung von Schwachstellen in diesem Zusammenhang.
- Intensivierung der internationalen Zusammenarbeit im Bereich der Cybersicherheit. Dies durch bilaterales und regionales Zusammenarbeiten im Bereich der Standardisierung und Technologieentwicklung.
- Die Schweiz hat die Delegierte Verordnung (EU) 2022/30 der KOM zur Ergänzung der Richtlinie 2014/53/EU zur Einführung von Cybersicherheitsanforderungen für bestimmte Typen von Funkanlagen übernommen. Dieser delegierte Rechtsakt wurde in die Verordnung über Fernmeldeanlagen (FAV) und die Verordnung des BAKOM über Fernmeldeanlagen (VFAV) überführt. Diese Anforderungen gelten ab dem 1. August 2025. Sie werden in einem Paket von drei harmonisierten Normen konkretisiert, die beim Europäischen Komitee für elektrotechnische

Normung (CENELEC) erarbeitet werden (FprEN 18031–1, FprEN 18031–2 und FprEN 18031–3). In der Schweiz ist das BAKOM für den Vollzug zuständig.

- Beispiel einer Eigeninitiative: Umsetzungsgesetzgebung zu Art. 48a FMG. Gemäss Art. 96a Abs. 3 FDV müssen Internetanbieterinnen die von ihnen gelieferten Modems unterhalten und updaten.

Massnahme 17

# NIS-2-Richtlinie

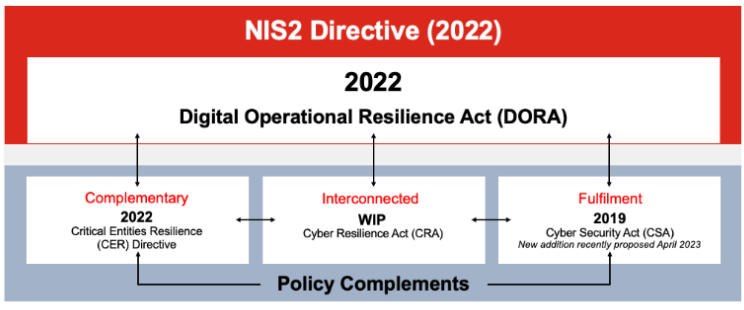
| | |
|---|---|
| **Vollständiger Name der Massnahme** | Richtlinie über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union |
| **Art der Massnahme** | Richtlinie |
| **Referenz (falls vorhanden)** | Richtlinie (EU 2022/2555) |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 16.01.2023 |
| **Federführung in der Bundesverwaltung** | BACS/BAKOM |

## Beschrieb

Mit der Überarbeitung der Richtlinie (EU 2022/2555) über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) wird das Ziel verfolgt, die Kapazitäten zur Reaktion des öffentlichen und privaten Sektors auf Sicherheitsvorfälle weiter zu verbessern. Mit der NIS-2-Richtlinie wird zunächst der Anwendungsbereich der Vorschriften ausgeweitet. Während bisher die EU-Mitgliedstaaten festlegten, welche Einrichtungen die Kriterien für die Einstufung als Betreiber wesentlicher Dienste erfüllen, wird mit der NIS-2-Richtlinie eine neue Regel eingeführt: So fallen alle mittleren und grossen Einrichtungen (gemäss einem Schwellenwert) in den Anwendungsbereich, die in den erfassten Sektoren tätig sind oder entsprechende Dienste erbringen. Die NIS-2-Richtlinie wird auch mittlere und grosse Einrichtungen aus einer grösseren Anzahl von Sektoren erfassen, die für die Wirtschaft und Gesellschaft von entscheidender Bedeutung sind, darunter Anbieter elektronischer Kommunikationsdienste und digitaler Dienste, die Abwasserwirtschaft sowie Postdienste auf zentraler und regionaler Ebene. Akteure in Bereichen wie Verteidigung, nationale und öffentliche Sicherheit, die Justiz, Banken oder Parlamente werden nicht zur Einhaltung der Vorschriften der Richtlinie verpflichtet. Die NIS-2-Richtlinie wird auch für öffentliche Verwaltungen auf zentraler und regionaler Ebene gelten. Darüber hinaus können die EU-Mitgliedstaaten beschliessen, dass sie auch für derartige Einrichtungen auf lokaler Ebene gilt.

Die in den Anwendungsbereich der Richtlinie fallenden Einrichtungen müssen **Cybervorfälle innerhalb von 24 Stunden melden** und in spätestens drei Tagen einen detaillierten Bericht vorlegen, der eine erste Bewertung des Sicherheitsvorfalls, seiner Schwere und seiner Auswirkungen sowie etwaige Kompromittierungsindikatoren (*indicators of compromise*, IoC) umfasst. Daneben führt die Richtlinie ein neues System von Rechtsbehelfen und Sanktionen ein.

Bei Verstössen gegen die Rechtsvorschriften drohen den betroffenen Einrichtungen Geldbussen von bis zu zwei Prozent ihres Umsatzes. Mit der Richtlinie wird zudem die Europäische Netzwerke CSIRT und EU-CyCLONe als Verbindungsorganisationen für Cyberkrisen offiziell eingerichtet, das die Zusammenarbeit und die koordinierte Bewältigung massiver Vorfälle unterstützen wird. Durch Ausschreibungen im Digital Europe Programme (Teilbereich Cybersicherheit) wird die Zusammenarbeit in den Netzwerken gefördert. Weiter wird ein freiwilliger Peer-Learning-Mechanismus eingeführt, der das gegenseitige Vertrauen stärken und das Lernen aus bewährten Verfahren und Erfahrungen verbessern soll. Die Richtlinie dient iber die Bereitstellung externer technischer Hilfe auch als Referenzmodell für die Zusammenarbeit der EU mit Drittländern und stärkt die Rolle der Kooperationsgruppe (Vertreter/-innen der EU-MS, die Kommission und ENISA) bei strategischen politischen Entscheidungen. Die Abhängigkeiten der verschiedenen EU-Richtlinien und Gesetzgebungen zur NIS 2 stellt sich dabei folgendermassen dar:




NIS2 Directive relation with other related regulations

## Stand der Dinge

Die Richtlinie ist am 16. Januar 2023 in Kraft getreten. Die EU-Mitgliedstaaten müssen die Vorschriften der Richtlinie innerhalb von 21 Monaten nach ihrem Inkrafttreten in nationales Recht umsetzen. Dies bedeutet, dass sie ihre Gesetze und internen Vorschriften an die neuen Anforderungen der Richtlinie anpassen müssen.

Nachfolgend die wichtigsten Punkte, die umgesetzt werden müssen:

- **Festlegung der Schwellenwerte:** Die EU-Mitgliedstaaten werden spezifische Schwellenwerte festlegen müssen, um zu bestimmen, welche mittleren und grossen Einrichtungen den Pflichten der NIS-2-Richtlinie unterliegen.
- **Einrichtung von Meldeverfahren:** Die unter die Richtlinie fallenden Einrichtungen müssen Mechanismen schaffen, mit denen sie Cybersicherheitsvorfälle innerhalb von 24 Stunden melden und innerhalb von drei Tagen nach einem Vorfall im Detail Bericht erstatten können.
- **Sanktions- und Beschwerdesystem:** Die EU-Mitgliedstaaten müssen Sanktionsregelungen einführen, die bei Nichteinhalten der Anforderungen greifen, sowie Rechtsbehelfsmechanismen einrichten, über die die betroffenen Unternehmen diese Sanktionen anfechten können.
- **Kapazitätsaufbau:** Der öffentliche sowie der private Sektor müssen ihre Cybersicherheitskapazitäten ausbauen, um den neuen, höheren Anforderungen der Richtlinie gerecht zu werden. Dies kann die Schulung des Personals, die Verbesserung der Sicherheitsinfrastruktur und die Einführung neuer Cybersicherheitstechnologien umfassen.
- **Aufbau von Kooperationsstrukturen:** Die Richtlinie sieht die Schaffung der europäischen Netze der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe, CSIRT) vor. Die EU-Mitgliedstaaten müssen sich daher an der Einrichtung und dem Betrieb der Netze beteiligen, um eine wirksame Zusammenarbeit bei schwerwiegenden Vorfällen zu gewährleisten.
- **Berichte und Bewertungen:** Die EU-Mitgliedstaaten müssen der Kommission regelmässig über die Umsetzung der Richtlinie und den Stand der Cybersicherheit Bericht erstatten. So sollen durch regelmässige Bewertungen diejenigen Bereiche ermittelt werden, in denen Verbesserungen oder Anpassungen erforderlich sind.
- **Technische Unterstützung und internationale Zusammenarbeit:** Die Richtlinie sieht zudem ein Referenzmodell für die Zusammenarbeit mit Drittländern vor. Die EU-Mitgliedstaaten müssen daher darauf hinarbeiten, solche internationalen Cybersicherheitspartnerschaften aufzubauen und zu stärken.

## Mögliche Auswirkungen auf die Schweiz

Die NIS-2-Richtlinie könnte verschiedene indirekte Auswirkungen auf die Schweiz haben, insbesondere aufgrund der starken Vernetzung der schweizerischen und europäischen Infrastrukturen und Unternehmen. Schweizer Unternehmen, die in kritischen Sektoren tätig sind und mit der EU interagieren oder Dienstleistungen für Kundinnen und Kunden mit Sitz in der EU erbringen, könnten gezwungen sein, die Anforderungen der NIS 2-Richtlinie zu erfüllen, um ihre Geschäftsbeziehungen aufrechtzuerhalten. So müssten sie etwa angemessene Cybersicherheitsmassnahmen implementieren und über einen Mechanismus zur Meldung von Sicherheitsvorfällen verfügen.

## Bereits ergriffene Massnahmen in der Schweiz

Das Informationssicherheitsgesetzes (ISG) sieht unter anderem eine Meldepflicht für Cybervorfälle bei kritischen Infrastrukturen vor. Diese Meldepflicht stellt eine gewisse Kompatibilität mir der nach NIS 1 eingeführten Meldepflicht in der EU sicher.

Massnahme 18

# CER-Richtlinie

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Richtlinie über die Resilienz kritischer Einrichtungen (CER) |
| **Art der Massnahme** | Richtlinie |
| **Referenz (falls vorhanden)** | Richtlinie (EU) 2022/2557 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 16.01.2023 |
| **Federführung in der Bundesverwaltung** | BACS/BAKOM/EDA-Digi |

## Beschrieb

Die Richtlinie über die Resilienz kritischer Einrichtungen (Critical Entities Resilience, CER) ist am 16. Januar 2023 in Kraft getreten. Sie ersetzt und erweitert im Kern den Anwendungsbereich der Richtlinie von 2008 über europäische kritische Infrastrukturen, die nur für den Energie- und Transportsektor gegolten hatte. Die neue Richtline deckt elf Sektoren ab: **Energie, Verkehr, Banken, Finanzmarktinfrastruktur, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, öffentliche Verwaltung, Weltraum und Produktion, Verarbeitung und Vertrieb von Lebensmitteln.** Die Richtlinie schafft einen Rahmen, der die EU-Mitgliedstaaten dabei unterstützen soll, die Anfälligkeit kritischer Einrichtungen zu verringern und deren physische Resilienz zu stärken. Die Mitgliedstaaten werden verpflichtet, eine nationale Strategie zur Stärkung der Resilienz kritischer Einrichtungen auszuarbeiten, mindestens alle vier Jahre eine Risikobewertung durchzuführen und eine **Liste der kritischen Einrichtungen** zu erstellen, die grundlegende Dienste erbringen. Diese Einrichtungen müssen die Risiken ermitteln, die die Erbringung grundlegender Dienste erheblich beeinträchtigen könnten, Massnahmen ergreifen, um ihre Resilienz zu gewährleisten, und den zuständigen Behörden Störfälle melden. Ausschreibungen im Horizon Europe Programm (Cluster 3, Resilient Infrastructures) fördern die Zusammenarbeit zur Umsetzung der CER Richtlinie. Die Richtlinie enthält zudem besondere Vorschriften für kritischer Einrichtungen von «besonderer europäischer Bedeutung», die einen wesentlichen Dienst für sechs oder mehr Mitgliedstaaten erbringen.

