Datenschutz

Silvia C. Bauer

Transfer von Daten im Lichte der EU-DSGVO

Am 25. Mai 2018 ist es soweit: Ab diesem Datum gilt die EU-Datenschutzgrundverordnung (DSGVO) unmittelbar in allen Mitgliedstaaten der Europäischen Union (EU). Sie verdrängt die bislang bestehenden nationalen Regelungen zum Datenschutz, wie z. B. das Bundesdatenschutzgesetz. Nur in einzelnen in der DSGVO konkret benannten Bereichen, wie z. B. dem Beschäftigtendatenschutz, kann der nationale Gesetzgeber noch eigenständige Regelungen treffen. Unternehmen, die personenbezogene Daten mit anderen Unternehmen austauschen, Daten in der Cloud eines IT-Providers speichern oder schlicht ihre IT-Systeme von einem Dritten warten lassen, müssen sich künftig an der DSGVO orientieren.

Und diese bringt einige Neuerungen sowohl für diejenigen mit sich, die die Daten weitergeben, als auch für diejenigen, die die Daten erhalten. So haften künftig alle – auch Auftragsverarbeiter – bei Unregelmäßigkeiten oder fehlendem Abschluss der erforderlichen Verträge mit bis zu 20 Mio. Euro bzw. 4 % ihres weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres. Allein daher empfiehlt sich ein Blick in das Gesetz und eine interne Prüfung, ob und wie das eigene Unternehmen die Anforderungen der DSGVO umsetzt.

1 Einleitung

Im Unternehmensalltag ist es kaum vorstellbar, keine Daten mit anderen auszutauschen. Daten werden an Lieferanten weitergegeben, von Adresshändlern für Marketingzwecke eingekauft, zentrale Stellen innerhalb einer Konzerngruppe erbringen Personaldienstleistungen für alle Konzernunternehmen, die IT-Hotline ist u.a. in Indien angesiedelt oder Daten werden kostengünstig in den USA gespeichert – um nur einige Beispiele zu nennen.

Immer dann, wenn es sich dabei um personenbezogene Daten natürlicher Personen, d.h. um Daten, die sich auf eine identifizierte oder identifizierbare Person beziehen (Art. 4 Abs. 1 DSGVO), handelt, ist künftig zu prüfen, ob ein entsprechender Austausch nach den Regelungen der DSGVO auch erlaubt ist. Als „personenbezogene Daten" gelten z.B. der Name, die E-Mail-Adresse, eventuelle Hobbies, der Beruf, Standortdaten, ID-Nummern aber auch IP-Adressen, LogIn-Daten oder Cookies („Daten"). Als „besondere personenbezogene Daten", die aufgrund ihrer Sensitivität eines besonderen Schutzes bedürfen, gelten z.B. die Gesundheit, Religion, Rasse, Herkunft, die Gewerkschaftszugehörigkeit oder künftig auch genetische bzw. biometrische Daten. Die natürliche Person wird als „Betroffener" bezeichnet.

Die DSGVO sieht je nach Verhältnis bzw. Verantwortungsverteilung der Beteiligten unterschiedliche Spielregeln vor, die diese bei einem Austausch von Daten einhalten müssen. In Betracht kommt eine Legitimierung des Austauschs auf Grundlage gesetzlicher Erlaubnistatbestände oder der Einwilligung des Betroffenen. Die Weitergabe kann zudem auf Grundlage einer Auftragsverarbeitung oder als Austausch zwischen „Joint Controllern" erfolgen.

Weiterhin muss stets in einem zweiten Schritt geprüft werden, wo der Empfänger der Daten seinen Sitz hat: Erfolgt eine Weitergabe der Daten an ein Unternehmen mit Sitz in einem Land außerhalb des Europäischen Wirtschaftsraums, das über kein – nach EU-Verständnis – angemessenes Datenschutzniveau verfügt, sind (neben dem im vorherigen Absatz beschriebenen Schritt hinaus) zusätzliche Garantien zu schaffen, um diesen Transfer zu rechtfertigen.

2 Rechtsgrundlagen für den Transfer von Daten

Die Weitergabe von Daten war bereits nach den Regelungen des BDSG und ist künftig auch nach den Regelungen der DSGVO dann zulässig, wenn sie gesetzlich erlaubt ist oder eine Einwilligung des Betroffenen vorliegt.[1]

a) Gesetzliche Erlaubnis

Als gesetzliche Erlaubnis kommt z.B. Art. 6 DSGVO in Betracht, der regelt, in welchen Fällen ein „Verantwortlicher" Daten „verarbeiten" darf. Als Verantwortlicher gilt nach Art. 4 Ziff. 7 DSGVO immer die Person, das Unternehmen oder die Behörde, die *„allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von Daten entscheidet."* Der Begriff der „Verarbeitung" umfasst nach Art. 4 Ziff. 2 DSGVO auch *„das Abfragen, (...), die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung"*, d.h. im Ergebnis jede Form der Weitergabe von Daten von einer Stelle an eine andere.

