Outsourcing im Massengeschäft sicher und rechtskonform

Matthias Bergt

von BOETTICHER Rechtsanwälte
mbergt@boetticher.com

Zusammenfassung

Auftragsdatenverarbeitung im Sinne von § 11 BDSG (Dienstleistervertrag, §§ 10 f. öst. DSG; Datenbearbeitung durch Dritte, Art. 10a schweiz. DSG; Auftragsverarbeitung, Art. 16 f. RL 95/46/EG – Datenschutzrichtlinie – DS-RL)[1] nutzt heute jedes Unternehmen täglich – nicht nur Großunternehmen im Rahmen des althergebrachten, umfangreich ausgehandelten IT-Outsourcing-Projekts. Vielmehr ist Auftragsdatenverarbeitung zu einem Massengeschäft geworden, in dem beispielsweise der E-Mail-Account, die Website und die Software-as-a-Service-Lösung für Buchhaltung oder Customer Relation Management „von der Stange" extern eingekauft werden – alles Auftragsdatenverarbeitung. In der Praxis werden die gesetzlichen Anforderungen an die abzuschließenden Verträge und die vorgeschriebene Kontrolle des Anbieters dabei recht konsequent ignoriert – hoher Aufwand für die Vertragsgestaltung und für eine ordnungsgemäße Kontrolle nicht ausreichende Fachkompetenz des Auftraggebers müssen als Argument für den Gesetzesverstoß herhalten. Ob die Daten beim Anbieter überhaupt ausreichend geschützt sind, bleibt oftmals unklar – ungeachtet der rechtlichen wie unternehmenspolitischen Risiken einer Datenpanne. Doch das geltende Recht hält Möglichkeiten bereit, auch im Massengeschäft rechtskonforme Auftragsdatenverarbeitung zu betreiben. Diensteanbieter sollten die Chance nutzen, sich durch entsprechende Angebote von ihren Wettbewerbern abzusetzen.

1 Rechtliche Grundlagen

Outsourcing von Datenverarbeitungsprozessen wird dann rechtlich problematisch, wenn personenbezogene Daten betroffen sind. „Personenbezogene Daten"[2] sind Angaben dann, wenn sie sich auf eine bestimmte (z.B. enthaltener Name) oder bestimmbare Person beziehen.[3] Da auch „bestimmbare" Personen umfasst sind, ist der Begriff sehr weit; die genauen Grenzen der Bestimmbarkeit sind allerdings schwer umstritten (vgl. zuletzt als gute Basis für eine künftige Lösung des Problems [KüKl13] [SpMü14]). Während EU- und deutsches Recht nur Daten von natürlichen Personen schützen, erfassen das österreichische und das schweizerische DSG auch juristische Personen.

---

[1] Im Folgenden werden im Text primär die Normen des BDSG zitiert; bei ihrem ersten Auftreten erfolgt in der Fußnote ein Hinweis auf eventuelle Parallelvorschriften, ggf. mit Hinweis auf abweichende Begriffe.

[2] Schweiz: „Personendaten".

[3] § 3 Abs. 1 BDSG; § 4 Nr. 1 öst. DSG; Art. 3 lit. a schweiz. DSG; Art. 2 lit. a DS-RL.

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 203-214.

Auftragsdatenverarbeitung[4] liegt vor, wenn eine verantwortliche Stelle[5] personenbezogene Daten nicht selbst verarbeitet, sondern dies durch einen weisungsgebundenen Dritten erledigen lässt. Auftragsdatenverarbeitung kennt dabei keine Erheblichkeitsschwelle, so dass die Regelungen zur Auftragsdatenverarbeitung auch dann zur Anwendung kommen, wenn nur gelegentlich, kurzzeitig oder in geringem Umfang personenbezogene Daten im Auftrag verarbeitet werden [Berg13, S. 796] [Plat13, Rn 23] – etwa bei einer kurzzeitigen Cloud-Nutzung.

Auftragsdatenverarbeitung ist nach EU-Recht dogmatisch eine Privilegierung: Obwohl personenbezogene Daten an eine andere Stelle weitergegeben werden, ist dafür keine Erlaubnis (durch Gesetz oder Einwilligung) erforderlich. Der Auftragnehmer, der in der EU oder im EWR tätig wird (auf den Sitz kommt es nicht an [Damm11, Rn 246] [Plat13, Rn 15]), wird dafür aus der Definition des „Dritten" (so das BDSG und die Datenschutz-Richtlinie)[6] herausgenommen, bzw. eine Datenweitergabe an ihn aus der Definition der „Übermittlung" (so das öst. DSG)[7]. Die Datenweitergabe zwischen Auftraggeber und Auftragnehmer stellt somit „nur" eine Nutzung der Daten dar [Petr11, Rn 43]. Der Auftragnehmer wird rechtlich als Teil des auslagernden Unternehmens behandelt (jedenfalls soweit die Verarbeitung im EU-/EWR-Bereich erfolgt) [Gabe13c, Rn 2] [Spin11, Rn 3]. Auf die im EU-Recht gewählte gesetzliche Fiktion [Damm11, Rn 244] [Gabe13c, Rn 2] verzichtet Art. 10a Abs. 3 schweiz. DSG und überträgt stattdessen die für den Auftraggeber geltenden Erlaubnistatbestände zum Umgang mit den Daten 1:1 auf den Auftragnehmer.

Nach § 11 Abs. 1 BDSG[8] bleibt der Auftraggeber für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich, so etwa für Ansprüche auf Schadensersatz oder Auskunftserteilung. Dabei haftet der Auftraggeber seinen Vertragspartnern über die Haftung für Erfüllungsgehilfen (§ 278 BGB[9]) auch für Verschulden des Auftragnehmers.