## Stand der Dinge

Im Rahmen eines delegierten Rechtsakt nahm die Kommission am 25. Juli 2023 für die elf in der CER-Richtlinie aufgeführten Sektoren eine Liste der wesentlichen Dienste an. Die Mitgliedstaaten müssen bis zum 17. Juli 2026 die kritischen Einrichtungen in den Sektoren ermitteln, die in der CER-Richtlinie festgelegt wurden. Um Risikobewertungen vorzunehmen und anschliessend die kritischen Einrichtungen zu ermitteln, greifen die Mitgliedstaaten auf die Liste wesentlicher Dienste zurück.

## Mögliche Auswirkungen auf die Schweiz

Die Richtlinie hat keine direkten Auswirkungen auf die Schweiz. Für Zulieferer kritischer Infrastrukturen kann es wichtig sein, zu wissen, welche Sektoren in der EU als kritisch gelten.

## Bereits ergriffene Massnahmen in der Schweiz

Die Schweiz hat in der «Nationalen Strategie zum Schutz kritischer Infrastrukturen» seine kritischen Sektoren und Teilsektoren bereits identifiziert.

Massnahme 19

# Cyber Solidarity Act

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung über die Massnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -Vorfällen |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung (EU) 2025/38 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 04.02.2025 |
| **Federführung in der Bundesverwaltung** | BACS/EDA-Digi |

## Beschrieb

Die Verordnung über Massnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen (Cyber Solidarity Act, CSA) ist am 4. Februar 2025 in Kraft getreten. Der CSA zielt darauf ab, die gemeinsamen Kapazitäten der EU zur Aufdeckung, Vorbereitung und Reaktion auf erhebliche Cybersicherheitsbedrohungen und -angriffe zu stärken.

Die wichtigsten Punkte des CSA sind folgende:

- Die Verordnung sieht die Einrichtung eines **europäischen Warnsystems für Cybersicherheit** vor, dass sich aus nationalen und grenzüberschreitenden *cyber hubs* zusammensetzt. Neben dem Informationsaustausch sind die *cyber hubs* für die Erkennung und Analyse von Cyberbedrohungen zuständig. Die Teilnahme an diesem Warnsystem ist für die Mitgliedstaaten freiwillig.
- Ein **Cybernotfallmechanismus** wird geschaffen, der die EU-Mitgliedstaaten finanziell und organisatorisch unterstützt, potenzielle Schwachstellen kritischer Einrichtungen (z. B. im Gesundheits-, Verkehrs- und Energiesektor) zu testen und die gegenseitige Unterstützung der nationalen Behörden zu fördern.
- Eine **EU-Cybersicherheitsreserve** wird eingerichtet, die aus Sicherheitsvorfall-Notdiensten des Privatsektors besteht und im Fall eines erheblichen Cybersicherheitsvorfalls auf Antrag eines EU-Mitgliedstaats oder von sonstigen Stellen der EU eingreifen kann. Zudem können auch mit DEP-assoziierte Drittländer Unterstützung aus der EU-Cybersicherheitsreserve beantragen, sofern ihre Teilnahme an der Reserve in dem Abkommen über ihre Assoziierung vorgesehen ist.
- Ein Mechanismus zur **Untersuchung von schwerwiegenden Cybersicherheitsvorfällen** durch die Agentur der EU für Cybersicherheit (ENISA) wird eingeführt.

## Stand der Dinge

Die Verordnung wurde am 15. Januar 2025 im EU-Amtsblatt veröffentlicht und am 4. Februar 2025 in Kraft getreten.

## Mögliche Auswirkungen auf die Schweiz

Die Schweiz ist nur indirekt betroffen von den Massnahmen der EU. Die Schweiz betreibt einen engen Informationsaustausch mit verschiedenen nationalen Behörden von EU-Mitgliedstaaten. Dieser Austausch ist für die Früherkennung wichtig. Es ist nicht davon auszugehen, dass der CSA diesen Austausch erschwert und es wird davon ausgegangen, dass die Schweiz weiterhin die nötigen Informationen über direkte Fachkontakte erhalten wird.

Einen Zugriff auf die EU-Cybersicherheitsreserve ist für die Schweiz keine dringend nötige Massnahme. In der Schweiz besteht bereits eine sehr enge Zusammenarbeit zwischen den Behörden und der Privatwirtschaft.

## Bereits ergriffene Massnahmen in der Schweiz

Innerhalb des Bundesamts für Cybersicherheit wird eine Untersuchungsstelle zu Cybersicherheitsvorfällen aufgebaut. Beide Initiativen entstanden aus Eigeninitiative. Der Austausch mit EU-Mitgliedstaaten ist gewährleistet.

Massnahme 20

# Ökodesign-Verordnung

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung zur Schaffung eines Rahmens für die Festlegung von Ökodesign-Anforderungen für nachhaltige Produkte |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Regulation (EU) 2024/1781 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 18.07.2024 |
| **Federführung in der Bundesverwaltung** | BAFU |

## Beschrieb

Ökodesign-Verordnung (Ecodesign Regulation, ESPR) schafft einen allgemeinen und harmonisierten Rahmen zur Festlegung von Anforderungen an das Produktdesign. Die Verordnung ersetzt die bestehende Ökodesign-Richtlinie 2009/125/EG und erweitert ihren Anwendungsbereich: Über Energieerzeugnisse hinaus gilt der neue Rechtsakt nun für alle Arten von Waren, die in der EU in Verkehr gebracht werden.

Die Verordnung betrifft fast alle Arten von Produkten mit gewissen Ausnahmen, wie Arzneimittel, Fahrzeuge, Lebens- und Futtermittel sowie Produkte aus dem Bereich Sicherheit und Verteidigung. Mit der neuen Verordnung wird ein Rechtsrahmen für die Einführung neuer Anforderungen geschaffen; sie betreffen die Haltbarkeit, Wiederverwendbarkeit, Nachrüstbarkeit und Reparierbarkeit von Produkten, das Vorhandensein von Stoffen, die der Kreislauffähigkeit entgegenstehen; Energie- und Ressourceneffizienz; Rezyklat Anteil, Wiederaufarbeitung und Recycling; Treibhausgas-Fussabdruck und Umweltfussabdruck sowie Informationsanforderungen, zu denen auch ein digitaler Produktpass (DPP) gehört. Die Europäische Kommission (KOM) wird befugt, delegierte Rechtsakte mit Ökodesign-Anforderungen zu erlassen, denen die Industrie in der Regel innerhalb von 18 Monaten nachkommen muss. Schliesslich werden Online-Marktplätze zur Zusammenarbeit mit Marktüberwachungsbehörden verpflichtet.

Beim DPP handelt es sich um einen produktespezifischen Datensatz, der die in den anwendbaren delegierten Rechtsakten genannten Informationen enthält und der über einen elektronischen Datenträger (z.B. QR-Code) zugänglich ist. Mit dem DPP wird die EU nicht nur die Ökodesign-Informationen, sondern auch Konformitätsnachweise, technische Unterlagen zum Produkt und weitere produktbezogene Informationen (wie z.B. Benutzerhandbücher, Gebrauchsanweisungen oder sicherheitsrelevante Informationen) digital zugänglich machen. Diese Informationen sollen entlang der industriellen Wertschöpfungskette dezentral erfasst und gespeichert und für Konsumenten, Wirtschaftsteilnehmer und Behörden unterschiedlich zugänglich gemacht werden. Bei Produkten aus Drittstaaten obliegt es den Importeuren dafür Sorge zu tragen, dass die von ihnen in Verkehr gebrachten Produkte den Ökodesign-Anforderungen entsprechen und dass ein DPP vorliegt. Zum DPP wird es in der EU ein zentrales DPP-Register - d.h. ein Verzeichnis sämtlicher eindeutigen Produktkennungen (UID) von den in der EU in Verkehr gebrachten oder in Betrieb genommenen Produkten geben, zu dem die Marktüberwachungsbehörden der EU-Mitgliedstaaten Zugang haben. Die Kommission wird ein öffentlich zugängliches Webportal erstellen, das es den Konsumenten ermöglicht, einen Teil der im DPP enthaltenen Daten zu suchen und zu vergleichen.

Bei der Vergabe öffentlicher Aufträge gelten künftig Ökodesign-Kriterien, um Anreize für die öffentliche Beschaffung umweltfreundlicher Produkte zu geben. Mit der neuen Verordnung wird ein direktes Verbot eingeführt, unverkaufte Textilien und Schuhe zu vernichten (KMU sind vorübergehend davon ausgenommen). Andere Produkte könnten folgen, wenn die Kommission ihre Befugnis nutzt, ähnliche Verbote zu erlassen. In Bezug auf online verkaufte Produkte wird die Ökodesign-Verordnung an das Gesetz über digitale Dienste angeglichen.

Zu beachten ist, dass ein inhaltlicher Bezug zwischen der Ökodesign-Verordnung und weiteren Legislativprojekten der EU besteht. Dies betrifft insbesondere die EU-Richtlinien 1) zur Förderung der Reparatur von Waren (Recht auf Reparatur) 2) zur Stärkung der Rolle der Konsumenten 3) über die Haftung für fehlerhafte

Produkte 4) über Verbraucherrechte, 5) über Umweltaussagen (Green Claims) sowie 6) über unlautere Geschäftspraktiken.

## Stand der Dinge

Die Verordnung trat am 18. Juli 2024 in Kraft. Nach einer Übergangsfrist von 24 Monaten ist die Vernichtung von unverkauften Textilien und Schuhen verboten. Mit der Ökodesign-Verordnung wird die Kommission befugt, delegierte Rechtsakte mit Ökodesign-Anforderungen zu erlassen. Unter der ESPR könnten die ersten delegierten Rechtsakte Ende 2025 mit einer Übergangsfrist von 18 Monaten verabschiedet werden. Der erste DPP wird in der EU mit der Batterieverordnung (EU) 2023/1542 für Elektrofahrzeugbatterien, Batterien für leichte Verkehrsmittel und grosse Industriebatterien (> 2 kWh) per 2027 eingeführt. Die Bauprodukteverordnung (kurz vor der formellen Verabschiedung) und der Vorschlag für die Spielzeugverordnung sehen voraussichtlich per 2028 einen DPP vor.

## Mögliche Auswirkungen auf die Schweiz

Die konkreten Auswirkungen hängen insbesondere von den delegierten Rechtsakten zu einzelnen Produkten ab die in den nächsten Jahren in Kraft treten.

Eine Regulierungsfolgenabschätzung von 2022 hat gezeigt, dass eine Übernahme der untersuchten Ökodesign-Anforderungen durch die Schweiz ein positives Kosten-Nutzen-Verhältnis erzielen würde. Bisher wurden die meisten Anforderungen, die im Rahmen der aktuell noch in Kraft stehenden EU-Ökodesign-Richtlinie erlassen wurden und die vor allem energierelevante Aspekte betrafen, in die Schweizer Energieeffizienzverordnung (EnEV) übernommen. Diese Angleichung an die in der EU verwendeten Regeln, Kategorien und Begriffe entspricht dem Bundesgesetz über technische Handelshemmnisse (THG). Für die betroffenen Schweizer Hersteller, Importeure und Händler erleichtert sich dadurch der Warenverkehr mit der EU.

