Stellungnahme

Auftragsdatenverarbeitung
03.04.2015

Kaum ein Unternehmen führt seine Datenverarbeitung heute allein mit eigenen Mitteln durch, weil das nicht effizient wäre. Professionelle Anbieter von Datenverarbeitungsdienstleistungen übernehmen Aufgaben, für die das nötige Know-How oder die erforderlichen Kapazitäten im eigenen Unternehmen nicht zur Verfügung stehen. Klare Regelungen zur Auftragsdatenverarbeitung sind essentiell für die Weiterentwicklung von Cloud Computing und die Wertschöpfung der gesamten europäischen Wirtschaft. Von der Praxistauglichkeit dieser Vorgaben hängt es ab, ob neue Geschäftsmodelle durch den Rechtsrahmen eher gefördert oder behindert werden.

Im Prozess der Auftragsdatenverarbeitung muss es eine klare Trennung der Verantwortlichkeiten und Zuständigkeiten zwischen Verantwortlichen und Auftragsverarbeiter geben. Diese Trennung hat sich in der Praxis bewährt. Weder Industrie noch Regulierungsbehörden wie der Artikel 29 Gruppe, sehen Handlungsbedarf, dieses System zu verändern. Unklare oder vermischte Verantwortlichkeiten werden komplexere Vertragsverhandlungen nach sich ziehen und die Umsetzung neuer Geschäftsideen verzögern. Eine gesamtschuldnerische Haftung stellt vor allem keinen Vorteil für den Betroffenen bzw. den Verbraucher dar, auch wenn es auf den ersten Blick den Anschein erweckt. Der BITKOM möchte dies anhand von Beispielen verdeutlichen und spricht sich für die Streichung des Bezugs zum Auftragsverarbeiter in den entsprechenden Vorschriften der DS-GVO (z.B. Art. 77) aus:

- **Vermischte Verantwortlichkeiten stärken nicht den Verbraucherschutz, im Gegenteil es ergeben sich Nachteile für den Betroffenen bzw. Verbraucher**

Unklare Verantwortlichkeiten können dazu führen, dass keine Seite sich für die Sicherheit und den Schutz der Daten verantwortlich fühlt und die Verantwortung auf die jeweils andere Seite geschoben wird. Ein solches Verhalten erschwert es dem Betroffenen, einen eindeutigen Adressaten für etwaige Haftungsansprüche zu identifizieren.

Die Annahme, dass der Betroffene einfach **zusätzlich** ein oder mehrere weitere Unternehmen (processors) in Anspruch nehmen kann, ist irrtümlich. Es wird hier übersehen, dass der eigentliche Vertragspartner des Betroffenen (z.B. seine Bank, seine Versicherung, sein Autohersteller) sich nach Art.77 (3) und Erwägungsgrund 118 DS-GVO **exkulpieren** kann, wenn er nachweist, dass der Fehler beim beauftragten Auftragsverarbeiter lag. Umgekehrt wäre der Auftragsdatenverarbeiter auf die Zusammenarbeit mit dem Auftraggeber angewiesen, wenn er sich exkulpieren wollte. Die Bereitschaft dazu dürfte auf Seiten des Auftraggebers aber gering sein, da er in diesem Fall als einziger in Haftung genommen werden würde.

Der Kunde, der bis zu diesem Zeitpunkt in der Regel nur den Verantwortlichen kannte, muss dann **alleine** herausfinden, wer von den oft zahlreichen Auftragsverarbeitern für den Fehler verantwortlich ist. Er kann sich nicht darauf verlassen, dass sein Vertragspartner und ursprünglicher Ansprechpartner, den er

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Susanne Dehmel
Mitglied der
Geschäftsleitung
Vertrauen & Sicherheit
Tel.: +49.30.27576-223
s.dehmel@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

sich ausgesucht hat und zu dem er ein Vertrauensverhältnis hat, im Zweifelsfall für die Datenschutz-Verstöße haftet, denn dieser wird mit großer Wahrscheinlichkeit, weiter auf den Auftragsverarbeiter verweisen. Diesen Auftragsverarbeiter kennt der Betroffene aber meist nicht bzw. er ist für ihn nicht leicht greifbar, sollte dieser im Ausland sitzen. Selbst wenn er ihn herausfindet, wird er seinen Anspruch in der Regel nicht ohne Anwalt und erheblichen Aufwand durchsetzen können. Die Folge könnte sein, dass der Betroffene seinen Anspruch gar nicht geltend macht bzw. machen kann.

