Blogartikel vom 20.02.2024
Compliance
Autorin: Rechtsanwältin Hannah Wiehler

Digital Service Akt (II)

Bei den letzten beiden Stufen handelt es sich im Vergleich zu den im vorherigen Beitrag behandelten Stufen um besonders regulierungsintensive Stufen.

3. Stufe

Der DSA definiert "Online-Plattformen" als eine Untergruppe der Hostingdienste, die im Auftrag von Nutzern Informationen speichern und öffentlich verbreiten. Hierbei ist die öffentliche Verbreitung von Inhalten ein entscheidendes Abgrenzungskriterium gegenüber anderen Host-Providern ist. Der DSA unterscheidet zwischen Individual- und Massenkommunikation und berücksichtigt Funktionen von Plattformen, durch die Inhalte öffentlich verbreitet werden können.

Besondere Aufmerksamkeit wird Messenger-Diensten wie WhatsApp oder Telegram gewidmet, bei denen zwar nicht das gesamte Funktionsspektrum als Online-Plattform gilt, aber Informationen durch die Nutzungsart öffentlich zugänglich gemacht werden können, z. B. in öffentlichen Gruppen oder Kanälen.

Der DSA ermöglicht eine Binnendifferenzierung innerhalb eines Plattformdienstes und unterwirft nur diejenigen Funktionen den Regelungen der dritten Stufe, durch die Inhalte öffentlich verbreitet werden können. Hierbei ist jedoch darauf hinzuweisen, dass die Bestimmung der genauen Nutzerzahlen einer Plattform bei diesem funktionsspezifischen Ansatz praktische Probleme aufwerfen könnte.

Es gibt auch Ausnahmen für bestimmte Dienste wie Cloud-Computing, Web-Hosting und den Kommentarbereich von Online-Zeitungen, wenn diese als unbedeutende Nebenfunktionen gelten. Soziale Netzwerke hingegen, insbesondere der Kommentarbereich, fallen immer in den Anwendungsbereich des DSA.

Klein- und Kleinstunternehmen sind unter bestimmten Bedingungen von der Befolgung bestimmter plattformspezifischer Pflichten befreit, es sei denn, sie gelten aufgrund ihrer Nutzeranzahl als sehr große Online-Plattformen.

<u>In der dritten Stufe ergeben sich folgende Pflichten für betroffene Unternehmen:</u>

- Artikel 21 f. DSA sieht im Vergleich zu den für alle Host-Provider geltenden Bestimmungen der Artikel 16 f. DSA ein anspruchsvolleres Beschwerdemanagement- und Streitbeilegungssystem vor. Die Endfassung des DSA ermöglicht nicht nur Nutzern, sondern auch meldenden Personen und Einrichtungen die Beschwerde bzw. Anrufung einer außergerichtlichen Streitbeilegungsstelle. Das Beschwerdemanagementsystem muss Beschwerdeberechtigten mindestens sechs Monate nach der Entscheidung des Anbieters die Möglichkeit zur elektronischen Beschwerde geben. Dies betrifft Entscheidungen über Beschränkungen wie Sperrung, Aussetzung, Entfernung von Inhalten oder Demonetarisierung.

Die Beschwerdemanagementsysteme müssen ebenfalls leicht zugänglich und benutzerfreundlich sein. Eine Pflicht zur rechtlichen Substanziierung der Beschwerde besteht nicht, aber bei klaren Beschwerden muss der Anbieter unverzüglich handeln. Plattform-Provider müssen Beschwerden zeitnah, diskriminierungsfrei und sorgfältig bearbeiten. Es gibt jedoch keine starren Fristen, um "Overblocking" zu vermeiden. Der DSA sieht keine konkreten Verfahrensrechte für die betroffene Gegenseite vor, und es bleibt abzuwarten, ob der EuGH in Zukunft eine präzisere Auslegung im Sinne der Grundrechte-Charta vornehmen wird.
Die letztendlichen Entscheidungen müssen unverzüglich und begründet mitgeteilt werden. Der Schiedsspruch der Streitbeilegungsstelle hat keine rechtliche Bindungswirkung. Plattform-Nutzer und von rechtswidrigen Inhalten Betroffene haben drei Optionen: Einlegen einer Beschwerde, Anrufung einer Streitbeilegungsstelle und gerichtlicher Rechtsschutz. Die privatrechtlichen Auswirkungen betreffen AGB-rechtliche Einschränkungen der Plattform-Anbieter. Die Frage, ob zusätzliche Verfahren in den AGB möglich sind, bleibt offen

