PRIVACY COMPLIANCE

Johannes Christian Rupprich, Diplom-Jurist, Datenschutz- und Complianceberater, Promovend bei Prof. Dr. Martin Henssler, Institut für Arbeits- und Wirtschaftsrecht, Universität zu Köln

Sebastian Feik, Diplom-Wirtschaftsjurist, Geschäftsführer der legitimis GmbH und externer Datenschutzbeauftragter und -auditor im Auftrag namhafter internationaler Konzerne

Praktische Auswirkungen des § 11 Abs. 5 BDSG bei Übergabe oder Rückgabe von Festplatten und anderen Endgeräten mit Datenträgern an IT-Dienstleister oder Hersteller

Johannes Christian Rupprich und *Sebastian Feik*

Welche praktischen Auswirkungen haben die rechtlichen Vorgaben des § 11 Abs. 5 BDSG in Anwendung auf IT-Dienstleister, Hersteller von Festplatten oder anderen Endgeräten mit Datenträgern zur Speicherung personenbezogenen Daten, wie sie in Laptops, Mobiltelefonen, Smartphones, Tablets und Druckern zu finden sind? Welche datenschutzrechtlichen Anforderungen obliegen einer verantwortlichen Stelle speziell im Kontext einer garantie-, gewährleistungs- oder wartungsbedingten Rückgabe bzw. Überlassung von Datenträgern?

I. Einleitung

Die zunehmende Durchdringung der im privaten wie geschäftlichen Bereich genutzten elektronischen Produkte, wie beispielsweise Laptops, Smartphones oder mobiler Datenträger, mit der Möglichkeit immer mehr personenbezogene Daten auf immer kleiner werdenden Datenträgern zu speichern, führt zu diversen datenschutzrechtlichen Herausforderungen.[1] Neben der allgemeinen datenschutzrechtlichen Herausforderung von Service und Support-Zugriffen stellt sich eine besondere datenschutzrechtliche Problematik bei einem unerwarteten Defekt des Systems, der es dem Anwender als verantwortliche Stelle unmöglich macht, weiterhin Zugriff auf die Daten zu nehmen oder diese wenigstens sicher zu löschen.[2] So kann es notwendig werden, das Gerät inklusive des verbauten Datenträgers an Dienstleister zur Geltendmachung von Garantie- oder Gewährleistungsansprüchen oder zur Wartung zu übergeben.

Insbesondere Unternehmen, die vertrauliche Daten auf klassischen Festplattenlaufwerken gespeichert haben, sehen sich im Falle eines Hardwaredefekts des Datenträgers zumeist dem Dilemma ausgesetzt, diesen entweder unter Aufgabe jeglicher Kontrollmöglichkeiten an den Hersteller oder einen entsprechenden Dienstleister übergeben zu müssen oder auf mögliche Garantie- oder Gewährleistungsansprüchen bzw. die Instandsetzung zu verzichten.

II. Ausgangssituation und Problemdarstellung

In der unternehmerischen Praxis kommt es heute regelmäßig vor, dass externe Dienstleister im Rahmen von Wartungs- und Serviceverträgen Zugang zu IT-Systemen und Datenträgern erhalten, die ebenso regelmäßig den Zugriff auf personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG ermöglichen. Die Wartung von Hard- und Software kann dabei entweder vor Ort beim Kunden, per Fernwartung oder beim Dienstleister selbst durchgeführt werden.[3] Gemäß § 11 Abs. 5 BDSG sind hierbei die Vorgaben der Auftragsdatenverarbeitung entsprechend anzuwenden, wenn der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Dies wird bei jeglicher Form der Wartung und Prüfung regelmäßig, aber nicht notwendigerweise, der Fall sein.[4]

Bei der hardwareseitigen Beauftragung zur Wartung steht der physische und logische Zugriff auf die Datenträger im Vordergrund. Die personenbezogenen Daten sind dabei gerade nicht Gegenstand des Zugriffs, selbst wenn diese am Rande zur Kenntnis genommen werden können. Die bloße Existenz von personenbezogenen Daten stellt jedoch schon für sich genommen eine gewisse datenschutzrechtliche Herausforderung bei der Wartung oder Reparatur dieser Systeme oder Datenträger dar. Besonders kritisch wird es, wenn es im Rahmen der Gewährleistung, einer Garantievereinbarung oder auf sonstige Weise zu einem Austausch von kompletten Systemen oder einzelnen Datenträgern kommt. Ob die Vertraulichkeit der Daten gewährleistet werden kann, ist dabei fraglich.

1. Datenschutzrechtliche Verantwortlichkeit

Primär sieht der Gesetzgeber im Rahmen des Datenschutzrechts vor, dass die „verantwortliche Stelle" für die ordnungsgemäße Sicherung und Sicherheit der auf den Datenträgern vorhandenen Daten verantwortlich ist. So sind durch den Auftraggeber angemessene technische und organisatorische Maßnahmen zu ergreifen, welche die sensiblen Daten bereits vorab dem Zugriff der Wartungstechniker entziehen.[5] Somit ist für den Datenschutz grundsätzlich der Auftraggeber die verantwortliche Stelle und mithin haftbar. Die alleinige Wartung oder Reparatur der Hardware hat dabei mit den Daten als solchen nichts im engeren Sinne zu tun, so dass den Vorgaben des BDSG bezüglich Datenvermeidung und Datensparsamkeit folgend, die Existenz von personenbezogenen Daten bei einer Über- oder Rückgabe von Systemen oder Datenträgern an einen Externen auszuschließen ist, soweit deren Weitergabe datenschutzrechtlich unzulässig ist. Zu denken ist an ein sicheres und irreversibles Löschen, eine ausreichende Verschlüsselung oder ein ähnliches Verfahren zur Entfernung der personenbezogenen Daten, um diesen Anforderungen nachzukommen.