Praktische Beispiele:

Beispiel 1 – IT-Service Provider
Frau Müller (data subject) stellt fest, von Ihrem Konto sind unberechtigte Abbuchungen erfolgt. Sie geht daher zu Ihrer örtlichen Bank (controller) und beschwert sich bei Ihrem Kundenberater Herr Mustermann, der sie seit Jahren betreut. Dieser berichtet Frau Müller, ihr Konto wurde gehackt, allerdings sei dies nicht die Schuld der Bank, denn für die IT-Sicherheit habe man extra den britischen IT-Provider X-solutions (processor) beauftragt. Herr Mustermann empfiehlt Frau Müller sich direkt an X-solutions zu wenden. Da Frau Müller kein Englisch spricht, bittet Sie Ihre Tochter bei der britischen Firma anzurufen. X-solutions versteht zwar den Ärger von Familie Müller, weist aber die Schuld ebenfalls von sich mit dem Hinweis, die Bank habe ihr die IT-Vorgaben gemacht. Frau Müller ist verärgert und wendet sich wiederholt an die Bank. Diese schafft es aber, den Fehler des IT-Providers nachzuweisen und kann sich damit exkulpieren. Frau Müller bleibt am Ende nichts anderes übrig, als X-solutions zu verklagen, ist sich aber unsicher, ob dies überhaupt in Deutschland möglich ist. Da Frau Müller die Sache schon viel Aufwand und Nerven gekostet hat, entscheidet sie sich gegen eine Klage mit der Begründung, es sei den Aufwand nicht wert.

Dieses Beispiel stellt die Auftragsdatenverarbeitung zur Veranschaulichung mit nur einem Verantwortlichen und einem Auftragsverarbeiter dar. In der Praxis sind die Konstellationen meist viel komplexer und involvieren zahlreiche Auftragsverarbeiter, sodass der Betroffene Schwierigkeiten haben wird, den richtigen Anspruchsgegner zu finden. In bestimmten Fällen z.B. in der Autoindustrie (connected car) sind zusätzlich Drittprovider angeschlossen, sodass ganze Ketten von Auftragsverarbeitern entstehen können, wie bei folgender Fallkonstellation:

Beispiel 2 - Connected Car
Wenn Herr Meier heute ein Auto kauft, dann wendet er sich im Defektfall an den Hersteller des Autos und wird nicht vor die Herausforderung gestellt, zu ermitteln, welcher Zulieferer für einen Defekt verantwortlich ist. In naher Zukunft werden Zulieferer zunehmend digitale Dienstleistungen (im Unterschied zu dinglichen Produkten) bereitstellen. Das können Kartendienste, eine Ortung, e-call, meine Blackbox oder automatische Steuerungssysteme sein. Nach den Planungen der EU müsste sich Herr Meier bei einem vermuteten Schaden an die Datenverarbeiter wenden, die er im Zweifel nicht kennt und mit denen er keine vertragliche Beziehung hat. Dies wird insbesondere dann schwierig, wenn die infrage kommenden Auftragsdatenverarbeiter mit Sub-Unternehmen zusammenarbeiten.

- **Ungerechtfertigte Belastung für Auftragsdatenverarbeiter, die oft keine Kenntnisse über die Bedeutung der Daten haben**

Bislang ist sowohl in der EU-Richtlinie als auch im deutschen Recht geregelt, dass die gesamte datenschutzrechtliche Verantwortung bei dem für die Datenverarbeitung Verantwortlichen liegt. Diese Rechtslage erlaubt es den Vertragsparteien, Rechte und Pflichten entlang von Vertragsbedingungen klar zuzuschreiben, um so im Falle eines Vertragsbruchs Rechtssicherheit auf beiden Seiten zu haben. Hier muss vor allem beachtet werden, dass alleine der Verantwortliche bestimmen kann, wie wichtig die Daten für ihn sind und wie sie geschützt werden müssen. Besonders in der Cloud haben Auftragsverarbeiter oft keine Kenntnis über die Bedeutung der Daten für den Verantwortlichen sowie die Risiken, die mit ihnen verbunden sind. Sie können daher weder Risikoprüfungen oder ähnliches durchführen noch Genehmigungen bei der Aufsichtsbehörde einholen. Gerade in Fällen, wo der Auftragsverarbeiter nur weisungsgebunden agieren darf, keine Möglichkeit hat, seinen Auftraggeber dahingehend zu kontrollieren, ob dieser die Berechtigung der Verarbeitung besitzt und auch nicht prüfen kann, was für Daten der Verantwortliche auf seinen Systemen speichert oder verarbeitet, ist eine gemeinsame Haftung nicht sinnvoll.