- Gemäß Artikel 22 DSA haben Plattform-Anbieter sicherzustellen, dass Meldungen von anerkannten "vertrauenswürdigen Hinweisgebern" (trusted flaggers) über das allgemeine Meldeverfahren nach Artikel 16 DSA eingehen und als solche identifiziert werden können. Die Pflicht zur Identifizierung und priorisierten Behandlung von Meldungen vertrauenswürdiger Hinweisgeber bezieht sich ausschließlich auf die Meldung rechtswidriger Inhalte und nicht auf Verstöße gegen die Nutzungsbedingungen der Plattform-Anbieter. Ein freiwilliger Einsatz vertrauenswürdiger Hinweisgeber für die Erkennung von "Hassrede" ist jedoch möglich.
  Diese Meldungen müssen unverzüglich und vorrangig behandelt werden, da die Sachkenntnis und Kompetenz der vertrauenswürdigen Hinweisgeber eine schnellere Bearbeitung ermöglichen sollen. Der Status als vertrauenswürdiger Hinweisgeber ist an die Unabhängigkeit der Einrichtungen von Online-Plattformen gebunden, und die Koordinatoren müssen ihre Aufgabe sorgfältig, genau und objektiv ausüben. Der Status kann widerrufen werden, wenn sich zeigt, dass diese Anforderungen nicht erfüllt sind. Als vertrauenswürdige Hinweisgeber können private Nicht-Regierungsorganisationen, Wirtschaftsverbände, staatliche Stellen wie Europol und Mitglieder internationaler Meldenetzwerke in Betracht kommen.
  Die Beziehung zwischen Artikel 22 DSA und der Whistleblowing-Richtlinie von 2019 bzw. dem deutschen Umsetzungsgesetz, dem Hinweisgeberschutzgesetz (HinSchG), wirft Fragen auf. Die Begrifflichkeiten unterscheiden sich, und eine direkte Qualifikation der Meldestellen von Plattform-Anbietern nach Artikel 16 und Artikel 20 DSA als Whistleblower-Meldestellen ist nicht gegeben. Dennoch könnte eine Verzahnung von DSA und Whistleblower-Schutz künftig möglich sein, insbesondere wenn die nach dem HinSchG einzurichtenden Whistleblowing-Behörden sich als vertrauenswürdige Hinweisgeber nach Artikel 22 DSA registrieren lassen, um Meldungen an Plattform-Anbieter weiterzuleiten.

- Die Artikel 20 bis 22 des DSA regeln hauptsächlich das Verfahren für den Umgang mit Meldungen oder Beschwerden über rechtswidrige Inhalte. Artikel 23 DSA befasst sich jedoch in begrenztem Umfang mit materiellen Vorgaben bezüglich der missbräuchlichen Verwendung von Online-Plattformen.
  Artikel 23 DSA behandelt zwei spiegelbildliche Situationen: erstens die häufige Einstellung offensichtlich rechtswidriger Inhalte durch einen Nutzer und zweitens die häufige Abgabe bzw. Einlegung offensichtlich unbegründeter Meldungen oder

Beschwerden von Nutzern oder Dritten. In beiden Fällen sollen Anbieter die Erbringung der Dienste für die betreffende Person temporär aussetzen können. Während der DSA nicht ausdrücklich die dauerhafte Sperrung eines Accounts verlangt, bleibt dies nach den Nutzungsbedingungen der Anbieter möglich, insbesondere im Falle schwerer Straftaten wie Darstellungen von sexuellem Missbrauch von Kindern.
Artikel 23 DSA hat regulatorische Auswirkungen in zwei Richtungen. Plattform-Provider sind aufsichtsrechtlich verpflichtet, gegen häufigen und offensichtlichen Missbrauch zu reagieren, mindestens in Form einer temporären Aussetzung des Dienstes. Gleichzeitig legt der Artikel bestimmte Mindestvoraussetzungen fest, insbesondere zum Schutz der Meinungsfreiheit der Nutzer. Dazu gehört die Warnung des betroffenen Nutzers vor einer Aussetzung.
Der Artikel sieht vor, dass der Anbieter seine beabsichtigte Entscheidung begründen und auf mögliche Rechtsbehelfe hinweisen muss. Hinsichtlich möglicher zivilrechtlicher Auswirkungen enthält Artikel 23 DSA keine konkreten Bestimmungen, weist jedoch darauf hin, dass nationale Schadensersatzansprüche gegen am Missbrauch beteiligte Personen unberührt bleiben.
Die Missbrauchsbestimmungen des Artikels 23 DSA werden den AGB-rechtlichen Spielraum der Anbieter begrenzen, und der Artikel hat teilweise Schutzgesetzcharakter im Sinne von Schadensersatzansprüchen und Unterlassungsansprüchen. Die erweiterten Transparenzpflichten in den Artikeln 24 und 27 DSA setzen zusätzliche Anforderungen an Anbieter, darunter die Pflicht zur Weiterleitung von Beschränkungen und Begründungen an die Kommission sowie die Offenlegung der wichtigsten Parameter ihrer Empfehlungssysteme.

