Die verpflichtende Einführung eines EU Single Sign-On

Kurzgutachten

im Auftrag der European netID Foundation

vorgelegt von

Professor Dr. Herwig Hofmann

Professor für europäisches und transnationales öffentliches Recht
Universität Luxemburg

Professor Dr. Rolf Schwartmann

Leiter der Kölner Forschungsstelle für Medienrecht an der
Technischen Hochschule Köln und
Mitglied der Datenethikkommission
Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.
Mitglied im Stiftungsrat der European netID Foundation

Rechtsanwalt Steffen Weiß, LL.M.

Mitglied der Geschäftsführung für Internationales bei der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

Januar 2021

Inhaltsverzeichnis

A. Executive Summary

- The discussion about using legislation as tool for regulating market dominance of large platforms has led to political initiatives on the European level in the context of the EU Digital Services Act Package as well as on the national level within EU member states (e.g. the German TTDSG).
- Article 114 TFEU (on the approximation of national laws for the establishment and functioning of the internal market) is a possible legal basis for the introduction of an EU-wide EU-SSO. This requires careful balancing of protected legal values. The measures suggested in this brief expertise have been reviewed for their compliance with the principle of proportionality.
- The Commission's draft Data Governance Act (DGA) does not specifically address an SSO but does contain rules on data sharing services within the requirements of its Article 11. Currently, the eIDAS-Regulation does not contain provisions for the introduction of a mandatory EU-SSO for information society services. Nonetheless, the regulation of an EU-SSO as accepted system of identification, could generally be introduced into the eIDAS-Regulation. Additionally, the eIDAS-Regulation can be used as blueprint for the introduction of a level of technical compatibility between different providers of an EU-SSO. On the other hand, it would appear sub-optimal to provide for a mandatory EU-SSO within the planned e-Privacy-Regulation.
- Legislation introducing a mandatory EU-SSO could contain the following formulation: "Any information-society service that uses one or several SSO-services for user authentication, shall implement an interface to an EU-SSO and offer such EU-SSO to its end-users."

B. Zusammenfassung der wesentlichen Ergebnisse Executive Summary

- Die bisherige Diskussion zur gesetzlichen Regulierung der Marktdominanz großer Plattformen im Rahmen eines EU Digital Services Act hat unter anderem zu politischen Vorstößen im Bereich der elektronischen Kommunikation auf europäischer und nationaler Ebene (vgl. TTDSG in Deutschland) geführt.
- Die EU-weite Einführung eines EU-SSO ist auf der Basis von Artikel 114 AEUV (Rechtsangleichung im Binnenmarkt) möglich. Die Rechtsgüter, die von einer solchen Maßnahme betroffen sind, müssen darin sorgfältig abgewogen werden. Die in diesem Kurzgutachten vorgeschlagenen Regelungen sind in dieser Hinsicht auf ihre Verhältnismäßigkeit geprüft.
- Der Kommissionsentwurf für einen Data Governance Act (DGA) enthält keine ausdrücklichen Regeln zu einem SSO, sieht aber in Artikel 11 Regeln zu einer gemeinsamen Datennutzung vor. Die Einführung eines verpflichtenden EU-SSO für Dienste der Informationsgesellschaft liegt bisher außerhalb der Regelungsziele der eIDAS-Verordnung. Grundsätzlich möglich wäre jedoch die Normierung des EU-SSO als anerkanntes Identifizierungssystem in der eIDAS-Verordnung. Darüber hinaus kann die eIDAS-Verordnung als technische Blaupause für die Einführung einer Kompatibilitätsschicht zwischen verschiedenen Anbietern eines EU-SSO dienen. Es erscheint hingegen nicht sinnvoll, Regeln zur verpflichtenden Einführung eines EU-SSO in einer avisierten e-Privacy-Verordnung vorzunehmen.
- Eine Norm zur verbindlichen Einführung eines EU-SSO könnte folgenden Text beinhalten: „Jeder Dienst der Informationsgesellschaft, der einen oder mehrere SSO-Dienste zur Authentifizierung gegenüber seinem Dienst verwendet, hat eine Schnittstelle zum EU-SSO zu implementieren und diese gegenüber Endnutzern anzubieten.“

C. Anwendungsbereich und Methodik des Gutachtens

Dieses Kurzgutachten umreißt die Möglichkeit und Ausgestaltung einer verpflichtenden Einführung eines EU-SSO für Dienste der Informationsgesellschaft. Hierzu werden die vorgesehenen Parameter für das obligatorische Anbieten eines solchen Systems dargestellt sowie ein vorgestelltes dezentrales Modell eines EU-SSO erläutert (vgl. E.). Sodann werden mögliche Handlungsoptionen nach dem Recht der Europäischen Union aufgezeigt und Abwägungskriterien für deren Ausgestaltung benannt (vgl. E. I. ff). Hieran schließt sich die Darlegung von Regulierungsoptionen in laufenden Gesetzesinitiativen auf EU-Ebene an (vgl. E. IV.). Den Abschluss bilden konkrete Formulierungsvorschläge mit Blick auf die verpflichtende Einführung eines EU-SSO (vgl. E. V. 1.) sowie zur Regulierung von Diensteanbietern, die an einem EU-SSO partizipieren möchten (vgl. E. V. 2.).

D. Einleitung – Die Diskussion um eine verpflichtende Einführung eines EU Single Sign-On

Authentifizierungssysteme versetzen Nutzer in die Lage, sich mit Hilfe eines „digitalen Ausweises“ auf Diensten (Verzeichnisdienste, Websites, Apps etc.) anzumelden.

Bei einem **Single Sign-On (SSO)** können sich Nutzer bei einem SSO-Dienst anmelden und im Weiteren automatisch bei weiteren Diensten der Informationsgesellschaft authentifiziert zu werden. Eine Speicherung und Verwaltung von Zugangsdaten beim Diensteanbieter wird obsolet. Der SSO-Dienst fungiert als eine Art „Datentreuhänder“, also als vertrauenswürdige Stelle, die nach den Vorgaben des EU-Datenschutzrechts Anmeldeinformationen speichern und im Rahmen einer Authentifizierung an den Diensteanbieter übermitteln soll[1]. Zugleich gibt die Stellung als SSO-Dienst aber auch die Möglichkeit, eine Fülle von Daten über ein Nutzerverhalten zu sammeln und zu verwerten.

SSO-Systeme bieten somit eine zentrale Nutzerprofilverwaltung mit zentraler Anmeldefunktionalität und sind nicht nur im E-Commerce zunehmend verbreitet[2]. Eine besondere Rolle im Bereich der Verbreitung von SSO-Diensten nehmen große Online-Plattformen ein (Google, Amazon, Facebook und Apple). Besagte Plattformen verfügen über einen sehr großen Nutzerbestand mit einer regelmäßig angeschlossenen Login-Funktionalität.

Dritte, die ihre Dienste der Informationsgesellschaft für die Öffentlichkeit anbieten, können regelmäßig davon ausgehen, dass potenzielle Nutzer bereits über ein Benutzerkonto bei den großen Online-Plattformen verfügen und verwenden diese Dienste für einen Single Sign-On auf ihren Webseiten.

---

[1] Engelbertz/Erinola/Herring/Somorovsky/Mladenov/Schwernk, Security Analysis of eIDAS – The Cross-Country Authentication Scheme in Europe, Ziff. 2.1 (abrufbar unter https://www.nds.ruhr-uni-bochum.de/media/ei/veroeffentlichungen/2018/12/10/eid-eidas-security.pdf, zuletzt abgerufen am 11.01.2021).

[2] Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 33 Rn. 448.

Der Rückgriff auf eine bestehende Nutzeridentität bei einer großen Online-Plattform im Rahmen eines SSO ist im Übrigen dem Umstand geschuldet, dass eine Registrierung oder die nochmalige Identifizierung eines Nutzers obsolet und Zugangsbeschränkungen damit reduziert werden. Durch das Verwenden von einheitlichen Zugangsdaten werden Nutzer insofern motiviert, Dienste der Informationsgesellschaft in Anspruch zu nehmen. Die Folge ist eine ausgesprochen hohe Marktdurchdringung der großen Plattformen mit Blick auf angebotene SSO-Dienste[3].

Die bestehende Marktsituation bei den Authentifizierungssystemen allgemein sowie den SSO-Diensten im Speziellen erzeugt bei den politischen Entscheidungsträgern verstärkten Handlungsbedarf im Bereich der elektronischen Identität.

Die **Europäische Kommission** sieht das Bedürfnis einer Regelung einer sicheren und vertrauenswürdigen „European e-ID“[4] und hat deren Entwicklung in das Arbeitsprogramm für das Jahr 2021 aufgenommen[5].

Das **Europäische Parlament** empfiehlt in einer Entschließung zum EU Digital Services Act (DSA) und damit einhergehender Grundrechtsfragen[6] die verpflichtende Einführung eines **europäischen Single Sign-On (EU-SSO)**: Online-Plattformen, die einen Single Sign-On-Dienst unterstützen, der über einen dominierenden Marktanteil verfügt, sollen verpflichtet werden, auch mindestens ein offenes Identifizierungssystem zu unterstützen, das auf einem nichtproprietären,

[3] https://www.datanyze.com/market-share/social-login--55 (zuletzt abgerufen am 11.01.2021).

