DEN
infobrief recht

12 / 2020
Dezember 2020

O ihr gnadenbringenden Standarddatenschutzklauseln

Die Europäische Kommission legt einen Entwurf neuer Standarddatenschutzklauseln vor und die Datenschutzgemeinde fragt sich: „Ja, ist denn heut` schon Weihnachten“?

Morgen, Kinder, wird’s was geben

Die Möglichkeit einer Vergabe von Zertifizierungen nach Art. 42 DSGVO rückt näher

(No) Return to Sender

Auskunftsanspruch aus Art.15 DSGVO umfasst nicht eigene E-Mails

O ihr gnadenbringenden Standarddatenschutzklauseln

Die Europäische Kommission legt einen Entwurf neuer Standarddatenschutzklauseln vor und die Datenschutzgemeinde fragt sich: „Ja, ist denn heut` schon Weihnachten“?

von Maximilian Wellmann

Kurz vor Weihnachten macht die Europäische Kommission mit ihrem Entwurf neuer Standarddatenschutzklauseln den Datenschützern ein verfrühtes Weihnachtsgeschenk. Wie jedoch auch im realen Leben, besteht für den Schenkenden stets die Gefahr mit dem zehnten Paar Socken beim Beschenkten weniger freudige Reaktionen auszulösen, als mehr resignierende Seufzer und ein pflichtschuldiges „Danke“ zu ernten. Ob die neuen EU-Standarddatenschutzklauseln geeignet sind eher die erste oder die zweite Reaktion auszulösen, wird dabei Gegenstand des nachfolgenden Beitrags sein.

I. Funktion und Wirkung von Standarddatenschutzklauseln

Bei den EU-Standarddatenschutzklauseln, handelt es sich um Bestimmungen, die Bestandteil eines Vertrages sein können, welcher eine Datenübermittlung an eine Stelle außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung (DSGVO) zum Gegenstand hat. Größtes Manko der aktuellen EU-Standarddatenschutzklauseln (Beschluss der Kommission v. 5.2.2010 – 2010/87/EU, Beschluss der Kommission v. 15.6.2001 – 2001/497/EG) ist allerdings, dass sie noch auf der Vorgängerregelung der DSGVO, der Datenschutz-Richtlinie aus dem Jahr 1995 (RL 95/46/EG) fußen und lediglich durch einen Kommissionsbeschluss aus 2016 im Bereich der Auftragsverarbeitung angepasst wurden (Beschluss der Kommission v. 16.12.2016 – C (2016)8471). Diese Entscheidung der Kommission erfolgte dabei im Lichte der ablehnenden Entscheidung des Europäischen Gerichtshofs (EuGH) in der Causa „Schrems I“ (EuGH, Urt. v. 6.10.2015 - C-362/14 – Schrems I)[1], in der das sog. „Safe Harbour“ Abkommen zwischen der EU und den USA gekippt wurde. Für den Datentransfer entfiel damit die maßgebliche Rechtsgrundlage und ein Zielkonflikt mit der DSGVO und seinem in Art. 44 S. 2 DSGVO normierten Gebot das europäische Datenschutzniveau „nicht zu untergraben“, entstand. Auf den Plan traten schon damals die EU-Standarddatenschutzklauseln, die bis zur Verabschiedung des EU-US Privacy Shields als maßgebliche Rechtsgrundlage für den Datentransfer in die USA fungierten.

Auch mit Blick auf aktuelle Verarbeitungskonstellation wie der Auftragsverarbeitung in Drittstaaten, bei der es auf Weisung des Verantwortlichen zu einer Datenverarbeitung des Auftragsverarbeiters kommt, bietet sich der Rückgriff auf Standarddatenschutzklauseln an. Hierüber ist es den Parteien möglich „standardisiert“ eine Vielzahl von materiellen Regelungen sowie das anwendbare Recht zu bestimmen. Ein gewichtiger Vorteil zeigt sich zudem darin, dass den Vertragsparteien ein hohes Maß an Rechtssicherheit mit Blick auf die datenschutzkonforme Verarbeitung personenbezogener Daten zu Teil wird und eine ansonsten notwendige Genehmigung des Datentransfers durch die zuständige Aufsichtsbehörde entfällt, soweit die Klauseln unverändert in das Vertragswerk eingebaut werden.

1 Vertiefend: Sydow, Kein sicherer Hafen für unsere Daten? DFN-Infobrief Recht 12/2015.

II. Und täglich grüßt das Murmeltier: Schrems II und seine Folgen

Nachdem die Europäische Kommission das EU-US Privacy Shield verabschiedet hatte, nahm der Stellenwert der EU-Standarddatenschutzklauseln für den Datentransfer in die USA allerdings (erneut) ab. Maßgebliche Rechtsgrundlage der Datenübertragung war danach ein Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO. Die gesetzliche Systematik der DSGVO sieht insoweit ein subsidiäres Verhältnis der EU-Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c DSGVO) zu einem solchen Angemessenheitsbeschluss vor, heißt es doch in Art. 46 Abs. 1 DSGVO wörtlich „Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt, (...)".