Art. 6 DSGVO erlaubt u.a. die Weitergabe von Daten

- sofern dies erforderlich ist für den Abschluss bzw. die Erfüllung von Verträgen oder vorvertraglichen Maßnahmen, Art. 6 Abs. 1 lit. b DSGVO;
- zur Erfüllung rechtlicher Verpflichtungen, Art. 6 Abs. 1 lit. c DSGVO;
- bei überwiegenden berechtigten Interessen der verantwortlichen Stelle bzw. eines Dritten im Vergleich mit den schutzwürdigen Interessen, Grundrechten oder Grundfreiheiten des Betroffenen, Art. 6 Abs. 1 lit. f DSGVO.

Unternehmen dürfen daher die Daten ihrer Kunden z.B. auf Grundlage des Art. 6 Abs. 1lit. b DSGVO an einen Lieferanten weitergeben. Dies ist regelmäßig erforderlich für die Erfüllung des Vertrages mit dem Kunden – andernfalls erhält der Kunde die Ware nicht. Zudem sind sie auf Grundlage des Art. 6 Abs. 1 lit. c DSGVO berechtigt, z.B. Daten an die Finanzbehörden zu übermitteln, sofern dies aus steuerrechtlichen Gründen erforderlich ist.

Viele Übermittlungen werden sich künftig durch Art. 6. Abs. 1 lit. f DSGVO rechtfertigen lassen: Danach dürfen Daten immer dann, wenn berechtigte Interessen des Unternehmens vorliegen, die gegenüber den schutzwürdigen Interessen des Betroffenen überwiegen, weitergegeben werden.[2] Auch wenn Interessenabwägungen stets subjektiv sind, je nach Position die unterschiedlichsten Interpretationen zulassen und daher zu einer gewissen Rechtsunsicherheit führen, ver-

1 Siehe u.a. zum Austausch von Daten nach heutiger Rechtslage: Kinast/Lellou, PraxRev 1/2017, S. 43 ff.

2 Siehe dazu auch: Bauer, PraxRev 2016, S. 159 ff., Albrecht, CR 2016, S. 88 ff.

birgt sich hier insbesondere für Konzerngruppen auch eine Chance: Auf Abs. 1 lit. f wird das sogenannte „kleine Konzernprivileg" gestützt.[3]

b) Das „kleine Konzernprivileg"

Auch Konzerngruppen müssen den Austausch von Daten zwischen ihren verschiedenen Konzernunternehmen rechtfertigen bzw. Einwilligungen der Betroffenen einholen. Der Gesetzgeber hat – obwohl die Konzernunternehmen häufig gemeinsame Interessen verfolgen, viele zentrale Services nutzen (z. B. eine zentrale IT- oder Personalabteilung), Berichtslinien zwischen den Unternehmen bestehen, Vorgesetzte von Mitarbeitern in anderen Konzernunternehmen sitzen und alle regelmäßig einem einheitlichen Regime unterliegen – keinen diesbezüglichen Regelungsbedarf gesehen und von konkreten Erleichterungen für den Austausch von Daten zwischen Konzernunternehmen abgesehen.[4]

Stattdessen hat er einen indirekten Weg gewählt, indem er in den Erwägungsgründen zu Art. 6 Abs. 1 lit. f DSGVO eine Art kleines Konzernprivileg für „Unternehmensgruppen" vorgesehen hat.[5] Zwar entfaltet ein Erwägungsgrund – im Gegensatz zu einer Norm – keine direkte gesetzliche Wirkung. Er gilt jedoch als eine Art Präambel bzw. wird als Begründung dem Gesetzestext vorangestellt.

