DFN
infobrief recht

5 / 2022
Mai 2022

Unus pro omnibus, omnes pro uno

Das Kammergericht Berlin legt die Debatte um datenschutzrechtliche Haftung von Unternehmen dem Gerichtshof der Europäischen Union vor

Zeitenwende: BGB goes digital

Die neuen Regelungen zu digitalen Diensten im Bürgerlichen Gesetzbuch

Ausgeschremst?

Bringt der geplante Transatlantische Datenschutzrahmen Sicherheit bei Datenübertragungen in die USA?

Unus pro omnibus, omnes pro uno

Das Kammergericht Berlin legt die Debatte um datenschutzrechtliche Haftung von Unternehmen dem Gerichtshof der Europäischen Union vor

von Nicolas John

Die datenschutzrechtlichen Haftungsnormen sind derzeit Gegenstand diverser gerichtlicher Entscheidungen.[1] Spätestens mit dem Vorlagebeschluss des Kammergerichts (KG) Berlin[2] an den Gerichtshof der Europäischen Union (EuGH) hat die Debatte um die datenschutzrechtliche Haftung und die damit verbundene Verhängung von Bußgeldern gegen Unternehmen weiter Fahrt aufgenommen. Von den Auswirkungen dieser Rechtsprechung sind Unternehmen und Organisationen aller Art betroffen. Der Beitrag gibt nachfolgend eine Übersicht zum aktuellen Stand der datenschutzrechtlichen Normen und der Rechtsprechung sowie potenziellen Auswirkungen.

I. Rechtliche Grundlagen und rechtspolitischer Hintergrund der Diskussion

Art. 83 DSGVO normiert das Bußgeldverfahren, welches Aufsichtsbehörden bei der Feststellung eines Verstoßes gegen Normen der DSGVO gemäß Art. 58 Abs. 2 lit. i) DSGVO gegen den Verantwortlichen oder Auftragsverarbeiter einleiten können. Art. 83 DSGVO sieht dabei einen umfassenden Kriterienkatalog vor, welcher bei der Verhängung einer Geldbuße zu berücksichtigen ist. Adressaten des Bußgeldes können sowohl natürliche als auch juristische Personen als Verantwortliche und Auftragsverarbeiter sein. In diesem Kontext weist das Unionsrecht im Vergleich zum deutschen Bußgeldrecht Besonderheiten auf. Grund dafür ist ein anderes Verständnis bei der Verhängung von Bußgeldern gegenüber Unternehmen.

In Deutschland wird im Rahmen des sog. „Rechtsträgerprinzips“ ein vorwerfbares Handeln einer Leitungsperson im Unternehmen verlangt und an die Handlung dieser natürlichen Person angeknüpft. Im Unionsrecht wird dagegen über das „Funktionsträgerprinzip“ das Bußgeld allein gegen die wirtschaftliche Einheit eines Unternehmens verhängt. Soweit man dieses Funktionsträgerprinzip bei den Haftungsnormen der DSGVO zugrunde legt, haftet ein Unternehmen unmittelbar, ohne dass eine konkret vorwerfbare Handlung einer Einzelperson vorliegen muss.

Zur Veranschaulichung: Im Rahmen des Diesel-Abgasskandals war schon zu einem frühen Zeitpunkt erwiesen, dass führende Angestellte der involvierten Automobilkonzerne Ordnungswidrigkeiten begangen hatten. Wer genau die verantwortlichen Manager waren, konnten die Staatsanwaltschaften allerdings häufig nicht beweisen. Nach dem Rechtsträgerprinzip ist eine genaue Bezeichnung der verantwortlichen Einzelpersonen allerdings erforderlich – auch um den Konzern selbst mit einem Bußgeld zu belasten. In Rechtsordnungen, die das Funktionsträgerprinzip gewählt haben, kann ein Unternehmen schon dann bebußt werden, wenn bewiesen ist, dass irgendeine, nicht näher bezeichnete angestellte Person eine Ordnungswidrigkeit im Zusammenhang mit ihrer Beschäftigung begangen hat. Viele ausländische Rechtsordnungen sehen dementsprechend das Funktionsträgerprinzip vor (so z. B. Großbritannien und die USA). Aus diesem Grund war die juristische Aufarbeitung des Dieselskandals in vielen Staaten deutlich einfacher möglich als in Deutschland.

Rechtspolitisch ist das Rechtsträgerprinzip auch in Deutschland umstritten. Im Koalitionsvertrag der abgelaufenen

1 Zum Beispiel: Uphues, Unbewiesen, abgewiesen, DFN-Infobrief Recht 6/2021; Uphues, Steh zu deinen Fehlern oder es kommt dir teuer zu stehen; DFN-Infobrief Recht 4/2021; John, Data Wars: Der Betroffene schlägt zurück, DFN-Infobrief Recht 10/2020.
2 KG Berlin, Beschl. v. 6. Dezember 2021, Az. 3 Ws 250/21.