Mit dem ruhigen Fahrwasser, in dem sich der Datentransfer befand, ist es aber seit dem jüngst ergangenen Urteil des EuGH (EuGH, Urt. v 16.7.2020 - C-311/18- Schrems II)[2], dass das EU-US Privacy Shield kippte, vorbei. Das Urteil stellt vielmehr erneut eine Zäsur in der Datenübertragungspraxis dar, ist allerdings mit Blick auf das Safe Harbour Urteil und seine inhaltlichen Aussagen jedoch nicht in Gänze neu. Auch die Auswirkungen des Urteils auf die hier diskutierten EU-Standarddatenschutzklauseln sind beachtlich, wurden diese doch dadurch erneut zum letzten Rettungsanker der europäisch-amerikanischen Datenübermittlung.

Aktuell können danach allein die unveränderten Standarddatenschutzklauseln aus 2010 als Rechtsgrundlage für einen Datentransfer in die USA oder einen sonstigen Drittstaat herangezogen werden. Gleichwohl ändert das Urteil des EuGH jedoch nichts an der datenschutzrechtlich problematischen Situation in den USA, in denen es staatlichen Sicherheitsbehörden möglich ist eine „nicht auf das zwingend erforderliche Maß" beschränkte Überwachung beispielsweise auf Grundlage des CLOUD Acts vorzunehmen. Um das Postulat des angemessenen Datenschutzniveaus im Empfängerland jedoch nicht zum „zahnlosen Tiger" verkommen zu lassen, hat der EuGH in Schrems II deshalb auch die Konturen der Anwendung der Standarddatenschutzklauseln nachgeschärft. Der Datenexporteur muss nunmehr nach Ansicht des EuGH vor der Datenübertragung unter Beachtung des konkreten Schutzniveaus für die übertragenen Daten eine Analyse des Übertragungswegs vornehmen, die mit der Speicherung im Drittstaat verbundenen Risiken evaluieren sowie eine Analyse zumutbarer Alternativen (z.B. Speicherung in Europa) vornehmen. Fällt diese Bewertung negativ aus und ist in der Folge zu konzedieren, dass das Schutzniveau nicht mit dem europäischen vergleichbar ist, muss der Datenexporteur zusätzliche Maßnahmen ergreifen, um den Schutz der Daten zu garantieren. Falls diese jedoch nicht ausreichen, dürfen im Ergebnis keine personenbezogenen Daten in den Drittstaat übertragen werden.

2 Vertiefend: Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 8/2020.

III. Der Entwurf neuer EU-Standarddatenschutzklauseln

Die Entscheidung des EuGH ist eine krachende „Watschen" für die Europäische Kommission und hat diese massiv unter Handlungsdruck gesetzt, die Rechtssicherheit im Bereich der transatlantischen Datenübertragung schnell wiederherzustellen. Zur Schadensbegrenzung wurden deshalb die Pläne zur Novellierung der Standarddatenschutzklauseln, die bereits seit 2017 in der Schublade lagen, eilig hervorgekramt und in die hier diskutierte Entwurfsvorlage gegossen. Treiber der Erneuerung ist dabei sicherlich auch die Tatsache, dass der BREXIT immer näher rückt und das Problem eines Drittstaates alsbald auch vor die eigene kontinentaleuropäische Haustür rücken wird.

Inhaltlich sieht der Entwurf der EU-Standarddatenschutzklauseln zwei Dokumente vor. Bei dem ersten Dokument handelt es sich um den Entwurf einer Beschlussvorlage der Kommission, der den Zweck und den Anwendungsbereich der Standarddatenschutzklauseln beschreibt, wohingegen im zweiten Dokument, dem sog. Annex, der konkrete Vertragstext folgt. Dieser beschreibt dabei verschiedene einschlägige Konstellationen der Verarbeitung und enthält Formulare, die von den Vertragsparteien entsprechend der beabsichtigten Datenübermittlung ausgefüllt und unterzeichnet werden können.

1. Zielsetzung

Grundlegend geht es dem Entwurf um die Bewältigung des Spagats zwischen neuen, immer komplexer werdenden transnationalen Verarbeitungsvorgängen, an denen oftmals mehrere Datenimporteure und –exporteure beteiligt sind und dem Schutz personenbezogener Daten in Drittstaaten außerhalb

der EU. Maßgeblich folgen die neuen Standarddatenschutzklauseln dabei dem Paradigma eines Schutzniveaus, das mit dem Schutzniveau im Geltungsbereich der DSGVO vergleichbar („equivalent“) ist. Diese Zielsetzung geht auf Art. 44 S. 2 DSGVO zurück und spiegelt den generellen Ansatz des Entwurfs wieder einer Anpassung der EU-Standarddatenschutzklauseln an die DSGVO vorzunehmen. Die Novellierung greift dabei sowohl tatsächlich als auch rechtlich geänderte Rahmenbedingungen auf und versucht angemessen auf die oben beschriebenen Entwicklungen mit sog. „safeguardes“ („geeignete Garantien“) zu reagieren, die die Auswirkungen der Gesetze des Bestimmungsdrittlands auf die Einhaltbarkeit der Standarddatenschutzklauseln durch den Datenimporteur regeln.