Laut Art. 4 Ziff. 19 DSGVO ist eine Unternehmensgruppe *„eine Gruppe, die aus einem herrschenden und den von diesen abhängigen Unternehmen"* besteht. Für diese sieht Erwägungsgrund 48 DSGVO, der sich auf Art. 6 Abs. 1 lit. f DSGVO bezieht, folgendes vor:

> *„Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt."*

Im Ergebnis erkennt der Gesetzgeber an, dass insbesondere interne Verwaltungszwecke als berechtigte Interessen, die den Austausch von Daten rechtfertigen können, gelten. Voraussetzung bleibt gleichwohl eine Abwägung der eigenen Interessen mit den ggf. entgegenstehenden schutzwürdigen Interessen der Betroffenen, eine Information der Betroffenen über diese berechtigen Interessen nach Art. 12 ff. DSGVO und idealerweise eine Dokumentation der Interessen.[6]

In diesem Zusammenhang wird allerdings abzuwarten sein, ob sich durch die nationalen Anpassungen im Bereich des Beschäftigtendatenschutzrechts ggf. für die Übermittlung von Beschäftigtendaten Einschränkungen ergeben. Der Gesetzgeber hat u. a. für diesen Bereich das sogenannte Datenschutzanpassungs- und Umsetzungsgesetz EU („DSAnpUG-EU")[7] umgesetzt, mit dem er dort, wo es die DSGVO zulässt, nationale Regelungen einführt. Das Gesetz wird wie die DSGVO ab Mai 2018 Anwendung finden.[8]

c) Weitere Erlaubnistatbestände

Daneben gelten u. a. Sondervorschriften für die Weitergabe von besonderen personenbezogenen Daten, wie z. B. Gesundheit, Religion oder Rasse, Art. 9 DSGVO[9] oder von Daten betreffend strafrechtliche Verurteilungen und Straftaten, Art. 10 DSGVO. Besondere personenbezogene Daten dürfen z. B. nur mit Einwilligung des Betroffenen oder damit der Verantwortliche bzw. der Betroffene seine Rechte basierend auf Arbeitsrecht oder Sozialschutz ausüben kann, verarbeitet werden.[10]

d) Einwilligung

Der Transfer von Daten kann auch durch eine Einwilligung gerechtfertigt werden, Art. 4 Ziff. 11, Art. 6 Abs. 1 lit. a DSGVO. Die Voraussetzungen sind in Art. 7 DSGVO definiert.[11] Sie muss jedenfalls freiwillig erteilt werden und kann jederzeit von dem Betroffenen widerrufen werden. Zudem ist sie zu dokumentieren.

Zur Legitimierung der Weitergabe von Daten ist die Einwilligung nur bedingt geeignet, da bereits die

3 Vgl. Lachenmann, DSRITB 2016, S. 535, 542; Plath in Plath, BDSG/DSGVO Kommentar, 2. Aufl. 2016, Art. 6 DSGVO, Rn. 22

4 Siehe Pauly in Paal/Pauly, Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 47 DSGVO, Rn. 1

5 Siehe dazu auch: Bauer, Datenschutzpraxis 8/2016, S. 18; Piltz, K&R 2016, S. 557, 565; Plath, in Plath, a.a.O., Art. 6 DSGVO, Rn. 22.

6 Siehe dazu Bauer, PRev, 2016, S. 159, 161; Piltz, K&R 2016, S. 629 ff.

7 „Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)".

8 Siehe Bundesratsdrucksache 332/17. Siehe ausführlich zu den Auswirkungen der DSGVO auf den Beschäftigtendatenschutz: Sörup/Marquardt, ArbR Aktuell 2016, 103 ff.

9 Vgl. Schmid/Kahl ausführlich zum Austausch besonderer personenbezogener Daten mit Cloud-Providern, ZD 2017, S. 54 ff.

10 Hier bleibt abzuwarten, ob sich aufgrund des DSAnpUG insbesondere im Beschäftigtendatenschutzrecht auf nationaler Ebene Anpassungen ergeben. Siehe dazu bereits oben, Ziff. 2 b).

11 Siehe dazu ausführlich, Bauer, PraxRev 2016, S. 159, 164

präzise Formulierung der konkreten Zwecke des Umgangs mit den Daten einige Schwierigkeiten bereiten wird. Zudem sind die Konsequenzen für den Fall des Widerrufs zu bedenken: Der Widerruf führt zunächst dazu, dass der Verantwortliche künftig keine Daten mehr weitergeben darf. Letztlich wird aber auch infrage stehen, ob der Empfänger die bereits übermittelten Daten löschen muss oder diese weiterhin verarbeiten darf. Häufig wird der Widerruf der Einwilligung z. B. damit begründet, dass die Daten schlicht nicht mehr in den USA verarbeitet werden sollen. Dann ist nicht nur die Weitergabe, sondern die ganze Verarbeitung umfasst und es müsste eine Löschung der Daten durch den Empfänger erfolgen. Dies umzusetzen, wird in der Praxis eher schwierig. Ist die Einwilligung das Mittel der Wahl, empfiehlt sich daher eine sehr sorgfältige Formulierung auch unter Berücksichtigung der Konsequenzen eines Widerrufs.