Von der Auftragsdatenverarbeitung abzugrenzen ist nach h. M. die so genannte Funktionsübertragung, die vorliegen soll, wenn sich der Auftrag nicht nur auf Hilfs- bzw. Unterstützungstätigkeiten beschränkt [GoKK12, Rn 9] [MöHe14, Rn 10, 11 ff.] [Petr11, Rn 20 ff.]; zum Meinungsstreit und insbesondere zu den beachtlichen Argumenten der Mindermeinung [Gabe13, Rn 14 ff.]; kritisch auch [Plat13, Rn 27 ff.]. Soll der Empfänger der Daten eine eigene Leistung erbringen (z. B. eigenverantwortlich Finanzprodukte vertreiben oder als Rechtsanwalt eine Klage schreiben), liegt eine Funktionsübertragung und damit eine Übermittlung[10] an den Empfänger vor, die einer Erlaubnis bedarf (Einwilligung, gesetzliche Erlaubnis). Im Bereich des klassischen IT-Outsourcings wie auch moderner Formen wie Software as a Service wird jedoch in aller Regel nach beiden Ansichten eine Auftragsdatenverarbeitung vorliegen, weil der Auftragnehmer nur nach den Weisungen des Auftraggebers mit den Daten verfahren soll.

---

4 § 11 BDSG; §§ 4 Nr. 5, 10 f. öst. DSG: „Dienstleistervertrag"; Art. 10a schweiz. DSG: „Datenbearbeitung durch Dritte"; Art. 2 lit. e, 16 f. DS-RL: „Auftragsverarbeitung").

5 § 3 Abs. 7 BDSG; § 4 Nr. 4 öst. DSG: „Auftraggeber"; Art. 3 lit. i schweiz. DSG: „Inhaber der Datensammlung"; Art. 2 lit. d DS-RL: „für die Verarbeitung Verantwortlicher".

6 § 3 Abs. 8 Satz 3 BDSG; Art. 2 lit. f DS-RL.

7 § 4 Nr. 12 öst. DSG.

8 § 6 Abs. 2 öst. DSG; vgl. Art. 12 lit. a, 23 Abs. 1 DS-RL und Art. 8 Abs. 4 schweiz. DSG.

9 § 1313 öst. AGBG.

10 § 3 Abs. 4 Nr. 3 BDSG; § 4 Nr. 12 öst. DSG; Art. 3 lit. f schweiz. DSG: „Bekanntgeben".

2 Der Auftragsdatenverarbeitungsvertrag

Die „Privilegierung der Auftragsdatenverarbeitung“ [Petr11, Rn 43] [Plat13, Rn 4] verbindet das Gesetz mit verschiedenen Anforderungen an die Form und den Inhalt des Vertrages.

2.1 Formale Anforderungen an den Vertrag

Der Auftrag muss nach § 11 Abs. 2 Satz 2 BDSG[11] schriftlich erteilt werden, d. h. mit Original-Unterschriften beider Seiten. Da eine ordnungsgemäße Auftragserteilung nach der Gesetzesbegründung[12] „die Ausnahme“ war, ist ein Verstoß gegen das Schriftformerfordernis seit 2009 als Ordnungswidrigkeit nach § 43 Abs. 1 Nr. 2b BDSG mit bis zu 50.000 Euro Bußgeld bedroht.

Nach der herrschenden – wenn auch falschen – Meinung in Deutschland ist ein Auftragsdatenverarbeitungsvertrag, der nicht schriftlich abgeschlossen ist, zudem nichtig. In Konsequenz soll der Auftragnehmer sich nicht auf die Privilegierung des § 11 BDSG berufen können, wenn er keinen (form)wirksamen Auftragsdatenverarbeitungsvertrag mit dem Auftraggeber abgeschlossen hat [Eckh13, S. 586 f.] [Plat13, Rn 40]. Der Auftragnehmer könne daher auf Schadensersatz haften [Plat13, Rn 40]. Weitere Konsequenz wäre aber auch, dass es sich um eine mit bis zu 300.000 Euro Bußgeld, ggf. bis zu zwei Jahren Haft, bedrohte unrechtmäßige Datenverarbeitung handeln würde (§§ 43 Abs. 2, 44 BDSG).

2.2 Inhaltliche Anforderungen an den Vertrag

Während die Datenschutz-Richtlinie in Art. 17 Abs. 1 noch relativ allgemein festhält, dass „der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind“ und diese Pflichten nach Art. 17 Abs. 3 zum Bestandteil des Auftrags gemacht werden müssen, stellt das nationale Recht präzisere Anforderungen an den Inhalt des Auftragsdatenverarbeitungsvertrags. Das österreichische Recht enthält in § 11 Abs. 1 DSG eine Reihe von Pflichten des Dienstleisters, deren genauere Ausgestaltung nach § 11 Abs. 2 DSG vertraglich zu regeln ist. Eine noch umfassendere, zudem nicht einmal abschließende Liste enthält § 11 Abs. 2 Satz 2 BDSG. Auch die Artikel-29-Datenschutzgruppe der europäischen Datenschutz-Aufsichtsbehörden hat eine Anforderungsliste aufgestellt [Arti12, S. 16 f.].

Der größte Teil der verpflichtenden Mindest-Inhalte des abzuschließenden Vertrags bereitet keine Schwierigkeiten; hier kann oft auf ohnehin vorhandene Unterlagen wie das Verfahrensverzeichnis oder jedenfalls Musterformulierungen zurückgegriffen werden. In der Vertragspraxis wesentlich problematischer ist die Festlegung der Sicherheitsmaßnahmen („technisch-organisatorische Maßnahmen“), die der Auftragnehmer einhalten muss [Holl14, S. 117].

---

[11] § 11 Abs. 2 öst. DSG; Art. 17 Abs. 4 DS-RL gestattet dagegen auch eine andere Form der Dokumentation, so dass angesichts des Vollharmonisierungsansatzes der DS-RL (dazu EuGH, Urt. v. 24.11.2011 – C-468/10, C-469/10) die Rechtmäßigkeit der deutschen und österreichischen Regelungen zweifelhaft ist; vgl. auch [EcKr14, S. 151].