2. Aufbau und Inhalt

Das für die Praxis maßgebliche Dokument stellt das Annexdokument dar. Nachfolgend sollen einige der darin enthaltenen Klauseln schwerpunktmäßig beschrieben werden.

Betrachtet man zunächst den Aufbau der Standarddatenschutzklauseln, gliedert sich dieser in einen ersten Teil mit allgemeinen Bestimmungen, einen zweiten Teil, in denen die Pflichten der Vertragsparteien („obligations of the parties“) konkret ausgestaltet werden und einen dritten Teil mit Schlussbestimmungen. Der zweite Teil ist das Kernstück der neuen EU-Standarddatenschutzklauseln und untergliedert sich in insgesamt vier Module, die verschiedene Konstellationen des Datentransfers aus dem Geltungsbereich der DSGVO beschreiben (Modul 1: Datentransfer Verantwortlicher – Verantwortlicher; Modul 2: Datentransfer Verantwortlicher – Auftragsverarbeiter; Modul 3: Datentransfer Auftragsverarbeiter- Auftragsverarbeiter; Modul 4: Datentransfer Auftragsverarbeiter – Verantwortlicher).

Systematisch wird dabei vor jeder einzelnen Standarddatenschutzklausel angegeben für welche der vier Konstellation des Datentransfers die nachfolgende Bestimmung einschlägig ist. Steigt man sodann in die Analyse der einzelnen Klauseln ein, sieht die erste Klausel vor, dass der Datenexporteur prüft, ob der Datenimporteur in der Lage ist, die nachfolgend aufgeführten vertraglichen Pflichten einzuhalten. Der Katalog statuiert dabei differenzierend zwischen den vier Verarbeitungskonstellationen, u.a. wechselseitige Pflichten der Parteien im Hinblick auf die Datenminimierung (II.1.3), der sicheren Übertragung personenbezogener Daten (II.1.5) und der vorzunehmenden Dokumentation (II. 1.9).

Die sich anschließende zweite Klausel greift das Problem kollidierenden nationalen Rechts auf, dass mit den EU-Standarddatenschutzklauseln in Konflikt steht. Hier geht Klausel II.2(a) von einer grundsätzlichen Vereinbarkeit nationaler Regelungen mit den EU-Standarddatenschutzklauseln aus. Wenn der Datenimporteur jedoch Grund zur Annahme hat, dass er Adressat einer nationalen Regelung wird, die mit den Vorgaben aus Klausel II.2(a) nicht vereinbar erscheint, lebt eine Notifizierungspflicht gegenüber dem Datenexporteur auf, der dann unverzüglich Maßnahmen zu ergreifen hat, um den sicheren Datentransfer wiederherzustellen oder ihm als ultima ratio sogar das Recht einräumt den Vertrag zu kündigen.

Die dritte Klausel betrifft den in der Praxis wichtigen Anwendungsfall eines verbindlichen behördlichen Auskunftsersuchens zur Weitergabe personenbezogener Daten durch den Datenimporteur (Stichwort: Überwachung). Klausel II.3.1 sieht hier vor, dass der Datenimporteur den Datenexporteur von dem Auskunftsersuchen unterrichtet soweit dies im Einklang mit den Vorgaben des jeweiligen nationalen Rechts unter den konkreten Umständen gestattet ist. Dabei ist jedoch der grundlegende Tenor der Standarddatenschutzklauseln zu beachten, dass eine Weitergabe nur dann erfolgen soll, wenn die Gesetze des Bestimmungsdrittlandes den Datenimporteur nicht daran hindern, diese Klauseln einzuhalten (Rekurs auf Klausel 2). Was den Umfang der Mitteilung angeht, sind Details zu den angeforderten personenbezogenen Informationen, das anfordernde Amt, die Rechtsgrundlage für den Antrag und die erteilte Antwort zu übermitteln. Zudem sieht die Klausel vor, dass der Importeur gegebenenfalls alle verfügbaren Rechtsmittel zur Anfechtung des Antrags ausschöpfen soll.

Die vierte Klausel behandelt den Einsatz von Unterauftragsverarbeitern. Diese Klausel ist gänzlich neu im Vergleich zur Vorgängerregelung und sieht vor; dass zwischen dem Datenimporteur und dem Unterauftragsverarbeiter ein schriftlicher Vertrag „written contract“ geschlossen wird, der dieselben Datenschutzbestimmungen enthält, denen der Datenimporteur nach den EU-Standarddatenschutzklauseln mit dem Datenexporteur unterliegt.

Auch die in Klausel Nr. 5 statuierten Betroffenenrechte werden umfassend neu geregelt. Der Datenimporteur erklärt sich

hiernach bereit, Betroffene unverzüglich in den Grenzen der zwingenden nationalen Bestimmungen zu benachrichtigen, wenn er einen rechtsverbindlichen Antrag einer Behörde auf eine Datenherausgabe erhält.