[4] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655 (zuletzt abgerufen am 11.01.2021).

[5] https://ec.europa.eu/info/sites/info/files/2021_commission_work_programme_annexes_en.pdf, Ziff. 8 (zuletzt abgerufen am 11.01.2021).

[6] Entschließung des Europäischen Parlaments vom 20. Oktober 2020 zu dem Gesetz über digitale Dienste sowie über die Grundrechte betreffende Fragen (2020/2022(INI)), Ziff. 22, abrufbar unter https://www.europarl.europa.eu/doceo/document/TA-9-2020-0274_DE.html, zuletzt abgerufen am 11.01.2021).

dezentralisierten und interoperablen Rahmen basiert. Entsprechende Forderungen finden sich ebenfalls in drei Initiativberichten des Europäischen Parlaments zum Digital Services Act.[7]

Auf **mitgliedstaatlicher Ebene** wurde in Deutschland ein Gesetzesentwurf zur Regelung des Datenschutzes und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien (TTDSG-E) vorgelegt[8]. Hierbei sollen anerkannte Dienste zur Verwaltung persönlicher Informationen, wozu auch die Verwaltung einer elektronischen Identität zu zählen ist, reguliert und einem nationalen Anerkennungsverfahren durch eine aufsichtsbehördliche Stelle unterworfen werden[9]. Dieser Ansatz wiederum geht auf eine Empfehlung[10] **der Datenethikkommission (DEK) der Bundesregierung** aus dem Oktober 2019 zurück. Die Kommission hat sich in ihrem Abschlussgutachten im Rahmen ihrer Überlegungen zu Datentreuhandsystemen mit sog. Privacy Management Tools befasst[11], denen sie in Handlungsempfehlung 21 großes Potential attestiert, sofern diese „praxisgerecht, robust und datenschutzkonform“ ausgestaltet sind[12].

Ein Zusammenschluss von **Aufsichtsbehörden** und der **Wirtschaft** im Rahmen des **Digital-Gipfels 2020 der deutschen Bundesregierung** setzt sich mit Datenmanagement- und Datentreuhandsystemen auseinander und stellt diesbezüglich Anforderungen für SSO-Dienste auf[13].

---

[7] Rechtsausschuss: https://www.europarl.europa.eu/doceo/document/A-9-2020-0177_DE.html, Ziff. 20 (zuletzt abgerufen am 11.01.2021); Binnenmarktausschuss: https://www.europarl.europa.eu/doceo/document/A-9-2020-0181_DE.html, Ziff. 5 (zuletzt abgerufen am 11.01.2021); Ausschuss für bürgerliche Freiheiten, Justiz und Inneres: https://www.europarl.europa.eu/doceo/document/A-9-2020-0172_DE.html, Ziff. 22 und 23 (zuletzt abgerufen am 11.01.2021).

[8] Entwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien sowie zur Änderung des Telekommunikationsgesetzes, des Telemediengesetzes und weiterer Gesetze des Bundesministeriums für Wirtschaft und Energie vom 14.07.2020 (TTDSG-E).

[9] § 3 TTDSG-E.

[10] Gutachten der *Datenethikkommission* (2019), Handlungsempfehlung 21.

[11] Gutachten der *Datenethikkommission* (2019), S. 133 ff.

[12] Gutachten der *Datenethikkommission* (2019), Handlungsempfehlung 21.

[13] *Schwartmann/Weiß*, Datenmanagement- und Datentreuhandsysteme - Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2020, S. 31, abrufbar unter

Die bisherige Diskussion einer gesetzliche Regulierung der Marktdominanz großer Plattformen im Rahmen eines EU Digital Services Act erscheint hinsichtlich SSOs nicht hinreichend. Auch politische Vorstöße im Bereich der elektronischen Kommunikation auf nationaler Ebene (vgl. TTDSG) scheinen nicht zuletzt wegen des nur nationalen Regelungsrahmens zu kurz zu greifen.

Umgesetzt werden soll die Idee eines EU-SSO-Angebots dadurch, dass Nutzer auf Dashboards die Einstellungen vornehmen, die von den Diensteanbietern übernommen werden müssen. Um die Vielzahl der Angebote mit den Anfragen der Nutzer zu verknüpfen, bedarf es eines zwischengeschalteten Dienstes, der die Einstellungen des Nutzers treuhänderisch verwaltet, ohne an der Nutzung der Daten zu verdienen. Da der Login zum Zugang zu den Angeboten im Netz dann nicht mehr über die Logins von Facebook, Google, Amazon und zunehmend Apple[14] erfolgt, sondern durch einen europäischen Treuhänder, der sich offenen Standards unterwirft und Daten nach der Vorgabe des EuGH aus Schrems II[15] verarbeitet und speichert, könnten mit diesem Mittel Nutzerinteressen nach europäischen Datenschutzstandards durchgesetzt werden. So wären die nicht europäischen Diensteanbieter, die per Login Nutzerdaten erhalten und auswerten, nur dann berechtigt in Europa ihre Dienste anzubieten, wenn sie sich den europäischen Standards für Datentreuhänder unterwerfen. Dieser Ansatz ist vor dem Hintergrund praktisch sehr bedeutsam, dass der datengetriebene Nutzerkontakt nach der Praxis der großen Browseranbieter bereits heute über die Nutzer-ID erfolgt und nicht mehr durch Cookies oder alternative Methoden wie Fingerprinting.

---

https://www.gdd.de/downloads/aktuelles/sonstiges/Fokusgruppe_Datenschutz-Datenmanagement_Datentreuhandsysteme_V1.0.pdf (zuletzt abgerufen am 11.01.2021).

[14] *Schwartmann*, Apple ID: Ein fairer Schlüssel zum Netz, abrufbar unter https://web.de/magazine/digital/apple-id-fairer-schluessel-netz-34843646 (zuletzt abgerufen am 11.01.2021).

[15] http://curia.europa.eu/juris/document/document.jsf;jsessionid=6BAFF3A6D8468445A0B6FBD4D7DD4C20?text=&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=10013022 (zuletzt abgerufen am 11.01.2021).

E. Szenario eines Europäischen Single-Sign On/gutachterlicher Auftrag

Das Kurzgutachten geht von folgenden Erwägungen aus:

Ein europäisches SSO soll für bestimmte Dienste der Informationsgesellschaft verpflichtend eingeführt werden. Diese Verpflichtung soll sich auf solche Dienste beziehen, die für den Zugang zu ihrem Angebot ein SSO anbieten. Dienste, die lediglich auf ein lokales Authentifizierungssystem des Dienstanbieters, der die Webseite selbst betreibt, zurückgreifen, sollen von einer gesetzlichen Verpflichtung ausgenommen sein.

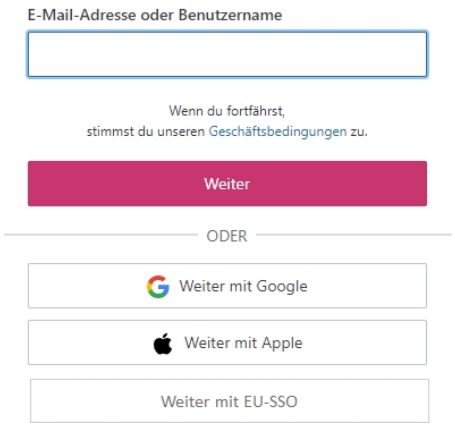

Abb. Illustration einer EU-SSO Implementierung bei einem Dienst der Informationsgesellschaft

Ein solches EU-SSO soll dabei folgende Charakteristika aufweisen:

- Aufbau eines **dezentralen Systems**, mit verschiedenen system-kompatiblen Diensten, das unterschiedliche nationale Lösungen und Initiativen zur Regulierung von SSO-Diensten innerhalb der EU obsolet werden lässt (Interoperabilität).
- Einführung eines **offenen Standards**: SSO-Account-Anbieter können nach einem Zertifizierungsverfahren ein EU-SSO anbieten; hierzu bedarf es der Festlegung von Bedingungen der Zertifizierung („anerkannte SSO-Dienste“, vgl. E. V. 2.).

- Nutzer eines EU-SSO sollen ihre bestehenden Konten verwenden und unter verschiedenen Anbietern wählen können.
- Definition eines **gemeinsamen technischen Standards**, damit jeder SSO-Account bei jedem SSO auf einer Webseite oder App funktioniert.
- Festlegung **klarer Regeln über Neutralität, Transparenz und Datenschutz** für betroffene Anbieter, so dass Nutzer und Unternehmen, die das SSO nutzen, faire und gleiche Nutzungsbedingungen haben.
- **Interoperabilität** mit bestehenden e-Government Authentifizierungssystemen: Ein Authentifizierungssystem für den privaten und den öffentlichen Sektor.