2. Einordnung

In der datenschutzrechtlichen Praxis im Umgang mit Datenträgern und IT-Systemen können in diesem Zusammenhang insbesondere folgende Fallgruppen unterschieden werden, die nachfolgend exemplarisch untersucht werden:

1. Routinemäßige Wartung von Datenträgern mit personenbezogenen Daten.
2. Rückgabe oder Übergabe entsprechender Datenträger im Rahmen von Garantie- und Gewährleistungsansprüchen an Externe bedingt durch einen physikalischen Datenträgerdefekt.

III. Rechtliche Bewertung

1. Routinemäßige Wartung von Datenträgern mit personenbezogenen Daten

Bei der routinemäßigen Wartung von Hard- und Software durch Externe sind die besonderen Anforderungen des § 11 BDSG zu beachten.

Unter der im BDSG selbst nicht definierten Wartung ist in Anlehnung an § 3a Abs. 4 lit. a BlnDSG „die Summe der Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Hard- und Software von Datenverarbeitungsanlagen; dazu gehören die Installation, Pflege, Überprüfung und Korrektur der Software sowie Überprüfung und Reparatur oder Austausch von Hardware" zu verstehen. Die Vorschrift enthält damit einen sehr weiten Anwendungsbereich.[6]

Grundsätzlich stellt sich hierbei die Frage nach den speziellen Anforderungen des § 11 BDSG, gemäß dem eine Auftragsdatenverarbeitung vorliegen könnte und somit die Einhaltung bestimmter Regularien zwischen der verantwortlichen Stelle und dem Dienstleister erfordern würde. Bei klassischen Wartungs- und Serviceverträgen wird jedoch keine Auftragsdatenverarbeitung angenommen, da die Daten an sich gerade nicht zur auftragsgemäßen Verarbeitung oder Nutzung überlassen werden.[7]

Gemäß § 11 Abs. 5 BDSG, der als gesetzliche Klarstellung eines Zweifelsfalls verstanden werden kann, gelten die Absätze 1 bis 4 entsprechend, „wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann".

Es ist dabei nicht notwendigerweise von einer Auftragsdatenverarbeitung i.S.d. BDSG zu sprechen.[8] Vielmehr handelt es sich um eine gesetzliche Fiktion mit der Anordnung einer entsprechenden Anwendung.[9]

a) Anwendbarkeit des § 11 Abs. 5 BDSG und die Konsequenzen

Bei der reinen Hardwarewartung wird in der Regel nur auf bestimmte Statusinformationen in Diagnosedateien zugegriffen, die keine personenbezogenen Daten enthalten, so dass die entsprechende Anwendbarkeit des § 11 Abs. 1 bis 4 BDSG zumindest für den Fall des sicheren Ausschlusses des Zugriffs auf personenbezogene Daten nicht zwangsläufig gegeben ist. Dies ist zweifelsohne der Fall, wenn der Zugriff des Dienstleistungsunternehmens durch ein kopiertes Testsystem erfolgt, in dem die personenbezogenen Daten von Anfang an nur anonymisiert vorliegen.[10] Weiterhin ist an einen komplett und ordnungsgemäß gelöschten Datenträger zu denken.

Bei der Wartung von Datenträgern ist die Offenbarung geschützter personenbezogener Daten im Zweifelsfall nie sicher auszuschließen. Schon die Möglichkeit des Datenzugriffs genügt, so dass es nicht darauf ankommen soll, ob ein Zugriff tatsächlich erfolgt oder durch Maßnahmen der verantwortlichen Stelle erschwert wird.[11]

Dabei sind die Fernwartung und die bei Datenträgern aufgrund der erforderlichen Ausstattung oftmals vorliegende Wartung außerhalb der Räumlichkeiten des Auftraggebers datenschutzrechtlich besonders problematisch. Bei einer Wartung vor Ort wären die Kontroll- und Eingriffsmöglichkeiten des eigenen Personals im Regelfall deutlich größer.

Bei der Wartung von Festplatten kann die Verschlüsselung eine entscheidende Rolle spielen. In diesem Kontext stellt sich zum einen die Frage, ob es sich bei verschlüsselten Daten überhaupt noch um personenbezogene Daten handelt und zum anderen ob eine Verschlüsselung dazu führt, dass der Zugriff auf personenbezogene Daten gemäß § 11 Abs. 5 BDSG als ausgeschlossen angesehen werden kann. Die Thematik

1 Zu BYOD siehe *Franck*, RDV 2013, 185; *von dem Bussche/Schelinski*, in: MAH IT-Recht, 2013, Teil 1. Rn. 468 ff.; *Conrad/Schneider*, ZD 2011, 153; Zur Durchsuchung von Computern, Smartphones und sonstigen Datenspeichern von Arbeitnehmern siehe *Niemeyer*, CB 2013, 133.