Ergänzt wird dieser Pflichtenkatalog noch durch Klauseln, die die Einlegung von Rechtsmitteln regeln (Nr. 6), Vorgaben zur Haftung (Nr. 7) und Entschädigung (Nr. 8) machen und Pflichten gegenüber den Aufsichtsbehörden (Nr. 9) statuieren.

3. Zusammenfassung und Bewertung

Die Europäische Kommission versucht mit der Vorlage des Entwurfs, die EU-Standarddatenschutzklauseln für den immer stärker zunehmenden internationalen Datenaustausch zukunftsfest zu machen. Auch wenn aus dem Schrems-Lager bereits skeptische Stimmen kommen, bleibt dennoch zu konstatieren, das inhaltlich vor allem die deutliche Erweiterung der Klauseln im Bereich der Unterauftragsverarbeitung ein Gewinn darstellt. Wohlmeinende Stimmen sprechen in Bezug auf die neuen EU-Standarddatenschutzklauseln gar vom „Schweizer Taschenmesser" des internationalen Datentransfers. Vormals nicht erfasste Fälle, wie der eines deutsches Unternehmens, das einen Vertrag mit der EU-Niederlassung eines US-Anbieters schließt, Teile der Datenverarbeitung aber bei deren Muttergesellschaft in den USA stattfinden, werden nunmehr erfasst. Auch die bisher unklare Konstellation eines in der EU ansässigen Auftragsverarbeiters, der für einen außerhalb der EU ansässigen Auftraggeber personenbezogene Daten verarbeitet, wird in den neuen Klauseln adressiert. Einen höheren Grad der Flexibilisierung schafft zudem die in I.6 implementierte „Docking Clause", die es Dritten, bisher nicht an dem Vertrag beteiligten Personen, ermöglicht durch das Ausfüllen entsprechender Anhänge dem Vertrag beizutreten. Daneben werden aber auch eine Vielzahl altbewährter Regelungen in den Entwurf des neuen Vertragswerkes überführt, sodass insgesamt eine deutliche Erweiterung des Anwendungsbereichs auszumachen ist.

IV. Auswirkungen auf Hochschulen und Forschungseinrichtungen

Die Relevanz neuer EU-Standardvertragsklauseln für Hochschulen und Forschungseinrichtungen sollte nicht unterschätzt werden. In Zeiten der Coronavirus-Pandemie haben eine Vielzahl von Hochschulen und Forschungseinrichtungen auf Hybridlehre umgestellt. Zur Umsetzung dieses hybriden Ansatzes ist in vielen Fällen Videokonferenzsoftware lizenziert worden, deren Anbietern wie beispielsweise ZOOM, ihren Hauptsitz in den USA haben. Im Zuge der Implementierung solcher Systeme wurden dabei auch zahlreiche Auftragsverarbeitungsverträge geschlossen, die den Einfluss des Verantwortlichen sichern und eine datenschutzkonforme Nutzung und Datenübertragung gewährleisten sollen. Integraler Bestandteil dieser Verträge sind dabei oftmals die alten EU-Standarddatenschutzklauseln. Sollte der jetzt vorgelegte Entwurf durch die Europäische Kommission zeitnah beschlossen werden, würde dies für die Hochschulen und Forschungseinrichtungen einen erheblichen Anpassungsbedarf nach sich ziehen, da sämtliche Verträge, die EU-Standarddatenschutzklauseln beinhalten, innerhalb der vorgesehenen Übergangsfrist von einem Jahr ab Inkrafttreten, zu ändern wären. Die positive Kehrseite dieses Anpassungsbedarfs wäre jedoch die (Wieder-) Herstellung des rechtssicheren Datentransfers in Drittstaaten, an dem mit Blick auf Datenschutzcompliance auch die Hochschulen und Forschungseinrichtungen interessiert sein dürften. Die Euphorie sollte dennoch nicht zu groß werden, vermag doch auch der Entwurf neuer Standarddatenschutzklauseln das Paradoxon zwischen amerikanischen Sicherheitsinteressen und dem Ziel der DSGVO, die in Europa verarbeiteten personenbezogenen Daten umfassend zu schützen, nicht aufzulösen. In welcher Form die EU-Standarddatenschutzklauseln letztlich beschlossen werden, kann zu diesem Zeitpunkt noch nicht beantwortet werden. Fest steht insoweit nur, dass die Konsultationsfrist am 10. Dezember 2020 endet und es bereits Anfang 2021 zu einer Beschlussfassung seitens der Europäischen Kommission kommen könnte.

Morgen, Kinder, wird's was geben

Die Möglichkeit einer Vergabe von Zertifizierungen nach Art. 42 DSGVO rückt näher

von Nicolas John

Die Idee des Gesetzgebers hinter Datenschutz-Zertifizierungen nach Art. 42 Datenschutz-Grundverordnung (DSGVO) war es, die Einhaltung der DSGVO zu verbessern, einen transparenteren Datenschutz zu schaffen und die Arbeit der Aufsichtsbehörden zu reduzieren. Doch vermisst man zwei Jahre nach Inkrafttreten der DSGVO noch immer die versprochenen Datenschutzsiegel i.S.d. Art. 42 Abs. 1 DSGVO. Aber das wird sich bald ändern. Der nachfolgende Beitrag schafft eine Übersicht zum aktuellen Stand der Akkreditierungs- und Zertifizierungsverfahren.