19. Legislaturperiode kündigten CDU/CSU und SPD an, das Sanktionsrecht für Unternehmen umfassend zu reformieren. Die Koalitionsparteien wollten sicherstellen, dass künftig auch die „von Fehlverhalten ihrer Mitarbeiterinnen und Mitarbeiter profitierenden Unternehmen stärker sanktioniert werden."[3] Die Bemühungen der Koalitionsparteien mündeten in den Entwurf eines sogenannten Verbandssanktionengesetz (VerSanG). Dieses hätte in Deutschland zwar nicht das Funktionsträgerprinzip eingeführt, das deutsche Recht aber an ausländische Rechtsordnungen angenähert, die dieses Prinzip längst kennen. Das VerSanG befand sich bereits in der Fassung eines Regierungsentwurfes, Forschung und Praxis hielten die Verabschiedung in der 19. Legislaturperiode für ausgemachte Sache. Doch die Koalition verabschiedete das Gesetz schließlich nicht. Insbesondere die Zusatzbelastung für Unternehmen aufgrund der Corona-Pandemie war ein Grund für die überraschende Wendung.

II. Inhalt des Vorlagebeschlusses des KG Berlin

Das KG Berlin hat mit Beschluss vom 6. Dezember 2021 (Az. 3 Ws 250/21) dem EuGH Fragen zur datenschutzrechtlichen Haftung und den Voraussetzungen einer Geldbuße gegen Unternehmen vorgelegt. Dem Verfahren vor dem KG liegt ein Bußgeldbescheid in Höhe von 14,5 Mio. Euro zugrunde, welches die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) gegen das Immobilienunternehmen Deutsche Wohnen verhängt hatte. Zuvor hatte das Landgericht (LG) Berlin das gleiche Verfahren mit der Begründung eingestellt, dass die Verhängung von Bußgeldern gegen Unternehmen wegen Datenschutzverstößen nach Art. 83 Abs. 4 bis 6 DSGVO nur unter den Voraussetzungen des in § 30 des Gesetzes über Ordnungswidrigkeiten (OWiG) festgelegten Rechtsträgerprinzips in Betracht kommt. Danach kann, wie oben eben erläutert, ein Bußgeld nur verhängt werden, wenn eine rechtswidrige und vorwerfbar begangene Tat einer Leitungsperson des Unternehmens vorliegt. Diese Voraussetzung sah das LG Berlin als nicht erfüllt an.

Mit diesem Urteil vertritt das LG Berlin eine diametral andere Auffassung als das LG Bonn[4]. Dieses hatte 2020 in einem Verfahren gegen einen Dienstleister das Funktionsträgerprinzip zugrunde gelegt und festgestellt, dass Art. 83 DSGVO eine unmittelbar bußgeldrechtliche Verbandshaftung legitimiere, ohne dass die Tatbestandsvoraussetzungen des § 30 OWiG erfüllt sein müssen. Dies ergebe sich insbesondere aus Erwägungsgrund 150 DSGVO, welcher auf den europäischen Unternehmensbegriff aus Art. 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) verweise.

Aufgrund dieser unterschiedlichen Rechtsauffassungen legte die Staatsanwaltschaft (StA) Berlin gegen die Entscheidung des LG Berlin Rechtsmittel ein, wodurch nun das KG Berlin über den Fall zu entscheiden hat. Auch aufgrund der oben dargestellten rechtlichen Debatte sah sich nun das Kammergericht berufen, die Frage um die Einbeziehung der Voraussetzungen des § 30 OWiG dem EuGH vorzulegen, um die Zweifel an der Auslegung der europäischen Haftungsnorm zu beseitigen. Im Kern geht es um die Klärung der Frage, ob das Rechtsträgerprinzip auch im Falle eines Verstoßes gegen europarechtlich determiniertes Datenschutzrecht gilt oder ob ein zuzuordnender objektiver Pflichtenverstoß genügt. Im Rahmen des Beschlusses lässt das KG Berlin erkennen, dass es selbst eher der Auffassung zuneigt, dass die Voraussetzungen des § 30 OWiG nicht einzubeziehen seien und damit eine direkte Unternehmenshaftung im Sinne des Funktionsprinzips gelte.

Die Entscheidung des EuGHs steht bislang noch aus.

III. Bedeutung der Diskussion für Hochschulen und Forschungseinrichtungen

Die rechtliche Diskussion um die Haftungsnormen der DSGVO ist auch für Hochschulen und Forschungseinrichtungen relevant. Denn soweit personenbezogene Daten verarbeitet werden, kann eine Haftung der Einrichtung im Falle einer Datenschutzverletzung entstehen. Soweit die Anwendbarkeit des § 30 OWiG bejaht wird, muss auch im Falle einer Datenschutzverletzung ein vorwerfbares Handeln einer Leitungsperson der Einrichtung vorliegen. Im Falle der Nichtanwendbarkeit ist dagegen jeder Verstoß gegen Datenschutzrecht innerhalb der Einrichtung von haftungsrechtlicher Relevanz.

Sobald die Entscheidung des EuGHs vorliegt, wird dies auch konkrete Auswirkungen auf die Praxis der Datenschutzbehörden haben. Bislang zeigen die unterschiedlichen Gerichtsentscheidungen die rechtlichen Unsicherheiten bei der Auslegung der

3 Koalitionsvertrag zwischen CDU, CSU und SPD v. 12. März 2018, S. 125.

4 LG Bonn, Urt. v. 11.11.2020, Az. 29 OWi 1/20.

Haftungsnormen. Ein Urteil des EuGHs wird daher künftig wohl zu einem einheitlichen Maßstab bei der datenschutzrechtlichen Haftung von juristischen Personen führen.