[12] BT-Drs. 16/12011, S. 35.

2.2.1 Sicherheitsanforderungen

Die erforderlichen Sicherheitsmaßnahmen müssen nach deutschem Recht „im Einzelnen" im Vertrag festgelegt werden. Es genügt daher nicht, einfach die „acht Gebote" aus der Anlage zu § 9 BDSG[13] abzuschreiben [Gabe13c, Rn 52] [Petr11, Rn 65]. Zwar müssen die Regelungen nicht bis ins letzte Detail gehen [Gabe13c, Rn 52] [Gosc10, S. 74], doch es sind zumindest konkrete Maßnahmen zu vereinbaren, deren Vorhandensein sich überprüfen lässt.

Welche Sicherheitsmaßnahmen der Auftragnehmer (mindestens) erfüllen muss, hängt davon ab, welche Sicherheitsmaßnahmen der Auftraggeber erfüllen müsste, würde er die Daten selbst verarbeiten [Berg12a, S. 45] [Petr11, Rn 58]. Denn der reine Umstand, dass die Datenverarbeitung ausgelagert wird, soll nach der gesetzlichen Konzeption das Sicherheitsniveau der Verarbeitung nicht verringern [Gabe13c, Rn 1] [Plat13, Rn 4].

In der Praxis ist zu beobachten, dass sich viele Auftraggeber bisher überhaupt keine Gedanken gemacht haben, welches Sicherheitsniveau bei ihnen erforderlich ist. Diese Frage lässt sich nur mit einer Abwägung im Einzelfall (§ 9 Satz 2 BDSG[14]) beantworten, wobei wesentlich die Frage ist, wie schutzbedürftig die konkret betroffenen Daten sind [Berg12a, S. 45] [Schu13, Rn 22]. Für den Auftragsdatenverarbeitungsvertrag kommt es zwar nur darauf an, ob das beim Auftragnehmer gegebene Sicherheitsniveau ausreicht; eine Prüfung der internen Sicherheitsstandards kann aber sinnvollerweise damit verbunden werden.

Da nach § 11 Abs. 1 Satz 1 BDSG bereits bei der Auswahl des Auftragnehmers die dortigen Sicherheitsmaßnahmen besonders zu berücksichtigen sind, kann ggf. auf im Auswahlprozess vorgelegte Darstellungen der Sicherheitsmaßnahmen, Sicherheitskonzepte und Zertifizierungen zurückgegriffen werden, die zum Vertragsbestandteil gemacht werden können [Berg13, S. 797 f.]. In der Praxis hat es sich auch bewährt, dem Auftragnehmer eine Liste möglicher Sicherheitsmaßnahmen bereitzustellen, in der er nur noch ankreuzen muss (und ggf. ergänzen kann), was er umsetzt [Berg13, S. 798]. Genügen die vorhandenen Sicherheitsmaßnahmen nicht den Anforderungen, müssen zusätzliche Maßnahmen im Vertrag vereinbart werden [Berg13, S. 798] [MöHe14, Rn 42]. Für verschiedene Anwendungsfälle gibt es mit den technischen Richtlinien des BSI[15] bzw. Schutzprofilen[16] Anforderungskataloge, die wegen ihres Umfangs und Detailgrads typischerweise jedoch nur bei höherem Sicherheitsbedarf Anwendung finden dürften.

Bei allen technischen Sicherheitsmaßnahmen darf allerdings auch der Aspekt der Vertrauenswürdigkeit des Auftragnehmers nicht außer Acht gelassen werden. Wenn nicht sichergestellt ist, dass der Provider seine vertraglichen Vertraulichkeitsverpflichtungen auch tatsächlich erfüllt, kommt er als Auftragnehmer nicht in Betracht. In diesem Zusammenhang können sich Probleme ergeben, wenn US-Unternehmen oder deren Töchter in der EU Daten verarbeiten, weil US-Behörden nach US-Recht die Herausgabe verlangen können, auch wenn dies nach EU-Recht unzulässig ist [Whit11] [Beie14]; vgl. auch die verklausulierte Fußnote 18 in [Konf12].

---

[13] Vgl. mit vergleichbarem Detailgrad Art. 9 schweiz. VDSG.

[14] § 14 Abs. 1 Satz 2 öst. DSG; Art. 17 Abs. 1 DS-RL; vgl. § 8 f. schweiz. DSG.

[15] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/index_htm.html.

[16] Vgl. https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/SchutzprofileProtectionProfiles/SchutzprofileProtectionProfiles_Aktuell/schutzprofile_pps_aktuell_node.html, http://www.commoncriteriaportal.org/pps/, http://www.sogisportal.eu/uk/pp_en.html.

2.2.2 Vereinfachung durch Standard-Verträge

Im Massengeschäft sind individuelle ausgehandelte Sicherheitsstandards und Verträge allerdings nicht denkbar, da dadurch jeder Kostenvorteil verloren ginge und kleinere Unternehmen faktisch auf Website, E-Mail und Ähnliches verzichten müssten. Doch haben viele Daten, deren Verarbeitung ausgelagert wird, vergleichbare Sicherheitsanforderungen. Der Auftragnehmer kann daher die Initiative ergreifen, ein Standard-Sicherheitsniveau definieren und seinen Kunden ein entsprechendes Vertragsmuster anbieten [Berg13, S. 799]. Für höhere Sicherheitsanforderungen ist ein Premium-Produkt denkbar. Um den Kunden die Arbeit zu vereinfachen, sollte der Anbieter klarstellen, für welchen Schutzbedarf das Angebot aus seiner Ansicht geeignet ist.

