Stellungnahme

Kurzpapier Nr. 13 der Datenschutzkonferenz Auftragsverarbeitung, Art. 28 DS-GVO[1]

16. Februar 2018

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Susanne Dehmel
Mitglied der Geschäftsleitung
Recht & Sicherheit
T +49 30 27576-223
s.dehmel@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Zusammenfassung

Bitkom begrüßt die Veröffentlichung des Kurzpapiers Nr. 13 der Datenschutzkonferenz, welches zu mehr Klarheit bezüglich der Auslegung der die Auftragsverarbeitung regelnden Vorschriften der Datenschutz-Grundverordnung beitragen soll. Wir halten jedoch eine differenziertere Bewertung von Wartungs- und Fernzugriffsfällen für notwendig. Eine pauschale Anforderung, für solche Fälle Auftragsverarbeitungsvereinbarungen abzuschließen, entnehmen wir der Datenschutz-Grundverordnung nicht. Möglichkeiten der sachgerechten Differenzierung und des rechtssicheren Umgang mit Wartungs- und Prüfungsverträgen erläutern wir nachfolgend und würden dazu gerne in einen Dialog mit der Datenschutzkonferenz eintreten.

Wartung und Fernzugriffsfälle

Im Kurzpapier wird unterschieden zwischen Fällen der rein technischen Wartung der Infrastruktur einer IT durch Dienstleister (z.B. Arbeiten an Stromzufuhr, Kühlung, Heizung) und Fällen der Wartung, bei denen die Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten besteht oder zumindest nicht ausgeschlossen werden kann. Bei letzteren nimmt die Datenschutzkonferenz an, dass es sich um eine Verarbeitung nach Art. 4 Nr. 2 DS-GVO handelt und dass daher auch eine Auftragsverarbeitungsvereinbarung zu treffen ist.

Aus Sicht der Praxis ist diese Abgrenzung nicht geeignet, um den Gegebenheiten unterschiedlicher Konstellationen der Wartung gerecht zu werden. Sie lässt sich unserer Meinung nach auch nicht direkt aus der Datenschutz-Grundverordnung entnehmen.

[1] https://www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf

1. Möglichkeit zur Kenntnisnahme

Zunächst einmal stellt sich die Frage, ob Dienstleistungen, bei denen nur die Möglichkeit besteht, auf personenbezogene Daten zuzugreifen oder, bei denen das zumindest nicht ausgeschlossen werden kann, tatsächlich als Fälle der Auftragsverarbeitung qualifiziert werden können, wenn die angeforderte Dienstleistung gerade nicht in der Verarbeitung diese Daten besteht, sondern z.B. in der Funktionsüberprüfung, Fehleranalyse oder Reparatur einer Anlage oder eines Geräts.

Beispiel Drucker: Techniker wartet einen Drucker (z.B. über angeschlossenes Analysetool) und kann theoretisch, die im Drucker gespeicherten Inhalte auslesen – soll aber nur den Drucker säubern und korrekt einstellen.

Beispiel Callcenter: Telefonanlage eines Callcenters wird von einem Techniker gewartet. Er kann dabei theoretisch die in der Anlage gespeicherten Telefonnummern zur Kenntnis nehmen, soll aber nur sicherstellen, dass die Tonqualität der Anlage einwandfrei ist.

Beispiel Reinigung: Wenn die Reinigungskraft im laufenden Betrieb die Büros saugt, kann sie theoretisch auf den Computern oder in herumliegenden Akten Daten einsehen. Das ist aber ausdrücklich nicht Teil ihrer Dienstleistung. Der Auftraggeber möchte gerade nicht, dass die Reinigungskräfte auf Inhalte zugreifen, auch wenn er es im Einzelfall nicht ausschließen kann, dass die tatsächliche Möglichkeit besteht.

Beispiel Autowerkstatt: Techniker analysiert Motorzustand und Verschleißzustand mittels angeschlossenem Analyseprogramm und kann dabei fahrzeugbezogene Daten zur Kenntnis nehmen.

Beispiel Werbeagentur: Die Werbeagentur, die Visitenkarten gestaltet, kann nicht ausschließen, dass im Fehlerfall des Graphikprogramms ein Techniker des Herstellers über eine kontrollierte Fernwartung Einstellungen optimiert. Der Einsatz des speziellen Graphikprogramms und ein theoretisch denkbarer Fernwartungseinsatz wäre nach dem Kurzpapier Nr. 13 nur mit Zustimmung des Auftraggebers der Visitenkarten möglich.