IV. Besonderheiten der Vorgaben zur Haftung für Behörden

Bei der Verhängung von Geldbußen gegen Behörden ist Art. 83 Abs. 7 DSGVO zu beachten. Danach sieht die DSGVO eine Öffnungsklausel für nationale Regelungen darüber vor, „ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können." In Deutschland hat der Gesetzgeber davon auf Bundesebene in § 43 Abs. 3 Bundesdatenschutzgesetz (BDSG) Gebrauch gemacht. Dieser statuiert, dass „gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 […] keine Geldbußen verhängt" werden. Eine Ausnahme gilt allerdings für öffentliche Stellen, die „als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen" (§ 2 Abs. 5 BDSG). Gegen diese können wiederum Geldbußen verhängt werden.

Das BDSG gilt aber nur für öffentliche Stellen des Bundes. Soweit eine Landesbehörde personenbezogene Daten verarbeitet ist das Landesdatenschutzgesetz (LDSG) des jeweiligen Landes maßgeblich. Auch auf Landesebene ist in verschiedenen Landesdatenschutzgesetzen ebenfalls von der Öffnungsklausel Gebrauch gemacht worden. Teilweise unterscheiden sich diese inhaltlich etwas von der Norm des § 43 BDSG. Das Grundmuster ist jedoch gleich: Gegen öffentliche Stellen kann nur dann ein Bußgeld verhängt werden, wenn diese in irgendeiner Art wirtschaftlich tätig ist. Die jeweiligen Haftungsnormen der LDSG[5] müssen im Einzelfall überprüft werden.

5 Baden-Württemberg: § 28 LDSG (BW); Bayern: Art. 22 BayDSG; Berlin: § 28 BlnDSG; Brandenburg: § 32 Abs. 3 BbgDSG; Bremen: § 23 Abs. 3 BremDSGVOAG; Hamburg: § 24 Abs. 3 HmbDSG; Hessen: § 36 Abs. 2 HD-SIG; Mecklenburg-Vorpommern: § 22 Abs. 3 DSG M-V; Niedersachsen: § 20 Abs. 5 NDSG; Nordrhein-Westfalen: § 33 Abs. 4 DSG NRW; Rheinland-Pfalz: § 24 LDSG (RLP); Saarland § 20 Abs. 5 S. 2 SDSG; Sachsen: § 19 Abs. 3 SächsDSG; Sachsen-Anhalt: § 31 Abs. 2 DSAG LSA; Schleswig-Holstein: § 19 Abs. 1 LDSG (SH); Thüringen: § 61 Abs. 4 ThürDSG.

V. Auffassungen der Datenschutzbehörden

Durch ihre Rolle als Aufsichtsbehörde sind die Datenschutzbehörden dafür zuständig, vorliegende Verstöße gegen die DSGVO zu rügen und ggf. mit Bußgeldern zu belegen. Bis das Urteil des EuGHs ergeht, wird noch etwas Zeit vergehen, die Datenschutzbehörden werden bis dahin weiterhin ihrer Aufsicht nachgehen und etwaige Verstöße gegen das Datenschutzrecht ahnden. Daher ist es auch im Fall der Diskussion um Art. 83 DSGVO von Relevanz, ob und welche Auffassung die jeweiligen Landesdatenschutzbeauftragten vertreten, um entsprechend darauf reagieren zu können.

Bislang haben sich nur wenige Landesdatenschutzbeauftragte oder Gesetzgeber zur Haftung geäußert. Die Äußerungen sind zudem nur genereller Natur und betreffen nicht explizit den hier besprochenen Vorlagebeschluss des KG Berlin.

1. Bayern

Der Bayrische Landesbeauftragte für den Datenschutz (BayLfD) schreibt in einer Kurzinformation, es sei zu prüfen, ob eine bayrische öffentliche Stelle als Unternehmen am Wettbewerb teilnimmt. Ist dies der Fall, sei anhand eines unionsrechtlichen Maßstabs zu prüfen, ob die betreffende bayerische öffentliche Stelle hinsichtlich des konkreten Tätigkeitsfelds (Art. 22 BayDSG: „soweit") als Unternehmen am Wettbewerb teilnimmt.[6]

2. Bremen

In der Begründung zum Bremischen Ausführungsgesetz zu DSGVO führt der Senat aus: „Nach Artikel 83 Absatz 7 der Verordnung (EU) 2016/679 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können. Absatz 3 stellt klar, dass von dieser Möglichkeit kein Gebrauch gemacht wird. Die Verhängung von Geldbußen gegen öffentliche Stellen ist

6 Kurzinformation des BayLfD, abrufbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/aki17.html (zuletzt abgerufen am 7.4.2022).

ausdrücklich ausgeschlossen."[7]

3. Hessen

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBfDI) schließt die Verhängung von Geldbußen gegen Behörden aus.[8]

4. Nordrhein-Westfalen

Die Landesregierung von Nordrhein-Westfalen führt in der Gesetzesbegründung zu Anpassungsgesetz des Datenschutzrechts aus: „Mit Absatz 4 wird von der Öffnungsklausel des Artikels 83 Absatz 7 DSGVO Gebrauch gemacht, national zu regeln, ob und in welchem Umfang gegen Behörden und sonstige öffentliche Stellen Geldbußen verhängt werden können. Auch Geldbußen nach § 33 sollen nicht gegen öffentliche Stellen nach § 5 Absatz 1 verhängt werden dürfen."[9]

5. Bezug zum Rechtsträgerprinzip

Die Stellungnahmen und Ausführungen der Landesdatenschutzbehörden oder Gesetzgebern konkretisieren die Haftungsnormen der Länder lediglich. Eine Auffassung bezüglich des Rechtsträgerprinzips aus dem Ordnungswidrigkeitenrecht hat bislang keine Landesdatenschutzbehörde ausdrücklich geteilt. Insoweit lässt sich kein konkreter Rückschluss auf die Auffassung der deutschen Aufsichtsbehörden ableiten.