Für Provider ergeben sich aus einem solchen standardisierten Vorgehen verschiedene Vorteile:

- Provider können sich als datenschutzkonforme Anbieter profilieren.
- Kurze Zusatzinformationen zum rechtlichen Hintergrund sowohl der ggf. angebotenen unterschiedlichen Sicherheitsniveaus als auch des angebotenen Auftragsdatenverarbeitungsvertrags können das oftmals fehlende Bewusstsein für die Erforderlichkeit schärfen.
- Sind sich die Kunden der rechtlichen Notwendigkeiten bewusst, scheiden alle Konkurrenten aus, die keine ordnungsgemäßen Verträge anbieten.
- Machen sich Kunden Gedanken über die Risiken, die ihren Daten drohen, scheiden Konkurrenten aus, die kein angemessenes Sicherheitsniveau bieten – oder dies jedenfalls nicht kommunizieren und garantieren. Diverse öffentlich gewordene Fälle des Abhandenkommens von Kundendaten haben vielen Unternehmen verdeutlicht, dass schlechte IT ihren Ruf gefährden kann.
- Der Provider muss nur seine selbst definierten Sicherheitsanforderungen einhalten, nicht auch verschiedenste Sonderwünsche einzelner Kunden berücksichtigen.
- Provider können den Vertrag zu ihren Gunsten gestalten und so eine Vielzahl rechtlicher und wirtschaftlicher Probleme vermeiden. Ein individuell ausgehandelter Vertrag wird immer für den Provider ungünstiger sein als sein Standard-Vertrag. Stammt der Vertragsentwurf gar vom Kunden, wird dieser ihn nach seinen Bedürfnissen gestalten; dieser Nachteil kann in der Praxis auch nicht mehr „herausverhandelt“ werden. In jedem Fall ist allerdings zu beachten, dass die Regeln nicht zu einseitig sein dürfen – denn Ziel ist es, dem Kunden die Erfüllung seiner gesetzlichen Verpflichtungen zu ermöglichen, so dass ein Mindestmaß an Kundenrechten gewahrt bleiben muss. Vertragsstrafen und ähnliche in einem Auftragsdatenverarbeitungsvertrag eigentlich dringend empfehlenswerte, für den Auftragnehmer jedoch sehr unangenehme Regelungen lassen sich in einem vom Provider gestellten Vertrag dagegen problemlos ausschließen.

Den Vertrag kann der Provider entweder dem Kunden zu Download, Ausdruck und Unterschrift bereitstellen – dabei ergibt sich das Risiko von Manipulationen des Textes – oder aber dem Kunden bereits einseitig unterschrieben zusenden.

2.2.3 Kontrollrechte und Umsetzung

Sicherheitsmaßnahmen müssen allerdings nicht nur vereinbart werden. Zudem muss der Auftraggeber vor Beginn der Verarbeitung und dann regelmäßig kontrollieren, ob diese Sicherheitsmaßnahmen tatsächlich umgesetzt werden (§ 11 Abs. 2 Satz 4 BDSG[17]) und das Ergebnis dokumentieren (§ 11 Abs. 2 Satz 5 BDSG). Das Unterlassen der Erstkontrolle ist bußgeldbedroht. Zudem liegt es im ureigensten Interesse des Auftraggebers, dass der Auftragnehmer ordnungsgemäß mit den Daten umgeht, da der Auftraggeber voll in der Haftung bleibt.

Bereits ein einzelner Kunde, der tatsächlich überprüfen will, ob die vereinbarten Sicherheitsmaßnahmen tatsächlich eingehalten werden, kann den Geschäftsbetrieb erheblich stören. Im Massenverkehr scheiden individuelle Prüfungen daher aus [Berg13, S. 799] [Borg14, S. 166]. Zudem verfügen viele Auftraggeber überhaupt nicht über die Fachkompetenz, ihren Auftragnehmer tatsächlich zu kontrollieren.

Wie sich aus den Materialien des Gesetzgebungsprozesses ergibt, hat der Gesetzgeber eine Vor-Ort-Kontrolle aber auch bewusst nicht vorgeschrieben.[18] Danach kann der Auftraggeber auch ein Testat eines Sachverständigen einholen, oder es kann im Einzelfall eine schriftliche Auskunft des Auftragnehmers genügen. Richtigerweise kann – über die Gesetzesbegründung hinaus – aber auch der Provider einen vertrauenswürdigen und sachkundigen Dritten mit der Überprüfung seiner Sicherheitsmaßnahmen beauftragen [Berg12a, S. 46] [Berg13, S. 796] [EcKr14, S. 152] [MöHe14, Rn 48b].

Während die Aufsichtsbehörden früher stets ein Recht des Auftraggebers verlangten, selbst vor Ort prüfen zu dürfen [Berg13, S. 800] [Euro10, S. 13], ist diese mit dem Wortlaut des Gesetzes nicht zu vereinbarende Anforderung zwischenzeitlich von vielen Landesdatenschutzbeauftragten aufgegeben worden. Das prominenteste Beispiel dürfte hier Google Analytics sein: Die Kontrolle von Google ist ausschließlich durch einen im Auftrag von Google erstellten Bericht eines Wirtschaftsprüfers vorgesehen, das Verfahren ist im Grundsatz mit dem Hamburgischen Datenschutzbeauftragten abgestimmt, vgl. [Hamb13] [Goog13, Anlage 1 Nr. 5]. Bereits im Auftragsdatenverarbeitungsvertrag müssen daher Regelungen zum Ersatz der Kontrolle des Auftraggebers durch Zertifizierungen durch unabhängige Dritte getroffen werden, einschließlich der Verpflichtung des Auftragnehmers, solche zu beauftragen und in den erforderlichen Abständen zu erneuern.