2 Legaldefinition der verantwortlichen Stelle siehe § 3 Abs. 7 BDSG.

3 Vgl. *Grützner/Jakob*, Compliance von A–Z, 2010, Fernwartung. Zu den spezifischen Problemen und Anforderungen siehe *Schierbaum*, Computer-Fachwissen, 6/2005 S. 4 ff.; *Gerling*, Datenschutz Praxis, 5/2009 S. 10 f.

4 *Petri*, in: Simitis, BDSG, 7. Aufl. 2011, § 11 Rn. 98 ff.

5 Für der Verschwiegenheitspflicht unterfallende Daten im Notariat siehe *Bettendorf*, in: Beck'sches Notar-Handbuch, 5. Aufl. 2009, M. Rn. 111 f.

6 *Petri*, in: Simitis, BDSG, § 11 Rn. 98.

7 Gola/Schomerus, BDSG, 11. Aufl. 2012, § 11 Rn. 14; Bergmann/Möhrle/Herb, BDSG 2013, § 11 Rn. 64 m. w. N.

8 Vgl. Gola/Schomerus, BDSG, § 11 Rn. 14 ff.

9 Bergmann/Möhrle/Herb, BDSG 2013, § 11 Rn. 64.

10 *Petri*, in: Simitis, BDSG, § 11 Rn. 100; ähnlich Bergmann/Möhrle/Herb, BDSG 2013, § 11 Rn. 65, die eine Gefahr des Zugriffs auf personenbezogene Daten wohl auch in diesem Fall nicht ausschließen wollen.

11 *Spoerr*, in: BeckOK BDSG, Ed. 6 2013, § 11 Rn. 80 m. w. N.

wird kontrovers diskutiert.[12] Im Ergebnis darf der Schutzzweck des BDSG durch eine Verschlüsselung, die zukünftig möglicherweise nicht mehr sicher ist, nicht unterlaufen werden, wobei mobile Datenträger besonders kritisch zu betrachten sind.[13]

Als Zwischenergebnis ist festzuhalten, dass in jedem Fall des externen Zugangs zu Datenträgern der verantwortlichen Stelle und somit auch der potentiellen Möglichkeit des Zugriffs auf personenbezogene Daten die Anforderungen des § 11 BDSG zu erfüllen sind.

Der Auftraggeber bleibt weiterhin allein verantwortlich für die Einhaltung des Datenschutzes und die Gewährleistung der Rechte der Betroffenen, auch wenn er eine rechtliche Einheit mit dem Auftragnehmer bildet.[14] Ein Verschulden des Auftragnehmers als Erfüllungsgehilfe ist dem Auftraggeber gemäß § 278 BGB zuzurechnen, was zu einer entsprechenden Haftung bei Pflichtverletzungen gegenüber den Betroffenen führen kann.[15] Eine eigene Haftung des Auftragnehmers kommt jedoch für den Fall in Betracht, dass dieser die Daten nicht den Weisungen des Auftraggebers entsprechend verwendet. Ein wichtiges Element der Auftragsdatenverarbeitung ist mithin die tatsächliche Weisungsgebundenheit des Auftragnehmers. Weiterhin ist der Auftraggeber für die Einhaltung der Anforderungen des § 11 BDSG verantwortlich, wobei es zu beachten gilt, dass die Privilegierungswirkung infolge einer Unwirksamkeit der Auftragsdatenverarbeitung nicht eingreift und auf eine etwaige Einwilligung des Betroffenen oder eine gesetzliche Zulässigkeit zurückgegriffen werden müsste.

b) Vertragliche Anforderungen

In jedem Fall sollten oben genannte Sachverhalte durch Wartungs- oder Serviceverträge gegebenenfalls mit entsprechenden Service-Level-Agreements und genauen Leistungsbeschreibungen geregelt werden.[16] Erfolgt die Leistung innerbetrieblich durch eigene Mitarbeiter handelt es sich um eine normale Datenverarbeitung und der Anwendungsbereich des § 11 Abs. 5 BDSG ist nicht eröffnet.[17] Die gegenseitigen Rechte und Pflichten zwischen dem Auftraggeber als verantwortlicher Stelle und dem Auftragnehmer sollten so umfassend wie möglich geregelt werden. Vertragstechnisch können die zu treffenden Vereinbarungen über die Auftragsdatenverarbeitung als Anlage zum Hauptvertrag ausgestaltet oder direkt in den Hauptvertrag integriert werden. Letztere Variante hat den Vorzug, widersprüchliche Regelungen zu vermeiden.[18]

Der Vertrag ist gemäß § 11 Abs. 2 Satz 2 BDSG schriftlich abzuschließen, will man nicht den Wegfall der Privilegierungswirkung mit der möglichen Konsequenz der Unzulässigkeit der Datenweitergabe und ein Bußgeld gemäß § 43 Abs. 1 Nr. 2b BDSG riskieren.[19] Vertraglich ist dabei die Weisungsgebundenheit des Auftragnehmers klar herauszustellen und diese – wenn nötig – auch im weiteren Verlauf tatsächlich zu leben.