I. Einleitung

Spätestens nach der „Schrems II"-Entscheidung des Europäischen Gerichtshofs (EuGH) und der damit einhergehenden Unwirksamkeit des EU-US-Privacy-Shield-Abkommens[1] werden viele Verantwortliche bei der Recherche nach Möglichkeiten für einen rechtmäßigen Datenexport auf die Zertifizierung gemäß Art. 42 DSGVO gestoßen sein. Denn diese können anstelle eines Angemessenheitsbeschlusses, wie es das Privacy-Shield war, unter bestimmten Umständen ebenso Datenexporte rechtfertigen (Art. 46 Abs. 2 lit. f DSGVO).

Aber die recherchierende Person wird ebenso schnell herausgefunden haben, dass die Durchführung einer Datenschutz-Zertifizierung in der Praxis mangels akkreditierter Zertifizierungsstellen in Deutschland bislang nicht möglich ist. Doch dieser Umstand ändert sich derzeit. Die deutsche Akkreditierungsstelle (DAkkS) und die Datenschutz-Aufsichtsbehörden führen seit Inkrafttreten der DSGVO die erforderlichen und komplexen Verfahren, Akkreditierungskriterien aufzustellen, um nun interessierte Stellen akkreditieren zu können. Erst mit dem Erhalt der Akkreditierung können diese Stellen beginnen, Datenschutz-Zertifizierungen für Verantwortliche und Auftragsverarbeiter auszustellen.

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

II. Bedeutung der Datenschutz-Zertifizierung

Die freiwillige Zertifizierung nach Art. 42 DSGVO stellt ein Mittel dar, die datenschutzkonforme Datenverarbeitung durch den Verantwortlichen oder Auftragsverarbeiter zu bescheinigen. Nach Erwägungsgrund 100 der DSGVO soll hierdurch die Einhaltung der Verordnung verbessert werden, da unabhängige Prüfer die Datenverarbeitungsprozesse überprüfen. Zudem soll eine höhere Transparenz für die betroffene Person geschaffen werden, indem ein schneller Überblick über das Datenschutzniveau der entsprechenden Produkte und Dienstleistungen ermöglicht wird.

Für den Verantwortlichen kann eine Zertifizierung beim Nachweis der Einhaltung seiner Pflichten, der Einhaltung des Privacy by Design und des Privacy by Default, der Einhaltung der Anforderungen an Auftragsverarbeiter oder bei der Beurteilung der Datensicherheit herangezogen werden. Dies stellt eine Privilegierung im Rahmen der aufsichtsrechtlichen Kontrolle dar. Es ist aber zu betonen, dass eine Zertifizierung weder die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters mindert, noch Aufsichtsbehörden bindet, noch die Haftung nach Art. 82 DSGVO ausschließt. Allerdings erleichtert dies dem Verantwortlichen oder Auftragsverarbeiter gegebenenfalls die ihm obliegende Beweisführung.

Ebenso kann der Verantwortliche oder insbesondere der Auftragsverarbeiter die Zertifizierung anhand eines ausge-

gebenen Datenschutzsiegels und/oder -prüfzeichens als Wettbewerbsvorteil nutzen, um die datenschutzkonforme Verarbeitung der personenbezogenen Daten innerhalb seines Produkts überzeugend gegenüber potenziellen Kundinnen und Kunden zu versichern.

Darüber hinaus kann die Zertifizierung wie oben schon erwähnt als geeignete Garantie i.S.d. Art. 46 Abs. 2 lit. f DSGVO für die Übermittlung von personenbezogenen Daten in Drittstaaten fungieren, soweit das Zertifizierungsverfahren i.S.d. Art. 42 Abs. 2 DSGVO speziell für den Datenexport vorgesehen ist.

III. Begriffsbestimmungen

Auf die Begriffe Akkreditierung und Zertifizierung ist aufgrund der Verwechslungsgefahr kurz einzugehen.
Die Akkreditierung stellt die Bestätigung und Anerkennung der technischen Kompetenz einer sogenannten Konformitätsbewertungsstelle (KBS) dar, welche die Zertifizierungen vornimmt. Durch den Nachweis gegenüber einer unabhängigen Akkreditierungsstelle wird sichergestellt, dass die KBS ihre Tätigkeiten fachlich kompetent, unter Beachtung gesetzlicher Anforderungen und auf international vergleichbarem Niveau erbringt.