Aufgrund der neuen Anforderungen in der ESPR, müssten Schweizer Hersteller, die ihre Produkte in der EU in Verkehr bringen, diese Produkte teilweise durch Konformitätsbewertungsstellen in der EU nach EU-Recht prüfen lassen. Zudem müssten Exporteure in manchen Produktbereichen (z.B. Bauprodukte) einen Bevollmächtigten mit Sitz in der EU benennen. Hersteller und Importeure müssten ihre Adresse sowohl auf dem Produkt selbst als auch im DPP angeben. Umgekehrt ist davon auszugehen, dass Produkte, welche in der EU mit einem DPP versehen sind, aufgrund der engen wirtschaftlichen Bindungen auch auf dem Schweizer Markt auftauchen. Für diese Fälle müsste die Schweiz sicherstellen, dass sie auch in Zukunft Zugang zu den Informationen für Konsumentinnen und Konsumenten, aber auch für Vollzugsbehörden und Zollorgane hat.

Schweizer Hersteller, die Produkte auf dem EU-Markt bereitstellen, können voraussichtlich selbst den DPP erstellen, Informationen eingeben und speichern sowie im DPP-Register registrieren und Sicherheitskopie bei einem DPP-Dienstleister speichern. Für Wirtschafsakteure, die Produkte sowohl auf dem EU als auch auf dem Schweizer Markt bereitstellen, wäre es wahrscheinlich administrativ weniger aufwändig, wenn die Schweiz sich am DPP-System der EU beteiligen oder ein identisches interoperables DPP-System einführen und dessen Gleichwertigkeit mit der EU vertraglich verankern könnte. Da über den DPP in der EU künftig auch Konformitätsnachweise und technischen Unterlagen digital bereitgestellt werden, würde die Marktüberwachung erleichtert, insbesondere wenn der Zugang zu geschützten Informationen mit der EU vertraglich vereinbart werden könnte.

Die Schweiz hat heute mit der EU ein Abkommen über die gegenseitige Anerkennung von Konformitätsbewertungen (MRA) für Produkte in 20 Sektoren. Es zeichnet sich ab, dass die EU auch für Produktebereiche wie Bauprodukte und Spielzeuge, die unter das MRA fallen, Ökodesignanforderungen inklusiv DPP einführen wird. In diesen Produktesektoren sind die technischen Vorschriften der Schweiz und der EU unter dem MRA als gleichwertig anerkannt. Die Frage, ob das MRA-Abkommen erweitert werden könnte, um auch die Ökodesign-Anforderung einzuschliessen und damit mögliche Handelshemmnisse abzubauen, muss geprüft werden. Es ist weiterhin unklar, ab wann die EU im Kontext der Beziehungen zwischen der Schweiz un der EU wieder zu einer Aktualisierung des MRA bereit sein wird.

## Bereits ergriffene Massnahmen in der Schweiz

**Bisherige Praxis:** Seit mehreren Jahren übernimmt die Schweiz die meisten Anforderungen betreffend Energieeffizienz aus den Durchführungsverordnungen zur Ökodesign-*Richtlinie* in die Energieeffizienzverordnung (EnEV). Im 2020 wurden für sechs Produktegruppen (bspw. Waschmaschinen und Geschirrspüler) erstmals

Anforderungen zur Ressourceneffizienz, zum Beispiel betreffend die Verfügbarkeit von Ersatzteilen und von Reparaturanleitungen, in die Energieeffizienzverordnung übernommen.

**Neue gesetzliche Grundlage:** Am 15. März 2024 wurde die parlamentarische Initiative 20.433 Schweizer Kreislaufwirtschaft stärken vom Parlament angenommen. Nach Ablauf der Referendumsfrist am 4. Juli wird der Bundesrat über das Inkrafttreten entscheiden. Art. 35i USG wird dem Bundesrat die Kompetenz verleihen, Ökodesign-Anforderungen an Produkte zu stellen und somit gleiche Marktzutrittsbedingungen für Unternehmen in der Schweiz und in der EU zu schaffen. Es ist explizit erwähnt, dass Regelungen der wichtigsten Handelspartner berücksichtigt werden sollen.

**Digitale Produktpässe:** Art. 35i betrifft auch Anforderungen an die Kennzeichnung von Produkten und die Bereitstellung von Informationen. Soll die Einführung des DPP ermöglicht werden, wäre eine weitere Anpassung der rechtlichen Grundlagen zu prüfen. Aus Eigeninitiative haben die betroffenen Bundesämter mit der Prüfung der Handlungsoptionen begonnen.

**Öffentliche Beschaffung:** Die parlamentarische Initiative sieht mit Art. 30 Abs. 4 BöB vor, dass die nachhaltige öffentliche Beschaffung gestärkt werden soll.

**Verbot und Berichterstattung der Zerstörung von Textilien und Schuhen:** Aus wirtschaftlicher und ökologischer Sicht soll – wenn immer möglich – vermieden werden, dass unverkaufte Neuwaren zerstört werden. Dies sagt der Bundesrat auch in seiner Antwort vom 23.08.2023 auf den Vorstoss: 23.3649 | Unverkaufte Nicht-Lebensmittel sollen nicht mehr weggeworfen werden! | Geschäft | Das Schweizer Parlament. Bereits heute kann der Bundesrat auf Grundlage von Artikel 46 Absatz 2 des Umweltschutzgesetzes (USG, SR 814.01) Unternehmen auf Verordnungsstufe verpflichten, Daten zu Abfällen und deren Entsorgung zu erheben und dem Bund auf Verlangen zur Verfügung zu stellen. Der Bundesrat hat bisher diesbezüglich keinen unmittelbaren Handlungsbedarf gesehen. Ein Verbot, unverkaufte Neuware zu zerstören, besteht heute in der Schweiz nicht.

Massnahme 21

# Digital Education Action Plan

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Digital Education Action Plan |
| **Art der Massnahme** | Aktionsplan |
| **Referenz (falls vorhanden)** | Aktionsplan für digitale Bildung (2021–2027) |
| **Aktueller Stand** | In Anwendung |
| **Datum des Inkrafttretens** | 30.09.2022 |
| **Federführung in der Bundesverwaltung** | SBFI |

## Beschrieb

Der Aktionsplan für digitale Bildung (2021–2027) sieht vor, die allgemeine und berufliche Bildung an das digitale Zeitalter anzupassen sowie Lehren aus der Covid-19-Krise zu ziehen, vor allem betreffend die Nutzung digitaler Technologien in der Bildung. Im Aktionsplan sind zwei Hauptprioritäten verankert:

**Die Förderung eines leistungsfähigen digitalen Bildungsökosystems** (strategische Priorität 1) in den Bereichen Infrastruktur, Ausbildung von Lehrkräften, Lerninhalte und Tools sowie **der Ausbau digitaler Kompetenzen** (strategische Priorität 2), seien es digitale Grundkenntnisse schon im Kindesalter oder die Ausbildung von mehr IT-Fachpersonen mit Fokus auf die Förderung von Mädchen und Frauen. Um diese Prioritäten umzusetzen, will die Europäische Kommission (KOM) den Austausch unter den EU-Mitgliedstaaten verbessern, Leitlinien erarbeiten und Machbarkeitsstudien auf verschiedenen Gebieten durchführen, neue Tools entwickeln (wie z. B. das im Oktober 2021 lancierte Selbstbeurteilungstool SELFIE für Lehrkräfte) und Synergien mit Programmen wie Erasmus+, Horizon Europe oder Digitales Europa nutzen.

Die **europäische Plattform für digitale Bildung** (European Digital Education Hub) gehört zu den zentralen Massnahmen im Bereich der digitalen Bildung. Die virtuelle Kooperationsgemeinschaft verfolgt das Ziel, die Zusammenarbeit und die sektorübergreifenden Synergien für die digitale Bildung in Europa zu stärken. Die Plattform verbindet die Interessenträger des gesamten Ökosystems der digitalen Bildung (formal, nichtformal und informell) und fördert Initiativen, die sich mit wichtigen Fragestellungen in Bezug auf Politik und Praxis befassen. Ausserdem wird die Plattform das Monitoring der digitalen Bildung in Europa und die Umsetzung des Aktionsplans für digitale Bildung unterstützen. Sie bietet Fablabs für die Gemeinschaft, virtuellen Erfahrungsaustausch, Mentoring und einen Project-Accelerator.

## Stand der Dinge

Der Aktionsplan ist in Umsetzung, Dauer: 2021 bis 2027.

Durchgeführte Massnahmen, Beispiele:

- Empfehlung des Rates zu den Schlüsselfaktoren für eine erfolgreiche allgemeine und berufliche Bildung
- Empfehlung des Rates zu Blended-Learning-Ansätzen für eine hochwertige und inklusive Primar- und Sekundarbildung
- Ethische Leitlinien für Lehrkräfte über die Nutzung von KI und Daten für Lehr- und Lernzwecke

Nächste Schritte, Beispiele:

- Unterstützung der Pläne für den digitalen Wandel in Bildungs- und Berufsbildungseinrichtungen durch Kooperationsprojekte im Rahmen von Erasmus+ (laufend)
- Entwicklung eines europäischen Rahmens für digitale Bildungsinhalte
- Einrichtung einer europäischen Plattform für den Austausch von Bildungsdaten und Inhalten der Hochschulbildung

Da es sich bei den von der KOM angenommenen Massnahmen um einen Aktionsplan und nicht um eine rechtliche Regelung handelt, können sie weder in Kraft treten noch sind die Mitgliedstaaten zu ihrer Umsetzung verpflichtet.

Die wichtigsten Massnahmen der KOM sind Empfehlungen des Rates, Referenzrahmen und Leitlinien für die digitale Bildung. Diese Massnahmen werden während der Laufzeit des Aktionsplans sukzessive weiterentwickelt und verabschiedet.

## Mögliche Auswirkungen auf die Schweiz

Da in diesem Bereich kein bilaterales Abkommen abgeschlossen wurde, haben die Vorschläge der KOM für die Schweiz keine verbindliche Wirkung. Die Schweiz und die EU haben jedoch ähnliche Prioritäten. Deshalb ist es für die Schweiz wichtig, die Arbeiten der EU bei der Digitalisierung der Bildung aufmerksam zu beobachten. Bis Ende 2021 nahm die Schweiz regelmässig an den Expertentreffen der ET-2020-Arbeitsgruppe «Digitale Bildung: Lernen, Lehren und Bewerten (WG DELTA)» der KOM teil. Die Gruppe wird auch bei der Umsetzung des Aktionsplans für digitale Bildung regelmässig konsultiert. Seit 2022 hat die EU die Schweiz allerdings aus politischen Gründen aus dieser Gruppe ausgeschlossen. Obwohl in der Schweiz in erster Linie die Kantone für das Bildungswesen zuständig sind, könnte sie vom Austausch bewährter Verfahren in der digitalen Bildung in der EU profitieren und sich von in der EU entwickelten Tools (z. B. SELFIE) und gemeinsamen Rahmen (z. B. DigCompEdu) inspirieren lassen.
Weiter ist zu erwähnen, dass die Anmeldung auf der europäischen Plattform für digitale Bildung und der Zugang zur virtuellen Gemeinschaft für alle kostenlos möglich ist. Die Schweizer Bildungsakteure können somit darauf zugreifen, um an den Diskussionen und am Austausch von bewährten Verfahren teilzunehmen. Einige Aktivitäten sind allerdings ausschliesslich den Mitgliedstaaten vorbehalten.

## Bereits ergriffene Massnahmen in der Schweiz

Die strategischen Prioritäten des Aktionsplans für digitale Bildung entsprechen den Schwerpunkten der Schweizer Politik im Bildungswesen.
Bei der strategischen Priorität 1 verfolgt auch die Schweiz das Ziel, relevante politische Massnahmen für die digitale Bildung zu formulieren und ein digitales Bildungsökosystem zu schaffen. Um die Kohärenz zwischen den Initiativen auf Bundes- und Kantonsebene sicherzustellen, arbeiten Bund und Kantone im Rahmen ihrer jeweiligen Zuständigkeiten eng im Koordinationsausschuss «Digitalisierung in der Bildung» zusammen.
In Bezug auf die strategische Priorität 2 trifft in der Schweiz der Bund gemeinsam mit den Kantonen und den anderen Akteuren aus Bildung, Forschung und Innovation (BFI) ebenfalls gezielte Massnahmen, um den Ausbau der digitalen Kompetenzen zu fördern. Der Aktionsplan «Digitalisierung im BFI-Bereich in den Jahren 2019 und 2020», der vom Staatssekretariat für Bildung, Forschung und Innovation (SBFI) in enger Zusammenarbeit mit den Akteuren aus Bildung und Forschung erarbeitet wurde, sowie die Berücksichtigung der Digitalisierung als Querschnittsthema in den Botschaften zur Förderung von BFI 2021–2024 und 2025–2028 bringen diesen Willen zum Ausdruck. Eine Übersicht über die Massnahmen für die Förderperiode 2025–2028, die die Digitalisierung und insbesondere digitale Kompetenzen betreffen, ist auf der Website des SBFI abrufbar.