Der Abschluss des Auftragsdatenverarbeitungsvertrags muss gemäß § 11 Abs. 2 S. 1 BDSG mit einem sorgfältig ausgewählten Auftragnehmer erfolgen und zwar „unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen".

c) Umsetzung des „10-Punkte-Katalogs"

Besonders problematisch stellen sich in der Praxis die Festlegung der technischen und organisatorischen Maßnahmen sowie das Erfordernis der Auswahl und Kontrolle durch den Auftraggeber dar. Die tatsächlichen Gründe dafür sind vielfältig.

Da es sich bei der Datenträgerwartung nicht um eine klassische Auftragsdatenverarbeitung handelt, d. h. dem Auftrag nach die Verarbeitung von personenbezogenen Daten gerade nicht erfolgen soll und die § 11 Abs. 1 bis Abs. 4 BDSG nur entsprechend anzuwenden sind, ist ein Standard-Auftragsdatenverarbeitungsvertrag entsprechend auf die konkrete Wartungssituation anzupassen. Hierbei ist auch auf eine Anpassung des „10-Punkte-Katalogs" gemäß § 11 Abs. 2 S. 2 Nr. 1–10 BDSG zu achten.[20]

d) Technische und organisatorische Maßnahmen

Welche technischen und organisatorischen Maßnahmen gemäß § 11 Abs. 2 S. 2 Nr. 3 BDSG erforderlich sind, muss im Einzelfall gemäß § 9 S. 2 BDSG anhand der erforderlichen Schutzbedürftigkeit festgelegt werden. Durch die vom Auftragnehmer zu verlangenden Maßnahmen ist sicherzustellen, dass die Wartung genauso sicher erfolgen kann, wie dies bei eigener Vornahme durch die verantwortliche Stelle der Fall wäre. Bei der Wartung von Datenträgern durch Externe ist diesbezüglich danach zu differenzieren, ob die Wartung in den eigenen Räumlichkeiten stattfindet oder beim Dienstleister.[21]

Erfolgt die Wartung in den eigenen Räumlichkeiten, sind die technischen und organisatorischen Maßnahmen in der Regel durch den Auftraggeber zu gewährleisten und insoweit nicht gesondert zu vereinbaren. Die bereits erwähnte Verschlüsselung stellt hierbei, wenn auf dem Gerät möglich, eine wichtige Maßnahme für den Auftraggeber dar. Eine weitere Maßnahme kann die protokollierte oder persönliche Kontrolle des Auftragnehmers sein.

12 Vgl. *Heidrich/Wegener*, MMR 2010, 803, 806; *Stiemerling/Hartung*, CR 2012, 60 ff.; *Hornung/Sädtler*, DuD 2013, 148, 151 ff.; Kontroverse Fachdiskussion zum Vorliegen personenbezogener Daten bei Verschlüsselung, *Spies*, MMR-Aktuell 2011, 313727.

13 Die Kryptographie stellt eine Möglichkeit der Pseudonymisierung dar, indem eine Verschlüsselung zum Einsatz kommt, die es mittels eines Schlüssels dem Besitzer – wie auch einem unberechtigten Dritten – ermöglicht, die Daten lesbar zu machen. Gleichwohl handelt es sich weiterhin um personenbezogene Daten; vgl. *Schild*, in: BeckOK BDSG, Ed. 6 2013, § 3 Rn. 107 m. w. N. Teilweise wird in der Verschlüsselung von Daten eine Anonymisierung gesehen, womit schon der Anwendungsbereich des BDSG nicht eröffnet wäre. Daten verlieren jedoch alleine durch die Verschlüsselung nicht ihre Qualität als personenbezogene Daten. Durch die Verschlüsselung, bei der es sich um eine technisch-organisatorische Maßnahme unter vielen handelt, wird lediglich sichergestellt, dass die Daten nicht ungehindert durch Unbefugte zur Kenntnis genommen werden können; vgl. *Ernestus*, in: Simitis, § 9 Rn. 173 f. Das BDSG bleibt somit für die derart verschlüsselten Daten weiterhin anwendbar; vgl. *Schild*, in: BeckOK BDSG, Ed. 6 2013, § 3 Rn. 107 m. w. N.; anders wohl *Heidrich/Wegener*, MMR 2010, 803, 806. Es muss bedacht werden, dass heute noch als sicher geltende Verschlüsselungsmethoden schon jetzt mit erheblicher Rechenleistung oder in naher Zukunft als leicht zu entschlüsseln gelten werden und ihre Schutzwirkung spätestens dann verlieren; vgl. nur *Hornung/Sädtler*, DuD 2013, 148, 152, die völlig zu Recht konstatieren: „Es lässt sich technisch kaum garantieren, dass heutige Verschlüsselungsverfahren so lange sicher sind." Allein auf den heutigen Stand der Technik abzustellen und nicht auf die weitere Entwicklung, kann zum Unterlaufen des BDSG führen. Das Gesetz kennt kein erlaubtes Risiko. Mit den gleichen Argumenten lässt sich auch gegen den Ausschluss des Zugriffs auf personenbezogene Daten gemäß § 11 Abs. 5 BDSG argumentieren. Man denke nur an den Fall abhandengekommener, wenn auch verschlüsselter Datenträger mit sensiblen Informationen, die zu einem späteren Zeitpunkt ohne weiteres durch Dritte zu entschlüsseln sind.

14 *Spindler*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 11 BDSG Rn. 3.