VI. Konsequenzen für Hochschulen und Forschungseinrichtungen

Eine Auswirkung der Rechtsprechung des EuGHs auf Hochschulen und Forschungseinrichtungen ist nur insoweit zu befürchten, als die Verhängung eines Bußgeldes möglich ist. An den Möglichkeiten der Verhängung eines Bußgeldes wegen Datenschutzverstößen (also den Tatbeständen, die zu einer Bebußung führen) wird das Urteil des EuGHs nichts ändern. Es bleibt beim Katalog der Tatbestände des Art. 83 Abs. 4 - 6. Hieraus ist insbesondere Art. 83 Abs. 5 lit. a) hervorzuheben, wonach bei einem Verstoß gegen die Grundsätze der Verarbeitung personenbezogener Daten (insbesondere Verarbeitung ohne Einwilligung oder sonstigen Berechtigungstatbestand) ein Bußgeld möglich ist. Aber auch Art. 83 Abs. 4 lit. a) ist in der Praxis von Relevanz, welcher statuiert, dass bei einem Verstoß gegen die Pflicht zum Treffen technischer und organisatorischer Maßnahmen zur Sicherheit der Verarbeitung die Verhängung eines Bußgeldes möglich ist.

Bei Hochschulen und Forschungseinrichtungen muss unterschieden werden, ob sie am Wettbewerb teilnehmen oder nicht.

Soweit die Hochschulen oder Forschungseinrichtungen öffentliche Stellen der Länder oder des Bundes sind, gelten für sie die Bestimmungen der jeweiligen LDSG oder des BDSG.[10] Nach den oben geschilderten Besonderheiten der Vorgaben zur Haftung von Behörden können sie grundsätzlich nicht bebußt werden, es sei denn sie nehmen als Unternehmen am Wettbewerb teil.

Wenn sie als Unternehmen am Wettbewerb teilnehmen, gilt für sie wiederum aktuell noch das Rechtsträgerprinzip. Die ausstehende Entscheidung des EuGHs ist deshalb für Hochschulen von Bedeutung: Entscheidet der EuGH gegen eine Vereinbarkeit des Rechtsträgerprinzips mit europäischem Datenschutzrecht, so würde wiederum der Nachweis eines datenschutzrechtlichen Pflichtverstoßes von irgendeinem Mitarbeiter der Einrichtung für die Bebußung ausreichen.

Hochschulen nehmen bei Erfüllung ihrer gesetzlichen Aufgaben (insb. im Rahmen der Forschung und Lehre) in der Regel nicht als Unternehmen am Wettbewerb teil. Sie nehmen nur dann als Unternehmen am Wettbewerb teil, wenn sie am Markt Waren und Dienstleistungen anbieten, die auch private Unternehmen

7 Mitteilung des Senats vom 30. Januar 2018, S. 69 f., abrufbar unter https://www.bremische-buergerschaft.de/drs_abo/2018-01-31_Drs-19-1501_e345f.pdf (zuletzt abgerufen am 07.04.2022).

8 Häufig gestellte Fragen auf der Seite des HBfDI, Unterpunkt Geldbuße, abrufbar unter https://datenschutz.hessen.de/infothek/h%C3%A4ufig-gestellte-fragen-hgf#Geldbu%C3%9Fe (zuletzt abgerufen am 7.4.2022).

9 Gesetzesentwurf der Landesregierung NRW des NRWDSAnpUG EU, S. 157, abrufbar unter https://www.im.nrw/sites/default/files/media/document/file/Gesetzentwurf%20DRS-1981.pdf (zuletzt abgerufen am 7.4.2022).

10 Das BDSG gilt dabei ausschließlich für Hochschulen oder Forschungseinrichtungen des Bundes.

anbieten. Ein Beispiel hierfür wäre der hochschuleigene Merchandise-Shop. Bietet eine Hochschule Merchandising-Produkte an (also z. B. Universitäts-Pullover oder -tassen), so nimmt sie mit diesem Angebot am Wettbewerb teil. Pflichtverstöße im Zusammenhang mit diesem Angebot können dann bebußt werden.

VII. Fazit

Die Debatte um die Haftung von Unternehmen und sonstigen juristischen Personen für Pflichtverstöße war im Ursprung rein rechtspolitisch. Durch den Vorlagebeschluss des KG Berlin und die divergierenden Entscheidungen von LG Bonn und KG Berlin wird daraus zumindest für das Datenschutzrecht eine rechtstatsächliche Debatte: Sieht womöglich schon das aktuell geltende europäische Datenschutzrecht eine Bebußung der gesamten juristischen Person unabhängig von den ihr zugehörigen natürlichen Personen vor?