Massnahme 22

# Richtlinie zur Verbesserung der Arbeitsbedingungen der Plattformarbeit

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Richtlinie zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit |
| **Art der Massnahme** | Richtlinie |
| **Referenz (falls vorhanden)** | Richtlinie (EU) 2024/2831 |
| **Aktueller Stand** | In Kraft getreten |
| **Datum des Inkrafttretens** | 01.12.2024 |
| **Federführung in der Bundesverwaltung** | BSV |

## Beschrieb

Die Europäische Kommission (KOM) hatte am 9. Dezember 2021 ein Massnahmenpaket vorgestellt, welches die Arbeitsbedingungen von Beschäftigten bei digitalen Plattformen umfassend regeln und verbessern soll. Mit den Vorschlägen sollen die Beschäftigten in der Branche die ihnen zustehenden Arbeitnehmerrechte und Sozialleistungen in Anspruch nehmen können. Der Vorschlag besteht aus einer Mitteilung, einem Vorschlag für eine Richtlinie, sowie einem Entwurf für Leitlinien.

In ihrer Mitteilung informierte die KOM über die Vorgehensweise und Massnahmen im Bereich Plattformarbeit, die durch zusätzliche Massnahmen der Mitgliedsstaaten, der Sozialpartner und anderer einschlägiger Akteure auf ihrer jeweiligen Ebene ergänzt werden sollten. Ein weiteres Ziel ist es, die Grundlagen für die Arbeit an künftigen globalen Standards für hochwertige Plattformarbeit zu schaffen.

Die vorgeschlagene Richtlinie zur Verbesserung der Arbeitsbedingungen soll zuerst sicherstellen, dass Personen, die eine Arbeit über eine Plattform ausführen, den rechtlichen Berufsstatus erhalten, der ihren tatsächlichen Arbeitsmodalitäten entspricht (Bekämpfung von «Schein-Selbstständigkeit»). Sie sieht zu diesem Zweck eine Vermutung zugunsten der Arbeitnehmer-Eigenschaft von Plattform-Beschäftigten vor. Entgegen dem ursprünglichen Vorschlag der Kommission und der Verhandlungsposition des EU-Parlaments enthält die Richtlinie allerdings keine Liste von Prüfkriterien mehr, anhand derjenigen festgestellt werden soll, ob ein Arbeitnehmer-Verhältnis vorliegt. Vielmehr beinhaltet der verabschiedete Rechtstext eine Aktivierung der Arbeitnehmer-Vermutung, wenn Tatsachen vorliegen, die auf Kontrolle und Leitung des Plattform-Beschäftigten durch die Plattform hinweisen. Die Definition dieser Tatsachen obliegt allerdings den EU-Mitgliedsstaaten. Die Richtlinie verpflichtet die Mitgliedsstaaten, angemessene und effektive Verfahren zur Bestimmung der Arbeitnehmer-Eigenschaft vorzusehen. Die erwähnte Vermutung zugunsten dieser Eigenschaft kann durch die Plattform umgestossen werden, wobei diese die Beweislast trifft, dass kein Arbeitsverhältnis vorliegt.

Den über die Plattform arbeitenden Personen werden sodann die mit dem Status „Arbeitnehmer/in“ verbundenen Arbeitnehmerrechte zustehen, was ihnen beispielsweise den Anspruch auf den Mindestlohn (wo vorhanden), Tarifverhandlungen, geregelte Arbeitszeiten, Gesundheitsschutz oder bezahlten Urlaub, ermöglichen würde. Anders als ursprünglich im Kommissionsvorschlag vorgesehen, gilt die gesetzliche Vermutung nicht in Verfahren in Steuer-, Straf- und Sozialversicherungsangelegenheiten. Die Mitgliedstaaten können jedoch nach ihrem nationalen Recht in solchen Verfahren die gesetzliche Vermutung anwenden.

Die neuen Vorschriften sehen darüber hinaus eine Reihe von Schutzbestimmungen im Falle der Verwendung von Algorithmen durch die Plattform vor. Sie sollen namentlich sicherstellen, dass eine Person, die Plattformarbeit leistet, nicht aufgrund einer Entscheidung eines Algorithmus oder eines automatisierten Entscheidungssystems entlassen werden kann. Stattdessen müssen die Plattformen sicherstellen, dass wichtige Entscheidungen, die die Personen, die auf der Plattform arbeiten, direkt betreffen, von Menschen überwacht werden.

Die Richtlinie sieht weiter Schutzvorschriften für Plattformarbeiter im Bereich des Datenschutzes vor. Plattformen wird es untersagt, bestimmte Arten personenbezogener Daten zu verarbeiten, etwa über persönliche Überzeugungen und den privaten Austausch mit Kollegen.

Der Text soll auch die Transparenz verbessern, indem er die Plattformen verpflichtet, die Arbeitnehmer und ihre Vertreter darüber zu informieren, wie ihre Algorithmen funktionieren und wie sich das Verhalten eines Arbeitnehmers auf die von automatisierten Systemen getroffenen Entscheidungen auswirkt.

Plattformen müssen Informationen über die von ihnen beschäftigten Selbstständigen an die zuständigen nationalen Behörden und an die Vertreter der Plattformbeschäftigten, wie z. B. Gewerkschaften, weitergeben.

## Stand der Dinge

Die Verordnung ist am 1. Dezember 2024 in Kraft getreten. Die Mitgliedsstaaten haben zwei Jahre Zeit haben, um diese in das nationale Recht zu überführen.

## Mögliche Auswirkungen auf die Schweiz

Die Richtlinie wird in der Schweiz nicht anwendbar sein, könnte aber Auswirkungen auf grenzüberschreitende Sachverhalte haben, die dem Recht eines EU-Mitgliedstaates unterstehen. So könnte beispielsweise eine Plattform in der Schweiz, deren Beziehungen zu den von ihr beschäftigten Personen durch ausländisches Recht geregelt sind (etwa wenn diese ihre Arbeit im Ausland verrichten), künftig als Arbeitgeber eingestuft werden, was entsprechende Pflichten mit sich bringen würde. Die Auswirkungen der Richtlinie variieren von Land zu Land, abhängig davon, wie die einzelnen Mitgliedstaaten die Richtlinie in ihr nationales Recht überführen.

## Bereits ergriffene Massnahmen in der Schweiz

Im Rahmen des Berichts «Digitalisierung – Prüfung einer Flexibilisierung des Sozialversicherungsrechts» vom 27. Oktober 2021 hatte der Bundesrat die gesetzlichen Rahmenbedingungen und die verschiedenen Optionen einer Weiterentwicklung des Sozialversicherungsrechts im Zusammenhang mit neuen digitalen Geschäftsmodellen eingehend analysiert. Im genannten Bericht hat der Bundesrat auch die Vor- und Nachteile einer Regelung geprüft, bei Plattformbeschäftigung eine unselbstständige Erwerbstätigkeit zu vermuten. Der Bericht kommt zum Schluss, dass diesbezüglich kein weiterer Handlungsbedarf besteht. Arbeitsrechtlich gesehen konnten durch den Entscheid des Kantonsgerichts Waadt zu einem Fahrer der Firma Uber und zwei Entscheiden des Bundesgerichts betreffend Uber und Uber Eats die relevanten Kriterien festgelegt werden, um die Plattformarbeit als unselbstständige Erwerbstätigkeit zu qualifizieren. Auch in diesem Bereich hat der Bundesrat keinen gesetzgeberischen Handlungsbedarf erkannt, was er zuletzt in seinem Bericht «Auswirkungen der Digitalisierung auf den Arbeitsmarkt – Monitoring 2022» vom 9. Dezember 2022 bestätigte.

Massnahme 23

# Europäische Blockchainstrategie

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Europäische Blockchain-Strategie |
| **Art der Massnahme** | Strategie |
| **Referenz (falls vorhanden)** | Blockchain Strategy |
| **Federführung in der Bundesverwaltung** | SIF |

## Beschrieb

Im Februar 2020 stellte die Europäische Kommission (KOM) in der Mitteilung «Gestaltung der digitalen Zukunft Europas» die Erarbeitung von Strategien im Bereich Quanten- und Blockchain-Technologie in Aussicht. Die KOM verwendet die Terminologie «Blockchain Strategy» als Überbegriff für Massnahmen, welche den Willen der EU, eine Führungsrolle im Bereich Blockchain übernehmen zu wollen, verwirklichen sollen. Die Strategie umfasst prinzipiell folgende Themenbereiche und Initiativen:

- **Aufbau einer paneuropäischen Blockchain für öffentliche Dienste**: Die «European Blockchain Partnership», welche die Kommission gemeinsam mit den EU-Mitgliedstaaten sowie den EWR-Staaten ins Leben gerufen hat, arbeitet an der European Blockchain Services Infrastructure (EBSI). Das ist eine gemeinsame Blockchain-Infrastruktur für öffentliche Dienstleistungen. Die Infrastrukturaktivitäten (wie die Beschaffung der Plattform EBSI) werden aus den Mitteln Digital Europe Programme (DEP) finanziert.
- **Anpassung des Regelwerks**: Die Kommission will im Bereich Blockchain Standards setzen und mit zukünftigen Gesetzgebungen Rechtssicherheit schaffen. Dazu zählen insbesondere die im Juni 2023 in Kraft getretene Verordnung Market in Crypto Assets («MiCA»), die ab dem 30. Dezember 2024 anwendbar sein wird, sowie das Pilotregime für Distributed Ledger Technology-basierte Finanzmarktinfrastrukturen. MiCA sieht zudem vor der Anwendung des neuen Regimes eine Reihe von zu definierenden, technischen Standards vor, die nacheinander in drei Paketen veröffentlicht werden sollen (siehe ESMA-Übersicht).
- **Investitionen in Forschung und Innovation**: Unter Horizon Europe und dem EU AI/Blockchain Investment Fund werden Investitionen in Forschung und Innovation finanziert.
- **Bildung und Gemeinschaftsförderung**: Die Kommission fördert die Bildung im digitalen Bereich und sucht den Austausch mit wichtigen Interessensvertretern der Blockchain-Community. Um Blockchain-Entwicklungen zu verfolgen und die Innovation zu fördern, hat die Kommission 2018 das «EU Blockchain Observatory & Forum» gegründet.

## Stand der Dinge

Die Arbeiten werden in den verschiedenen Themenbereichen verfolgt und die Initiativen lanciert.

## Mögliche Auswirkungen auf die Schweiz

Die Schweiz hat die Nutzung der DLT/Blockchain frühzeitig mit einem Paket reguliert, das 2021 in Kraft getreten ist. Die neue Regulierung in der EU könnte zu mehr Wettbewerb für Schweizer Anbieter führen, da sie einen rechtlichen Rahmen für den Einsatz der Blockchain-Technologie im Finanzsektor schafft. Hinzu kommt, dass MiCA keinen EU-Marktzugang für Anbieter aus Drittstaaten (z. B. der Schweiz) vorsieht. Gleichzeitig äussern zahlreiche Fachleute in der EU Bedenken im Zusammenhang mit der Anwendung von MiCA, die ihrer Ansicht nach unzulänglich ist und in der Praxis grosse Probleme mit sich bringen wird.