Die Kontrolle durch den Auftraggeber muss allerdings beim Ausweichen auf Testate Dritter genau so umfassend sein wie wenn der Auftraggeber die Kontrollen selbst vorgenommen hätte [Berg13, S. 800]. Im Massenverkehr sollte bereits im Vertrag ein klares Anforderungsprofil an die Qualifikation und Unabhängigkeit des Dritten aufgestellt werden, denn schließlich sollen alle anderen Kontrollrechte des Kunden ausgeschlossen werden. Der Dritte muss sachkundig und unabhängig sein; in Betracht kommen beispielsweise vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierte Sachverständige [Berg13, S. 800], Liste unter [BSI-Aud]. Problematisch ist, dass eine vollständige Zertifizierung etwa nach ISO 27001 bzw. IT-Grundschutz [BSIITG] aufwendig und nicht billig ist. Der Auditor muss dafür Dokumente sichten, eine Vor-Ort-Prüfung durchführen und ein Auditbericht erstellen, hinzu kommt eine Prüfung des Berichts durch die Zertifizierungsstelle im BSI. Einen Kompromiss, ggf. nur für weniger schutzbedürftige Daten oder weniger sensible Kunden, kann hier unter Umständen eine

[17] Ähnlich § 10 Abs. 1 Satz 2 öst. DSG; Art. 10a Abs. 2 schweiz. DSG; Art. 17 Abs. 2 DS-RL.

[18] BT-Drs. 16/13657, S. 18.

thematisch beschränkte Prüfung, ggf. auch durch andere Personen wie einen IT-kundigen Rechtsanwalt, darstellen.

Zudem muss der Provider eine umfassende Zertifizierung in Auftrag geben, anhand derer sich für jede einzelne vereinbarte Sicherheitsmaßnahme ergibt, ob diese umgesetzt ist oder nicht [Berg12a, S. 46] [GoKK12, Rn 21]. Insoweit ist der praktische Nutzen mancher Zertifikate jedoch stark limitiert [RaRo13, S. 628]. Aus praktischen Gründen sollten Vertrag und Testat des Dritten – zumindest im Rahmen einer Zusammenfassung mit Verweis auf die Ausführungen im Einzelnen – in der Darstellung gleich aufgebaut sein. Bietet der Provider auch noch eine entsprechende Checkliste an, kann der Kunde die einzelnen Sicherheitsmaßnahmen nacheinander prüfen und abhaken und damit auch seiner Pflicht zur Dokumentation der Kontrolle nachkommen, da ein Ergebnisprotokoll genügt [Gabe13c, Rn 39].

Hat der Provider seinen Sicherheitsstandard unabhängig zertifizieren lassen, ist dies zudem ein weiteres Argument im Wettbewerb gegenüber nicht oder nur selbst zertifizierten, möglicherweise außereuropäischen Anbietern [KüBi14, S. 152].

2.2.4 Weitere Regelungsgegenstände

Nicht alle wichtigen Inhalte eines Auftragsdatenverarbeitungsvertrags lassen sich § 11 Abs. 2 Satz 2 BDSG entnehmen. Sinnvoll sind auch Regelungen zu den folgenden Aspekten – je nachdem, ob der Vertrag aus Auftraggeber- oder Auftragnehmersicht entworfen wird, können sie aber auch weggelassen werden, um sich einen rechtlichen Vorteil zu verschaffen:

- Welche Sicherheitsmaßnahmen erforderlich sind, kann sich im Laufe der Zeit aufgrund technologischer wie politischer Entwicklungen ändern. Längerfristige Verträge sollten daher Regelungen darüber enthalten, dass die zu treffenden technisch-organisatorischen Maßnahmen ggf. anzupassen sind, um den erforderlichen Sicherheitsstandard zu halten, und wie ggf. anfallende Zusatzkosten von den Parteien zu tragen sind [Berg13, S. 798] [EcKr14, S. 149]
- Wird der Kontrollbericht des Zertifizierers erst nach Vertragsschluss bereitgestellt, sollte der Vertrag ein Rücktrittsrecht für den Fall vorsehen, dass der Kontrollbericht nicht behebbare Mängel feststellt werden [Berg12, S. 46], ähnlich [Petr11, Rn 57]. Ein Kontrollbericht, der den gesetzlichen Anforderungen entspricht, kann allerdings auch werbewirksam sein, wenn er vorab bereitgestellt wird; in diesem Fall wäre die Klausel unnötig.
- Bei einem eventuellen Einsatz von Subunternehmern muss sichergestellt sein, dass der Auftraggeber auch diese auf die Einhaltung der Sicherheitsmaßnahmen kontrollieren kann [Berg13, S. 798]. Der Auftraggeber muss also die Subunternehmer und die Orte der Datenverarbeitung kennen und für alle Subunternehmer, die mit seinen Daten in Kontakt kommen könnten, die Zertifizierung überprüfen. Zu beachten ist, dass Unterauftragsverhältnisse auch bei der Wartung von EDV-Anlagen nach § 11 Abs. 5 BDSG vorliegen, sobald nicht sicher ausgeschlossen werden kann, dass der Wartungsunternehmer mit personenbezogenen Daten in Kontakt kommt [MöHe14, Rn 43a] – ein Risiko, das fast immer besteht. Aus Sicht des Auftragnehmers müssen unbedingt Regelungen über den Einsatz von Subunternehmern getroffen werden, wenn diese erfolgen sollen. Denn ohne vertragliche Regelung darf der Auftragnehmer keine Unteraufträge erteilen [Gabe13c, Rn 47].