- Artikel 25 DSA enthält allgemeine Vorgaben für die Benutzeroberfläche (Interface) von Online-Plattformen. Er verbietet jegliche Gestaltung, Organisation oder Betriebsweise des Online-Interfaces, durch die Nutzer getäuscht, manipuliert oder anderweitig in ihrer Entscheidungsfreiheit beeinträchtigt oder behindert werden. Dies zielt insbesondere auf die Verwendung von sogenannten "Dark Patterns" ab, die in der Praxis dazu dienen, die Nutzer in ihrer Entscheidungsfindung zu beeinflussen.
  Die Norm hat einen allgemeinen Anwendungsbereich und geht über spezifische Vorgaben des Verbraucher- und Datenschutzrechts hinaus. Die speziellen Irreführungsverbote der UGP-Richtlinie (Richtlinie über unlautere Geschäftspraktiken) und der DS-GVO (Datenschutz-Grundverordnung) bleiben unberührt.
  Gemäß Artikel 25 Absatz III DSA wird die Kommission ermächtigt, das abstrakte Verbot durch Leitlinien für die Praxis zu konkretisieren. Insbesondere das Verbot der stärkeren Hervorhebung bestimmter Auswahlmöglichkeiten (wie im Beispiel des "Cookie Banners") wird dabei genannt. Es ist zu erwarten, dass die Kommission sich mit diesem Thema in ihren Leitlinien auseinandersetzen wird. Diese Vorschrift gibt der Kommission die Befugnis, erheblichen Einfluss auf die praktische Nutzererfahrung im Internet zu nehmen, und wird daher in Zukunft von großer Bedeutung sein

- Artikel 26 DSA beinhaltet eine wettbewerbsrechtliche Spezifikation des Schnittstellen-Designs in Bezug auf kommerzielle Werbung. Gemäß dieser Bestimmung sind Anbieter von Online-Plattformen verpflichtet, kommerzielle Werbung klar zu kennzeichnen. Diese Pflicht wird auch auf Nutzer ausgedehnt, die kommerzielle Kommunikation veröffentlichen, nachdem das Trilog-Verfahren abgeschlossen wurde.
  Die Transparenzvorschriften in Artikel 26 DSA enthalten zudem ein sachlich begrenztes Verbot des Profilings zu Werbezwecken. Insbesondere ist das Profiling unter Verwendung von Parametern wie "rassischer" oder ethnischer Herkunft, politischer, religiöser oder weltanschaulicher Überzeugung sowie der Gewerkschaftszugehörigkeit

einer Person untersagt. Dieses Verbot steht im Einklang mit den Datenschutzbestimmungen, insbesondere Artikel 9 der Datenschutz-Grundverordnung (DS-GVO). Es berührt jedoch nicht die weitergehenden Vorschriften des Datenschutzrechts, einschließlich der Rechte der Nutzer gemäß Artikel 22 DS-GVO.
Die Durchsetzung dieser Bestimmungen kann sowohl durch Aufsichtsbehörden als auch durch private Rechtsmittel erfolgen. Mitbewerber und anspruchsberechtigte Organisationen haben das Recht, Verstöße gegen diese Bestimmungen gemäß dem Wettbewerbsrecht geltend zu machen. Schadensersatzansprüche von Einzelpersonen aufgrund von Verletzungen des Nutzungsvertrags oder deliktischer Ansprüche nach § 823 BGB dürften jedoch oft am Fehlen eines nachweisbaren Schadens scheitern. Eine alternative Möglichkeit könnte darin bestehen, Verstöße gegen Artikel 26 DSA als Grund für die Kündigung des Nutzungsvertrags zu verwenden, wie es in der Richtlinie über digitale Inhalte vorgesehen ist.