Die Zertifizierung ist dagegen die Bestätigung durch eine dritte Seite (der KBS), dass vorgeschriebene Anforderungen nach einer bestimmten Norm – bei der Datenschutz-Zertifizierung die ISO-Norm EN-ISO/IEC 17065/2012 gemäß Art. 43 Abs. 1 S. 2 lit. b DSGVO – erfüllt werden. Zum jetzigen Zeitpunkt haben sich zwar schon diverse „Datenschutz-Zertifikate“ und „Datenschutzsiegel“ in verschiedenen Formen auf dem europäischen Markt etabliert, jedoch stellen diese keine Zertifizierungen i.S.d. Art. 42 DSGVO dar und entfalten daher nicht die Wirkungen der Art. 42-Zertifizierungen.

IV. Stand der Akkreditierungs- und Zertifizierungsverfahren

Nach Art. 42 Abs. 5 S. 1, 43 Abs. 1 DSGVO sind akkreditierte Zertifizierungsstellen oder die Aufsichtsbehörden parallel für die Erteilung der Zertifizierungen zuständig. Doch um international anerkannte Zertifizierungen vornehmen zu können, bedarf es zunächst allgemein anerkannte Akkreditierungskriterien, um anschließend Kriterien für die Zertifizierungsverfahren erarbeiten zu können. Hierfür müssen sich verschiedene Stellen auf europäischer und nationaler Ebene abstimmen.

Gemäß § 39 Bundesdatenschutzgesetz (BDSG) obliegt die Akkreditierungsbefugnis in Deutschland der DAkkS und den Aufsichtsbehörden. Die Kriterien für eine Akkreditierung hatte die DAkkS und die Aufsichtsbehörden schon bis August 2018 entwickelt und von der Datenschutzkonferenz (DSK) beschließen lassen. Anschließend waren diese dem Europäischen Datenschutzausschuss (EDSA) zur Stellungnahme vorzulegen. Doch aufgrund fehlender Leitlinien für den EDSA konnte die Einreichung erst im Januar 2020 geschehen. Ende Mai 2020 wurden nach der Rückmeldung des EDSA die Kriterien nochmals angepasst, die DSK fasste einen neuen Beschluss hierüber und die Kriterien wurden erneut beim EDSA eingereicht. Die Stellungnahme steht laut Website der DAkkS aktuell noch aus.[2]

Anträge auf Akkreditierung sind dennoch schon seit dem 1. Januar 2019 möglich, welche einheitlich bei der DAkkS einzureichen sind. Um akkreditiert werden zu können, muss die interessierte Stelle ein Zertifizierungsprogramm vorlegen, welches umfangreich die Prozesse und Kriterien für ihre Prüfungen beschreibt. Anhand dieses Programms findet die Abnahme der Kriterien der Stelle durch die zuständige Aufsichtsbehörde und der DAkkS statt. Zum jetzigen Zeitpunkt wurden von interessierten Stellen schon entsprechende Anträge gestellt, eine Abnahme hat bislang jedoch noch nicht stattgefunden.

Sobald die Akkreditierung von der Datenschutz-Aufsichtsbehörde und der DAkkS bewilligt wurde, muss die zuständige Aufsichtsbehörde noch eine Befugniserteilung i.S.d. § 39 BDSG aussprechen, damit die Zertifizierungsstelle tätig werden darf. Stimmen aus den Datenschutzzentren prognostizieren dabei eine potenzielle Durchführung der ersten Zertifizierungsverfahren für das erste Halbjahr 2021.[3]

2 https://www.dakks.de/content/projekt-datenschutz (zuletzt abgerufen am 10.11.2020).
3 So z.B. Krasemann, DuD 2020, 645, 648

V. Ausblick und Bedeutung für Hochschulen und Forschungseinrichtungen

Auch wenn die DSGVO nun schon über zwei Jahre in Kraft ist, hat sich der Prozess für die Implementierung von Datenschutz-Zertifizierungen erheblich verzögert, nicht zuletzt, weil die komplexe Kommunikation aufgrund der Zuständigkeitsmechanismen zwischen den europäischen und nationalen Organen sich als zeitintensiv herausstellt.

Dennoch sollte das Instrument der Zertifizierungen nach Art. 42 DSGVO nicht als zu aufwendig oder nutzlos abgetan werden. Gerade im Forschungs- und Hochschulbereich können Zertifizierungen beispielsweise als Auswahlmerkmal auf der Suche nach datenschutzkonformer Software dienen. Soweit ein Softwareanbieter (als potenzieller Auftragsverarbeiter) der interessierten Hochschule (als potenzielle Verantwortliche) durch seine Zertifizierungen den Datenschutz und die Datensicherheit versichern kann, wird in vielen Fällen eine aufwändige Detailprüfung der Software entfallen können.

Aber auch für die Hochschule als Datenverarbeiterin kann eine Zertifizierung von Interesse sein. Die DSGVO-konforme Datenverarbeitung anhand eines europäischen Datenschutzsiegels bestätigt zu sehen, wird sensibilisierten Studierenden in Zeiten von digitalen Semestern positiv ins Auge fallen. Außerdem fände auf diese Weise eine Überprüfung der Datenverarbeitungsprozesse der Hochschule durch eine unabhängige dritte Zertifizierungsstelle statt und könnten bei Bedarf entsprechend angepasst werden.