F. Einführung eines verpflichtenden SSO („EU-SSO“)

I. Notwendigkeit einer Rechtsgrundlage für eine rechtsverbindliche EU-Regelung

Um eine europaweite gesetzliche Regelung eines EU-SSO einführen zu können, bedarf es einer Rechtsgrundlage im EU-Recht. Hierbei kommt insbesondere die EU-Binnenmarktkompetenz, die zur Rechtsangleichung auf EU-Ebene und zum Abbau von Wettbewerbsverzerrungen erlaubt, in Frage.

Bestehende und potentielle Unterschiede in nationalen Normen können das Funktionieren des Binnenmarktes gefährden. Dies gilt insbesondere beim elektronischen Handel und der Bereitstellung von Dienstleistungen im Internet als sich entwickelnde Bereiche des Binnenmarktes. In diesen Bereichen wird, wie in der Einleitung zu diesem Kurzgutachten beschrieben, von Webseiten zunehmend ein Sign-On vorausgesetzt.

Rechtsgüter, die bei einer solchen Regelung abzuwägen sind, sind neben nationalen Regelungsbefugnissen, auch die Rechtspositionen der durch eine solche Maßnahme Verpflichteten und Begünstigten. Dabei geht es vor allem einerseits

um Regelungen zur Ausübung der Rechte der Unternehmensfreiheit einschließlich der Vertragsfreiheit, aber auch um Fragen des Verbraucherschutzes und des Schutzes der Privatsphäre und persönlicher Daten.

II. Rechtsgrundlagen für die Regelung im Binnenmarkt

1. Voraussetzungen für die Nutzung des Artikels 114 AEUV als Rechtsgrundlage für die Einführung eines EU-SSO

Artikel 114 AEUV ist die zentrale Norm für die Rechtsangleichung im Binnenmarkt. Diese Norm beinhaltet aber keine allgemeine Regelungskompetenz für alle, den Binnenmarkt betreffenden Fragestellungen. Maßnahmen aufgrund von Artikel 114 AEUV als Rechtsgrundlage können insbesondere auf die **Behebung von Marktbehinderungen gerichtet** sein und dadurch das **Funktionieren des Binnenmarktes verbessern**. Maßnahmen auf dieser Grundlage **können rechtliche oder faktische Markthindernisse** ausräumen, sie müssen jedoch über die Behinderungen hinausgehen, die sich aus schlichten Unterschieden nationaler Regelungen ergeben.

Voraussetzung für die Anwendung von Artikel 114 AEUV als Rechtsgrundlage für die EU-weite Einführung eines verpflichtenden EU-SSO ist demnach die **Notwendigkeit einer Angleichungsmaßnahme für den Binnenmarkt** nach Artikel 26 AEUV. Angleichungsmaßnahmen **räumen unmittelbare und mittelbaren rechtliche oder tatsächliche Hemmnisse** für das Funktionieren des Binnenmarktes aus. Dementsprechend wird die Rechtsgrundlage des Artikels 114 AEUV für harmonisierende Maßnahmen genutzt, die geeignet sind, die Ausübung der Grundfreiheiten des Binnenmarktes zu fördern.

a. Abbau rechtlicher Hindernisse für den Binnenmarkt

Beispiele für das Ausräumen **rechtlicher Hindernisse** finden sich bei einer Vielzahl von Richtlinien zur Harmonisierung des Verbraucherschutzrechts. Sie erlauben zum Beispiel, Zugangshindernisse von Verbrauchern bei einem grenzüberschreitenden Kauf von Waren und Dienstleitungen abzubauen und eventuelle Wettbewerbsverzerrungen zu reduzieren.

Ähnlich liegt es bei der Harmonisierung von SSO-Standards durch die Einführung eines EU-SSO. Eine solche Maßnahme erlaubt auch kleineren Anbietern einen Markteintritt in grenzüberschreitende Märkte, weil so eine gesteigerte Rechtssicherheit über die anzuwendenden Schutzstandards erreicht wird.

b. Abbau tatsächlicher Hindernisse für den Binnenmarkt

Im Rahmen des Abbaus **tatsächlicher Hindernisse** für den Binnenmarkt kann Artikel 114 AEUV auch zum Abbau von Verzerrungen des Binnenmarktes durch unterschiedliche Regeln und Marktzugangsschranken als Rechtsgrundlage genutzt werden. So können durch Einführung eines EU-SSO bestehende Marktverzerrungen potentiell abgebaut werden. Ein für den gesamten Binnenmarkt zertifiziertes EU-SSO zur Anmeldung auf Webseiten würde somit potenziell Zugangsmöglichkeiten zu Webseiten in der Union erleichtern. Nutzer müssten sich nicht für jede Webseite mit verschiedenen Passwörtern und Einwahldaten ausweisen. Gleichzeitig wäre die Sicherheit für die Betreiber von Webseiten erhöht, indem die tatsächliche Identität der Nutzer bereits geklärt wäre, unabhängig vom Ort der Einwahl. Die Möglichkeit, sich als Nutzer leichter und sicherer grenzüberschreitend auf Webseiten zu identifizieren ist für eine Vielzahl von Anwendungen notwendig und stärkt das Vertrauen aller Handelspartner, wie die bereits festzustellende Verbreitung von SSOs im Internet zeigt. Die europaweite Einheitlichkeit der Identitätsnachweise und ihr grenzüberschreitender Einsatz von Internetnutzern wie für Webseitenbetreiber ist also ein Element zur Stärkung des elektronischen Binnenmarktes.

c. Abbau von Wettbewerbsverzerrungen

Obwohl nicht ausdrücklich genannt, werden auch im Wettbewerbsrecht Spezialnormen wie Artikel 103 und 109 AEUV primär für die Rechtsangleichung von Verfahrensnormen zur öffentlichen Durchsetzung des Wettbewerbsrechts genutzt. Rechtsangleichung zur Verhinderung von Wettbewerbsverzerrungen hingegen wird in der Praxis des EU-Rechts nach Artikel 114 AEUV vorgenommen.

d. Harmonisierung unterschiedlicher Regelungsstandards

Schließlich kann das Bestehen von unterschiedlichen Regelungsstandards in verschiedenen Mitgliedstaaten oder deren bevorstehende Schaffung eine Maßnahme nach Artikel 114 AEUV erlauben. Unterschiedliche Regelungsstandards in verschiedenen Mitgliedstaaten können de facto zu einer Zersplitterung des EU-Binnenmarktes führen, weil Verbraucher aus anderen Mitgliedstaaten meist nicht über einen Zugang zu einem nationalen SSO, zum Beispiel in Form einer nationalen e-ID, für die Authentifizierung bei einer Webseite in einem anderen Mitgliedstaat verfügen würden.

In diesem Zusammenhang können sowohl das Fehlen von nationalen Regelungen in einigen Mitgliedstaaten als auch die geplanten Vorschriften in anderen Mitgliedstaaten (beispielsweise im Rahmen eines Entwurfs zum deutschen TTDSG) zu unterschiedlichen anwendbaren Rechtsnormen im Binnenmarkt führen. Diese Unterschiede, die rechtlich und tatsächlich Hürden für einen grenzüberschreitenden Handel mit Waren und Dienstleistungen im elektronischen Binnenmarkt schaffen würden, wären dann ein möglicher Gegenstand der Rechtsangleichung; dies insbesondere, wenn sich daraus eine Aufsplitterung und eine Gefahr für die Entwicklung des Binnenmarktes ergeben könnte. Keine Identifizierungs- bzw. Authentifizierungsmöglichkeiten im grenzüberschreitenden Handel zur Verfügung zu haben, kann somit insbesondere als ‚Behinderung des Marktzugangs gewertet werden.

2. Zwischenergebnis

Zusammenfassend kann daher festgestellt werden, dass die Einführung eines EU-SSO auf der Basis von Artikel 114 AEUV zur Rechtsangleichung im Binnenmarkt möglich ist.

III. Regelungsgehalt auf der Gesetzgebungsebene statt durch delegierte Rechtsakte oder Umsetzungsakte

Bei einem Entwurf einer Rechtsangleichung nach Artikel 114 AEUV müssen die Fragestellungen der möglichen Art und Weise sowie des Umfangs der Rechtsangleichung erörtert werden. Hierbei sind insbesondere Gesichtspunkte des Subsidiaritätsprinzips und der Verhältnismäßigkeit zu berücksichtigen.