- Der Auftraggeber bleibt bei der Auftragsdatenverarbeitung für alle Datenverarbeitungen verantwortlich (§ 11 Abs. 1 BDSG[19]). Auch wenn der Auftragnehmer seine Einhaltung der Sicherheitsmaßnahmen hat zertifizieren lassen, haftet der Auftraggeber dem Betroffenen für jegliches Verschulden des Auftragnehmers. Dabei greift für den Betroffenen sogar die Beweislastumkehr des § 7 BDSG. Damit der Auftraggeber beim Auftragnehmer Regress nehmen kann, ist eine Beweislastumkehr auch im Auftragsdatenverarbeitungsvertrag sinnvoll [Berg13, S. 798] [MöHe14, Rn 21, 45]. Zur Erzielung einer besseren Compliance ebenfalls hilfreich sind Vertragsstrafen bei Datenschutzverstößen [MöHe14, Rn 46].
- Umgekehrt wäre aus Sicht des Auftragnehmers eine Haftungsbegrenzung sinnvoll. Im Massenverkehr besonders zu beachten ist hier das strenge AGB-Recht.
- Ein Zurückbehaltungsrecht des Auftragnehmers – und, falls eingesetzt, aller Subunternehmer – an personenbezogenen Daten muss aus Sicht des Auftraggebers unbedingt ausgeschlossen werden [Berg13, S. 798]. Anderenfalls kann der Auftraggeber seinen gesetzlichen Pflichten (z. B. Auskunft, Löschung, Berichtigung) ggf. nicht nachkommen, wenn er nicht zunächst alle – ggf. unbegründeten – Forderungen des Anbieters erfüllt.
- Der Auftragnehmer sollte sich verpflichten, bei „Datenpannen“ (§ 42a BDSG[20]) den Auftraggeber bei der Information der Aufsichtsbehörde und der Betroffenen zu unterstützen, und zwar über die Mindestanforderungen des § 11 Abs. 2 Satz 2 Nr. 8 BDSG hinaus [GoKK12, Rn 18g] [Petr11, Rn 80]. Ebenso sollte nicht nur eine Informationspflicht über sicher festgestellte schwerwiegende Datenverluste i. S. d. § 42a BDSG vereinbart werden, sondern auch über nur mögliche, und zwar unabhängig von ihrer Schwere [Berg13, S. 798] [Plat13, Rn 109].
- Bei Problemen während des Vertrages ergibt sich regelmäßig die Frage, ob ein bestimmter Verstoß des Auftragnehmers bereits einen wichtigen Grund im Sinne des § 314 BGB für eine außerordentliche Kündigung darstellt und ob eine Abmahnung entbehrlich ist. Klare Regelungen im Vertrag schaffen angesichts des offenen Wortlauts der §§ 314 Abs. 1 Satz 2 und 323 Abs. 2 Nr. 3 BGB für beide Parteien Rechtssicherheit [Berg13, S. 798].
- Nach dem rechtlichen Ende des Vertrags dürfen die Pflichten des Auftragnehmers nicht sofort entfallen, sondern sie müssen so lange fortbestehen, bis die Datenverarbeitung tatsächlich beendet ist [Eckh13, S. 588]. In diesem Zusammenhang sollte vorab festgelegt werden, wann die Daten zu löschen sind, aus Sicht des Providers notfalls als fingierte Zustimmung des Auftraggebers [Berg12b]. Aus Sicht des Auftraggebers sollte Kostenfreiheit jedenfalls der Löschung ausdrücklich vereinbart werden [Eckh13, S. 588], während der Provider darauf achten sollte, ausdrücklich eine Vergütungspflicht für die mangels Weisung zur Löschung fortgesetzte Speicherung der Daten zu vereinbaren.
- Weil die Privilegierung der Auftragsdatenverarbeitung nur dann gilt, wenn die Daten niemals das EU-/EWR-Gebiet verlassen, muss der Vertrag zumindest ganz grundlegende Regeln („nur innerhalb EU/EWR“) über den Ort der Verarbeitung enthalten. Sobald die Daten etwa in die USA fließen, handelt es sich nicht mehr um Auftragsdatenverarbeitung, sondern um Übermittlung, und zwar um eine Übermittlung in einen Drittstaat, für die eine

[19] § 6 Abs. 2 öst. DSG; vgl. Art. 12 lit. a, 23 Abs. 1 DS-RL und Art. 8 Abs. 4 schweiz. DSG.

[20] § 24 Abs. 2a öst. DSG.

besondere Zulässigkeitsprüfung und ein besonderer Vertrag erforderlich sind (dazu sogleich unter 3).

- Die Artikel-29-Datenschutzgruppe der europäischen Datenschutz-Aufsichtsbehörden hält insgesamt 14 Regelungsbereiche für unabdingbar in einem Auftragsdatenverarbeitungsvertrag [Arti12, S. 16 f.]; hierzu [ScHa12]. Dazu gehören über die genannten Aspekte hinaus insbesondere auch die Verpflichtung des Providers, Zugriffswünsche von Behörden auf die im Auftrag verarbeiteten Daten mitzuteilen, das Vorhalten von Logfiles und deren Auswertung sowie eine generelle Zusicherung des Anbieters, dass seine interne Organisation und seine Maßnahmen zur Datenverarbeitung (und ggf. die seiner Subunternehmer) die nationalen und internationalen Standards einhalten.

3 Auftragnehmer außerhalb EU/EWR

Auftragsdatenverarbeitung im engeren Sinne des EU-Rechts liegt nur dann vor, wenn die Verarbeitung ausschließlich in der EU bzw. dem EWR stattfindet (§ 3 Abs. 8 Satz 3 BDSG; § 12 Abs. 1 Satz 1 Fall 2 öst. DSG). Sollen die Daten dagegen in einem Drittstaat verarbeitet werden, liegt eine Übermittlung vor, die einer gesonderten Rechtsgrundlage bedarf [Gabe13c, Rn 25].