Die Entscheidung des EuGHs wird daher in der Praxis weitreichende Konsequenzen haben. Sie kann für einen einheitlichen europäischen Haftungsmaßstab im Datenschutzrecht sorgen. Sollte der EuGH entscheiden, dass das in Deutschland geltende Rechtsträgerprinzip nicht mit europäischem Recht vereinbar ist, so würde das die Haftung von juristischen Personen ausweiten. Diese Ausweitung ist jedoch nur beweisrechtlicher Natur. An den Tatbeständen, die zu einer Haftung führen, wird die Entscheidung nichts ändern. Für juristische Personen des öffentlichen Rechts hat die Entscheidung gleichermaßen Bedeutung – allerdings nur sofern sie als Unternehmen am Wettbewerb teilnehmen. Die Teilnahme am Wettbewerb ist weiterhin Grundvoraussetzung für die Bebußung von juristischen Personen des öffentlichen Rechts.

Zeitenwende: BGB goes digital

Die neuen Regelungen zu digitalen Diensten im Bürgerlichen Gesetzbuch

von Johanna Schaller

Mit der Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (Digitale-Inhalte-Richtlinie, kurz: DIDRL) und der Warenkaufrichtlinie (WKRL) wird das Bürgerliche Recht modernisiert und an die fortschreitende Digitalisierung in Deutschland angepasst.

I. Hintergrund

Das „Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen“ wurde am 25.6.2021 „auf den letzten Drücker“, kurz vor Ablauf der Umsetzungsfrist am 1.7.2021 beschlossen und gilt nun seit dem 1.1.2022. Hiermit zieht ein Verbrauchervertrag über digitale Produkte ins Bürgerliche Gesetzbuch (BGB) (§§ 327 ff.) ein. Dieser betrifft den größten Wachstumsmarkt der letzten Jahre, nämlich Verträge über Datenbanken, Smartphones, Smart-TVs, Cloud-Services, Plattform-Angebote, Social-Media, Werbeanwendungen, E-Books, interpersonelle Kommunikationsdienste (E-Mail, Messenger Dienste), Datenträger wie DVDs, CDs, USB Sticks, Speicherkarten sowie die Bereitstellung elektronischer Dateien im Rahmen von 3D-Drucken von Waren. Geregelt wird unter anderem die Verpflichtung der Verkäufer und Anbieter zu Software-Aktualisierungen und Sicherheitsupdates, um eine dauerhafte Nutzbarkeit der Inhalte zu gewährleisten. In einem Atemzug mit der DIDRL umgesetzt wurde die WKRL, die ebenfalls mit der Digital Market Strategy der Europäischen Union (EU) im Jahr 2015 angekündigt wurde. Beide schließen sich in ihrem Anwendungsbereich jeweils gegenseitig aus. Es gibt also keine Überschneidungen - entweder gelangt die eine oder die andere Richtlinie zur Anwendung. Die Umsetzung der WKRL und der DIDRL stellt wohl die weitreichendste Reform des BGB-Vertragsrechts seit der Schuldrechtsreform im Jahr 2002 dar. Das BGB-Vertragsrecht wird digitaler und Verbraucherrechte werden gestärkt. Die Umsetzung des DIDL erfasst nur B2C-Verträge und ist damit reines Verbraucherrecht.[1]

II. Zentrale Neuregelungen

Digitale Inhalte werden in § 327 Abs. 2 BGB definiert als „Daten, die in digitaler Form erstellt und bereitgestellt werden“. Unter digitalen Dienstleistungen sind nach dem Gesetz Dienstleistungen zu verstehen, die die Erstellung, Verarbeitung oder die Speicherung von Daten in digitaler Form oder den Zugang zu solchen Daten ermöglichen, sowie Dienstleistungen, die gemeinsame Nutzung der vom Verbraucher oder von anderen Nutzern der entsprechenden Dienstleistungen in digitaler Form hochgeladenen oder erstellten Daten oder sonstige Interaktionen mit dessen Daten ermöglichen.

Eine wesentliche Änderung des Verbraucherrechts stellt die Gleichstellung von subjektivem mit objektivem Fehlerbegriff im Rahmen des Mangelbegriffs dar (§ 327e BGB).[2]
Das Produkt ist danach nur dann frei von Mängeln, wenn es den subjektiven Anforderungen, den objektiven Anforderungen und den Anforderungen an die Integration entspricht. Wenn der Unternehmer durch den Vertrag zu einer fortlaufenden Bereitstellung über einen Zeitraum (dauerhafte Bereitstellung) verpflichtet ist, ist der maßgebliche Zeitraum für die Beurteilung des Vorliegens eines Produktmangels der gesamte vereinbarte Zeitraum der Bereitstellung (Bereitstellungszeitraum).
Überdies definiert das Gesetz in § 327e Abs. 2 S. 2-4 BGB die wesentlichen Begrifflichkeiten für die Mangelfreiheit: die Funktionalität als die Fähigkeit eines digitalen Produkts, seine Funktionen seinem Zweck entsprechend zu erfüllen; die Kompatibilität als die Fähigkeit eines digitalen Produkts, mit Hardware oder

1 McGrath, Das Dilemma der Digitalen Dienste, DFN-Infobrief Recht 3/2021, S. 5.

2 McGrath, Das Dilemma der Digitalen Dienste, DFN-Infobrief Recht 3/2021, S. 6.

Software zu funktionieren, mit der digitale Produkte derselben Art in der Regel genutzt werden, ohne dass sie konvertiert werden müssen, sowie die Interoperabilität als die Fähigkeit eines digitalen Produkts, mit anderer Hardware oder Software als derjenigen, mit der digitale Produkte derselben Art in der Regel genutzt werden, zu funktionieren.