## Bereits ergriffene Massnahmen in der Schweiz

Das SFI verfolgt die Entwicklungen aufmerksam und beurteilt den EU-Rahmen im Kontext der regulatorischen Arbeiten zum Einsatz der Blockchain-Technologie auf den Finanzmärkten.

Massnahme 24

# Gesetz für ein interoperables Europa

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Gesetz für ein interoperables Europa |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung 2022/0379 (COD) |
| **Aktueller Stand** | In Kraft |
| **Datum des Inkrafttretens** | 11.04.2024 |
| **Federführung in der Bundesverwaltung** | BK |

## Beschrieb

Das Gesetz für ein interoperables Europa (Interoperable Europe Act, IEA) soll den grenzüberschreitenden Datenaustausch erleichtern und den digitalen Wandel des öffentlichen Sektors beschleunigen. Die Rechtsvorschriften müssen dazu beitragen, die Ziele der Digitalen Dekade der EU zu erreichen, insbesondere das Ziel, bis 2030 100 Prozent der wichtigsten öffentlichen Dienste online zur Verfügung zu stellen.

Mit den Rechtsvorschriften wird ein neuer Rahmen für die Zusammenarbeit zwischen den EU-Mitgliedstaaten und der Europäischen Kommission (KOM) bei Fragen der grenzüberschreitenden Interoperabilität und der digitalen öffentlichen Dienste geschaffen. In diesem Rahmen vereinbaren die Mitgliedstaaten und die KOM gemeinsame Prioritäten und Lösungen im Hinblick auf die Interoperabilität.

Darüber hinaus verpflichtet das Gesetz die EU-Institutionen sowie öffentliche Einrichtungen und Agenturen, Interoperabilitätsbewertungen durchzuführen, um bereits bei der Erarbeitung politischer Massnahmen im digitalen Bereich sowie digitaler öffentlicher Dienste Interoperabilitätsaspekte zu ermitteln und zu berücksichtigen.

Die neuen Rechtsvorschriften erleichtern zudem die gemeinsame Nutzung und Weiterverwendung von Lösungen sowie den Datenaustausch zwischen Verwaltungen, indem unnötiger Verwaltungsaufwand aufgrund rechtlicher, organisatorischer, semantischer und technischer Hindernisse für die Interoperabilität beseitigt wird. Dadurch können Kosten und Zeitaufwand für Bürgerinnen und Bürger, Unternehmen und den öffentlichen Sektor selbst verringert werden.

Die Verordnung gilt für Einrichtungen des öffentlichen Sektors, einschliesslich der Organe und Einrichtungen der EU. Die Umsetzung des Gesetzes für ein interoperables Europa wird durch das Programm für ein digitales Europa (Digital Europe) finanziert.

## Stand der Dinge

Der aktuelle Stand des IAE ist wie folgt:

1. Verabschiedung: Das Europäische Parlament hat den IAE am 6. Februar 2024 verabschiedet.
2. Governance-Struktur: Es wurde ein Interoperable Europe Board eingerichtet, um den Rahmen für die Zusammenarbeit im Bereich der Interoperabilität zu steuern und zu überwachen. Das Europäische Parlament hat sich für eine breitere Beteiligung relevanter Interessengruppen an diesem Gremium eingesetzt.
3. Monitoring: Der IAE sieht vor, dass die Kommission einen jährlichen Bericht über die Entwicklung von Free-Software-Interoperabilitätslösungen für öffentliche Dienste erstellen muss.

Das Gesetz für ein interoperables Europa trat am 11. April 2024 in Kraft. Entsprechend dem im Gesetz festgelegten Zeitplan werden die meisten Bestimmungen innerhalb von drei Monaten nach Inkrafttreten anwendbar.

Ausnahmen:

- Die europäischen Organe, Einrichtungen und Agenturen sowie öffentliche Stellen werden ab Januar 2025 Interoperabilitätsbewertungen durchführen.
- Die EU-Mitgliedstaaten benennen die zuständigen nationalen Behörden neun Monate nach Inkrafttreten des Gesetzes, d. h. im Januar 2025.

## Mögliche Auswirkungen auf die Schweiz

Der IAE gilt für Einrichtungen der Union und öffentliche Stellen, die transeuropäische digitale öffentliche Dienste regeln, bereitstellen, verwalten oder erbringen. Er hat somit keine direkten Auswirkungen auf die Schweiz.

## Bereits ergriffene Massnahmen in der Schweiz

In der Schweiz sind am 1. Januar 2024 EMBAG und EMBAV zur Förderung der Interoperabilität in Kraft getreten. Diese Massnahme steht im Kontext der Digitalisierung der Verwaltung und ist keine direkte Reaktion auf die EU-Massnahme.

Massnahme 25

# Zugang zu Finanzdaten

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung über einen Rahmen für den Zugang zu Finanzdaten |
| **Art der Massnahme** | Gesetzespaket |
| **Referenz (falls vorhanden)** | 2023/0205 (COD) |
| **Aktueller Stand** | Nicht in Kraft |
| **Datum des Inkrafttretens** | Voraussichtlich Anfang-Mitte 2025 |
| **Federführung in der Bundesverwaltung** | SIF |

## Beschrieb

Wie erwartet, legte die Europäische Kommission im Rahmen des «Paket für den Zugang zu Finanzdaten und Zahlungen» am 28. Juni 2023 einen Vorschlag für eine Verordnung für einen Rahmen für den Zugang zu Finanzdaten («FiDA») vor. Die FiDA soll Rechte und Pflichten zur Verwaltung des Austauschs von Kundendaten im Finanzsektor über Zahlungskonten hinaus festlegen mit der Erwartung, dass dies zu innovativeren Finanzprodukten und -dienstleistungen und zu einem verstärkten Wettbewerb im Finanzsektor führt. Der Anwendungsbereich der FiDA umfasst neben Zahlungsdaten auch Nicht-Bankdaten, wie, wie Versicherungs-, Anlage- und Rentendaten erweitert. Weiter beruht der Vorschlag auf dem Grundsatz, dass die Kunden von Finanzdienstleistungen Eigentümer der von ihnen bereitgestellten Daten und der in ihrem Namen erstellten Daten sind und diese kontrollieren.

Der «Open Finance»-Vorschlag – via «FiDA» - baut auf «Open Banking» auf, das mit der zweiten Zahlungsdienstleistungsrichtlinie («PSD2») lanciert werden sollte. Die Richtlinie fiel in der Praxis aber hinter die Erwartungen zurück, u.a. aufgrund von inkonsistenter Adoption und Divergenzen in der Infrastruktur. Entsprechend wurde im gleichen Paket wie «FiDA» auch die Zahlungsdienstleistungsrichtlinie überarbeitet («PSD3»), bzw. als direkt anwendbare Verordnung neu aufgesetzt («PSR»). Dadurch soll u.a. die Funktionsweise von «Open Banking» durch die Beseitigung bestehender Hindernisse verbessert werden.

## Stand der Dinge

**«FiDA»:**

- Parlament und Rat haben mit den Arbeiten am Vorschlag begonnen, aber haben beide noch keine Verhandlungsposition gefasst.

**«PSD3/PSR»:**

- Positionen des Parlaments in erster Lesung am 23. April 2024 (Richtlinie / Verordnung): Verschiedene Anpassungen, insbesondere bei den Transparenzanforderungen und beim Kundenschutz.
- Der Rat hat sein Verhandlungsmandat für die interinstitutionellen Verhandlungen noch nicht finalisiert.

## Mögliche Auswirkungen auf die Schweiz

Die FiDA sowie die PSD3/PSR sollen die Position der EU im Bereich Innovation und Digitalisierung stärken. In der Schweiz gibt es keine analoge Regelung, welche die Finanzinstitute verpflichten würde, ihre Daten auf Anfrage der Kundinnen und Kunden an Drittanbieter weiterzugeben. Das EFD folgt den Vorgaben des Bundesrates. Der Ansatz ist marktorientiert. Der Bundesrat hat dem EFD den Auftrag erteilt, ihn regelmässig über die Fortschritte und den Handlungsbedarf zu informieren.

Mit der Motion 22.3890 «Rahmengesetz für die Sekundärnutzung von Daten» wird der Bundesrat beauftragt, die Grundlagen zu schaffen, damit spezifische Infrastrukturen für die Sekundärnutzung von Daten in strategisch relevanten Bereichen rasch initialisiert und aufgebaut werden können. Das BJ hat die vorliegende Massnahme der EU im Rahmen seiner ordentlichen Gesetzgebungsarbeiten zur Kenntnis genommen. Zum jetzigen Zeitpunkt lässt sich allerdings noch nicht sagen, wie diese Massnahme berücksichtigt und in das Vorhaben zur Sekundärnutzung von Daten integriert werden kann.

## Bereits ergriffene Massnahmen in der Schweiz

Derzeit bestehen die Massnahmen in der Schweiz darin, Ziele zu formulieren, die Fortschritte im Land genau zu beobachten und regelmässig den Bedarf an weiteren Massnahmen zu beurteilen.

Massnahme 26

# Verzerrende drittstaatliche Subventionen

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung über den Binnenmarkt verzerrende drittstaatliche Subventionen |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung (EU) 2022/2560 |
| **Aktueller Stand** | In Kraft |
| **Datum des Inkrafttretens** | 12.07.2023 |
| **Federführung in der Bundesverwaltung** | SECO/EDA |

## Beschrieb

Am 12. Juli 2023 trat die Verordnung über drittstaatliche Subventionen («FSR», Verordnung [EU] 2022/2560) in Kraft. Diese neuen Vorschriften ermöglichen es der Europäischen Kommission (KOM), «durch drittstaatliche Subventionen verursachte Verzerrungen zu beseitigen», und der EU, offen für Handel und Investitionen zu bleiben und dabei gleiche Wettbewerbsbedingungen für alle im Binnenmarkt tätigen Unternehmen zu gewährleisten.

Vor Inkrafttreten der FSR wurden die Marktverzerrungen, welche durch drittstaatlichen Subventionen entstanden, nicht erkannt, während die von EU-Mitgliedstaaten gewährten Subventionen nach den EU-Beihilfevorschriften einer «sorgfältigen Prüfung» unterzogen werden:

- Die **GD COMP** ist für die Einhaltung der FSR in Bezug auf Zusammenschlüsse verantwortlich;
- Die **GD GROW** ist für die Einhaltung der FSR in Bezug auf die Verfahren zur Vergabe öffentlicher Aufträge verantwortlich.

Sämtliche Bereiche, Unternehmen und Sektoren sind betroffen.

## Stand der Dinge

Die FSR ermöglicht es der KOM, zu untersuchen, **(i)** ob Unternehmen aus Drittstaaten, die Unternehmen in der EU übernehmen, mit öffentlichen Geldern unterstützt wurden, und **(ii)** ob Unternehmen aus Drittstaaten, die an Ausschreibungen in der EU teilnehmen, mit öffentlichen Geldern unterstützt wurden. Darüber hinaus kann die KOM **(iii)** von sich aus Informationen über mutmassliche drittstaatliche Subventionen, die den Binnenmarkt verzerren, prüfen.

Am 26. März 2024 zog sich das chinesische Unternehmen *CRRC Locomotive aus einem Ausschreibungsverfahren des bulgarischen Verkehrsministeriums zurück. Dieser Rückzug erfolgte, nachdem die Kommission am* 16. Februar 2024 die erste Prüfung nach der FSR angekündigt hatte.

Weitere Prüfungen wurden in der Folge im Bereich der erneuerbaren Energien eingeleitet. Dabei waren jedes Mal chinesische Unternehmen involviert. Auch andere Sektoren sind betroffen: Am 23. April 2024 führte die KOM eine unangekündigte Inspektion in den Räumlichkeiten der chinesischen Sicherheitsfirma *Nuctech (Gepäckscanner) in Rotterdam und Warschau durch. Am 13. Mai 2024 rückten zwei weitere chinesische Firmen in den Fokus von Untersuchungen: ein Konsortium, dem die deutsche Tochtergesellschaft von LONGi* (Hongkong) angehört, und ein zweites Konsortium aus zwei Unternehmen der *Shanghai Electric Group* (China).