1. Subsidiarität

Die Binnenmarktharmonisierung nach Artikel 114 AEUV gibt eine nach Artikel 4(2) a) AEUV geteilte Zuständigkeit vor und muss daher nach Subsidiaritätsgesichtspunkten betrachtet werden. Gleichwohl kann aber nur eine Maßnahme der Union und nicht einzelner Mitgliedstaaten eine nach Artikel 114 AEUV erforderliche Rechtsangleichung zur Erleichterung und zum Funktionieren des Binnenmarktes erreichen. Ob eine Maßnahme in der Sache besser durch Mitgliedstaaten oder auf EU-Ebene geregelt werden kann, ergibt sich schon aus der Prüfung der Anwendungsvoraussetzungen des Artikel 114 AEUV. Daher ist mit Blick auf die Subsidiarität die Frage nach dem Regelungsgegenstand weniger bedeutsam als die nach der „Regelungstiefe“ auf Unionsebene.

a. Rechtsformenwahl

Zwar wird eine Maßnahme der Rechtsangleichung grundsätzlich in Form von einer Richtlinie erlassen. Allerdings ist auch der Weg über eine Verordnung möglich, wenn eine vollständige Vereinheitlichung nach dem begründeten Ermessen des Unionsgesetzgebers notwendig erscheint.

b. Regelungstiefe auf EU-Ebene

Neben der Rechtsform ist aber auch die Frage zu klären, wie detailliert eine Regelung auf Unionsebene erfolgt, welche Bestandteile ihr als nicht-essentielle Elemente der Gesetzgebung an die Kommission zum Erlass in Form von delegierten Rechtsakten (Artikel 290 AEUV) übertragen werden können und wie viel Freiheit den Mitgliedstaaten bei Umsetzung der unionsrechtlichen Regelungen (Artikel 291(1) AEUV) gegenüber dem Erfordernis „einheitlicher Bedingungen für die

Durchführung der verbindlichen Rechtsakte der Union“, die durch die Kommission in Durchführungsakten erlassen werden, verbleiben. Dies ist im Einzelnen in dem auf Artikel 114 AEUV basierenden Unions-Gesetzgebungsakt zu regeln.

In Anbetracht der Details zu einem EU-SSO dürften einheitliche EU-Durchführungsregeln zur Natur des SSO und zu den Fragen der Zertifizierung von SSO-Anbietern erforderlich sein. Ein solcher Durchführungsrechtsakt kann daher auch die Frage der Bedingungen der Ermächtigung privater Zertifizierungsstellen und privater EU-SSO Anbieter regeln und dazu detaillierte Regeln enthalten. Der EU-Gesetzgeber hat aber auch weitgehendes Ermessen zur Delegation von Maßnahmen an die Kommission sowie an private Zertifizierungsstellen.

2. Verhältnismäßigkeit

Um dem Verhältnismäßigkeitsprinzip zu genügen, muss eine Maßnahme nach Artikel 114 AEUV nicht nur geeignet sein, den Binnenmarkt zu fördern, sondern sie muss auch erforderlich sein, also die Rechtspositionen Anderer möglichst gering belasten.

Zu beachten sind zwei Typen von Rechtspositionen. Zum einen stellt sich – ähnlich wie bei der Subsidiaritätsprüfung – die Frage nach Eingriffen in die Regelungshoheit von Mitgliedstaaten. Hier ist insbesondere die Frage nach der Notwendigkeit von Voll- oder Teilharmonisierung zu stellen.

Zum anderen sind individuelle Grundrechte einzelner Marktteilnehmer einzubeziehen. Insbesondere ist es hierbei zu berücksichtigen, dass Maßnahmen aufgrund von Artikel 114 AEUV ein hohes Schutzniveau in Bezug auf eine Reihe von Gütern, unter anderem bei Sicherheit und Verbraucherschutz erfordern (Artikel 114(3) AEUV).

a. Voll- oder Teilharmonisierung, Pilotprojekte

Die Frage nach der Notwendigkeit von Voll- oder Teilharmonisierung auf europäischer Ebene ist entsprechend den Erfordernissen des Regelungsgegenstandes

zu beantworten – hier des Zugangs zu Webseiten im Binnenmarkt, die eine Nutzeridentifizierung bzw. -authentifizierung benötigen. Teilharmonisierung erlaubt Mitgliedstaaten in den Bereichen, in denen sie Regelungsbedarf sehen, weitere Maßnahmen zu ergreifen. Vollharmonisierung regelt einen spezifischen Lebenssachverhalt abschließend, unter Verdrängung der nationalen Regelungskompetenz.

Grundsätzlich erlaubt Artikel 114(1) AEUV dort, wo die Schaffung des Binnenmarktes dies erfordert, eine Vollharmonisierung. Mitgliedstaatliche Regelungsbefugnisse treten nach dem Regelungsgedanken des Artikels 4 AEUV hinter die Regelungsbefugnisse der Union zurück, wenn die Union von ihrem Recht der Regelung Gebrauch macht und nach Artikel 2(2) AEUV nehmen die Mitgliedstaaten „ihre Zuständigkeit wahr, sofern und soweit die Union ihre Zuständigkeit nicht ausgeübt hat."

Soweit also notwendige Regelungen zu Fragen der Natur eines SSO und der Zertifizierung von EU-SSO-Diensten vorgesehen sind, stehen den Mitgliedstaaten keine Regelungsbefugnisse zu, die gegenüber der Union geltend gemacht werden können.

Möglich erscheint aber nach Artikel 114 AEUV auch die Schaffung von Pilotprojekten in einer ersten Phase der Schaffung von EU-SSOs, die bspw. nur einzelne Mitgliedstaaten betrifft, sofern die Mitgliedstaaten hierin einwilligen. Dabei dürfen aber inzident keine neuen Hindernisse für das Funktionieren des Binnenmarktes geschaffen werden.

b. Schutzniveau, Grundrechte und Grundfreiheiten

Rechtsangleichung muss sich grundsätzlich an den Werten der Union orientieren. Dabei sind einige spezifische Beispiele in „Horizontalklauseln"' wie Sicherheit und der Schaffung eines hohen Verbraucherschutzniveaus in Artikel 114 (3) AEUV ausdrücklich genannt. Entsprechend verweist die Verbraucherschutznorm im AEUV (Artikel 169 AEUV) auf Artikel 114 AEUV als anwendbare Rechtsnorm.

In diesem Zusammenhang müssen die EU-Institutionen bei Maßnahmen einer Rechtsangleichung ein hohes Verbraucherschutzniveau anstreben.

Neben den in Artikel 114(3) AEUV genannten Horizontalklauseln sind aber auch andere sogenannte „Querschnittsklauseln“ des EU-Vertrags anwendbar. Dazu ist auch ein hohes Datenschutzniveau zu zählen, das sich nicht nur aus Artikel 16 AEUV, sondern auch aus den Artikeln 7 und 8 der EU-Grundrechtecharta ergibt. Die Sicherstellung eines standardisierten und hohen europäischen Datenschutzniveaus ist dabei sowohl als eine Maßnahme zur Erhöhung der Sicherheit des elektronischen Geschäftsverkehrs als auch zum Schutz der daran teilnehmenden Verbraucher geeignet. Soweit Vorschriften über die Rechtsangleichung auch Fragen des Datenschutzes betreffen, liegt mit Artikel 16 AEUV eine Spezialnorm zur Schaffung von EU-Datenschutzrecht vor, sie steht nach allgemeinem Verständnis nicht in einem Verhältnis der Spezialität zu Artikel 114 AEUV. Zwar kann, soweit die Querschnittskompetenz für den Binnenmarkt ein hohes Datenschutzniveau anstrebt, auch Artikel 16 AEUV als Rechtsgrundlage für eine Harmonisierungsmaßnahme mit herangezogen werden. Gemeinhin ist aber für Maßnahmen der EU, die primär der Rechtsangleichung dienen und sekundär dabei auch ein hohes Datenschutzniveau anstreben, Artikel 114 AEUV als Rechtsgrundlage anwendbar. Die Maßnahmen, die dabei ergriffen werden, müssen ihrerseits ein hohes Datenschutzniveau sicherstellen.

Diese Erwägungen zu Schutzstandards von Horizontalklauseln sind damit auch bei Überlegungen zur Verhältnismäßigkeit einer EU-SSO Regelung einzubeziehen.

Im Übrigen kann eine Beschränkung der „Unternehmerischen Freiheit“ (Artikel 16 der EU-Grundrechtecharta) und in diesem Rahmen auch der Vertragsfreiheit von Anbietern von Webseiten als auch von Anbietern von SSO-Lösungen im EU-Binnenmarkt durch oder aufgrund gesetzlicher Regeln, die den Wesensgehalt der Grundrechte achten, im Rahmen der Abwägung mit anderen Grundrechten

oder zur Sicherstellung von Allgemeinwohlinteressen verhältnismäßig eingeschränkt werden (Artikel 52(1) EU-Grundrechtecharta). Zwar können SSO-Dienste aus Sicht von digitalen Diensten als kritische Komponenten in der Kundenbeziehung angesehen werden und damit der Ausübung der Unternehmensfreiheit unterfallen. Insbesondere eine mögliche Verpflichtung des Zur-Verfügung-Stellens zumindest eines EU-SSOs neben anderen dürfte als besonders milde Einschränkung der unternehmerischen Freiheit angesehen werden, da die Nutzung eigener oder anderer, nicht zertifizierter SSOs, weiterhin möglich wäre.