Doch als Alternative für den Datenexport in die USA wird die Zertifizierung vermutlich unter dem Eindruck der „Schrems II"-Entscheidung vorerst nicht weiterhelfen. Denn um als geeignete Garantie i.S.d. Art. 46 Abs. 2 lit. f DSGVO für den Datenexport zu fungieren, muss die hierauf speziell zugeschnittene Zertifizierung den Nachweis erbringen, dass der Datenempfänger im Drittland die Verarbeitung entsprechend den Anforderungen der DSGVO durchführt. Die Wertungen des Urteils sind neben dem behandelten Privacy-Shield und den Standardvertragsklauseln ebenso auf die anderen Garantien des Art. 46 DSGVO anzuwenden. Der EuGH gibt vor, dass das Datenschutzniveau im Drittland gleichwertig dem der Union sein muss. Vergleichbar ist die Situation der Zertifizierung mit der der Standarddatenschutzklauseln[4]: Der Verantwortliche oder Auftragsverarbeiter muss bei einem Datenexport in die USA sicherstellen, dass der Schutz der personenbezogenen Daten gleich dem der Union ist. Nur dann kann die Zertifizierungsstelle die Zertifizierung für einen Datenexport vornehmen. Um dies zu erreichen, müsste der Verantwortliche oder Auftragsverarbeiter mit zusätzlichen Maßnahmen sicherstellen, dass nationale Sicherheitsbehörden in den USA nicht ohne die Möglichkeit eines hiergegen gerichteten Rechtswegs auf die Daten zugreifen können. Wie diese Maßnahmen konkret aussehen müssen, ist einzelfallabhängig und wird derzeit viel diskutiert.

Ob die Zertifizierungen in den kommenden Jahren wenigstens im europäischen Bereich Erfolg haben werden, wird maßgeblich vom Aufwand und den Kosten, aber auch der Akzeptanz der Kunden abhängen. Es stellt ein vielversprechendes Werkzeug dar, um im Datenschutz-Dschungel für einen besseren Überblick zu sorgen und das Datenschutz-Niveau dauerhaft zu erhöhen.

4 Zum Entwurf der neuen Standarddatenschutzklauseln siehe Wellmann, O ihr gnadenbringenden Standarddatenschutzklauseln, DFN-Infobrief Recht 12/2020.

(No) Return to Sender

Auskunftsanspruch aus Art.15 DSGVO umfasst nicht eigene E-Mails

von Steffen Uphues

Ein Urteil aus der jüngeren Vergangenheit hat den Inhalt des Auskunftsanspruchs nach Art. 15 Datenschutz-Grundverordnung (DSGVO) weiter präzisiert. Zu E-Mails, deren Inhalt der betroffenen Person bekannt sind, muss der Verantwortliche keine Auskunft erteilen. Dahingehend äußerte sich das Landesarbeitsgericht (LAG) Niedersachsen in einer Entscheidung vom 09. Juni 2020 (Az. 9 Sa 608/19). Darüber hinaus stellte das Gericht klar, dass die Übersendung verschlüsselter ZIP-Dateien keine zulässige Übermittlung darstelle, sofern die betroffene Person hiermit nicht einverstanden ist.

I. Der Auskunftsanspruch aus Art. 15 DSGVO

1. Sinn und Zweck des Anspruchs

Der Auskunftsanspruch ist ein zentrales Element im datenschutzrechtlichen System der Betroffenenrechte. Erst hierdurch und durch die Einhaltung der Informationspflichten aus Art. 13, 14 DSGVO erhält die betroffene Person vom „Ob“ und Umfang einer Datenverarbeitung Kenntnis. Dies bietet ihr dann die Möglichkeit, die Verarbeitungen auf deren Rechtmäßigkeit untersuchen zu lassen und die Rechte auf Berichtigung, Löschung sowie Einschränkung effektiv wahrzunehmen. Mittlerweile ist gerichtlich geklärt, dass auch im Arbeitsverhältnis neben dem Einsichtsanspruch aus § 83 Betriebsverfassungsgesetz (BetrVG) ein datenschutzrechtlicher Auskunftsanspruch wahrgenommen werden kann.[1]

2. Anspruchsinhalt

Art. 15 DSGVO normiert ein Auskunftsrecht für betroffene Personen. Hiernach kann man in einem ersten Schritt vom Verantwortlichen Informationen dazu verlangen, ob eine Verarbeitung personenbezogener Daten stattfindet. Sofern dies der Fall ist, kann man in einem zweiten Schritt Auskunft über diese Daten verlangen. Daneben stehen einem weitere Informationen zu; so etwa die Benennung der Verarbeitungszwecke oder ob die Daten an weitere Empfänger übermittelt wurden.