Beide Konsortien haben angekündigt, sich von der Ausschreibung Rumäniens für den Bau und Betrieb eines Solarparks zurückzuziehen. Die KOM hat daher ihre am 3. April 2024 eingeleitete Prüfung abgeschlossen. Als Reaktion darauf veröffentlichte die chinesische Handelskammer bei der EU ein Kommuniqué, in dem sie die FSR als «Zwangsmittel und diskriminierendes Instrument» bezeichnete. Die Kammer warnt vor einer «Eskalation protektionistischer Tendenzen in der EU». Am 10. Juni leitete die KOM eine erste eingehende Prüfung ein, um die Übernahme der alleinigen Kontrolle über PPF Telecom Group B.V, unter Ausschluss des tschechischen Geschäfts, durch die *Emirates Telecommunications Group Company PJSC («e&»)* auf der Grundlage der FSR zu untersuchen. Die KOM befürchtet zunächst, dass e& drittstaatliche Subventionen erhalten haben könnte, die den EU-Binnenmarkt verzerren könnten.

Die KOM begrüsst die raschen Ergebnisse (siehe die Rede von M. Vestager vom 9. April 2024), die durch die FSR insbesondere bei den öffentlichen Ausschreibungen erzielt wurden. Infolge eines Personalproblems hat die GD COMP die neue Direktion K eingerichtet, um die FSR (für die Prüfung von Anmeldungen von Zusammenschlüssen) umzusetzen. In den kommenden Jahren ist deshalb mit einer wirksameren Umsetzung zu rechnen.

## Mögliche Auswirkungen auf die Schweiz

Schweizer Unternehmen, die im EU-Binnenmarkt wirtschaftlich tätig sind, sehen sich in der EU neuen Prüf- und Durchsetzungsbefugnissen der Kommission ausgesetzt, was zu einem erhöhten administrativen Aufwand und zu Rechtsunsicherheit führt.

Die Unternehmen müssen grundsätzlich sämtliche finanziellen Zuwendungen der vergangenen drei Jahre aus subventionsrechtlicher Sicht aufbereiten, um potenziellen Meldepflichten nachzukommen und auf Anfragen der Kommission die erforderlichen Informationen übermitteln zu können. Diese Informationen sind nicht nur erforderlich, um zu beurteilen, ob ein künftiger Unternehmenszusammenschluss oder eine Beteiligung an öffentliche Ausschreibungen in der EU anmeldepflichtig ist, sondern auch für den Fall, dass die Kommission eine Prüfung von Amts wegen einleitet (z. B. im Falle einer Beschwerde durch Konkurrenten). Weil das Konzept der «finanziellen Zuwendung» im Rahmen der FSR sehr weit gefasst ist, dürften die Abklärungs- und Datenerhebungspflichten erheblich sein.

Damit eine finanzielle Zuwendung eine den EU-Binnenmarkt verzerrende drittstaatliche Subvention darstellt, muss sie die Wettbewerbsposition des begünstigten Unternehmens verbessern und den Wettbewerb im EU-Binnenmarkt tatsächlich oder potenziell beeinträchtigen. Diese Bewertung ist einzelfallabhängig, umfasst eine Abwägung der positiven und negativen Auswirkungen der drittstaatlichen Subventionen auf den EU-Binnenmarkt und kann zu weitreichenden Abhilfemassnahmen führen. Die Abwägungsprüfung lässt der Kommission einen grossen Ermessenspielraum, was entsprechend zu Rechtsunsicherheit führt.

Grundsätzlich ist aber anzumerken, dass die Drittstaaten-Subventionsverordnung in der bisherigen Praxis und gemäss zahlreichen Aussagen der Kommission primär gegen Unternehmen aus nicht-marktwirtschaftliche Volkswirtschaften, also nicht gegen Schweizer Unternehmen, gerichtet ist. Entsprechend ist aktuell kaum mit Untersuchungen gegen Schweizer Unternehmen zu rechnen.

## Bereits ergriffene Massnahmen in der Schweiz

Die Schweiz hat in diesem Bereich keine eigenen Massnahmen ergriffen.

Massnahme 27

# Neue Verbraucheragenda

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Neue Verbraucheragenda |
| **Art der Massnahme** | Gesetzespaket |
| **Referenz (falls vorhanden)** | COM (2020) 696 final |
| **Aktueller Stand** | In Anwendung |
| **Datum des Inkrafttretens** | Publiziert am 13.11.2020 |
| **Federführung in der Bundesverwaltung** | BFK |

## Beschrieb

Die neue Verbraucheragenda, die eine Vision für die EU-Verbraucherpolitik im Zeitraum 2020–2025 umfasst, wurde von der europäischen Kommission (KOM) am 13. November 2020 kommuniziert. Darin wird vorgeschlagen, mehrere Richtlinien anzupassen, um die Konsumentenrechte vor allem im Hinblick auf Digitalisierung, Nachhaltigkeit und die Covid-19-Krise adäquat zu schützen.

Im digitalen Bereich will die KOM verstärkt gegen Online-Täuschung und versteckte Werbung vorgehen und die Interessen der Konsumentinnen und Konsumenten beim Erarbeiten von Vorschriften zu künstlicher Intelligenz (KI) berücksichtigen. Die EU revidierte hierzu die Richtlinie zur Produktesicherheit und die Maschinenrichtlinie (neukonzipiert als Verordnung), um die derzeitigen Vorschriften an die fortschreitende Digitalisierung und die Zunahme verbundener Produkte anzupassen. Um den Verbraucherschutz im Hinblick auf die Digitalisierung von Finanzdienstleistungen für Privatkundinnen und -kunden zu stärken, wurden auch die Richtlinien über Verbraucherkredite und über Finanzdienstleistungen im Fernabsatz überarbeitet. Zusätzlich soll mit der Revision der Vorschriften über die Sicherheit von Spielzeugen u.a. ein sicherer Umgang mit neuen Risiken bei mit dem Internet verbundenem Spielzeug und KI-Spielzeug gewährleistet sowie digitale Produktinformationen bereitgestellt werden. Dieser Vorschlag befindet sich aber noch im Gesetzgebungsverfahren. Auch die neuen, horizontalen Vorschriften für die Verwendung von KI im Rahmen des «AI Act» (s. Massnahme 5) sollen zum Schutz der Verbraucher beitragen.

Im Umweltbereich erliess die EU zudem eine neue Richtlinie zur Stärkung der Rolle der Verbraucher beim Übergang zur grünen Wirtschaft, der es den Konsumentinnen und Konsumenten erlauben soll, sich besser über die Haltbarkeit von Produkten zu informieren, und der sie besser vor Praktiken wie Greenwashing und programmierter Obsoleszenz schützt. Ähnliche Ziele verfolgt die neue Richtlinie zur Untermauerung und Kommunikation ausdrücklicher Umweltaussagen («Green Claims Directive»), die sich noch im Gesetzgebungsverfahren befindet.

Im Rahmen der Überarbeitung der Richtlinie für den Warenhandel wurden zudem Reparaturen und nachhaltigere Produkte gefördert werden. Diese Ambition unterliegt auch den neuen Vorschriften zur Förderung der Reparatur von Waren, die nach Annahme durch die Co-Gesetzgeber am 10. Juli 2024 im Amtsblatt publiziert worden ist.

Ein angemessener Konsumentenschutz erfordert schliesslich auch eine gute Zusammenarbeit innerhalb der EU und mit internationalen Partnern. Die KOM will die internationale Zusammenarbeit vor allem mit China verstärken, um dem aufstrebenden Online-Handel Rechnung zu tragen.

## Stand der Dinge

Am 13. November 2020 verabschiedete die Europäische Kommission (KOM) die neue Verbraucheragenda. Es handelt sich um eine Aktualisierung des umfassenden strategischen Rahmens der EU-Verbraucherpolitik, der 2012 angenommen wurde.

## Mögliche Auswirkungen auf die Schweiz

Die Verbraucheragenda umfasst eine Vision und einen Aktionsplan für die Verbraucherpolitik der EU und hat insofern keine direkten Auswirkungen auf die Schweiz. Mit Ausnahme des bilateralen Luftverkehrsabkommens (aufgrund dessen die Schweiz unter anderem die Verordnung EU/261/2004 über Ausgleichs- und Unterstützungsleistungen für Fluggäste im Fall der Nichtbeförderung und bei Annullierung oder grosser Verspätung von Flügen übernommen hat) und des bilateralen Landverkehrsabkommens (aufgrund dessen die Schweiz insbesondere die Verordnung (EG) 1371/2007 über die Rechte und Pflichten der Fahrgäste im Eisenbahnverkehr sowie die Verordnung (EU) 181/2011 über die Fahrgastrechte im Kraftomnibusverkehr übernommen hat) gibt es derzeit kein Abkommen, das die Schweiz zur Übernahme von EU-Rechtsvorschriften zum Konsumentenschutz verpflichtet.

Die KOM betont in der Verbraucheragenda mehrmals, wie wichtig die Zusammenarbeit unter den Behörden ist, um ein hohes Konsumentenschutzniveau zu gewährleisten. Die Zusammenarbeit zwischen EU-Behörden ist in der Verordnung EU/2017/2394 geregelt, die die Möglichkeit vorsieht, Abkommen mit Drittstaaten abzuschliessen.

## Bereits ergriffene Massnahmen in der Schweiz

Die Schweiz hat Konsumentenschutzvorschriften insbesondere in folgenden Bereichen autonom nachvollzogen: Pauschalreisen, Produkthaftung, Haustürgeschäfte, Konsumkredite, unlautere Geschäftspraktiken und Produktsicherheit. Trotz dieses autonomen Nachvollzugs bestehen gewisse Differenzen zwischen der schweizerischen und der europäischen Konsumentenschutzgesetzgebung. Allerdings werden derzeit Anpassungen des Schweizer Rechts in den Bereichen Pauschalreisen, Verkauf von Gütern, Verträge über digitale Güter und Dienstleistungen, unlautere Geschäftspraktiken und Produktesicherheit diskutiert oder geprüft. In Bezug auf die geplante Obsoleszenz hat der Bundesrat in seinem Bericht «Modernisierung des Gewährleistungsrechts» vom 16. Juni 2023 hingegen keinen gesetzgeberischen Handlungsbedarf erkannt. Er ist der Ansicht, dass das Problem auf der Grundlage der geltenden, allgemeinen Regeln lösbar ist.

Massnahme 28

# Aktionsplan für die europäische Demokratie

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Aktionsplan für Demokratie in Europa |
| **Art der Massnahme** | Aktionsplan |
| **Referenz (falls vorhanden)** | Aktionsplan für Demokratie in Europa |
| **Federführung in der Bundesverwaltung** | BAKOM/BK |

## Beschrieb

Die Europäische Kommission (KOM) will sicherstellen, dass die im Rahmen der «digitalen Dekade Europas» angestrebten Fortschritte die **Achtung von Demokratie und Grundrechten** in der EU nicht untergraben. Zu diesem Zweck hat die KOM im Dezember 2020 Garantien in Form eines europäischen Aktionsplans für Demokratie (European Democracy Action Plan, EDAP) angenommen. Dieser soll eine Antwort auf die neuen Herausforderungen bieten, die mit der digitalen Revolution entstanden sind, wie z. B. wiederkehrende Einmischung in demokratische Prozesse, Bedrohung von Medienschaffenden oder mangelnde Transparenz von IT-Giganten.