Ein offener Standard, mit vergleichbarer Reichweite und gesetzlich als Alternative zu den „GAFA-Logins“ wirksam implementiert, würde europäischen Nutzern zudem die Freiheit geben, nicht mehr Logins zu nutzen, die nicht nach EU Standards datenschutzrechtlich zertifiziert wären, um sicheren und komfortablen Zugang zur wachsenden Anzahl von digitalen Diensten, Inhalten und öffentlichen Dienstleistungen zu erhalten. Hinzu kommt, dass die wachsende Nutzungsintensität von Logins die Markmacht der marktbeherrschenden Plattformen weiter erhöht. Die **obligatorische Einführung** eines offenen und interoperablen SSO-Systems auf Basis verbindlicher Standards zur europäischen ID-Anmeldung für digitale Dienste und nachgelagerte Dienste könnte dazu beitragen, die Abhängigkeit von den Anmeldediensten der GAFAs zu verringern und dem **Nutzer die Wahl eines alternativen EU-Login zu** Diensten oder Plattformen zu öffnen, die gegenwärtig zur Identifizierung und/oder Authentifizierung weiterhin auch ein Login mit Google, Amazon, Facebook oder Apple anbieten.
Datenschutz, Verbraucherschutz, Sicherheit auf dem Markt sind als Gemeinwohlinteressen der Union anerkannt und können damit die Einschränkung der Unternehmensfreiheit erlauben. Schließlich ist bei der Abwägung verhältnismäßiger Eingriffe in Grundrechte und Freiheiten nicht außer Acht zu lassen, dass eine EU-weite Einführung eines EU-SSO eine Maßnahme wäre, die insbesondere die Dienstleistungsfreiheit im Binnenmarkt schwächer einschränkt, als dies bei einer Vielzahl von eventuell nicht kompatiblen Regeln auf nationaler Ebene der Fall wäre.

3. Räumlicher Anwendungsbereich

Der räumliche Anwendungsbereich eines verpflichtenden Angebots von EU-SSOs für alle auf Nutzer im EU-Binnenmarkt ausgerichtete Webseiten kann durch das EU-Recht so ausgestaltet werden, dass keine rechtswidrigen extraterritorialen Anwendungen des EU-Rechts entstehen. Im Internetrecht ist anerkannt (siehe nachfolgend der räumliche Anwendungsbereich der EU-Datenschutz-Grundverordnung), dass der Anknüpfungspunkt für eine Regelung nicht nur das Auswirkungsprinzip sein kann – eine Wirkung des Internetauftritts im Territorium der EU und des Binnenmarkts. Auch das gezielte Werben um in der EU ansässige Nutzer oder solche Nutzer, die sich von der EU aus in Dienste einwählen, ist eine Handlung, die sich im EU-Territorium auswirkt. Eine solche auf den Binnenmarkt ausgerichtete Tätigkeit lässt sich zum Beispiel an der Zulassung von Nutzern mit EU-URLs zu im Internet angebotenen Diensten festmachen. Sie ist aber auch durch die Nutzung von in spezifischen Sprachversionen gestalteten Webeseiten und der Nutzung spezifischer Länderkennungen oder eines EU-Domains anzunehmen.

Eine spezifische Regelung zum räumlichen Anwendungsbereich, die als Anregung dienen kann, ist in der EU-Datenschutz-Grundverordnung (DSGVO) vorhanden. Die DGSVO findet nach ihrem Artikel 3 nicht nur Anwendung auf eine Datenverarbeitung, die im „Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet“ (Artikel 3(1) DSGVO), sondern auch auf „Daten von betroffenen Personen, die sich in der Union befinden“ (Artikel 3(2) DSGVO) und auf eine Verarbeitung, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht, „Personen in der Union Waren oder Dienstleistungen anzubieten“. Entsprechende Regelungen zum räumlichen Anwendungsbereich können auch im Rahmen einer EU-SSO- Regelung eingeführt werden, um den räumlichen Anwendungsbereich völkerrechtskonform auszuweisen und keine rechtlich problematische Extraterritorialität entstehen zu lassen.

IV. Mögliche Regulierungsoptionen in bestehenden Gesetzgebungsinitiativen auf EU-Ebene

1. eIDAS-Verordnung

a. Überblick

Die eIDAS-Verordnung[16] verfolgt das Ziel, die Interoperabilität zwischen nationalen Identifizierungssystemen zu erleichtern[17] und ein angemessenes Sicherheitsniveau bei elektronischen Identifizierungsmitteln und Vertrauensdiensten sicherzustellen. Hierzu legt sie Bedingungen fest, unter denen die Mitgliedstaaten elektronische Identifizierungsmittel für natürliche sowie juristische Personen, die einem notifizierten Identifizierungssystem eines anderen Mitgliedstaats unterliegen, anerkennen (Art. 6 bis 12).

Bürgerinnen und Bürgern soll es ermöglicht werden, mit ihren eigenen elektronischen Identitäten, Online-Dienste in anderen EU-Ländern nutzen zu können. Bestehende Hindernisse bei der grenzüberschreitenden Verwendung elektronischer Identifizierungsmittel im Rahmen der Authentifizierung zumindest für öffentliche Dienste in anderen Mitgliedstaaten sollen beseitigt werden. Insofern verfolgt die eIDAS-Verordnung lediglich den Ansatz gewünschter Synergieeffekte von notifizierten Identifizierungsmitteln und ihrer freiwilligen Übernahme durch die Privatwirtschaft[18]. Gerade mit Blick auf die Einbeziehung des privaten Sektors in die Regeln der eIDAS-Verordnung besteht aus Sicht der EU-Kommission weiter Verbesserungsbedarf[19]. Die Verordnung verfolgt im Übrigen ausdrücklich nicht das Ziel, in bestehende elektronische Identitätsmanagementsysteme und einer zugehörigen Infrastruktur in den Mitgliedstaaten einzugreifen[20].

---

[16] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung).

[17] ErwG 9 eIDAS-Verordnung.

[18] ErwG 17 S. 1 eIDAS-Verordnung.

[19] Vgl. https://ec.europa.eu/digital-single-market/en/news/digital-identity-and-trust-commission-launches-public-consultation-eidas-regulation (zuletzt abgerufen am 11.01.2021).

[20] ErwG 12 eIDAS-Verordnung.

Die im Rahmen der eIDAS-Verordnung bisher notifizierten Identitätssysteme basieren auf hoheitlichen Identitätsdokumenten, aus denen digitale Identitäten unmittelbar oder mittelbar (z.B. zum Einsatz auf Mobiltelefonen) abgeleitet werden[21]. Vereinzelt werden solche Systeme auch auf Basis privater Initiativen gemeldet[22]. Sie bilden jedoch weiterhin die Ausnahme. Hinsichtlich ihres Sicherheitsniveaus gewährleisten die notifizierten Systeme mehrheitlich einen zumindest hohen Vertrauensschutz.

Neben einem Anerkennungsmechanismus für elektronische Identifizierungsmittel legt die eIDAS-Verordnung Regeln für Vertrauensdienste, so insbesondere zu elektronische Transaktionen fest (Art. 13 bis 45). Nach Art. 3 Nr. 16 der eIDAS-Verordnung ist ein Vertrauensdienst ein elektronischer Dienste, der in der Regel gegen Entgelt erbracht wird und aus der Erstellung, Überprüfung und Validierung von elektronischen Signaturen, Zeitstempeln, Siegeln und Zertifikaten besteht. Ebenso gelten als Vertrauensdienste solche Anbieter, die die Erstellung, Überprüfung und Validierung für die Website-Authentifizierung, die Zustellung elektronischer Einschreiben oder die Bewahrung von elektronischen Signaturen, Siegeln oder Zertifikaten betreffen.

Die Mitgliedstaaten können weiterhin nationale Vorschriften für Vertrauensdienste beibehalten und einführen, soweit diese durch die eIDAS-Verordnung nicht vollständig harmonisiert sind[23]. Entsprechend kommt der Anwendungsvorrang der Verordnung nur in Betracht, soweit eine grenzüberschreitende Verwendung der Vertrauensdienste in Frage steht[24]. Die Verordnung legt auch einen Rechtsrahmen für elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Dokumente, Dienste für die Zustellung elektronischer Einschreiben und Zertifizierungsdienste für die Website-Authentifizierung fest[25].

---

[21] ABl. OJ C 116 vom 8.4.2020, S. 7–10.
[22] https://www.spid.gov.it/ (zuletzt abgerufen am 11.01.2021).
[23] ErwG 24 eIDAS-Verordnung.
[24] Vgl. *Roßnagel*, MMR 2015, 359 (361).
[25] Art. 1 lit. c eIDAS-Verordnung.

b) Regulierung von SSO-Diensten

Die eIDAS-Verordnung reguliert keinen eigenständigen SSO, sondern stellt auf technischer Ebene eine Kompatibilitätsschicht zwischen einzelnen nationalen Identitätslösungen, so auch bspw. einem SSO, bereit. Hierzu werden eIDAS-Nodes eingesetzt, die den Informationsaustausch im Sinne der eIDAS-Verordnung und ihrer technischen Spezifikationen ermöglichen[26].