Zentral für die Gewährleistung der Funktionsfähigkeit und Sicherheit digitaler Inhalte und Dienste ist die neue Pflicht zur Aktualisierung, gem. § 327f BGB.[3] Hiernach müssen während des maßgeblichen Zeitraums Aktualisierungen, die für den Erhalt der Vertragsmäßigkeit des digitalen Produkts erforderlich sind, bereitgestellt werden und der Verbraucher über diese Aktualisierungen informiert werden. Zu diesen erforderlichen Aktualisierungen gehören auch Sicherheitsaktualisierungen.

Bei einem Vertrag über die dauerhafte Bereitstellung eines digitalen Produkts ist der Bereitstellungszeitraum, in allen anderen Fällen der Zeitraum maßgeblich, den der Verbraucher „aufgrund der Art und des Zwecks des digitalen Produkts und unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann". Diese Regelung birgt große Unsicherheiten für die Unternehmer. Denn auch wenn die Festlegung einer starren Frist auf Grund der großen Vielfalt der digitalen Produkte nicht sachgerecht sein dürfte, erscheint eine derart offen gehaltene Formulierung aus Gründen der Rechtssicherheit wenig zielführend. Der Zeitraum für die Bereitstellung von Aktualisierungen kann unter Umständen länger sein, als die gesetzlich geregelte Dauer der Produktgewährleistung (2 Jahre)[4] , sodass aus den Update-Pflichten faktisch eine wesentliche längere Verpflichtung des Unternehmers hinsichtlich des Produkts gegenüber dem Verbraucher resultiert.
§ 327i BGB benennt die Rechte des Verbrauchers bei Mängeln des digitalen Produkts: Nacherfüllung, Beendigung des Vertrages, Minderung des Preises, Schadensersatz oder Ersatz der vergeblichen Aufwendungen.

Obwohl § 327e Abs. 3 BGB den objektiven Mangel den subjektiven Anforderungen gleichstellt, ermöglicht die Regelung des § 327h BGB, dass die Parteien von diesen objektiven Anforderungen durch Vereinbarung abweichen können. Dazu muss der Verbraucher vor Abgabe seiner Vertragserklärung eigens davon in Kenntnis gesetzt werden, dass ein bestimmtes Merkmal des digitalen Produkts von den objektiven Anforderungen abweicht, und diese Abweichung muss im Vertrag ausdrücklich und gesondert vereinbart werden. Für diese gesonderte und explizite Vereinbarung genügt bereits das Ankreuzen eines Kästchens, nicht aber der Vertragsabschluss an sich oder ein vorangekreuztes Kästchen. Damit folgt für die Praxis, dass letztlich durch Vorformulierungen Abweichungen möglich sind, die der Verbraucher dann lediglich gesondert anklicken muss.

Bedeutung hat überdies die Neufassung des § 312 BGB. Zunächst erfasst die neue Formulierung in Abs. 1, nach der Verbraucherverträge keine „entgeltliche Leistung" mehr erfordern, sondern dass sich der Verbraucher „zur Zahlung eines Preises verpflichtet", auch die „digitale Darstellung eines Wertes", mithin etwa virtuelle Währungen, die aber nicht unter das Geldrecht fallen. Des Weiteren umfasst der Anwendungsbereich gem. Abs. 1a BGB nunmehr auch Verträge, bei denen der Verbraucher dem Unternehmer seine personenbezogenen Daten bereitstellt oder sich hierzu verpflichtet.
Hierzu regelt auch § 327 Abs. 3 BGB explizit, dass der vom Verbraucher zu zahlende Preis in der Zurverfügungstellung von Daten liegen kann.[5]

III. Geltung der neuen Regelungen

Für Altverträge, die bis zum 31. Dezember 2021 abgeschlossen werden, gilt noch das alte Recht des BGB. Die neuen Regelungen betreffen also Verträge, die ab dem 1. Januar 2022 abgeschlossen werden. Überdies können die Regelungen aber auch für Verbraucherverträge über die Bereitstellung digitaler Produkte, die vor dem 1. Januar 2022 geschlossen wurden Geltung entfalten, wenn die Bereitstellung des digitalen Produkts erst ab dem 1. Januar 2022 erfolgt.
Unternehmer bzw. Verkäufer trifft die Obliegenheit, die von ihnen verwendeten Allgemeinen Geschäftsbedingungen (AGB) rechtzeitig an die neuen Regelungen anzupassen. Des Weiteren müssen Verkäufer besonders darauf achten, eine Harmonisierung ihrer neuen Pflichten mit ihren Lieferantenverträgen herzustellen, insbesondere was die Verpflichtung zur Bereitstellung von Updates angeht.

3 McGrath, Das Dilemma der Digitalen Dienste, DFN-Infobrief Recht 3/2021, S. 6.
4 ErwGr. 47 DIDRL (2019/770)
5 McGrath, Das Dilemma der Digitalen Dienste, DFN-Infobrief Recht 3/2021, S. 7.