- Artikel 28 DSA legt zusätzliche Verpflichtungen für Plattformanbieter fest, die für Minderjährige zugänglich sind. Diese Anbieter müssen über die allgemeinen Vorgaben hinaus zusätzliche, verhältnismäßige Maßnahmen ergreifen, um ein hohes Maß an Privatsphäre, Sicherheit und Schutz zu gewährleisten. Diese Maßnahmen könnten beispielsweise das Standardausstatten des Interfaces mit dem höchsten Maß an Privatsphäre und Sicherheit beinhalten.
  Es ist jedoch wichtig zu beachten, dass Anbieter nicht verpflichtet sind, Daten über das Alter ihrer Nutzer zu erheben, wie in Artikel 28 Absatz III DSA festgelegt. Dies könnte dazu führen, dass die Verpflichtungen aus Artikel 28 hauptsächlich für Plattformen gelten, die für Minderjährige zugänglich sind und in einer für den Anbieter erkennbaren Weise überwiegend von Minderjährigen genutzt werden.
  Die praktische Umsetzung dieser Bestimmung könnte davon abhängen, inwieweit Plattformanbieter freiwillig Daten über das Alter ihrer Nutzer sammeln. Der Anreiz für die Anbieter, dies zu tun, könnte aufgrund der erhöhten Privatsphäreanforderungen und des Verbots von Profiling-basierter Werbung gemäß Artikel 26 Absatz II DSA begrenzt sein.
  Die Kommission wird befugt, nach Anhörung des Ausschusses für digitale Dienste (gemäß Artikel 88 Absatz I DSA) Leitlinien zu entwickeln, die praktisch umsetzbar sind und von den Anbietern befolgt werden können. Diese Leitlinien könnten dazu beitragen, möglichen Umgehungstaktiken, wie dem bewussten Nichterheben von Daten über das Alter der Nutzer, entgegenzuwirken

- Die Artikel 30 bis 32 DSA legen Verbraucherschutzvorschriften für Online-Plattformen fest, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen. Diese Vorschriften gelten jedoch nicht für Klein- oder Kleinstunternehmer, es sei denn, es handelt sich um sehr große Online-Plattformen gemäß Artikel 33 DSA.
  Die besondere Stellung von Fernabsatz-Plattformen als informatorisches Bindeglied zwischen Unternehmer und Verbraucher wird betont, und die Verbraucherschutzvorschriften sollen die Durchsetzung bereits bestehender Verbraucherschutzrechte gegenüber den auf der Plattform registrierten Unternehmern erleichtern.
  Artikel 30 DSA legt fest, dass Plattform-Anbieter im Vorfeld der Dienstnutzung von Unternehmern Informationen wie Name, Anschrift, Telefonnummer, E-Mail-Adresse, Zahlungskonto und Handelsregistereintragung abfragen müssen. Der Anbieter ist dazu verpflichtet, diese Daten "nach besten Kräften" zu überprüfen und den Nutzern

zugänglich zu machen. Eine Übermittlung an Dritte ist nur auf behördliche oder gerichtliche Anordnung hin gestattet.
Artikel 31 DSA verpflichtet Anbieter von Fernabsatz-Plattformen, ihre Online-Schnittstellen so zu gestalten, dass Unternehmer ihren unionsrechtlichen Informationspflichten nachkommen können. Dies beinhaltet Informationen zu Verbraucher-Widerrufsrechten, Wareneigenschaften, Produktidentifizierung und Kontaktdaten der beteiligten Wirtschaftsakteure. Der Anbieter muss sich auch nach besten Kräften um die Überprüfung dieser Informationen bemühen.
Artikel 32 DSA verlangt von Plattform-Anbietern, Nutzer zu informieren, wenn sie Kenntnis davon erlangen, dass rechtswidrige Produkte oder Dienstleistungen auf ihrer Plattform angeboten werden. Die Informationen müssen persönlich an alle Nutzer weitergeleitet werden, die das Produkt oder die Dienstleistung in den letzten sechs Monaten erworben haben. Falls die Kontaktdaten nicht verfügbar sind, müssen die Informationen öffentlich und leicht zugänglich bereitgestellt werden.
Die DSA-Bestimmungen können auch zivilrechtliche Haftungsfolgen haben, insbesondere im Falle schuldhafter Nichterfüllung der Informations-, Überprüfungs- und Weiterleitungspflichten. Die Haftung kann sich mittelbar über eine entsprechende Auslegung vertraglicher Nebenpflichten gegenüber den Nutzern und auf Basis von Schadensersatzansprüchen gegenüber Dritten ergeben.