Praktische Beispiele:

Beispiel 3 Cloud Computing
Der Auftragsdatenverarbeiter hat oftmals keine Möglichkeit, den Inhalt der Daten zur Kenntnis zu nehmen. So hat ein Infrastrukturprovider im Rahmen von Cloud Computing keinen Zugang zu den Daten, die bei ihm verarbeitet werden und kennt damit auch die Risiken nicht, die mit ihnen verbunden sind. Ihn auch für die Daten seiner Kunden eigenverantwortlich und haftbar zu machen, zwingt ihn letztlich, sich zur Einschätzung seines Haftungsrisikos mehr Kenntnis über die Daten anzueignen, als für die vereinbarte Vereinbarung erforderlich ist und ist somit nicht datenschutzfreundlich.

Eine Auftragsdatenverarbeitung findet aber nicht nur beim Cloud Computing statt, sondern auch z.B. bei ausgelagerten Callcentern, Marketingaktionen durch externe Agenturen, Dienstleisterverträge zur Datenträgerentsorgung, externe Lohn- bzw. Gehaltsabrechnung oder ausgelagerte Rechenzentren. Eine gesamtschuldnerische Haftung würde gerade kleine oder mittlere Unternehmen treffen, wie bei folgender Fallkonstellation:

Beispiel 4 Callcenter
Unternehmen (controller) übertragen ihre Kommunikationsschnittstelle zu den (potenziellen) Kunden oft auf externe Callcenter (processor). Diese Callcenter bieten ihre Telefondienste dann z.B. in den Bereichen Bestallabwicklung, Beschwerdemanagement, Kundenrückgewinnung oder Werbung an. In vielen Fällen werden Ihnen dabei konkrete Vorgaben von den Unternehmen gemacht, wie die Service-Leistung durchzuführen ist. Sollte die Datenverarbeitung z.B. aufgrund einer unzureichenden Einwilligung grundsätzlich unzulässig sein, könnte unter einer gesamtschuldnerischen Haftung nicht nur das Unternehmen, sondern auch das Callcenter selbst haften.

- **Vermischte Verantwortlichkeiten machen das ohnehin komplexe Verhältnis der Auftragsverarbeitung in der Praxis noch komplizierter, unattraktiver und führen zu Rechtsunsicherheit**

Die weitreichenden Konsequenzen und negative Auswirkungen auf Kosten, Verwaltungsaufwand und die Wettbewerbsposition der europäischen Wirtschaft werden oftmals nicht erkannt. Gerade Cloud-Dienstleister spielen sowohl im Geschäftsverkehr als auch in der öffentlichen Verwaltung zunehmend eine Rolle. Eine gesamtschuldnerische Haftung kann insbesondere den Anreiz schaffen, dass der Verantwortliche nicht mehr genau prüft, welcher Auftragsdatenverarbeiter sichere und zuverlässige Dienste anbietet, sondern hauptsächlich den Preis als Basis für seine Entscheidung zugrunde legt. Dies kann zu einer Abwärtsspirale führen (Race to the bottom) und sich nicht nur negativ auf europäische IT-Provider auswirken, die in Sicherheitsstruktur investieren, sondern auch auf den Verbraucher, der im Falle einer Sicherheitslücke der Leidtragende ist.

Zudem würde sich die Erweiterung des Haftungsrisikos des Processors nachteilig für europäische Dienstleister auswirken, da ein Geschädigter in den seltensten Fällen einen Zivilprozess im Ausland (Drittstaat) anstrengen würde. Die Berücksichtigung des Haftungsrisikos bei der Kalkulation würde sich hauptsächlich für europäische Unternehmen auswirken. Das Ziel der DSGVO, hier eine vergleichbare Wettbewerbssituation auch im internationalen Vergleich bei Datenverarbeitern zu unterstützen wird dadurch konterkariert.

- **Formulierungsvorschlag zu Artikel 77 DS-GVO**

"1. Any data subject who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to claim compensation from the controller for the damage suffered.
2. Where more than one controller is involved in the processing, each controller shall be jointly and severally liable with the other for the entire amount of the damage to the extent that the joint controllers' respective liability has not been determined in the written arrangement referred to in Article 24
3. The controller shall be exempted from this liability, in whole or in part, if the controller proves that the controller and the processors used by the controller are not responsible for the event giving rise to the damage."