IV. Fazit und Bedeutung für Hochschulen

Wie eingangs erörtert, finden die §§ 327 ff. BGB nur auf Verbraucherverträge Anwendung. Daher sind sie primär nicht von Relevanz für von der Hochschule geschlossene B2B-Verträge, mit Herstellern und Anbietern von Software, Cloudservices oder anderen Anbietern von Produkten mit digitalen Inhalten.

Grundsätzlich betrifft das neue Kaufrecht also nur Händler, die digitale Produkte an Verbraucher verkaufen oder digitale Dienstleistungen erbringen, Online-Shops, die an Verbraucher verkaufen und Hersteller, die evtl. von Händlern in Regress genommen werden.

Das neue Kaufrecht kann somit allein dann relevant werden, wenn die Hochschule digitale Produkte (Inhalte und Dienstleistungen) gegen einen Preis (Geldwert oder die Zurverfügungstellung von Daten) als Unternehmer gegenüber Verbrauchern bereitstellt. Auch Tätigkeiten der öffentlichen Hand, so auch der Hochschulen als juristische Personen des öffentlichen Rechts, können unter den Begriff des Unternehmers gem. § 14 BGB fallen. Voraussetzung dafür ist, dass die konkreten Betätigungen als gewerbliche oder selbstständige berufliche Tätigkeit zu qualifizieren sind.

Die Frage, ob die Hochschule als Unternehmer im Verhältnis zu Verbrauchern, in Gestalt der Studenten oder Dritter, tätig wird, dürfte in der Regel zu verneinen sein. Eine unternehmerische Tätigkeit läge aber dann vor, wenn die Hochschulen wiederholt und mit Gewinnerzielungsabsicht ihren Studenten oder Dritten digitale Produkte oder Dienste gegen Entgelt anbietet. In diesem Falle wären auch die Verträge mit den Herstellern und Lieferanten auf einen Gleichlauf mit den aktualisierten Pflichten der Unternehmer zu überprüfen und anzupassen.

Ausgeschremst ?

Bringt der geplante Transatlantische Datenschutzrahmen Sicherheit bei Datenübertragungen in die USA?

von Owen Mc Grath

Am 25. März dieses Jahres haben die US-Regierung und die Europäische Kommission bekannt gegeben, dass sie sich über die Grundlagen eines neuen Datenschutzabkommens geeinigt haben. Damit soll es zukünftig möglich sein, Daten in den USA mit den europäischen Datenschutzrecht vereinbar verarbeiten zu können. Warum das bisher nicht möglich ist und welche Erfolgschancen das Abkommen hat, soll Inhalt dieses Beitrages sein.

I. Bisherige Rechtslage

Nach der europäischen Datenschutz-Grundverordnung (DSGVO) dürfen personenbezogene Daten nur dann in ein Land, in welchem die DSGVO keine Anwendung findet (Drittland), übermittelt und in diesem verarbeitet werden, wenn dort ein angemessenes datenschutzrechtliches Schutzniveau besteht. Die Feststellung der Angemessenheit des Schutzniveaus obliegt nach Art. 45 Abs. 1, 3 DSGVO der Europäischen Kommission.

In den letzten Jahren hat die Kommission bereits zweimal einen Angemessenheitsbeschluss für den Datentransfer in die USA gefasst. Zuerst das Safe-Harbour-Abkommen und zuletzt das EU-US-Privacy-Shield. Beide Abkommen wurden durch den Gerichtshof der Europäischen Union (EuGH) als unzureichend erklärt. Die Entscheidungen tragen den Namen des Klägers Max Schrems: Schrems I und Schrems II.[1]

Die Abkommen wurden als unzureichend erklärt, weil insbesondere US-Geheimdienste in weiten Teilen Zugriff auf die in den USA verarbeiteten Daten hatten. Betroffenen stand trotz eingerichteten Vermittlungsstellen keine Möglichkeit des effektiven Rechtsschutzes zur Verfügung.

Durch Wegfall der Abkommen ist eine Datenübermittlung in die USA nicht mehr auf Art. 45 DSGVO zu stützen. Nach Art. 46 DSGVO ist die Übermittlung personenbezogener Daten in ein Drittland allerdings auch ohne Angemessenheitsbeschluss möglich, „sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen." Zur Umsetzung dieser Vorgaben stehen den für die Datenverarbeitung verantwortlichen Personen (Verantwortliche) sog. Standardvertragsklauseln (SCC=Standard Contractual Clauses) zur Verfügung.[2] Hierbei handelt es sich um von der Europäischen Kommission entwickelte Vertragstexte, welche bei der Vertragsentwicklung zwischen Verantwortlichen und Verarbeitern in Drittländern eingebunden werden können.[3] Allein der Einsatz von SCCs reicht aber nicht aus, um den Anforderungen des Art. 46 DSGVO gerecht zu werden. Es bedarf ferner des Einsatzes von technisch-organisatorischen Maßnahmen (TOM), welche das Datenschutzniveau sichern.[4] Das kann zum Beispiel die Verschlüsselung von Daten sein. Abseits des Art. 46 DSGVO besteht noch die Möglichkeit die Übermittlung unter den recht engen Möglichkeiten des Art. 49 Abs. 1 DSGVO zu rechtfertigen. Die Hürden für diese Möglichkeit liegen aber, ohne dass hier eine nähere Auseinandersetzung stattfinden soll, sehr hoch und sind damit nur nachrangig in Erwägung zu ziehen.