Die Anforderungen und Haftungsbestimmungen können aufgrund des vollharmonisierenden Charakters der DSA-Bestimmungen in Zukunft zu einer einheitlicheren Rechtslage in der EU führen.

4. Stufe

Die vierte Stufe des DSA konzentriert sich auf die Bewältigung von "systemischen Risiken", die von großen Online-Plattformen ausgehen. Hierbei handelt es sich um potenzielle Gefahren, die sich nicht nur auf individueller, sondern auch auf gesellschaftlicher Ebene manifestieren können. Beispiele hierfür sind die Verbreitung von Desinformation, Hate Speech und die Manipulation der öffentlichen Meinung durch Plattformen wie Facebook oder Twitter.

<u>In der vierten Stufe ergeben sich folgende Pflichten für die Unternehmen:</u>

- Die Anwendungsbereiche der Regulierungen erstrecken sich auf Anbieter, die in der Europäischen Union mindestens 45 Millionen monatlich aktive Nutzer verzeichnen. Der Fokus liegt darauf, bestehende Vorschriften zu verschärfen und neue Instrumente zur Fremd- und Selbstregulierung einzuführen. Besondere Aufmerksamkeit wird den Bereichen Empfehlungssysteme (Art 38 DSA), Online-Werbung (Art.39,46 DSA) und Transparenzberichtspflichten(Art 42 DSA) gewidmet. Hierdurch soll nicht nur eine bessere Kontrolle über die Aktivitäten der Plattformen ermöglicht, sondern auch die Transparenz gegenüber den Nutzern gestärkt werden.

- Ein Schlüsselaspekt der vierten Stufe ist die Identifizierung und Minimierung der erkannten systemischen Risiken (Art 34 bis 37, 39 bis 41, 45 und 48 DSA). Plattformen werden verpflichtet, Mechanismen zu etablieren, um diese Risiken zu erkennen, zu analysieren und geeignete Maßnahmen zu ergreifen. Dies schließt präventive Maßnahmen ebenso ein wie Krisenreaktionsmechanismen, um in kritischen Situationen schnell und effektiv reagieren zu können.

1. Allgemeine Risikobewertung
   Nach Artikel 34 sind Anbieter von großen Plattformen und Suchmaschinen verpflichtet, die Risiken aus ihren Diensten und verbundenen Systemen, insbesondere den Algorithmen, zu ermitteln, zu analysieren und zu bewerten. Auf dieser Grundlage müssen angemessene Risikominimierungsmaßnahmen ergriffen werden. Jährlich ist eine Risikobewertung durchzuführen, die systemische Risiken betrifft, wobei bereits nachteilige Auswirkungen ausreichen, ohne dass es zu rechtswidrigen Beeinträchtigungen durch illegale Inhalte kommen muss.
   Die genannten Risiken betreffen unter anderem "Fake News" und die Verwendung von "Social Bots" zur gezielten Desinformation.

2. Risikominimierung
   Die Minimierung der systemischen Risiken dient vor allem öffentlichen Interessen, und zivilrechtliche Durchsetzung oder Sanktionierung kommt neben aufsichtsrechtlichen Maßnahmen normalerweise nicht in Betracht. Allerdings könnten in bestimmten Fällen Verletzungen von Risikominimierungspflichten Schadensersatzansprüche gemäß Delikts- oder Schuldrecht auslösen, sofern die Verletzung individueller Rechtsgüter direkt auf erkennbare Gefahrenpotenziale zurückzuführen ist, die gemäß den DSA-Vorgaben hätten minimiert werden können. Es werden jedoch noch viele Details in dieser Hinsicht offengelassen.