Es erscheint nicht passend für Dienstleistungen einen Auftragsverarbeitungsvertrag nach Artikel 28 DS-GVO abzuschließen, bei denen die Datenverarbeitung gerade nicht der gewünschte Vertragsgegenstand ist.[2] Da die Datenverarbeitung gar nicht dem Willen des Auftraggebers entspricht, kann er schwerlich einen Vertrag darüber abschließen. Das wäre

[2] S. 30 WP 169 Art. 29 Datenschutzgruppe Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“: „Für eine Einstufung als Auftragsverarbeiter muss eine Organisation daher zwei grundlegende Bedingungen erfüllen: Sie muss in Bezug auf den für die Verarbeitung Verantwortlichen rechtlich eigenständig sein, und **sie muss personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeiten**.“

eher ein „negativer Auftragsverarbeitungsvertrag“, der die Verarbeitung ausschließen soll. Dann wäre es aber kein Fall nach § 28 DS-GVO, sondern man könnte eine vertragliche Vereinbarung genügen lassen, die sicherstellt, dass über gelegentlich der Auftragserfüllung einsehbare Daten Vertraulichkeit gewahrt ist und dass diese Daten vom Auftragnehmer nicht verarbeitet werden dürfen.

Die Definition der Verarbeitung in der Verordnung 2016/679 entspricht der in bereits in der RL 95/46 enthaltenen. Hätte man solche Fälle bereits damals als Verarbeitung eingeordnet, hätte es den § 11 Abs. 5 BDSG (alt) als spezielle Regelung nicht bedurft – man hätte (bisher) solche Fälle auf Basis der RL 95/46 europaweit direkt als Auftragsverarbeitung einordnen können.

Während nach § 11 Abs. 5 BDSG (alt) die Vorgaben für die Auftragsverarbeitung nur entsprechend anzuwenden waren und es so noch eine gewisse Flexibilität zur Anpassung der Verträge gab, gibt es bei der Datenschutz-Grundverordnung bei Annahme des § 28 DS-GVO nur dessen Geltung mit allen Rechten und Pflichten ohne Ausnahme. Würde man die oben genannten Fälle nach § 28 DS-GVO abwickeln, stieße man jedoch auf eine Reihe von Vorgaben, die hier nicht passen. Stehen beispielsweise die zu wartenden Geräte beim Kunden, hat das Wartungsunternehmen in der Regel wenig Einfluss auf die technisch-organisatorischen Maßnahmen wie z.B. Zutrittskontrolle (für deren Umsetzung es als Auftragsverarbeiter theoretisch verantwortlich wäre).

Gegen die generelle Anwendung der Auftragsverarbeitungsvorschriften spricht aus unserer Sicht auch folgender Gedanke: Wenn sich allein schon aus der DS-GVO eine Fortführung der gedanklichen Regelung des § 11 Abs. 5 BDSG (alt) ergibt, warum legt der deutsche Gesetzgeber dies dann in Spezialgesetzen nochmal fest (vgl. § 80 SGB X-neu, vgl. auch Entwurf BayDSG vom 28.09.2017, Art. 5 Abs. 3[3])?

2. Dienstleistungen für Auftragsverarbeiter

Die meisten Unternehmen, die Datenverarbeitungs-Dienstleistungen im Auftrag anbieten beschäftigen auch selbst Dienstleister mit Aufgaben wie den in den oben beschriebenen Beispielen. Sie nutzen Dienstleister für die Wartung ihrer Anlagen und Geräte (mit denen sie sowohl ihre eigenen Daten als auch Daten im Auftrag verarbeiten). Nimmt man entgegen der oben ausgeführten Argumentation und mit dem Kurzpapier Nr. 13 an, dass diese Dienstleistungen grundsätzlich als Auftragsverarbeitungsverhältnisse ausgestaltet sein müssen, stellt sich die Frage, ob diese Auftragsverarbeitung nun als Teil der Erfüllung der Auftragsverarbeitungen des beauftragenden Unternehmen für seine Kunden zu bewerten

[3] https://www.stmi.bayern.de/assets/stmi/ser/gesetzentwuerfe/baydsg_stand_28_09_2017.pdf

sind, oder ob sie für sich genommen nur im Verhältnis des Auftrag gebenden Unternehmen mit dem Wartungsdienstleister zu werten sind. Natürlich dient die Instandhaltung von Geräten und Anlagen indirekt auch den Datenverarbeitungen im Auftrag, die darauf abgewickelt werden. Aber sie stellen andererseits auch die grundsätzliche Arbeitsfähigkeit des Unternehmens sicher und werden in der Regel nicht eigens als Teil der Verarbeitung oder der technisch-organisatorischen Maßnahmen in den Auftragsverarbeitungsaufträgen des Unternehmens genannt sein.