Die Rechtsgrundlage ist dabei zweistufig zu prüfen: Da eine Übermittlung und keine Auftragsdatenverarbeitung vorliegt, muss auf der ersten Stufe die Übermittlung an einen Dritten überhaupt zulässig sein. Als Rechtsgrundlage hierfür kommen je nach Einzelfall die gesetzlichen Erlaubnistatbestände insbesondere der §§ 28, 29 und 32 BDSG in Betracht. Die Übermittlung ist dabei zulässig, wenn eine Interessenabwägung – deren Maßstab je nach Norm unterschiedlich ist – zu Gunsten der Übermittlung ausgeht. Typischerweise überwiegen aber zunächst einmal die Interessen des Betroffenen, dass seine Daten nicht an jedermann weitergegeben werden dürfen. Schließt der Auftraggeber allerdings einen Vertrag, der inhaltlich die Anforderungen an eine Auftragsdatenverarbeitung erfüllt, kann dies dazu führen, dass die Datenübermittlung zulässig wird, weil nunmehr die Interessen des Auftraggebers die Interessen des Betroffenen überwiegen [Konf11, S. 11].

Zu berücksichtigen ist allerdings, dass sensible Daten nach § 3 Abs. 9 BDSG, also etwa über politische Ansichten, Religion oder Gesundheit, in der Praxis nicht übermittelt werden dürfen. Sie dürfen daher auch nicht in einem Drittstaaten-Cloud-Service gespeichert werden [Konf11, S. 11].

Ist die erste Stufe der Prüfung – also die grundsätzliche Erlaubnis zur Übermittlung der Daten – genommen, müssen auf zweiter Stufe die Anforderungen der §§ 4b, 4c BDSG für eine Übermittlung ins Ausland erfüllt werden. Hierfür gibt es mehrere Möglichkeiten. Es kann sich zunächst um einen „sicheren“ Drittstaat handeln; aufgrund des Haftungsrisikos kommen dabei faktisch nur die Staaten in Betracht, die die EU-Kommission als „sicher“ anerkannt hat, vgl. die Liste in [Gabe13a, Rn 22]. Für andere Drittstaaten ist eine Vereinbarung der Standardvertragsklauseln für Auftragsdatenverarbeitung [Komm10] [Simi11b, Rn 47 ff.] meist die sinnvollste Lösung. Aufgrund der nach den Enthüllungen von Edward Snowden aufgekommenen Widerstände der Aufsichtsbehörden gegen Datenübermittlungen insbesondere in die USA [Konf13] und der grundsätzlichen [Simi11a, Rn 78] wie konkreten [KüBi14, S. 153 f.] Bedenken gegen „Safe Harbor“ sollten Übermittlungen auf der Basis der „Safe-Harbor“-Regeln (dazu [Gabe13a, Rn 23 f.] [Simi11a, Rn 70 ff.]), verbindlichen Unternehmensregelungen (dazu [Gabe13b, Rn 28 ff.]) und Genehmigungen im Einzelfall (dazu [Gabe13b, Rn 15 ff.]) nur im wohl überlegten Ausnahmefall erfolgen. Wichtig ist dabei, dass die Standardvertragsklauseln

unverändert vereinbart werden müssen; anderenfalls ist eine Genehmigung im Einzelfall durch die Aufsichtsbehörde erforderlich [Gabe13b, Rn 22]. Zulässig sind nur formale Anpassungen und Ergänzungen des Standardvertrages, soweit die Ergänzungen nicht zu diesem im Widerspruch stehen.

Erfolgt eine Übermittlung in Drittstaaten erst auf der Subunternehmer-Ebene, müssen die Standardvertragsklauseln Auftragsdatenverarbeitung unter Durchbrechung der Leistungskette unmittelbar zwischen dem Auftraggeber und Drittstaaten-Subunternehmer vereinbart werden [Arti10, S. 4].

Bei jeder Nutzung eines Drittstaaten-Auftragnehmers – und sei es erst auf der Subunternehmer-Ebene – ist zu beachten, dass diese Übermittlung dem Betroffenen nicht verheimlicht werden darf. Einerseits umfasst der Auskunftsanspruch nach § 34 Abs. 1 Satz 1 Nr. 2 BDSG sowohl Auftragsdatenverarbeiter als auch Empfänger von übermittelten Daten [MeHi13, Rn 20]. Andererseits muss eine geplante Datenübermittlung in Drittstaaten auch ins Verfahrensverzeichnis (§ 4e Satz 1 Nr. 8 BDSG) aufgenommen werden.

4 Fazit

Mit dem beschriebenen Vorgehen lässt sich Auftragsdatenverarbeitung auch im Massengeschäft gesetzeskonform umsetzen, ohne übermäßigen Aufwand treiben zu müssen, der die Vorteile des Outsourcings sonst schnell übersteigen würde. Da die Aufsichtsbehörden bei Kontrollen standardmäßig auch die Auftragsdatenverarbeitungsverträge prüfen, sollte jedes Unternehmen seinen Provider entsprechend in die Pflicht nehmen. Für die Provider kann sich daraus ein Werbeargument ergeben, solange die Konkurrenz Datenschutz erst dann bedenkt, wenn der Verlust der Kundendatenbank in der Zeitung gemeldet wird.

Literatur

[Arti10] Artikel-29-Datenschutzgruppe: Häufig gestellte Fragen zu bestimmten Aspekten im Zusammenhang mit dem Inkrafttreten des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG, WP 176 (2010).

[Arti12] Artikel-29-Datenschutzgruppe: Stellungnahme 05/2012 zum Cloud Computing, WP 196 (2012).

[Beie14] S. Beiersmann: Urteil: US-Durchsuchungsbefehle gelten auch für in Europa gespeicherte Cloud-Daten, ZDNet, http://www.zdnet.de/88191879/ (2014).

[Berg12a] M. Bergt: Datenschutzrechtliche Erstkontrolle durch vertrauenswürdige Dritte. In: Der IT-Rechts-Berater (ITRB), Otto Schmidt (2012) 45-47.

[Berg12b] M. Bergt: Unzulässige Löschung eines E-Mail-Accounts. In: Der IT-Rechts-Berater (ITRB), Otto Schmidt (2012) 56.

