Annika Selzer

Die Zukunft von Auftragsdatenverarbeitungskontrollen

Änderungen und Chancen durch die DSGVO

1 Auftragsdatenverarbeitungskontrollen gemäß Bundesdatenschutzgesetz[1]

§ 11 Abs. 2 Satz 4 BDSG regelt, dass sich der Auftraggeber einer Auftragsdatenverarbeitung[2] (ADV) vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen zu überzeugen hat. Diese Kontrollen im Zeitalter massenhafter, internationaler Auslagerungen von Datenverarbeitungsvorgängen (z. B. durch die Inanspruchnahme von Cloud Services) zu bewältigen, stellt sowohl Auftraggeber als auch Auftragsverarbeiter vor große Herausforderungen. Problematisch ist hierbei u. a. die mögliche geographische Distanz zwischen beiden Parteien, die – zumindest bei regelmäßigen persönlichen Vor-Ort-Kontrollen – zu Schwierigkeiten führt. Auch die Kosten für derartige Kontrollen und das fehlende Prüf-Know-How – vor allem bei kleinen und mittelständischen Unternehmen – stellen den Auftraggeber von ADVs vor Herausforderungen.

2 Auftragsdatenverarbeitungskontrollen gemäß Datenschutzgrundverordnung

Die Datenschutzgrundverordnung (DSGVO) wirkt diesem Problem durch eine wesentliche Neuerung entgegen: Anders als die Datenschutzrichtlinie, die in Deutschland durch eine Novellierung des Bundesdatenschutzgesetzes umgesetzt wurde, versieht die Datenschutzgrundverordnung Datenschutzzertifizierungen erstmals großflächig mit einer konkreten Rechtsfolge und stellt u. a. klar, dass der Auftraggeber einer Auftragsdatenverarbeitung durch eine Zertifizierung seinen Kontrollpflichten nachkommen kann.

Art. 42 Abs. 1 DSGVO regelt hierzu: *Die Mitgliedstaaten [….] und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren [….], die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird.*[3] *Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen.*

Wichtig ist es anzumerken, dass gemäß Art. 42 Abs. 4 DSGVO eine Zertifizierung nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung der Datenschutzgrundverordnung mindert. Art. 28 Abs. 5 DSGVO regelt konsequenterweise, dass die Einhaltung eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter als *Faktor* herangezogen werden kann, um hinreichende Garantien nachzuweisen. Da Art. 28 Abs. 5 DSGVO bei der Datenschutzzertifizierungen als „möglichen Faktor" spricht, wird es in der Praxis auf den konkreten Sachverhalt ankommen, um zu beurteilen, ob eine Datenschutzzertifizierung die Auftragsdatenverarbeitungskontrolle vollständig oder nur teilweise erbringen kann. Wichtige Entscheidungshilfen für die Beurteilung könnten u. a. Faktoren wie der Schutzbedarf, der Umfang der verarbeiteten personenbezogenen Daten, die Konsequenzen der Offenlegung bzw. des Löschens oder der Manipulation der Daten sein. Diese Faktoren werden bereits heute häufig von verantwortlichen Stellen herangezogen, um zu entscheiden, in welchem Umfang (persönliche Vor-Ort-Kontrolle, Interview, Fragebogen etc.) und Prüfturnus (i. d. R. zwischen 1-3 jährlich) eine Auftragsdatenverarbeitungskontrolle durchgeführt wird.

Der Prüfturnus für Datenschutzzertifizierungen nach der Datenschutzgrundverordnung liegt gemäß Art. 42 Abs. 7 DSGVO bei max. drei Jahren, wobei es sinnvoll erscheint, auch bei dessen Festlegung die zuvor genannten Faktoren heranzuziehen.

Eine große Rolle wird im Rahmen der Datenschutzzertifizierung nach der Datenschutzgrundverordnung der Europäischen Kommission, den Aufsichtsbehörden und dem Europäischen Datenschutzausschuss zugemessen: So wird die Zertifizierung etwa von der jeweils zuständigen Aufsichtsbehörde bzw. von hierfür akkreditierten Stellen[4] vergeben und kann von diesen auch

1 Dieser Beitrag wurde vom Bundesministerium für Bildung und Forschung (BMBF) sowie vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen von CRISP gefördert.

2 Eine Auftragsdatenverarbeitung nach BDSG liegt vor, wenn der Auftragsverarbeiter personenbezogene Daten im Auftrag des Auftraggebers verarbeitet und der Auftraggeber die vollen Weisungsbefugnisse für die Verarbeitung besitzt.

Annika Selzer

Wissenschaftliche Mitarbeiterin am Fraunhofer-Institut für sichere Informationstechnologie.

E-Mail: annika.selzer@sit.fraunhofer.de

3 Gem. Art. 42 Abs. 2 DSGVO können die Zertifizierungsverfahren darüber hinaus vorgesehen werden, um nachzuweisen, dass die Verantwortlichen oder Auftragsverarbeiter, die nicht unter die DSGVO fallen, im Rahmen der Übermittlung an Drittländer geeignete Garantien bieten.