1 Hierzu: Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 8/2020.

2 Hierzu: Wellmann, O ihr gnadenbringenden Standarddatenschutzklauseln, DFN-Infobrief Recht 12/2020.

3 Abrufbar unter: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de.

4 Hierzu: John, New Schrems, new Me(crosoft), DFN-Infobrief Recht 2/2022.

II. Das neue Trans-Atlantic Data Privacy Framework

Ende März haben nunmehr die Europäische Kommission und die US-Regierung Informationen zu einem neuen Abkommen herausgegeben, welches an die Stelle der aufgehobenen Angemessenheitsbeschlüsse rücken soll. Das Factsheet zum sog. Trans-Atlantic Data Privacy Framework[5] informiert in wenigen Stichpunkten über die Eckdaten des Abkommens.

Zukünftig soll ein freier und sicherer Datenstrom zwischen der EU und teilnehmenden US-Unternehmen möglich sein.
US-Nachrichtendienste sollen nur noch Zugriff auf Daten haben, soweit dies zum Schutz der nationalen Sicherheit notwendig ist. Zur Wahrung der Datenschutz- und Bürgerrechte sollen die Geheimdienste geeignete Verfahren einführen.

Weiterhin soll ein zweistufiges Rechtsbehelfssystem etabliert werden, welches die Beschwerden der europäischen Bürger in Bezug auf den Zugriff von Geheimdiensten bearbeitet. Geleitet werden soll dieses von einem quasigerichtlichen Gremium, welches berechtigt sein soll, umfassend zu ermitteln und Abhilfemaßnahmen anordnen zu können.

Unternehmen aus den USA, welche Daten aus der EU verarbeiten, sollen strengen Verpflichtungen zum Schutz der Daten unterliegen. Hierunter fällt auch die Selbstzertifizierung vor dem US-Handelsministerium.

Diese Eckpunkte sollen nunmehr in einen gesetzlichen Rahmen gegossen werden. Auf Seiten der USA soll dies mittels sog. Executive Orders geschehen. Hierbei handelt es sich um Verwaltungsvorschriften, die unmittelbar durch die US-Regierung erlassen werden und keine Parlamentsgesetze darstellen. Von Seiten der EU soll ein entsprechender Angemessenheitsbeschluss entworfen werden. Die Einigung über die finalisierten Texte soll informell erfolgen und nicht mittels Staatsvertrag. Sowohl der Europäische Datenschutzausschuss als auch die einzelnen Mitgliedsstaaten können sich zum Angemessenheitsbeschluss äußern.

Ein endgültiger Beschluss wird frühestens in sechs Monaten erwartet.

5 Abrufbar unter: https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf.pdf.

III. Kommt bald Schrems III?

Unklar ist fürs Erste, ob der geplante Angemessenheitsbeschluss der Prüfung des EuGH, mit welcher zeitnah nach Veröffentlichung zu rechnen ist, standhalten wird.

Insofern anzuzweifeln ist insbesondere, ob das angekündigte zweistufige Rechtsbehelfssystem den Anforderungen an einen gerichtlichen Rechtsbehelf gerecht wird und, ob die Umsetzung der Anforderungen an die USA mittels Executive Orders ausreichen. Der EuGH forderte in seinem Urteil zum Privacy-Shield „klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme“. Executive Orders binden in der Regel nur intern die Verwaltung und sind nicht einklagbar.

Ferner drängt sich die Frage auf, ob die Beschränkung der Zugriffsrechte der US-Geheimdienste auf Fälle, die dem Schutz der nationalen Sicherheit dienen, nicht Tür und Tor für eine weite Auslegung der Begriffe öffnet. Dehnt man den Schutz der nationalen Sicherheit gerade in präventiver Hinsicht aus, wird eine Beschränkung der Zugriffsrechte zur Makulatur verkommen.

Es bleibt abzuwarten, wie der EuGH das finalisierte Abkommen bewertet.

IV. Fazit und Auswirkungen für wissenschaftliche Einrichtungen

Die gesicherten Informationen zum geplanten Transatlantischen Datenschutzrahmen beschränken sich auf wenige Seiten bedeutungsschwangeren Text. Trotz Ausbleibens konkreter rechtlicher Ausgestaltungen, werden schon jetzt kritische Stimmen laut, die die Vereinbarungen für unzureichend erachten.
Bis die finalen Rechtsdokumente vorliegen, fordern Verarbeitungen personenbezogener Daten in den USA weiterhin komplizierte Umgehungstaten im Einklang mit Art. 46, 49 DSGVO.
Soweit es bisher ersichtlich ist, wird auch nach Entwurf und Inkrafttreten des neuen Angemessenheitsbeschlusses auf lange Sicht nicht die gewünschte Rechtssicherheit erreicht werden.
Für Hochschulen und wissenschaftliche Einrichtungen bedeutet das auf absehbare Zeit, soweit möglich auf Datenverarbeitungen im US-Ausland zu verzichten und bei Einführung des neuen Angemessenheitsbeschlusses nicht zu viel Vertrauen in die Zulässigkeit entsprechender Datentransfers zu stecken.

Impressum

Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz.

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: DFN-Verein@dfn.de

Redaktion

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der WESTFÄLISCHEN WILHELMS-UNIVERSITÄT, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung
Unter Leitung von Prof. Dr. Thomas Hoeren
Leonardo-Campus 9
D-48149 Münster
E-Mail: recht@dfn.de