[Berg13] M. Bergt: Rechtskonforme Auftragsdatenverarbeitung im Massengeschäft. In: Datenschutz und Datensicherheit (DuD), Springer (2013) 796-801.

[Borg14] G. Borges: Cloud Computing und Datenschutz. In: Datenschutz und Datensicherheit (DuD), Springer (2014) 165-169.

[BSIAud] Bundesamt für Sicherheit in der Informationstechnik: Zertifizierte ISO 27001-Auditoren für Audits auf der Basis von IT-Grundschutz, https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Zertifizierung27001/Auditoren/iso27001auditoren_node.html.

[BSIITG] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Standards, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html.

[Damm11] U. Dammann: Kommentierung zu § 3 BDSG. In: S. Simitis: BDSG, Nomos (2011).

[Eckh13] J. Eckhardt: Auftragsdatenverarbeitung. In: Datenschutz und Datensicherheit (DuD), Springer (2013) 585-591.

[EcKr14] J. Eckhardt, R. Kramer: Auftragsdatenverarbeitung. In: Datenschutz und Datensicherheit (DuD), Springer (2014) 147-152.

[Euro10] EuroCloud Deutschland_eco e.V.: Leitfaden Cloud Computing – Recht, Datenschutz & Compliance (2010).

[Gabe13a] D. Gabel: Kommentierung zu § 4b BDSG. In: J. Taeger, D. Gabel, BDSG, R&W (2013).

[Gabe13b] D. Gabel: Kommentierung zu § 4c BDSG. In: J. Taeger, D. Gabel, BDSG, R&W (2013).

[Gabe13c] D. Gabel: Kommentierung zu § 11 BDSG. In: J. Taeger, D. Gabel, BDSG, R&W (2013).

[GoKK12] P. Gola, C. Klug, B. Körffler: Kommentierung zu § 11 BDSG. In: P. Gola, R. Schomerus, BDSG, Beck (2012).

[Goog13] Google: Vertrag zur Auftragsdatenverarbeitung für Google Analytics, http://www.google.com/analytics/terms/de.pdf (2013).

[Gosc10] A. Gosche: 1 Jahr Praxiserfahrung mit dem novellierten § 11 Abs. 2 BDSG. In: J. Taeger: Digitale Evolution – Herausforderungen für das Informations- und Medienrecht, OlWiR (2010) 73-87.

[Hamb13] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: Hinweise für Webseitenbetreiber mit Sitz in Hamburg, die Google Analytics einsetzen, http://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_ Hinweise_fuer_Webseitenbetreiber_in_Hamburg_01.pdf (2013).

[Holl14] C. Holländer: Auftragsdatenverarbeitung: Aus der Praxis der Aufsichtsbehörden. In: Der IT-Rechts-Berater (ITRB), Otto Schmidt (2014) 116-117.

[Komm10] Europäische Kommission: Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (2010/87/EU), ABl. L 39/5 (2010).

[Konf12] Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Orientierungshilfe – Cloud Computing, http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf (2011).

[Konf13] Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Datenschutzkonferenz: Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten, http://www.bfdi.bund.de/DE/Home/homepage_Kurzmeldungen2013/PMDerDSK_SafeHarbor.html (2013).

[KüBi14] J. Kühling, M. Biendl: Datenschutz – Basis und Bremse des Cloud Computing. In: Computer und Recht, Verlag Otto Schmidt (2014) 150-156.

[KüKl13] J. Kühling, M. Klar: Unsicherheitsfaktor Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität. In: Neue Juristische Wochenschrift (NJW), Beck (2013) 3611-3617.

[MeHi13] J. G. Meents, B. Hinzpeter: Kommentierung zu § 34 BDSG. In: J. Taeger, D. Gabel, BDSG, R&W (2013).

[MöHe14] L. Bergmann, A. Herb: Kommentierung zu § 11 BDSG. In: L. Bergmann, R. Möhrle, A. Herb: Datenschutzrecht, Boorberg (2014).

[Petr11] T. Petri: Kommentierung zu § 11 BDSG. In: S. Simitis: BDSG, Nomos (2011).

[Plat13] K.-U. Plath: Kommentierung zu § 11 BDSG. In: K.-U. Plath: BDSG, Otto Schmidt (2013).

[RaRo13] M. Rath, B. Rothe: Cloud Computing: Ein datenschutzrechtliches Update. In: Kommunikation und Recht, Deutscher Fachverlag (2013) 623-629.

[ScHa12] C. Schröder, N. C. Haag: Stellungnahme der Art. 29-Datenschutzgruppe zum Cloud Computing – Gibt es neue datenschutzrechtliche Anforderungen für Cloud Computing? In: Zeitschrift für Datenschutz (ZD), Beck (2012) 495-501.

[Schu13] J. Schultze-Melling: Kommentierung zu § 9 BDSG. In: J. Taeger, D. Gabel, BDSG, R&W (2013).

[ScWi14] H.-J. Schaffland, N. Wiltfang: BDSG, Kommentierung zu § 11 BDSG, Erich Schmidt (2014).

[Simi11a] S. Simitis: Kommentierung zu § 4b BDSG. In: S. Simitis, BDSG, Nomos (2011).

[Simi11b] S. Simitis: Kommentierung zu § 4c BDSG. In: S. Simitis, BDSG, Nomos (2011).

[Spin11] G. Spindler: Kommentierung zu § 11 BDSG. In: G. Spindler, F. Schuster: Recht der elektronischen Medien, Beck (2011).

[SpMü14] L. Specht, S. Müller-Riemenschneider: Dynamische IP-Adressen: Personenbezogene Daten für den Webseitenbetreiber? – Aktueller Stand der Diskussion um den Personenbezug. In: Zeitschrift für Datenschutz (ZD), Beck (2014) 71-75.

[Whit11] Z. Whittaker: Microsoft admits Patriot Act can access EU-based cloud data, ZDNet, http://www.zdnet.com/blog/igeneration/-/11225 (2011).