Mit Blick auf einen SSO-Dienst als nationale Lösung für eine elektronische Identität (e-ID), würde mittels eIDAS grundsätzlich eine **Interoperabilität zu anderen e-ID-Lösungen** in anderen Mitgliedstaaten der Europäischen Union hergestellt werden können. Der Aspekt einer verpflichtenden Einführung ist aktuell nicht von der Verordnung vorgesehen. Zwar zielt ein EU-SSO auch darauf ab, grenzüberschreitend eingesetzt zu werden, die Notifikation dieses Systems ist jedoch keine aus der eIDAS-Verordnung abzuleitende Pflicht.

Die Entscheidung, alle, einige oder keines der elektronischen Identifizierungssysteme der Kommission zu notifizieren, die auf nationaler Ebene zumindest für den Zugang zu öffentlichen Online-Diensten oder bestimmten Diensten verwendet werden, ist Sache der Mitgliedstaaten[27]. Insofern ist dieser Grundsatz der Verordnung mit dem avisierten Vorhaben eines verpflichtenden europäischen SSO **inkompatibel**.

Allerdings wäre eine Berücksichtigung eines EU-SSO in der eIDAS-Verordnung dergestalt denkbar, dass dieser Single Sign-On als **anerkanntes europäisches Identitätssystem** keiner Notifikation durch die Mitgliedstaaten bedarf, um Anerkennung in den übrigen Mitgliedstaaten bei der Inanspruchnahme von Verwaltungsleistungen oder anderer Dienstleistungen zu genießen. Damit könnte er-

[26] Vgl. eIDAS Interoperability Architecture (Version 1.2) vom 31.08.2019, abrufbar unter https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Interoperability%20Architecture%20v.1.2%20Final.pdf (zuletzt abgerufen am 11.01.2021).

[27] ErwG 13 S. 3 eIDAS-Verordnung.

reicht werden, dass ein EU-SSO nicht nur im Bereich der Privatwirtschaft Anwendung findet, sondern auch im Bereich eines **grenzüberschreitenden e-Governments**.

2. Zwischenergebnis

Die Einführung eines verpflichtenden EU-SSO für Dienste der Informationsgesellschaft liegt bisher außerhalb der Regelungsziele der eIDAS-Verordnung. Möglich wäre jedoch die zukünftige Normierung des EU-SSO als **anerkanntes Identifizierungssystem** in der eIDAS-Verordnung, bspw. zur Inanspruchnahme von grenzüberschreitenden Verwaltungsleistungen oder anderer Dienstleistungen in den Mitgliedstaaten.

Hierbei gilt es zu bedenken, dass Hintergrund der Verabschiedung der Verordnung die Anerkennung vorhandener e-ID-Lösungen in den Mitgliedstaaten war, ohne in vorhandene Identifikationssysteme einzugreifen. Ein europäisches SSO wäre demgegenüber Dienst, der zwar interoperabel sein soll, d.h. bestehende SSO-Anbieter können sich in das System des EU-SSO eingliedern, dies allerdings auf Basis eines **zentral gesteuerten Anerkennungsverfahrens**.

Die eIDAS-Verordnung bietet zum jetzigen Stand bereits dergestalt eine Blaupause für ein EU-SSO, indem sie Vorgaben für die Anerkennung von Identifikationsmitteln enthält. Für einen solchen Prozess bedarf es u.a. der **Festlegung technischer Spezifikationen** für das Herstellen einer Kompatibilitätsschicht zwischen den verschiedenen EU-SSO-Anbietern. Hier legt die eIDAS-Verordnung mit Blick auf die eingerichteten Nodes diverse Blickrichtungen frei.

3. Digital Services Act Package

a. Überblick

Mit dem Digital Services Act (DSA)[28] und dem Digital Markets Act (DMA)[29] möchte die Kommission einen neuen **Rechtsrahmen für Dienste der Informationsgesellschaft** schaffen. Bisher wurden die rechtlichen Rahmenbedingungen für solche Dienste in der e-Commerce Richtlinie aus dem Jahr 2000 festgelegt[30]. Insbesondere mit Blick auf „dominierende" Online-Plattformen sieht die EU-Kommission nunmehr einen gesetzgeberischen Handlungsbedarf. Die Dominanz solcher Plattformen zeige sich in verschiedenen Bereichen, so unter anderem in einer Art **Wächterrolle (sog. „Gatekeeper")**, die es ihnen ermögliche, eigene Strukturen zwischen Unternehmen und Verbrauchern zu betreiben. Wettbewerber hätten kaum eine Möglichkeit, mit besagten Plattformen zu konkurrieren[31]. Auch ein Zugriff auf eine Vielzahl personenbezogener Daten sei mit dieser Rolle verknüpft [32].

Insofern zielt der Vorschlag der Kommission für ein Gesetzespaket darauf ab, einen sichereren digitalen Raum zu schaffen, in dem die Grundrechte aller Nutzer digitaler Dienste geschützt sind. Daneben sollen gleiche Wettbewerbsbedingungen geschaffen werden, um Innovation, Wachstum und Wettbewerbsfähigkeit, sowohl im europäischen Binnenmarkt als auch weltweit zu fördern[33]. Der DMA

---

[28] European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final.

[29] European Commission, Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final.

[30] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr").

[31] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services (zuletzt abgerufen am 11.01.2021).

[32] European Commission, Inception Impact Assessment for the Digital Services Act package, Ares(2020)2877647 vom 04.06.2020, S. 2.

[33] https://ec.europa.eu/digital-single-market/en/digital-services-act-package (zuletzt abgerufen am 11.01.2021).

möchte Betreiber zentraler digitaler Plattformen als besagte „Gatekeeper“ identifizieren und Verpflichtungen und Verbote für solche Dienste formulieren, um unlautere Geschäftspraktiken zu verhindern. Dies beinhaltet das Verbot der Diskriminierung zugunsten eigener Dienste (Art.6 Abs. 1 lit. d DMA), eine Gewährleistung der Interoperabilität mit der eigenen Plattform (Art. 6 Abs. 1 lit. c und f. DMA) und Vorgaben zur Teilung von Daten (Art. 6 Abs. 1 lit. i DMA).
Demgegenüber sollen mittels des DSA verschiedene Intermediäre im Bereich der digitalen Dienste reguliert werden. So werden, unter anderem, Regeln zur Haftung, bezogen auf Informationen Dritter, die weitergegeben und gespeichert werden, aufgestellt (Kapitel II). Ebenso werden unterschiedlichste Sorgfalts- und Transparenzverpflichtungen formuliert, wobei diese von der Stellung und der Dienstleistung des jeweiligen Intermediärs abhängig gemacht werden (Kapitel III). Ferner finden sich im DSA Regeln zur Implementierung und Durchsetzung der Verordnung an sich (Kapitel IV).

b. Regulierung von SSO-Diensten

Weder im Entwurf für einen DSA, noch für einen DMA, finden sich Hinweise auf eine Regulierung von SSO-Diensten. Allerdings sieht der DMA eine gesetzliche Regelung zu einem Identifizierungsdienst eines „Gatekeepers“ vor (Art. 5 lit. e DMA). Die Nutzung, das Anbieten solcher Dienste oder eine Interaktion mit selbigen darf für Geschäftskunden solcher Plattformen nicht verpflichtet sein. Ziel der Regelung ist das Einwirken auf die Marktdominanz großer Plattform, einschließlich ihrer angeschlossenen Dienste. Das Bedürfnis einer Regelung einer sicheren und vertrauenswürdigen „European e-ID“ geht damit nicht einher, wird jedoch seitens der Kommission ohne direkten Verweis auf einen DSA erwähnt[34] und in das Arbeitsprogramm der Kommission für das erste Quartal 2021 in Form eines Gesetzesentwurfs aufgenommen[35]. Seitens des EU-Parlaments findet sich

[34] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655 (zuletzt abgerufen am 11.01.2021).

[35] https://ec.europa.eu/info/sites/info/files/2021_commission_work_programme_annexes_en.pdf, Ziff. 8 (zuletzt abgerufen am 11.01.2021).

in einer Entschließung zum DSA und damit einhergehender Grundrechtsfragen ein expliziter Verweis auf SSO-Dienste[36].

Als ein neuer Rechtsrahmen für Dienste der Informationsgesellschaft wäre das Gesetzespaket zum Digital Service Act grundsätzlich **geeignet**, ein europäisches SSO zu regeln. Immerhin sollen, ausweislich des vorgelegten Szenarios für ein EU-SSO (vgl. D.), Dienste der Informationsgesellschaft und damit Intermediäre verschiedener Art und Größe - verpflichtet werden, einen europäischen SSO anzubieten, sollten sie einen SSO-Login zu ihren Diensten gestatten. Das Anbieten eines EU-SSO wäre dann eine weitere Pflicht für Dienste der Informationsgesellschaft, respektive der großen Online-Plattformen, die durch das Digital Service Package formuliert würde. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit (vgl. Abwägungen unter E.), kann eine solche Verpflichtung insoweit das **reibungslose Funktionierens des Binnenmarktes** gewährleisten. Dies war bereits eines der erklärten Ziele der e-Commerce Richtlinie[37] und findet sich im Digital Services Act entsprechend wieder[38].