Die KOM sieht Massnahmen zur **1) Förderung freier und fairer Wahlen 2) Unterstützung freier und unabhängiger Medien und 3) Bekämpfung von Desinformation** vor. Im Aktionsplan wird der das Gesetz über digitale Dienste ergänzende Rahmen erwähnt. Dieser gewährleistet die Überwachung, Rechenschaftspflicht und Transparenz und schafft eine **Koregulierungssicherung für den überarbeiteten und gestärkten Verhaltenskodex über die Desinformation**.

Die im EDAP vorgesehenen Initiativen (vor allem jene in den Bereichen der Stärkung des Verhaltenskodex und der Vorschriften zur Transparenz für politische Werbung) ergänzen die Massnahmen, die im Rahmen des Digital Services Act (DSA) vorgeschlagen werden.

Konkret hat die KOM im Rahmen dieses Aktionsplans im September 2021 eine Empfehlung zur Erhöhung der Sicherheit von Journalistinnen und Journalisten und anderen Medienschaffenden, online und offline, veröffentlicht. Zudem sind Massnahmen zur Förderung des Medienpluralismus und zur Verbesserung der Transparenz der Eigentumsverhältnisse im Medienbereich vorgesehen. In diesem Zusammenhang verfügt die EU seit Mai 2024 über einen europäischen Rechtsakt zur Medienfreiheit, der einen Satz neuer Vorschriften zum Schutz des Pluralismus und der Unabhängigkeit der Medien umfasst (vgl. auch Massnahme 29). Im Jahr 2024 trat überdies eine neue Richtlinie zur Verbesserung des Schutzes von Journalisten und Menschenrechtsverteidigern vor missbräuchlichen Gerichtsverfahren (SLAPP) in Kraft. Diese Richtlinie regelt die gerichtliche Verfolgung in Zivilsachen mit grenzüberschreitendem Bezug.

## Stand der Dinge

Im Vorfeld der Europawahlen 2023 führte die KOM eine Untersuchung der Umsetzung des Aktionsplans durch und identifizierte eine Reihe von Bereichen, in denen die EU die bestehenden und sich verändernden Herausforderungen proaktiv angehen kann. So legte die KOM eine Empfehlung für inklusive und stabile Wahlverfahren in der Union und für die Stärkung des europäischen Charakters und eine effiziente Durchführung der Wahlen zum Europäischen Parlament, einen Vorschlag für eine Richtlinie zur Transparenz der Interessenvertretung im Auftrag von Drittländern sowie eine Empfehlung zur Förderung der Mitwirkung und der

wirksamen Beteiligung von Bürgerinnen und Bürgern und Organisationen der Zivilgesellschaft an politischen Entscheidungsprozessen.

## Mögliche Auswirkungen auf die Schweiz

Der Aktionsplan für Demokratie betrifft auch die Schweiz, insbesondere im Zusammenhang mit den Aktivitäten zur Resilienz der Wahlprozesse, im Kampf gegen Desinformation und in Bezug auf die Transparenz von Interessenvertreter/-innen aus Drittstaaten.

Die Schweiz ist bisher nicht in das 2019 eingerichtete Europäische Kooperationsnetzwerk für Wahlen eingebunden. In Anbetracht der konkreten Pläne für einen engeren Austausch innerhalb dieses Netzwerks, namentlich über Fragen der Integrität von Wahlen (wie Cybersicherheit von Wahlen), wäre es für die Schweiz von Vorteil, künftig enger in die Arbeiten einbezogen zu sein.

Im sicherheitspolitischen Bericht hält der Bundesrat fest, dass Beeinflussungsaktivitäten und Desinformation durch die Stärkung der Früherkennung, der Lageverfolgung, der Resilienz der Schweizer Bevölkerung und durch aktive Behördenkommunikation begegnet werden soll. In Erfüllung des Po. 22.3006 SiK-N verabschiedete der Bundesrat am 19.6.2024 den Bericht «Beeinflussungsaktivitäten und Desinformation». Der Bericht legt dar, inwiefern die Schweiz von Beeinflussungsaktivitäten im Informationsraum betroffen ist, welche Eigenschaften der Schweiz dabei relevant sind und mit welchen zusätzlichen Massnahmen der Bundesrat diesen Bedrohungen begegnen will. Vor diesem Hintergrund würde die Schweiz von einer stärkeren Einbindung in die Kooperationsstrukturen der EU, insbesondere in das Schnellwarnsystem (Rapid Alert System, RAS) profitieren.

Gemäss Richtlinienentwurf würde die Transparenzpflicht für Interessenvertreter/-innen aus Drittstaaten und damit auch für Schweizer Akteure gelten, nicht aber für solche aus den EU- und EWR-Staaten. Auf der anderen Seite wären die EU- und EWR-Staaten verpflichtet, ein nationales Transparenzregister zu betreiben. In Bezug auf die konkrete Ausgestaltung der Richtlinie sind einige Fragen offen, weshalb sich die Auswirkungen auf die Schweiz noch nicht abschliessend beurteilen lassen.

## Bereits ergriffene Massnahmen in der Schweiz

In Bezug auf die Transparenz der Politikfinanzierung wurde die Gesetzgebung des Bundes angepasst. Die neuen einschlägigen Bestimmungen sind am 23. Oktober 2022 in Kraft getreten und wurden anlässlich der Nationalratswahlen 2023 erstmals angewendet. Die Entwicklung der europäischen Regulierung hat keine direkten Auswirkungen auf die Schweiz, ist aber eventuell mit Blick auf künftige Änderungen der Gesetzgebung zu beobachten. In der Schweiz gibt es aktuell keine spezifischen Gesetze oder Regeln zur Bekämpfung von Desinformation. Hingegen beschloss der Bundesrat am 19.6.2024 zusammen mit der Verabschiedung des Berichtes «Beeinflussungsaktivitäten und Desinformation» zusätzliche Massnahmen, um den Bedrohungen im Informationsraum zu begegnen.

Massnahme 29

# European Media Freedom Act

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Verordnung zur Schaffung eines gemeinsamen Rahmens für Mediendienste im Binnenmarkt |
| **Art der Massnahme** | Verordnung |
| **Referenz (falls vorhanden)** | Verordnung 2024/1083 |
| **Aktueller Stand** | In Kraft |
| **Datum des Inkrafttretens** | 07.05.2024 |
| **Federführung in der Bundesverwaltung** | BAKOM |

## Beschrieb

Das Medienfreiheitsgesetz zielt darauf ab, die Integrität des Binnenmarkts zu stärken und damit den Medienpluralismus und die Unabhängigkeit der Medien in der Union zu schützen. Mit der Rechtsvorschrift werden folgende Ziel verfolgt:

- Schutz der redaktionellen Unabhängigkeit, indem die Mitgliedstaaten verpflichtet werden, die tatsächliche redaktionelle Freiheit der Mediendiensteanbieter zu respektieren
- Schutz journalistischer Quellen, einschliesslich vor Verwendung von Spähsoftware
- Sicherstellung der unabhängigen Funktionsweise der öffentlich-rechtlichen Medien, insbesondere durch Gewährleistung angemessener, nachhaltiger und vorhersehbarer finanzieller Mittel und Förderung der Transparenz bei der Ernennung der Leitung oder der Mitglieder der Verwaltungsräte der öffentlich-rechtlichen Medien
- Sicherstellung der Transparenz in Bezug auf das Medieneigentum, indem die Mediendiensteanbieter spezifische Informationen über sie offenlegen (z. B. Firma, Kontaktangaben, Eigentumsverhältnisse)
- Gewährleistung von Schutzvorkehrungen gegen die ungerechtfertigte Entfernung von Medieninhalten durch sehr grosse Online-Plattformen (gemäss dem Gesetz über digitale Dienste), die nach professionellen Standards produziert wurden, aber als mit den allgemeinen Geschäftsbedingungen unvereinbar angesehen werden
- Einführung eines Rechts auf persönliche Anpassung des Multimedia-Angebots auf Geräten und Schnittstellen, wie z. B. Smart-TVs, damit die Nutzerinnen und Nutzer die Standardeinstellungen nach ihren eigenen Präferenzen ändern können
- Sicherstellung, dass die Mitgliedstaaten die Auswirkungen grosser Zusammenschlüsse auf dem Medienmarkt auf den Medienpluralismus und die redaktionelle Unabhängigkeit anhand von Medienpluralismus-Tests bewerten
- Gewährleistung von mehr Transparenz bei der Publikumsmessung für Mediendiensteanbieter und Werbetreibende, um das Risiko von überhöhten oder verzerrten Nutzungsdaten zu minimieren
- Schaffung von Transparenzanforderungen für die Vergabe staatlicher Werbung an Mediendiensteanbieter und Online-Plattformen durch Behörden und öffentliche Körperschaften
- Intensivierung und Ausweitung der Zusammenarbeit und Koordinierung zwischen den Medienregulierungsbehörden, auch im Hinblick auf Massnahmen in Bezug auf Mediendienste von ausserhalb der Union

Mit den Rechtsvorschriften wird ein neues Europäisches Gremium für Mediendienste eingesetzt. Dieser unabhängige Zusammenschluss von nationalen Medienbehörden wird die Gruppe europäischer Regulierungsstellen für audiovisuelle Mediendienste (ERGA) ersetzen. Das Gremium wird die wirksame und einheitliche Anwendung des EU-Medienrechtsrahmens fördern, insbesondere indem es die KOM bei der Ausarbeitung von Leitlinien für die Medienregulierung unterstützt. Es kann auch Stellungnahmen zu nationalen Massnahmen und Entscheidungen sowie zu Zusammenschlüssen auf Medienmärkten, die diese Märkte beeinflussen, abgeben.

## Stand der Dinge

Die Verordnung trat am 7. Mai 2024 in Kraft und wird ab dem 8. August 2025 anwendbar, mit einigen Ausnahmen. So wird z.B. die Einrichtung des europäischen Gremiums für Mediendienste schon ab dem 8. Februar 2025 fällig sein.

## Mögliche Auswirkungen auf die Schweiz

Es ist noch nicht absehbar, welche Auswirkungen diese Regelung auf die Schweiz haben wird. Die erste Massnahme, von der die Schweiz betroffen ist, wird die Einsetzung des europäischen Gremiums für Mediendienste sein. Die Schweiz hat zurzeit Beobachterstatus in der ERGA; es ist fraglich, ob dieser im neuen Gremium gewährleistet ist.

## Bereits ergriffene Massnahmen in der Schweiz

Die Schweiz hat in diesem Bereich keine eigenen Massnahmen ergriffen.

Massnahme 30

# Standardisierungsstrategie

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Standardisierungsstrategie |
| **Art der Massnahme** | Strategie |
| **Referenz (falls vorhanden)** | Strategie COM (2022) 31 |
| **Aktueller Stand** | Publiziert |
| **Datum des Inkrafttretens** | 02.02.2022 |
| **Federführung in der Bundesverwaltung** | SECO |

## Beschrieb

Am 2. Februar 2022 hat die KOM nach mehrmaligem Verschieben eine neue Normungsstrategie veröffentlicht, welche darauf abzielt, die globale Wettbewerbsfähigkeit der EU zu stärken, den Wandel hin zu einer resilienten, grünen und digitalen Wirtschaft zu ermöglichen und demokratische Werte in Technologieanwendungen zu verankern. Die EU betrachtet die Fähigkeit, internationale Normen für digitale Produkte, Prozesse und Dienstleistungen als globaler Benchmark zu gestalten, von entscheidender Bedeutung im Wettlauf um die digitale Führerschaft. Die Strategie sieht fünf Massnahmenbündel vor: 1) den Normungsbedarf in strategischen Bereichen antizipieren, priorisieren und bewältigen; 2) Verbesserung von Governance und Integrität des europäischen Normungssystems; 3) stärkere Führungsrolle Europas bei globalen Normen; 4) Förderung der Innovation und 5) Generationenwechsel bei den Sachverständigen erleichtern. Zur Umsetzung der Strategie wurde auch die Verordnung 1025/2012 über die Normung abgeändert, die am 19.12.2022 im Amtsblatt publiziert wurde und 20 Tage später in Kraft trat.