4 Gem. Art. 43 Abs. 2 und 3 DSGVO dürfen Zertifizierungsstellen nur dann akkreditiert werden, wenn sie u. a. ihre Unabhängigkeit und ihr Fachwissen nach-

widerrufen werden, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden. Darüber hinaus ist es Aufgabe der Aufsichtsbehörde bzw. des Europäischen Datenschutzausschusses, die Kriterien zu genehmigen, auf die sich das Zertifizierungsverfahren stützt, um für höchstmögliche Transparenz bei der Zertifizierung zu sorgen. Darüber hinaus ist die Europäische Kommission befugt, Anforderungen an das Verfahren mittels delegierter Rechtsakte zu erlassen (Art. 42 Abs. 3 u. 5 und Art. 43 Abs. 1, 5 u. 8 DSGVO). Insbesondere die Regelungen bezüglich der Transparenz der Zertifizierungsverfahren und der Möglichkeit der Genehmigung von Kriterien durch den Europäischen Datenschutzausschuss sind zu begrüßen. In ihnen liegt die Chance, möglichst einheitliche Kriterien und Prüfkataloge für die Datenschutzzertifizierung in Europa zu entwickeln und somit vorzubeugen, dass die verantwortlichen Stellen wie bisher einen Dschungel von Zertifizierungsanbietern und verfahren vorfinden werden. Bisher war es verantwortlichen Stellen nahezu unmöglich zu erkennen, welche Qualität sowohl der Anbieter als auch dessen Zertifizierungsverfahren hatten, wie sich die einzelnen Datenschutzzertifizierungen voneinander unterscheiden und ob die Zertifizierungsverfahren überhaupt geeignet sind, eine ADV-Kontrolle zu ersetzen. Zwar wird dieser Zustand bereits durch die Zertifizierungsregelungen der Datenschutzgrundverordnung deutlich verbessert, jedoch ist es wünschenswert, ihn weiter zu vereinheitlichen, indem Kriterienkataloge und Zertifizierungsverfahren europaweit möglichst einheitlich formuliert werden. Um möglichst vielen Branchen den Zugang zu Datenschutzzertifizierungen zu ermöglichen, wäre es darüber hinaus u. a. wünschenswert, dass die Kriterienkataloge einheitliche Anforderungen je Branche der verantwortlichen Stelle abbilden würden, um den verantwortlichen Stellen transparent aufzeigen zu können, welche Auftragsverarbeiter die für die verantwortliche Stelle geltenden, branchenspezifischen Datenschutzanforderungen umsetzen.

3 Automatisierte Datenschutzkontrollen als zukünftiges Modell für ADV-Kontrollen

Derzeit gibt es im Rahmen von öffentlich geförderten Forschungsprojekten Bestrebungen, den Umsetzungsgrad von Datenschutzmaßnahmen eines Cloud-Betreibers zum Schutz der personenbezogenen Daten, die ein Cloud-Nutzer in der Cloud verarbeiten lässt, auf Basis von automatisierten Datenschutzkontrollen im laufenden Betrieb automatisiert messbar zu machen. So schlägt z. B. das BMBF-geförderte Projekt V*eriMetrix* vor, automatisierte Kontrollen vorwiegend kundenspezifisch auf den virtuellen Maschinen eines bestimmten Kunden durchzuführen, um aus verschiedenen Parametern u. a. Erkenntnisse über den Verarbeitungsstandort, datenschutzkonform ausgestaltete Zugangs- und Zugriffskonfigurationen, den Grad der Mandantentrennung und der Datenlöschung zu gewinnen. Hierbei wurde bei der Entwicklung des Kontrollkonzepts besonderer Wert auf einheitliche, branchenspezifische Anforderungskataloge sowie ein transparentes Verfahren gelegt, auf welchen die Datenschutzkontrollen beruhen. Darüber hinaus wurde eine Benutzeroberfläche entwickelt, die es auch dem nicht datenschutzversierten Cloud-Nutzer ermöglicht, sich schnell und einfach einen Überblick über den Umsetzungsgrad von Datenschutzeigenschaften seines Cloud-Betreibers zu machen. Es ist davon auszugehen, dass die Anforderungen an Datenschutzzertifizierungen, welche die Datenschutzgrundverordnung aufstellt, durch die Kontrollkonzepte automatisierter Datenschutzkontrollen umgesetzt werden können und damit grundsätzlich geeignet wären, eine ADV-Kontrolle in Zukunft zu ersetzen.

Durch die Änderungen bezüglich der Rechtswirkung von Datenschutzzertifizierungen durch die Datenschutzgrundverordnung ergeben sich also Chancen, die Kriterienkataloge (und Konzepte) automatisierter ADV-Kontrollen im Cloud-Umfeld durch die Aufsichtsbehörden bzw. den Europäischen Datenschutzausschuss bestätigen zu lassen und somit den Einsatz automatisierter, branchenspezifischer Datenschutzzertifizierungen für das Cloud-Umfeld zu unterstützen. Diese Form der Zertifizierung würde sehr viele Vorteile bieten – sowohl bezüglich der geringeren Kosten für automatisierte Kontrollen als auch bezüglich der Möglichkeit, die Umsetzung des Datenschutzes kontinuierlich zu überwachen, um auf ggf. kritische Messergebnisse umgehend reagieren zu können.

gewiesen haben, Verfahren für die Erteilung und den Widerruf der Datenschutzzertifizierung festgelegt haben und der zuständigen Aufsichtsbehörde nachgewiesen haben, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen. Die Zertifizierungsstellen sind für die angemessene Bewertung, die der Zertifizierung zugrunde liegt, verantwortlich.

Literatur

Härting: Datenschutz-Grundverordnung – Das neue Datenschutzrecht in der betrieblichen Praxis, 2016.

Jäger/Kraft/Selzer/Waldmann: Die teil-automatisierte Verifizierung der getrennten Verarbeitung in der Cloud, in: DuD 2016, S.305-309.

Plath (Hrsg.): BDSG – DSGVO – Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2016.

Roßnagel (Hrsg.): Europäische Datenschutz-Grundverordnung. Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts, 2017.

Wedde: EU-Datenschutz-Grundverordnung – Kurzkommentar mit Synopse BDSG/ EU-DSGVO, 2016.