15 *Eckhardt*, DuD 2013, 585, 586.

16 Bei Hardware-Wartungsverträgen handelt es sich nach h. M. um Werkverträge, siehe auch *von dem Bussche/Schelinski*, in: MAH IT-Recht, 2013, Teil 1. Rn. 126.

17 *Kiesche/Wilke*, CuA 3/2008, 6, 9.

18 Vgl. *Spoerr*, in: BeckOK BDSG, Ed. 6 2013, § 11 Rn. 88.

19 *Petri*, in: Simitis, BDSG, 7. Aufl. 2011, § 11 Rn. 64; Gola/Schomerus, BDSG, 11. Aufl. 2012, Rn. 17; Zur Problematik der Urkundeneinheit und zur Folge von Formverstößen siehe *Spoerr*, in: BeckOK BDSG, Ed. 6 2013, § 11 Rn. 88 ff.; Laut Art. 17 Abs. 4 RiLi 95/46/EG soll auch eine nicht der Schriftform entsprechende Dokumentation möglich sein.

20 Vgl. *Eckhardt*, DuD 2013, 585, 586.

21 Eigene Räumlichkeiten verstehen sich in diesem Zusammenhang als Räumlichkeiten, welche vollumfänglich im Verantwortungsbereich der verantwortlichen Stelle liegen und durch diese entsprechend kontrolliert und verwaltet werden können.

Für den Fall der externen Wartung sind hingegen die erforderlichen Maßnahmen umso kritischer zu prüfen und die entsprechenden Maßnahmen auch durch den Auftragnehmer sicherzustellen.

Für das praktische Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer bedeutet dies, dass praxisrelevante vertragliche Regelungen bezüglich des Datenschutzes zu treffen sind.[22]

e) Auswahl und Kontrolle des Dienstleisters – Zertifikate Dritter als Lösung

Gemäß § 11 Abs. 2 S. 4 und 5 BDSG hat sich der Auftraggeber „vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen", wobei das Ergebnis zu dokumentieren ist. Das Gesetz fordert zwar eine kritische Prüfung durch den Auftraggeber, jedoch statuiert es gerade keine Pflicht zur eigenständigen Vor-Ort-Kontrolle, zumal dies bei großen Dienstleistern zu einem unkontrollierten Auditierungstourismus führen würde, was dem Ziel der getroffenen technischen und organisatorischen Maßnahmen geradezu diametral entgegensteht. Aus den Materialien des Innenausschusses des Deutschen Bundestags ergibt sich zudem, dass der Gesetzgeber sogar ausdrücklich von der Normierung einer persönlichen und unmittelbaren Vor-Ort-Kontrollpflicht des Auftraggebers abgesehen hat und auch ein Testat eines Sachverständigen ausreicht.[23] Der Auftraggeber muss sich beim Rückgriff auf Dritte bei der Überprüfung auch von der Einhaltung der technischen und organisatorischen Maßnahmen „überzeugen", d. h. Einsicht in die entsprechenden Zertifikate und Protokolle nehmen und diese auf das erforderliche Schutzniveau hin prüfen.[24] Dabei kann es einen entscheidenden Wettbewerbsvorteil für einen Anbieter darstellen, wenn er sich bei einer großen Anzahl von Auftraggebern durch eine unabhängige Stelle überprüfen lässt.[25] Nur wenn der Auftraggeber Zweifel an der Zuverlässigkeit des Auftragnehmers haben muss, wird eine eigene Kontrolle notwendig.[26]

f) Unterauftragsverhältnisse

Die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen ist gemäß § 11 Abs. 2 S. 2 Nr. 6 BDSG vertraglich zu regeln. Praxisnah erscheinen dem Einzelfall angepasste Lösungen dieses kritischen Regelungspunktes, da sich auf der einen Seite die Haftung des Auftraggebers auf den Subunternehmer ausweitet, sich aber auf der anderen Seite oft eine gewisse Abhängigkeit des Auftragnehmers von weiteren Dienstleistern ergibt.[27]

Der Auftraggeber sollte die Beauftragung von Subunternehmen von der schriftlichen Zustimmung des Auftraggebers abhängig machen. Ferner sollten Unteraufträge die Kontrollrechte des Auftraggebers auch beim Unterauftragnehmer vorsehen.[28] Alternativ ist auch an die Vereinbarung von vorab festgelegten Unterauftragsnehmern oder an ein Sonderkündigungsrecht zu denken. Als weiteres Zulässigkeitskriterium kann eine Zertifizierung des Subunternehmers als Vertragsbestandteil verlangt werden, wonach die Zustimmung bei Erfüllung dieses oder anderer festzulegender Kriterien nicht unbillig verweigert werden darf.

22 Grundlagen hierzu bilden regelmäßig §§ 631 BGB oder 611 BGB.

23 BT-Drs. 16/13657, S. 18.

24 Vgl. *Petri*, in: Simitis, BDSG, § 11 Rn. 59; *Weichert*, DuD 2010, 679, 685, sieht die Selbstzertifizierung des Anbieters als nicht ausreichend an. Die Prüfung durch einen externen unabhängigen Dritten soll jedoch möglich sein.

25 Bergmann/Möhrle/Herb, BDSG 2013, § 11 Rn. 48b.

26 *Hallermann*, RDV 2012, 226, 227.