Unerlässlich wäre jedoch eine vorzunehmende **Abgrenzung** zur geplanten European e-ID der Kommission, die insoweit eine zentrale Identität darstellen soll. Bei vorgesehenen EU-SSO geht es jedoch nicht um die Regulierung einer europäischen Identität, sondern vielmehr um einen interoperablen SSO-Standard, an dem Anbieter von SSO-Diensten partizipieren können.

4. ePrivacy

Der durch die ePrivacy-Richtlinie[39] bezweckte Schutz personenbezogener Daten im Bereich der elektronischen Kommunikation sowie die Ermöglichung eines

---

[36] Entschließung des Europäischen Parlaments vom 20. Oktober 2020 zu dem Gesetz über digitale Dienste sowie über die Grundrechte betreffende Fragen (2020/2022(INI)), Ziff. 22.

[37] Vgl. bereits ErwG 10 S. 1 Richtlinie 2000/31/EG.

[38] European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final, ErwG 106.

[39] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

freien Verkehrs dieser Daten entfaltet seine Regelungswirkung hinsichtlich der SSO-Dienste vorrangig dann, wenn Nutzer solche Dienste tatsächlich in Anspruch nehmen und Daten entsprechend preisgegeben werden. Die Pflicht zum Anbieten eines EU-SSO ist jedoch ein der Datenverarbeitung vorgelagerter Zustand. Daher wäre es **wenig sinnvoll**, Regeln zur verpflichtenden Einführung eines EU-SSO in einer avisierten e-Privacy-Verordnung vorzunehmen. Eine e-Privacy-Verordnung könnte jedoch solche Dienste dergestalt adressieren, als dass Nutzer diese auf Basis einer Einwilligung und unter Wahrung von Informationspflichten nutzen können[40]. Ebenso kann durch die anstehende e-Privacy-Verordnung adressiert werden, dass die Erbringung eines Telemedien- oder elektronischen Kommunikationsdienstes nicht von einer Verwaltung persönlicher Informationen, abseits der jeweiligen Identität, abhängig gemacht werden darf. Dies Maßgabe kann das Vertrauen in ein EU-SSO stärken, der insoweit umfangreiche zentrale Datenpools vermeiden möchte.

5. Data Governance Act

Mit dem Vorschlag eines Data Governance Act (DGA)[41] möchte die EU-Kommission einen Rechtsrahmen für die Governance gemeinsamer europäischer Datenräume schaffen[42]. Hierdurch sollen Daten für eine Nutzung verschiedener Akteure verfügbar gemacht und ihre Nutzung insofern gefördert werden. Eine wichtige Rolle spielen hierbei sog. „Datenmittler“, die als Schnittstelle zwischen den datenverwendenden Stellen fungieren sollen. Ausgangspunkt einer gemeinsamen Datennutzung bilden Daten des öffentlichen Sektors zur Weiterverwendung in Fällen, in denen diese Daten den Rechten Dritter unterliegen (bspw. aus Gründen des Schutzes personenbezogener Daten oder resultierend aus dem Schutz der Rechte des geistigen Eigentums und des Geschäftsgeheimnisses)[43]. Der

[40] Vgl. § 9 TTDSG-E.

[41] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final.

[42] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Eine europäische Datenstrategie, COM(2020) 66 final, S. 14.

[43] Vgl. Art. 3 Abs. 1 DGA,

DGA bildet hierbei keine Legitimation bzw. Rechtsgrundlage für eine Datennutzung, sondern schafft Mechanismen für eine Weiterverwendung bestimmter Kategorien geschützter Daten des öffentlichen Sektors[44]. Ferner wird weder eine Verpflichtung für öffentliche Stellen geschaffen, eine Weiterverwendung von Daten zu erlauben, noch befreit der DGA öffentliche Stellen von ihren Geheimhaltungspflichten[45].

Um insbesondere das Vertrauen in eine gemeinsame Datennutzung zu stärken, sieht Kapitel III des Entwurfs ein Anmeldeverfahren für Datenmittler bzw. -intermediäre vor und knüpft besagtes Verfahren an die Erfüllung verschiedenster technischer und organisatorische Anforderungen (vgl. Art. 10 u. 11 DGA). Hierbei referenziert der DGA allgemein auf „Anbieter von Diensten für die gemeinsame Datennutzung“ und bezieht hierdurch sowohl öffentliche wie auch Anbieter aus der Privatwirtschaft ein.

Ein SSO wird durch den Gesetzesentwurf nicht ausdrücklich adressiert, da es um eine gemeinsame Verwendung von Daten geht, deren Zugang durch ein Authentifizierungsverfahren, wie ein SSO, erst ermöglicht wird. Ein EU-SSO kann im Bereich der Data Governance jedoch als ergänzende vertrauensschaffende Maßnahme gesehen werden, um eine wirksame Trennung einer Verarbeitung von Inhaltsdaten des öffentlichen Sektors und von Daten für eine Authentifizierung zu ermöglichen.

Die im Entwurf für formulierten technisch-organisatorischen Anforderungen für solche Dienste enthalten im Übrigen bereits teilweise geeignete Vorlagen für eine Anerkennung von Anbietern eines EU-SSO (vgl. nachfolgend V. 2.).

Die Stiftung European netID Foundation bietet die Voraussetzungen für einen Datenintermediär im Sinne des Art. 11 DGA.

---

[44] Proposal for a Data Governance Act a.a.O., S. 8.
[45] Art. 3 Abs. 3 DGA.

V. Umriss einer gesetzlichen Regelung

Eine Norm zur Einführung einer verpflichtenden Verwendung eines EU-SSO könnte aus folgenden Elementen bestehen.

1. Verpflichtende Verwendung von EU-SSO-Diensten

a. Normtext

Art. X – Definitionen

Für die Zwecke dieser [Richtlinie][Verordnung] gelten die folgenden Begriffsbestimmungen:

1. „Dienste der Informationsgesellschaft" sind Dienste im Sinne von Artikel 1 Absatz 1 lit. b der Richtlinie (EU) 2015/1535;

2. „SSO-Dienst“ ist jeder Dienst der Informationsgesellschaft, bei dem sich Endnutzer authentisieren, um automatisch bei anderen Diensten der Informationsgesellschaft authentifiziert zu werden;

3. „EU-SSO-Dienst“ ist jeder SSO-Dienst, der erfolgreich ein Anerkennungsverfahren gem. Art. Z durchlaufen hat

Art. Y – Verpflichte Verwendung von EU-SSO-Diensten

Jeder Dienst der Informationsgesellschaft[1], der einen oder mehrere SSO-Dienste[2] zur Authentifizierung[3] gegenüber seinem Dienst verwendet, hat eine Schnittstelle zum EU-SSO[4] zu implementieren und diese gegenüber Endnutzern[5] anzubieten.

b. Kommentierung

Zu Art. Y - Dienste der Informationsgesellschaft[1]

Adressaten der Norm für eine verpflichtendes Anbieten eines europäischen SSO sind Dienste der Informationsgesellschaft. Art. 1 Nr. 1 lit. b der RL 2015/1535 definiert solche Dienste als „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung“. Das Angebot muss daher eine

- regelmäßig gegen Entgelt,

- elektronisch,
- im Fernabsatz,
- auf individuellen Abruf eines Empfängers erbrachte

Dienstleistung darstellen. Vorstehende Merkmale sind durch den jeweiligen Dienst kumulativ zu erfüllen[46]. Eine gegen Entgelt erbrachte Leistung liegt bereits dann vor, wenn sich der betreffende Dienst durch Werbung oder durch den Handel mit Nutzerdaten oder anderweitig (quer-)finanziert[47]. Als eine „elektronisch erbrachte Dienstleistung" wird eine solche Dienstleistung definiert, die mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird[48]. Eine im Fernabsatz erbrachte Dienstleistung stellt regelmäßig eine Dienstleistung dar, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird[49]. Das Merkmal des individuellen Abrufs eines Empfängers schließt solche Dienste der Informationsgesellschaft aus, die im Wege einer Übertragung von Daten ohne individuellen Abruf gleichzeitig für eine unbegrenzte Zahl von einzelnen Empfängern erbracht werden, wie zum Beispiel Fernseh- und Hörfunkdienste[50].