Beispiel Entsorger: In der Regel werden Auftragsverarbeiter auch einen Entsorger haben, mit dem sie selbst eine Auftragsverarbeitung abgeschlossen haben. Dieser wird meist für die Entsorgung aller Unterlagen und Datenträger zuständig sein – unabhängig ob diese Daten des Unternehmens selbst oder seiner Auftraggeber enthalten. Könnte eine Auftragsverarbeiter nur dann seinen Entsorgungsdienstleister wechseln, wenn alle seine Kunden dem zustimmen bzw. einer entsprechenden Information nicht widersprechen (Art. 28 Abs. 2)?

Beispiel Server: Ähnlich stellt sich die Lage dar, wenn ein Unternehmen seine Server durch den Hersteller oder einen Partner des Herstellers warten lassen und nun die Server gegen Produkte eines anderen Herstellers und damit gleichzeitig auch eines anderen Wartenden austauschen möchten.

Würden solche Konstellationen, als Teil der Auftragsverarbeitung gewertet, die der Nutzer des Geräts für seine Kunden erbringt, hätte dies weitreichende Folgen. Eine Folge wäre, dass er jeden Wechsel des Wartungsdienstleisters oder des Geräts, welcher mit einem solchen verbunden ist, seinen Kunden, deren Daten betroffenen sein könnten, mitteilen und sich ggf. genehmigen lassen müsste. Dies wird in der Mehrzahl der Fälle z.B. bei Callcenter-Beauftragungen weder im Interesse des Auftragnehmers noch des Auftraggebers sein. Im Zweifel könnte der Auftraggeber den Wechsel eines Gerätes oder Wartungspartners verhindern. In Konstellationen von mehreren Subunternehmen könnten solche Ereignisse zu ganzen Benachrichtigungsketten führen. Das erscheint nicht sachgerecht.

Die DS-GVO sieht die Einbeziehung von externen Dienstleistern, wenn es um die Sicherstellung der Verfügbarkeit und Integrität geht und die damit verbundene Weitergabe oder Kenntnisnahmemöglichkeit von personenbezogene Daten geht, als Wahrung berechtigter Interessen durch den verantwortlichen (ErwGr. 49). Es erschient widersinnig bei anderen Motiven der Einbindung von Dienstleistern dann eine Auftragsverarbeitung annehmen zu müssen, nur weil das Ziel der Fehleranalyse vielleicht eine Farbkorrektur darstellt und nicht einen Sicherheitsmangel.

Zusätzlich ergibt sich aus der DS-GVO auch die Argumentation, dass ein Unternehmen solche Aufträge und ggf. auch damit verbundene nicht vermeidbare Datenübermittlungen z.B. in Notfällen, in dem es um die Arbeitsfähigkeit von IT-Anlagen geht, die für kritische Anwendungen oder die generelle Produktionsfähigkeit des Unternehmens geht, bereits im berechtigten Interesse des Unternehmens möglich sein müssen. Dafür spricht z.B. Artikel 49 Abs. 1 (g) DS-GVO, der sogar Übermittlungen in Drittstaaten nach einer Interessenabwägung zulässt wenn diese nicht wiederholt erfolgt und nur eine begrenzte Zahl von betroffenen Personen betroffen ist.

3. Europäische Praxis

Nach unserer Kenntnis bestand bisher in Deutschland durch den § 11 Abs. 5 BDSG (alt) eine besondere Rechtslage, während die anderen EU-Mitgliedsstaaten solche zusätzlichen Regelungen nicht eingeführt haben. Dementsprechend wurde dort auch schon bisher nur zwischen Fällen der eindeutigen Auftragsverarbeitung und Fällen unterschieden, bei denen flexibel nur die notwendigen vertraglichen Regelungen getroffen werden konnten. Wir gehen davon aus, dass dort auch zukünftig bei Wartungsfällen nur dann eine Auftragsverarbeitung angenommen werden wird, wenn Gegenstand des Vertrages tatsächlich die Verarbeitung von personenbezogenen Daten ist. Für die einheitliche Auslegung der Datenschutz-Grundverordnung und zur Vermeidung von Schwierigkeiten und langwierigen Verhandlungen bei länderübergreifender Zusammenarbeit zwischen Unternehmen ist es aus unserer Sicht wichtig, dies zu berücksichtigen.

Berlin, Februar 2018

Bitkom vertritt mehr als 2.500 Unternehmen der digitalen Wirtschaft, davon gut 1.700 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 400 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.