27 *Eckhardt*, DuD 2013, 585, 587.

28 *Petri*, in: Simitis, BDSG, 7. Aufl. 2011, § 11 Rn. 76.

2. Rückgabe oder Übergabe entsprechender Datenträger im Rahmen von Garantie- und Gewährleistungsansprüchen an einen Dritten bedingt durch einen physikalischen Datenträgerdefekt

Rechtlich und operativ herausfordernd stellt sich der potentielle Zugriff auf personenbezogene Daten im Falle von Servicetätigkeiten durch einen Dienstleister dar, wenn ein physikalischer Zugriff auf diese Daten technisch nicht möglich ist und die verantwortliche Stelle ihren Sicherungspflichten nicht mehr nachkommen kann.

a) Problem bei defekten Systemen und Datenträgern

Im Rahmen von Garantie- oder Gewährleistungsansprüchen kommt es der Sache immanent regelmäßig vor, dass die verantwortliche Stelle aufgrund des physikalischen Defekts der Datenträger selbst nicht mehr in der Lage ist, mit vertretbarem Aufwand ihren entsprechenden Sicherungspflichten nachzukommen, zumal dadurch die vertraglichen Ansprüche gefährdet würden. Da schon für eine Reparatur unvermeidbar personenbezogene Daten mit übergeben werden müssen, ist der Vorgang als äußerst kritisch zu bewerten. Besonders brisant wird es jedoch, wenn der Datenträger nicht nur, wie in der Fallgruppe 1 durch den Auftragnehmer gewartet wird, sondern wenn es im Rahmen der garantie-, gewährleistungs-, oder wartungsbedingten Rückgabe bzw. Überlassung von entsprechenden Datenträgern an Externe zu einem Austausch des Datenträgers kommt. Der Verbleib des Originaldatenträgers ist nicht mehr nachvollziehbar und somit der Kontrolle des Auftraggebers völlig entzogen. Einem möglichen Datenabfluss wäre ohne weitere Regelungen Tür und Tor geöffnet.

b) Verantwortlichkeit und Anwendbarkeit des § 11 Abs. 5 BDSG

In dieser Situation stellt sich praktisch wie rechtlich die Frage nach der Verantwortlichkeit für den Datenschutz sowie der entsprechenden Vorgehensweise im Rahmen der sicheren und vertraulichen Datenverarbeitung, respektive des Datenschutzes.

Die datenschutzrechtliche Verantwortung verbleibt auch in diesem Fall trotz augenscheinlicher Unmöglichkeit bei der verantwortlichen Stelle.

Auch ist § 11 Abs. 5 BDSG anwendbar, nach welchem vertragliche Regelungen getroffen werden müssen und operative Vorgaben gelten, wenn ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.[29] Es kann insoweit auf die bereits erfolgten Ausführungen verwiesen werden.

c) Besonderheiten

Aus Sicht der verantwortlichen Stelle sind im Vergleich zur Fallgruppe 1 nunmehr vertragliche Regelungen zu treffen, die dem Dienstleister u. a. alle erforderlichen technischen und organisatorischen Maßnahmen abverlangen, da der Auftraggeber sie selbst nicht mehr treffen kann, ohne seine Ansprüche zu gefährden.[30]

Insbesondere ist die konkrete Verpflichtung des Dienstleisters zur Löschung der Daten zu vereinbaren und eine lückenlose Dokumentation der Datenlöschung, gegebenenfalls entlang der Prozesskette, zu fordern. Die Vereinbarung einer angemessen hohen Vertragsstrafe erscheint angebracht.

Für den Dienstleister stellt gerade eben dieser Sachverhalt die Herausforderung dar, organisatorische und technische Maßnahmen zu implementieren und vorzuhalten, die den Vorgaben dieser vertraglichen Spezifikation entsprechen.

Die meisten Hersteller von klassischen Datenträgern haben auf diese Problematik bereits mit sog. Hard Drive Retention Vereinbarungen reagiert, die den Verbleib der Datenträger beim Kunden regeln. Falls ein defekter Datenträger nicht mehr repariert werden kann und ersetzt

29 Gola/Schomerus, BDSG, § 11 Rn. 15.

30 Gola/Schomerus, BDSG, § 11 Rn. 15.

werden muss, bleibt der Datenträger Eigentum des Kunden. Damit wird sichergestellt, dass vertrauliche Unternehmensdaten das Unternehmen nicht verlassen.

IV. Zusammenfassung der Lösungsansätze für die Praxis

1. Grundsätzlich gelten für alle Konstellationen von Wartungs- oder Serviceleistungen die Vorgaben des § 11 BDSG. So hat zunächst die für den Datenträger verantwortliche Stelle den Datenschutz zu gewährleisten und entsprechende vertragliche Regelungen sowie entsprechende eigene Sicherungsmaßnahmen zu treffen.
   Konkret bedeutet dies, dass zwischen Auftraggeber (verantwortliche Stelle) und Auftragnehmer (Dienstleister) mindestens folgende Punkte schriftlich geregelt werden müssen:
   1. Gegenstand und Dauer des Auftrages;
   2. Technische und organisatorische Maßnahmen nach Anlage zu § 9 BDSG, die durch den Dienstleister implementiert sein müssen, um den Datenschutz im Rahmen der Leistungserbringung zu gewährleisten;[31]
   3. Umgang mit Unterlagen des Auftraggebers;
   4. Umgang mit Unterauftragsverhältnissen;
   5. Kontrollrechte des Auftraggebers;
   6. Rückgabe von Datenträgern und Umgang mit diesen.