3. Art der Datenübermittlung

Nimmt eine betroffene Person ihr Auskunftsrecht wahr, hat der Verantwortliche eine Kopie aller relevanten personenbezogenen Daten herauszugeben. Sofern ein hierauf gerichteter Antrag elektronisch gestellt wird, hat der Verantwortliche auch elektronisch zu antworten. In Erwägungsgrund 63 S. 4 DSGVO wird ausgeführt, dass der Verantwortliche sich bemühen soll, darüber hinaus auch einen Zugriff per Fernzugang zu einem sicheren System bereitzustellen. Dabei kann es sich etwa um einen Zugriff über Cloud-Dienste oder ZIP-Dateien handeln. Hierdurch könne der betroffenen Person ein direkter Zugang zu den begehrten Informationen geboten werden.

II. Die Entscheidung des LAG Niedersachsen

Der Kläger war nach Ende seines Beschäftigungsverhältnisses gerichtlich gegen seine ehemalige Arbeitgeberin vorgegangen. Unter anderem machte er seinen Auskunftsanspruch aus Art. 15 DSGVO geltend. Er verlangte in diesem Zuge unter ande-

1 Hierzu John, Mein Name ist Hase, ich weiß von nichts, DFN-Infobrief Recht 06/2020.

rem auch eine Kopie aller E-Mails, die während des Beschäftigungsverhältnisses von ihm verfasst wurden.

1. Zum Anspruchsinhalt

Zumindest mit Blick auf die E-Mails verneinte das LAG Niedersachsen einen Anspruch. Diese seien vom Kläger erstellt worden und ihm somit bekannt. Der Auskunftsanspruch beziehe sich nicht auf solche Dokumente, die den Anspruchstellern vorliegen. Gerade wenn ein Verantwortlicher in größerem Umfang personenbezogene Daten verarbeitet, müsse eine betroffene Person beim Einfordern von Kopien deutlich formulieren, welche konkreten Dokumente zugänglich gemacht werden sollen. Der Sinn und Zweck der Norm liege darin, Informationen zu denjenigen Dokumenten zu erhalten, die dem Zugriff der betroffenen Person bislang entzogen waren. Durch Art. 15 DSGVO soll der Betroffene die Möglichkeit erhalten, die Datenverarbeitung überprüfen zu können. Wenn man diesen Grundsatz auf den vorliegenden Fall anwendet, sei der Auskunftsanspruch hinsichtlich der E-Mails abzulehnen. Eine darauf gerichtete Überprüfung durch den Kläger sei nicht nötig, da er an den Konversationen beteiligt war und somit schon Kenntnis hiervon hat. Ausweislich der Begründung des LAG Niedersachsen sei es nicht Ziel des Auskunftsanspruchs, dass alle Unterlagen, die personenbezogene Daten der betroffenen Person enthalten, zugänglich zu machen sind. Es solle eben lediglich eine Überprüfbarkeit der Datenverarbeitung ermöglicht werden.

2. Zur Art der Übermittlung

Die ehemalige Arbeitgeberin hatte dem Kläger die Informationen in verschlüsselten ZIP-Dateien zukommen lassen. Das dazugehörige Passwort erhielt er separat. Nach Ansicht des LAG Niedersachsen reiche eine derartige Übermittlung nicht aus, um den Auskunftsanspruch einer betroffenen Person zu erfüllen. Grundsätzlich befinde sich der Ort der zu erbringenden Leistung, also der Übermittlung der Informationen, am Wohnort des Anspruchstellers. Die Möglichkeit des Fernzugriffs, die in Erwägungsgrund 63 S. 4 DSGVO genannt wird, sei nur als „Plus“ für den Anspruchsteller zu verstehen. Sofern er damit einverstanden ist, könne derart verfahren werden. Andernfalls aber könne eine Übermittlung von ZIP-Dateien nicht das Zuschicken auf schriftlichem oder elektronischem Wege ersetzen. Ein alleiniger Fernzugriff könne „für in IT-Sachverhalten unerfahrene Personen zu Hürden führen“ und sei somit gegen den Willen des Anspruchstellers nicht zulässig.

III. Fazit für öffentliche Hochschulen und Forschungseinrichtungen

Aus diesem Urteil lassen sich für öffentliche Hochschulen und Forschungseinrichtungen im Wesentlichen zwei Aussagen ziehen: Zum einen muss man betroffenen Personen im Zuge eines Auskunftsersuchens nur diejenigen Daten zugänglich machen, die ihr bislang noch nicht bekannt sind. Dabei ist der Sinn und Zweck der Norm – die Überprüfung einer Datenverarbeitung – maßgeblich. Zum anderen sind die Informationen, die man nach Art. 15 Abs. 3 DSGVO zu übermitteln hat, grundsätzlich auf Papier (per Brief) oder elektronisch (etwa per Mail) zur Verfügung zu stellen. Ein Fernzugriff ist nur bei Einverständnis der betroffenen Person geeignet, die Leistungspflicht des Verantwortlichen zu erfüllen. Es ist abschließend darauf hinzuweisen, dass eine verspätete und unvollständige Auskunft zur Zahlung eines Schadensersatzes führen kann.[2] Die Erfüllung eines Auskunftsbegehrens sollte demnach nicht „auf die leichte Schulter“ genommen werden.

2 Hierzu John, Data Wars: Der Betroffene schlägt zurück, DFN-Infobrief Recht 10/2020

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