3. Krisenreaktionsmechanismen und -protokolle
   Die Artikel 36 und 48 DSA behandeln spezielle Regelungen für Krisensituationen im Gegensatz zu den Artikeln 34 f., die die Verhütung systemischer Risiken im "Normalbetrieb" des Dienstes betreffen. Eine Krise wird als außergewöhnliche Umstände definiert, die eine ernsthafte Bedrohung der öffentlichen Sicherheit oder Gesundheit darstellen, wie bewaffnete Konflikte, terroristische Handlungen, Naturkatastrophen und Pandemien.
   Die Kommission kann auf Empfehlung des Europäischen Gremiums für Digitale Dienste Anbieter großer Plattformen und Suchmaschinen gemäß Artikel 48 des DSA zur Ausarbeitung von Krisenprotokollen anhalten. Diese Protokolle sollen einen verschärften und auf die akute Situation zugeschnittenen Einsatz von allgemeinen Risikominimierungsmaßnahmen vorsehen. Zusätzlich dazu ermächtigt Artikel 36 des DSA die Kommission, auf Empfehlung des Gremiums hoheitliche Eingriffsbefugnisse auszuüben. Dies ermöglicht es der Kommission, Anbieter für bis zu drei Monate konkret zur Durchführung von Maßnahmen zu verpflichten, um eine schwerwiegende Bedrohung zu verhindern, zu beseitigen oder zu begrenzen. Die Effektivität dieser dreistufigen Anordnungskette, insbesondere in akuten Krisensituationen, bleibt jedoch abzuwarten.

4. Verhaltenskodexe und Normen
   Ein weiterer wesentlicher Bestandteil sind die vorgesehenen Verhaltenskodexe, die von Gremien und der Europäischen Kommission überwacht werden sollen. Diese Kodexe sollen sicherstellen, dass Plattformen ethische Standards einhalten und sich gesellschaftlich verantwortungsbewusst verhalten.

5. Audits und Compliance Abteilungen
   Die Einhaltung dieser Regelungen wird durch unabhängige Audits überprüft, um Transparenz und Rechenschaftspflicht zu gewährleisten. Dabei wird betont, dass die Auswirkungen auf die zivilrechtliche Haftung begrenzt sind, da viele dieser Regelungen dem öffentlichen Interesse dienen.

6. Datenzugang und Kontrolle
   Artikel 40 des Digital Services Act (DSA) gemäß der EU-Verordnung 2022/2065 ermöglicht der Kommission und dem Digitalen Dienste Koordinator des zuständigen Mitgliedstaats (in Deutschland die Bundesnetzagentur) Zugang zu den überwachungsrelevanten Daten des Anbieters, um die Einhaltung des DSA zu überwachen und zu bewerten. Dabei wird darauf geachtet, die berechtigten Interessen von Anbietern und Nutzern, insbesondere den Schutz von personenbezogenen Daten und Geschäftsgeheimnissen, zu berücksichtigen.
   Der Datenzugang soll den Behörden Einblick in die Funktionsweise der vom Anbieter verwendeten Algorithmen geben. Ein "begründetes Verlangen" genügt zur Rechtfertigung des Datenzugangs, ohne dass ein konkreter Verstoßverdacht vorliegen muss. Allerdings muss der Zweck des Verlangens auf die Kontrolle der DSA-Vorschriften oder die Bewertung der mit dem Betrieb der Plattform oder Suchmaschine verbundenen Risiken abzielen. Es ist nicht zulässig, spezifische Nutzerinformationen für die Überprüfung der Einhaltung anderer Rechtsvorschriften anzufordern.
   Zusätzlich müssen Anbieter unter bestimmten Bedingungen zugelassenen Forschern Zugang zu ihren Daten gewähren, insbesondere für die Erforschung systemischer Risiken gemäß den geregelten Voraussetzungen von Artikel 40 des DSA.

In der Gesamtschau wird der Digital Services Act als wegweisende Veränderung im digitalen Raum betrachtet, da er erstmals ein umfassendes Regulierungsumfeld für die Bewältigung systemischer Risiken auf internationaler Ebene schafft. Die vierte Stufe des DSA wird als entscheidender Schritt angesehen, um den Herausforderungen der digitalen Ära zu begegnen und eine ausgewogene und verantwortungsbewusste Nutzung digitaler Plattformen zu fördern. Es wird erwartet, dass die Umsetzung dieser Regelungen einen positiven Einfluss auf die digitale Landschaft in der Europäischen Union haben wird, indem sie einen Rahmen für fairere, transparentere und sicherere Online-Dienstleistungen schafft. Insbesondere in Fällen in denen die Sorgfaltspflichten und Transparenzpflichten nicht umgesetzt werden, drohen erhebliche Bußgelder von bis zu 6% des weltweiten Jahresumsatzes sowie Abmahnungen. Allein deswegen sollte die Motivation der betroffenen Unternehmen groß sein, die Anforderungen des DSA zu erfüllen.