2. Die unter IV.1. genannten Regelungen sollten grundsätzlich ausreichen, soweit die Dienstleistung in den Räumlichkeiten der verantwortlichen Stelle erfolgt. Sobald es sich um die Übergabe des Datenträgers handelt, bietet sich aus praktischer Sicht die Löschung der Daten in geeigneter Form durch die verantwortliche Stelle vor Übergabe des Datenträgers an. Datenträger sind dabei durch Methoden, die dem Stand der Technik entsprechen, wie beispielsweise den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik, zu löschen.[32]
   Grundsätzlich ist hierbei festzuhalten, dass dieses Löschen nicht in jedem Fall eine 100%ige Garantie für eine unmögliche Rekonstruktion geben kann.
   Alternativ kommt die komplett verschlüsselte Übergabe des Datenträgers in Betracht (Vollverschlüsselung).[33]

3. Die Fallgruppe 2, in der ein Dienstleister oder Hersteller im Rahmen von entsprechenden Leistungen defekte Datenträger erhält, stellt sich praktisch wesentlich komplexer dar, da die verantwortliche Stelle durch den Defekt bedingt, ihren eigenen durch das BDSG auferlegten Sicherungspflichten nicht in vollem Umfang nachkommen kann. Diesbezüglich sind verschiedene Aspekte zu erfüllen:
   a) Gesetzliche Pflichten der verantwortlichen Stelle: Nach § 11 Abs. 5 BDSG hat die verantwortliche Stelle im Rahmen ihrer eigenen datenschutzrechtlichen Verantwortung die Vorgaben der Auftragsdatenverarbeitung mit dem Dienstleister zu erfüllen. Hierbei ist aus Sicht der verantwortlichen Stelle vollumfänglich auf Kap. IV. 1 zu verweisen.
   b) Operative Möglichkeiten und Notwendigkeiten des Dienstleisters: Im Rahmen der gesetzlichen und vertraglichen Pflichten, die dem Dienstleister im Falle der Wartung, Reparatur und Rücknahme defekter Datenträger obliegen, bieten sich verschiedene Standardisierungen für den Dienstleister (Auftragnehmer) an:
      aa) Standardisierte Dokumentation technisch-organisatorischer Maßnahmen zur Gewährleistung der gesetzlichen Forderungen.
      bb) Überführung voran genannter Dokumentation in ein standardisiertes Vertragswerk, das Bestandteil der Beauftragung der verantwortlichen Stelle wird.
      cc) Implementierung eines standardisierten Löschungs- oder Vernichtungsprozesses bei Erhalt der Datenträger.[34] In diesem Zusammenhang ist auf die in Kap. IV. 2 genannten Verfahren abzustellen.

   Die eventuell auf den Datenträgern enthaltenen Daten sind in keinem Fall Bestandteil oder Inhalt der (mechanischen) Prüfungen. Von daher sollte ein Dienstleister in diesem Fall vor Beginn etwaiger Arbeiten am Datenträger als solchem diese Routinen standardisiert implementieren und durchlaufen. So sollte unterbunden sein, dass sich bei der weiteren Analysen oder späteren Weiterverwendung der Datenträger noch personenbezogene Daten auf diesen (reparierten) Datenträgern befinden.

V. Ergebnis

Der Umgang mit Datenträgern birgt datenschutzrechtliche Herausforderungen. Wenngleich die strikten und umfänglichen Vorgaben des § 11 BDSG nicht notwendigerweise in jedem Fall gesetzlich Anwendung finden, so wird bei der vertraglichen Situation zwischen verantwortlicher Stelle und Dienstleister auf die formalen Vorgaben und Sicherungsmaßnahmen der Auftragsdatenverarbeitung entsprechend abgestellt.

Eine besonders kritische Situation bei der Sicherung und Gewährleitung von datenschutzrechtlichen Sicherheitsmaßnahmen stellt die Wartung und Reparatur physikalisch defekter Datenträgern dar. In diesem Fall erfolgt praktisch ein Übergang der Pflichten von der verantwortlichen Stelle auf den Dienstleister, da die sog. verantwortliche Stelle als solche nicht länger in der Situation ist, ihren eigenen Sicherheitspflichten nachzukommen.

Dies hat praktische Auswirkungen auf IT-Dienstleistungsunternehmen sowie Hersteller im Rahmen von Gewährleistungs- und Haftungsansprüchen, da diese in erster Linie beim Erhalt einer entsprechenden Hardware (Datenträger) dafür Sorge zu tragen haben, dass die auf diesen Datenträgern möglicherweise vorhandenen personenbezogenen Daten in entsprechender Art und Weise gelöscht oder vernichtet werden.