Zu Art. Y - SSO-Dienste[2]

Eine gesetzliche Definition von SSO-Diensten existiert auf europäischer Ebene bis dato nicht. Es bietet sich an, einen SSO-Dienst als jeden Dienst der Informationsgesellschaft zu definieren, bei dem sich Endnutzer authentisieren, um automatisch bei anderen Diensten der Informationsgesellschaft authentifiziert zu werden. Eine Authentisierung bedeutet im Kontext eines SSO den Nachweis der eigenen Identität gegenüber dem SSO-Dienst. Eine Authentisierung von Daten

---

[46] *Kühling/Buchner/Buchner/Kühling*, DS-GVO Art. 4 Nr. 25 Rn. 4.
[47] Vgl. *Schumacher* K&R 2015, 771 (776).
[48] Art. 1(1) lit. b ii) Richtlinie Richtlinie (EU) 2015/1535.
[49] *Jandt/Steidle*, Datenschutz im Internet, B. I. 1. Rn. 72.
[50] *Jandt/Steidle*, Datenschutz im Internet, B. I. 1. Rn. 74.

kann auch in anderen Szenarien erfolgen, z.B. dass Daten nicht bei der Übertragung über ein Netzwerk verändert wurden oder aus einer bestimmten Quelle stammen[51].

Zu Art. Y – Authentifizierung[3]

Die „Authentifizierung“ ist ein elektronischer Prozess, der die Bestätigung der elektronischen Identifizierung einer natürlichen oder juristischen Person oder die Bestätigung des Ursprungs und der Unversehrtheit von Daten in elektronischer Form ermöglicht[52]. D.h. die Authentisierung des jeweiligen Nutzers gegenüber dem SSO-Dienst und dessen Authentifizierung durch den SSO-Dienst gegenüber dem jeweiligen Dienst der Informationsgesellschaft stehen in einem untrennbaren Zusammenhang.

Zu Art. Y - Schnittstelle zum EU-SSO[4]

Eine Schnittstelle dient in der Regel zum Austausch von Daten nach festgelegten Regeln. Diese werden durch die technischen Spezifikationen einer Schnittstelle untermauert. Eine gesetzliche Definition einer Schnittstelle findet sich bereits in Art. 4 Nr. 11 der Richtlinie 2010/40/EU[53]: Hiernach ist eine „Schnittstelle“ eine Einrichtung zwischen Systemen, die der Verbindung und der Kommunikation zwischen den Systemen dient. Mit Blick auf einen EU-SSO bedarf es einer Kommunikation zwischen dem jeweiligen zertifizierten Dienst und dem Dienst der Informationsgesellschaft im Rahmen der Authentifizierung von Nutzern.

Zu Art. Y – Endnutzer[5]

Die Richtlinie (EU) 2018/1972[54] definiert den „Endnutzer“ als einen Nutzer, der keine öffentlichen elektronischen Kommunikationsnetze oder öffentlich zugänglichen elektronischen Kommunikationsdienste bereitstellt. Die Begrifflichkeit

---

[51] *Auer-Reinsdorff/Conrad*, Handbuch IT- und Datenschutzrecht, A. 6. Rn 449.

[52] Art. 3 Nr. 5 eIDAS-Verordnung.

[53] Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern.

[54] Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation.

schließt, wie es bereits nationale Gesetze vorsehen, sowohl natürliche als auch juristische Personen ein. Ebenso muss der Endnutzer nicht zwingend Vertragspartner des Dienstes der Informationsgesellschaft sein[55]. Insoweit ist das im gesetzlichen Wortlaut erwähnte „Anbieten“ eines EU-SSO ausreichend.

2. Anerkannte Dienste für ein EU-SSO

Normen zur konkreten gesetzlichen Umsetzung dieser Empfehlungen könnten wie folgt lauten.[56]

a. Normtext

Art. Z Anerkannte Dienste für ein EU-SSO

(1) Dienste, die ein EU-SSO anbieten, können unter der Voraussetzung anerkannt werden, dass sie kein wirtschaftliches Eigeninteresse[1] an den im Auftrag der Endnutzer verwalteten Daten haben. Dem steht nicht entgegen, dass der Dienst für die Verwaltung der Daten ein Entgelt erhebt. Die Anerkennung setzt weiterhin voraus, dass die Dienste ein Sicherheitskonzept vorlegen, das eine Bewertung der Qualität und Zuverlässigkeit des Dienstes ermöglicht.[4] Dies gilt insbesondere im Hinblick auf den Nachweis, dass der Dienst sowohl technisch als auch organisatorisch in der Lage ist, die Anforderungen an den Datenschutz und die Datensicherheit, die sich aus der Verordnung (EU) 2016/679 ergeben, zu erfüllen.[5] Die Kommission kann Durchführungsrechtsakte erlassen, mit denen technische Standards für Diensteanbieter eines EU-SSO festgelegt werden.

(2) Zuständig für die Anerkennung von Diensten zur Verwaltung persönlicher Informationen ist der Europäische Datenschutzbeauftragte.

---

[55] S. bereits der Endnutzerbegriff im Rahmen der Telekommunikation, vgl. *Scheurle/Mayen/Lünenbürger/Stamm* TKG § 3 Rn. 19.

[56] Die hier erörterten Ansätze wurden in Deutschland im Rahmen des Entwurfes zum TTDSG diskutiert.

b. Kommentierung

Art. Z Abs. 1 S. 1 - Anerkannte Dienste für ein EU-SSO

Zu Art. Z Abs. 1 S. 1, 2 - Kein wirtschaftliches Eigeninteresse und Finanzierung der Angebots[1]

Die Entwicklung und das Angebot eines EU-SSO muss finanziert werden. Der Anbieter eines solchen Systems, kann als Datentreuhänder[57] und Schnittstelle zu den Nutzern in die Lage geraten, personenbezogene Daten auszuwerten und für Zwecke zu nutzen, die über die reine Verwendung zur Identitätsverwaltung hinausgehen. Der TTDSG-E in Deutschland hatte zunächst die mittlerweile im Entwurf wieder verworfene Idee verfolgt, dem durch eine Formulierung Rechnung zu tragen, wonach „Dienste, die die Verwaltung persönlicher Informationen anbieten, (nur) unter der Voraussetzung anerkannt werden (können, dass sie kein wirtschaftliches Eigeninteresse an den im Auftrag der Endnutzer verwalteten Daten haben und zudem unabhängig von Unternehmen sind, die ein solches Interesse haben können."

Da eine mittelbare wirtschaftliche Abhängigkeit nie auszuschließen ist, würde eine Norm in dieser Form leerlaufen. Sie würde den gesamten Gedanken von Privacy Information Management Systems (PIMS) – als Beispiel für mögliche funktionale Erweiterung eines EU-SSO – konterkarieren und widerspräche auch der Empfehlung der DEK. Danach kann der „Betrieb derartiger Systeme (…) privatwirtschaftlich organisiert sein, wenn dabei der Betreiber an der Verwaltung und nicht an der Nutzung der Daten verdient"[58]. Soll der Anbieter des SSO-Dienstes nicht staatlich organisiert und finanziert sein, muss privaten Anbietern eine Möglichkeit zur Refinanzierung des Dienstes eingeräumt werden. Um dies klarzustellen, wird hier eine Formulierung vorgeschlagen, die auf mittelbare Eigeninteressen abstellt und ein Entgelt für die Nutzung des Dienstes zulässt. Auf diese Weise wäre auch im Sinne der DEK klargestellt, dass Dienste ein Entgelt für die Verwaltung der Daten erheben, nicht aber an deren Nutzung verdienen

[57] *Schwartmann/Weiß*, Datenmanagement- und Datentreuhandsysteme a.a.O., S. 17 ff.
[58] Gutachten der *Datenethikkommission* (2019), S. 134.

dürfen. Um den Nutzer als Verbraucher zu entlasten, liegt es nahe, das Angebot über Nutzungsentgelte der es nutzenden Unternehmen zu refinanzieren.

Zu Art. Z Abs. 1 S. 3 und 4 - Sicherheitskonzept

Im Rahmen eines Dienstes für ein EU-SSO sind Fragen der Datensicherheit und der TOMs relevant, die für die Frage der europarechtlichen Einführungspflicht keiner Erörterung bedürfen.

Zu Art. Z Abs. 2 - Akkreditierungseinrichtung

Denkbar sind sowohl öffentliche als auch private Akkreditierungseinrichtungen. Der Vorteil einer öffentlichen Stelle ist deren auch langfristig garantierte Unabhängigkeit. Auf europäischer Ebene käme als Akkreditierungseinrichtung beispielsweise der Europäische Datenschutzbeauftragte in Betracht. Er ist als Mitglied des Europäischen Datenschutzausschusses zuständig für die Datenschutzaufsicht über EU-Organe und Stellen. In dieser Eigenschaft scheint diese Behörde besser geeignet zu sein, als eine willkürlich benannte Datenschutzaufsichtsbehörde eines Mitgliedstaates, die Interessen eines EU-SSO bündeln. Eine Ansiedlung der Verantwortlichkeit zur Akkreditierung beim Europäischen Datenschutzausschuss selbst, scheint auch denkbar. Ein möglicher Nachteil wäre hier jedoch die wechselnde Zuständigkeit, und eine mögliche Überlastung der für die Kohärenz verantwortlichen Einrichtung. Anzuerkennen ist jedoch, dass eine solche Funktion unabhängig davon, wo sie verortet würde, eine nennenswerte Ausweitung der gegenwärtigen Aufgabenzuweisung der damit betrauten Stelle darstellen würde.