Die KOM hat im Zusammenhang mit der Normungsstrategie vom 2. Februar 2022 die Expertengruppe «Hochrangiges Forum für europäische Normung» eingesetzt. Das Forum ist damit beauftragt, in den folgenden Bereichen Hilfestellung zu bieten:

- bei der Ermittlung und Umsetzung jährlicher Prioritäten für die europäische Normung zur Unterstützung eines grünen, digitalen, fairen und resilienten Binnenmarkts
- bei der Ermittlung eines potenziellen künftigen Normungsbedarfs zur Unterstützung von Rechtsvorschriften, Programmen und Strategien der Union.

Das Forum hat zudem die Aufgabe, die KOM in folgenden Bereichen zu beraten:

- zu Fragen in Zusammenhang mit der europäischen Normungspolitik
- bei der Koordinierung der wirksamen Vertretung der Interessen der EU in internationalen Normungsorganisationen und -gremien
- in Bezug auf Möglichkeiten zur Sicherstellung von bedarfsgerechten europäischen Normungstätigkeiten mit dem Ziel einer umweltfreundlicheren, digitaleren, faireren und resilienteren Wirtschaft der Union
- betreffend Möglichkeiten zur besseren Verknüpfung von Forschungs-, Entwicklungs- und Innovationstätigkeiten, zum Ausbau der Lehre an Hochschulen und zur Ausweitung von Fachwissen und Kompetenzen im Bereich der Normung

Parallel wird der Fortlaufende Plan für die IKT-Normung von der KOM in Zusammenarbeit mit der Europäischen Multi-Stakeholder-Plattform für IKT-Standardisierung entwickelt und jährlich aktualisiert. Darin werden alle als politische Prioritäten der EU ermittelten Themen aufgeführt, bei denen Normung, Normen oder technische IKT-Spezifikationen eine Schlüsselrolle bei der Umsetzung der Politik spielen sollten. Der Plan beinhaltet Technologien von «horizontaler Bedeutung», deren Anwendung im Kontext von IKT-Infrastrukturen und IKT-Normung grosse Auswirkungen auf verschiedene technische Bereiche hat.

Von Bedeutung für die Normungsstrategie der EU ist zudem das am 05. März 2024 veröffentlichte Urteil zum Fall C588/21 P («Malamud»-Fall), der sich mit dem Zugang der Öffentlichkeit zu europäischen, harmonisierten Normen auseinandersetzte – d.h. Normen, die von den Normungsorganisationen auf Anfrage der Kommission und zur Unterstützung von europäischen (Gesetzgebungs-)Massnahmen entwickelt werden. Das Urteil war aufgrund dessen möglichen Implikationen für die Normungsprozesse mit grossem Interesse erwartet worden. Der

Gerichtshof der Europäischen Union (EuGH) urteilte nun, dass harmonisierte Normen zwar nach wie vor dem Urheberrechtsschutz unterliegen, aber hob die Entscheidung der Kommission auf, den Zugang zu den im Fall relevanten Normen zu verweigern. Auf Seiten der europäischen Stakeholder ist man noch daran zu evaluieren, welche Folgen das Urteil für das Normungssystem als Ganzes hat.

## Stand der Dinge

Am 2. Februar 2022 hat die Europäische Kommission (KOM) die Normungsstrategie veröffentlicht, in der sie ihren Ansatz zu Normen im Binnenmarkt und auf globaler Ebene darlegt.

## Mögliche Auswirkungen auf die Schweiz

Die Schweiz ist von der Massnahme (Strategie) insofern betroffen, als sie sich soweit wie möglich am europäischen Normenwesen beteiligt (vgl. nachstehend) und dieses über die EFTA auch mitfinanziert. Gleichzeitig gilt die europäische Normenverordnung 1025/2012 für die Schweiz nicht, was dazu führt, dass die Schweiz in den darin verankerten Prozessen nicht direkt involviert sein kann.

Internationale Normen, vor allem harmonisierte Europäische Normen, haben auch für die Schweiz eine grosse Bedeutung: Die Schweiz harmonisiert ihre rechtlichen Anforderungen an Produkte mit den Vorschriften der EU (gemäss dem Bundesgesetz über die technischen Handelshemmnisse (THG; SR 946.51)). In dem von der EU entwickelten sog. «new approach»-System legt das EU-Recht jedoch nur mehr die grundlegenden Anforderungen fest. Diese grundlegenden Anforderungen an Produkte werden erst durch harmonisierte europäische Normen konkretisiert. Damit auch in der Schweiz nicht nur die grundlegenden Anforderungen gelten, sondern diese ebenfalls konkretisiert werden, übernimmt die Schweiz die harmonisierten europäischen Normen in der Regel unverändert in ihr nationales Normungswerk.

Die Schweiz nimmt an der «European Multistakeholder Platform on ICT Standardisation» (MSP) teil. Dabei handelt es sich um eine Plattform zum Informationsaustausch zwischen KOM, Mitgliedstaaten, Normungsgemeinschaft und Zivilgesellschaft, die unter anderem mit der KOM den «EU Rolling Plan» für die Normung im IKT-Bereich erarbeitet. Die Schweiz ist als Beobachterin auch im Komitee für Normung vertreten, das mit der Verordnung (EU) 1025/2012 eingesetzt wird.

Die Schweiz ist zudem Mitglied bei den europäischen Normungsorganisationen, namentlich bei CEN und CENELEC sowie ETSI; nach einer kleinen Revision (im Jahr 2022) der Verordnung (EU) 1025/2012 im Rahmen der EU-Normungsstrategie wurde sie in die Kategorie «Rot» dieser Organisationen aufgenommen. Als Mitglied der Kategorie «Rot» hat die Schweiz vollen Zugang zu allen Ausschüssen und Arbeitsgruppen, allerdings wird bei einem knappen Abstimmungsresultat ihre Stimme bei der Zweitauszählung nicht mehr berücksichtigt. Die Schweiz kann sich daher an der Erarbeitung der Normen beteiligen, aber nicht mehr an der Abstimmung, ob die Norm von der Normenorganisation angenommen oder abgelehnt werden soll. Es gilt zu sagen, dass eine solche Gewichtung der Stimmen schon vor der Revision der Verordnung (EU) 1025/2012 möglich war.

Ebenfalls als Beobachterin nimmt die Schweiz über die EFTA am «High-Level Forum on European Standardisation» teil. Gemäss der «Strategie Digitale Schweiz» wurden folgende Technologien und Anwendungsbereiche als prioritär festgelegt und könnten von einer Normung profitieren: Immobilienplanung und -bau, Smart City, künstliche Intelligenz usw. Diese Themen werden teilweise auch in der europäischen Normungsstrategie behandelt (s. Rolling Plan for ICT Standardisation).

Darüber hinaus hat der Bundesrat an seiner Sitzung vom 31. August 2022 einen Bericht über die Förderung der Normungsorganisationen im Bereich der Digitalisierung zur Kenntnis genommen. Der Bericht liefert dabei Erkenntnisse, welche einen Beitrag zur Förderung der technischen Normungsarbeit in der Schweiz leisten. Diese Etappe ist entscheidend, damit die Interessen der Schweiz in den europäischen und internationalen Normungsorganisationen koordiniert vertreten werden.

## Bereits ergriffene Massnahmen in der Schweiz

Aus eigener Initiative heraus haben die Schweizerische Normenvereinigung (SNV) und das Eidgenössische Institut für Metrologie (METAS) eine Auslegeordnung angestossen, damit alle Involvierten der Qualitätsinfrastruktur der Schweiz prüfen können, wo aufgrund der Digitalisierung mögliche Synergieeffekte erzielt werden könnten. Das umfasst die Normung, aber auch das Akkreditierungswesen und das legale Messwesen.

Der Direktor der SNV hat sich auf eigene Initiative beworben und wurde von der Generalversammlung für die Amtsperiode 2024/25 in den CEN-Verwaltungsrat gewählt. Diese Ernennung ist als Möglichkeit zu betrachten, die Tätigkeit der Schweiz in den Normungsorganisationen auf europäischer und internationaler Ebene auszuweiten. Durch eine Vertretung der Schweiz in diesen Gremien sollen Impulse für eine stärkere Wahrnehmung ihrer Interessen gesetzt werden.

Massnahme 31

# Strategie für das Web 4.0 und virtuelle Welten

| | |
|---|---|
| **Vollständiger Name der Massnahme** | Strategie für das Web 4.0 und virtuelle Welten |
| **Art der Massnahme** | Strategie |
| **Referenz (falls vorhanden)** | Strategie für das Web 4.0 und virtuelle Welten |
| **Federführung in der Bundesverwaltung** | BAKOM |

## Beschrieb

Die EU-Kommission (KOM) verabschiedete am 11. Juli 2023 eine Strategie für das Web 4.0 und virtuelle Welten. Die Strategie soll dazu beitragen, dass die EU die Chancen der nächsten Generation des World Wide Web nutzen und gleichzeitig ein offenes, sicheres und faires digitales Umfeld für die Bürger/innen und Unternehmen gewährleisten kann. Die Strategie baut auf der Arbeit der Europäischen Kommission zu virtuellen Welten und Konsultationen mit Bürger/innen, Hochschulen und Unternehmen auf. Unter anderem bilden 23 Empfehlungen, die im April 2023 auf einem europäischen Bürgerforum zu virtuellen Welten erarbeitet wurden, die Richtschnur für die Aktionen, die in der Strategie für das Web 4.0 und virtuelle Welten enthalten sind.

Die Strategie basiert auf vier Säulen:

- **Stärkung der Mündigkeit und Kompetenzen der Menschen:** Um die Akzeptanz für technologische Entwicklungen zu fördern und alle Menschen zur Teilhabe zu befähigen, soll sensibilisiert und digitale Kompetenzen gestärkt werden. Die Kommission will unter anderem ein Online-Pool von Spezialist/innen für virtuelle Welt aufbauen, damit die Bürger/innen auf sichere und vertrauenswürdige Informationen zugreifen können. Durch Programme wie *Digitale Europe* oder *Creative Europe* sollen Projekte im Bereich Kompetenzentwicklung für Zielgruppen wie Frauen und Mädchen oder Kunstschaffende gefördert werden.
- **Unternehmen**: Ein europäisches Web 4.0-Industrieökosystem soll gefördert werden. Bis zum ersten Quartal 2024 will die Kommission die Einrichtung einer neuen europäischen Partnerschaft zur Aufstellung eines industriellen und technologischen Fahrplans prüfen. Die Kultur- und Kreativwirtschaft soll im Rahmen von *Creative Europe* bei der Erprobung neuer Geschäftsmodelle in virtuellen Welten unterstützt werden.
- **Behörden**: Virtuelle Welten sollen zur Verbesserung von Sektoren wie dem Gesundheitswesen und öffentlichen Dienstleistungen beitragen. Die Kommission wird im Rahmen von *Horizon Europe* und *Digital Europe Programme* zwei Initiativen unterstützen: „CitiVerse“, eine immersive städtische Umgebung, die für Stadtplanung und -management genutzt werden kann, und einen europäischen virtuellen Zwilling des Menschen, der den menschlichen Körper nachbildet, um die klinische Entscheidungsfindung und die personalisierte Behandlung zu unterstützen.
- **Governance**: In Zusammenarbeit mit Interessenträgern der Internet-Governance in der ganzen Welt sollen Standards für offene und interoperable virtuelle Welten und das Web 4.0 gefördert werden, um sicherzustellen, dass sie nicht von einigen wenigen grossen Akteuren dominiert werden.

## Stand der Dinge

Die Strategie befindet sich in der Umsetzungsphase.

## Mögliche Auswirkungen auf die Schweiz

Aktuell sind für die Schweiz keine Folgen zu erwarten.

## Bereits ergriffene Massnahmen in der Schweiz

Die Schweiz hat in diesem Bereich keine eigenen Massnahmen ergriffen.