So gilt es für die verantwortlichen Stellen sowohl vertragliche Standardanforderungen gemäß den Vorgaben der Auftragsdatenverarbeitung vorzuhalten, als auch Prüfungsroutinen, die eine gewissenhafte Auswahl der Dienstleister gewährleisten, zu implementieren. Für Anbieter entsprechender Dienstleistungen und Hersteller, die mit solchen Dienstleistungen konfrontiert sind (Haftungsansprüche, Garantieansprüche), bietet es sich an, mittels standardisierter Prozesse und technischer, wie mechanischer Verfahren zu gewährleisten, dass valide Methoden implementiert werden, um den Ansprüchen der Kunden zu genügen. Zum Nachweis der Existenz dieser Prozesse und Maßnahmen bieten sich aussagekräftige Testate Dritter an.

31 Aus rein praktischer Sicht sind hierbei zu nennen (ohne Anspruch auf Vollständigkeit): Verpflichtung der Mitarbeiter auf das Datengeheimnis, Schulungskonzept der Mitarbeiter zur Sensibilisierung, technische Sicherheit eigener Hardware.

32 Baustein M 2.167 Sicheres Löschen von Datenträgern; BSI Grundschutzkatalog (www.bsi.bund.de); Zum sicheren Löschen von Daten auf Festplatten; siehe *Fox*, DuD 2009, 110 ff.

33 Baustein M 4.29 Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme; BSI Grundschutzkatalog (www.bsi.bund.de); zur Partitions- und Systemverschlüsselung mit TrueCrypt: *Fox*, DuD 2008, 475, 478.

34 Geeignete Methoden sind bspw. in der DIN 66399:2012 „Vernichtung von Datenträgern" beschrieben.

VI. Checkliste Datenträgerwartung

	Verantwortliche Stelle	Vertraglicher Dienstleister
Situation	Routinemäßige Wartung und Reparatur von Datenträgern	
Verantwortung	Datensicherheitspflichten entsprechend Anlage zu § 9 BDSG Regelungen entsprechend § 11 Abs. 2 BDSG	Datensicherheitspflichten entsprechend Anlage zu § 9 BDSG
Maßnahme	Vertragliche Regelung (standardisiert) Löschung der Daten Vollverschlüsselung	Dokumentation der Sicherheitsmaßnahmen
Regelungsbestandteile/ Methoden[35]	Schulung, Sensibilisierung, Datensicherheitsmaßnahmen § 11 Abs. 2 Nr. 3, 5, 10 BDSG BSI Grundschutzkatalog M 2.167, M 2.433 BSI-TL 03420 Degausser (Entmagnetisierung) 5220.22-M-Standard VSITR-Standard Bruce-Schneier-Algorithmus Guttmann-Methode DIN 66399 (Schredder) Thermische Zerstörung	-/-

	Verantwortliche Stelle	Vertraglicher Dienstleister
Situation	Wartung und Reparatur defekter Datenträger	
Verantwortung	Regelungen entsprechend § 11 Abs. 2 BDSG	Datensicherheitspflichten entsprechend Anlage zu § 9 BDSG
Maßnahme	Vertragliche Regelung (standardisiert)	Dokumentation der Sicherheitsmaßnahmen
Regelungsbestandteile/ Methoden[35]	Schulung, Sensibilisierung, Datensicherheitsmaßnahmen § 11 Abs. 2 Nr. 3, 5, 10 BDSG	Standardisierte Löschung oder Vernichtung von Datenträgern bei Übernahme

35 Siehe auch Leitfaden zum Sicheren Datenlöschen, V 2.0, BITKOM 2008.

Datenschutzrechtliche Besonderheiten bei der Beauftragung eines Steuerberaters durch Unternehmen[1]

Rudi Kramer

Rudi Kramer, Rechtsanwalt, Nürnberg
Datenschutzreferent, DATEV eG
Mitglied des Vorstands des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Im bundesdeutschen Datenschutzrecht gibt es immer wieder Sachverhalte, welche die Ausnahme von der Regel darstellen Die Grundlage hierfür ist oftmals in feinen Unterscheidungen bei der Sachverhaltsgestaltung oder in einer bewussten gesetzgeberischen Entscheidung bzw. in einer spezielleren Rechtsvorschrift zu finden, welche nach § 1 Abs. 3 BDSG den Vorschriften des BDSG vorgeht. In der Praxis führt dies immer wieder zu Irritationen, wenn die spezielleren Vorschriften nur einen datenschutzrechtlichen Randbereich oder eine sehr spezielle Gestaltung betreffen. Ein schönes Beispiel dafür stellt die Beauftragung eines Steuerberaters dar, welches hier ausführlicher erörtert werden soll. Dabei werden die Thematiken der Rechtsgrundlage der Erhebung von Daten durch den Steuerberater, das Rechtsverhältnis der Mandatierung aus datenschutzrechtlicher Sicht sowie Konsequenzen aus berufsrechtlichen Verschwiegenheitsregelungen sowie § 203 StGB dargestellt.

Die Beauftragung eines Steuerberaters gehört zum Alltagsgeschäft eines Unternehmens. Die Statistik der Bundesteuerberaterkammer weist zum 01.01.2013 einen Bestand von 91.248 Mitgliedern aus,[2] welche

1 Der Aufsatz stellt die persönliche Ansicht des Autors dar.

2 BSTBK, Berufsstatistik 2012, http://www.bstbk.de/export/sites/standard/de/ressourcen/Dokumente/01_bstbk/berufsstatistik/Berufsstatistik_2012.pdf (letzter Abruf 12.01.2014).