3 Auftragsverarbeitung

Die bislang in § 11 BDSG geregelte Auftragsdatenverarbeitung ist künftig Teil des Kap. IV „Verantwortlicher und Auftragsverarbeiter" der DSGVO. Dort werden in den Art. 24 ff. DSGVO die Rechte und Pflichten für beide Parteien im Rahmen des Austauschs von Daten festgelegt.

a) Wer ist Auftragsverarbeiter?

Nach Art. 4 Ziff. 8 DSGVO ist Auftragsverarbeiter derjenige, der Daten im Auftrag eines anderen verarbeitet. Diese weite Definition hat zu der Diskussion geführt, ob künftig nicht jede Stelle, die eine Aufgabe für einen Verantwortlichen übernimmt, als Auftragsverarbeiter gilt. Grundsätzlich kommt es in diesem Zusammenhang nach überwiegender Meinung darauf an, ob der Auftragsverarbeiter in Bezug auf den Verantwortlichen eine rechtlich eigenständige Einheit ist und gleichwohl die Verarbeitung ausschließlich im Auftrag des Verantwortlichen erfolgt. Der Verantwortliche muss gegenüber dem Auftragsverarbeiter weisungsbefugt sein, sodass der Auftragsverarbeiter die Daten nur entsprechend dem Willen des Verantwortlichen und keinesfalls für eigene Zwecke nutzen darf. Der Verantwortliche tritt gegenüber dem Betroffenen auf und ist für die Wahrung der Rechte des Betroffenen auf Auskunft, Löschung etc. verantwortlich.[12] Typische Auftragsverarbeiter sind z. B. IT-Service-Provider, Cloud-Anbieter, Rechenzentren, aber auch abhängige Call-Center oder Entsorgungsunternehmen für Datenträger.

b) Weitergabe der Daten an den Auftragsverarbeiter

Der Auftragnehmer ist künftig Empfänger der Daten und steht damit faktisch außerhalb der verantwortlichen Stelle, Art. 4 Abs. 9 DSGVO.[13] Hier wird diskutiert, ob u. a. durch diese neue Definition die Weitergabe – im Gegensatz zu heute – nicht mehr privilegiert sei und daher eine Rechtsgrundlage, wie Art. 6 Abs. 1 lit. f DSGVO, diese Weitergabe rechtfertigen muss.[14] Letztlich kann diese Diskussion hier dahinstehen, da im Ergebnis davon auszugehen ist, dass jedenfalls die Weitergabe gerechtfertigt werden kann. Zu beachten ist daneben, dass z. B. die Informationspflichten über den Einsatz des Auftragsverarbeiters ausgeweitet werden, da u. a. über die Empfänger seitens des Auftraggebers zu informieren ist, Art. 12 ff. DSGVO.

c) Neue Pflichten für Auftraggeber

Nach Art. 28 Abs. 1 DSGVO ist der Auftraggeber – wie bisher – zu einer sorgfältigen Auswahl des Auftragsverarbeiters verpflichtet. Er muss bei seiner Auswahl insbesondere prüfen, ob der Auftragsverarbeiter hinreichende Garantien dafür bietet, dass geeignete technisch-organisatorische Maßnahmen umgesetzt werden, die die Daten angemessen schützen. Maßstäbe für die Auswahl sind u. a. das Fachwissen, die Zuverlässigkeit und die Ressourcen des Auftragsverarbeiters. Im Gegensatz zu § 11 BDSG fordert Art. 28 DSGVO nicht mehr, dass der Auftraggeber den Auftragsverarbeiter vor Beginn der Verarbeitung und sodann regelmäßig kontrollieren muss.

Allerdings muss der Auftraggeber als Verantwortlicher die in Art. 5 Abs. 2 DSGVO vorgesehenen Rechenschaftspflichten erfüllen: Danach muss er u. a. nachweisen, dass er eine sorgfältige Auswahl getroffen hat und im Vertrag die technisch-organisatorischen Maßnahmen ausreichend dokumentiert sind bzw. diese letztlich auch umgesetzt werden. Im Ergebnis trifft ihn daher gleichwohl eine Überwachungs- und Kontrollpflicht, sodass sich keine Erleichterungen ergeben.

12 Siehe dazu u. a. die Stellungnahme 1/2010 der Artikel 29-Datenschutzgruppe zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsdatenverarbeiter", WP 169, 16.2.2010, S. 30

13 Vgl. Schreiber in Plath, BDSG, a.a.O., Art. 4 DSGVO, Rn. 29

14 Siehe dazu u. a. Schmidt/Freund, ZD 2017, S. 14 ff.; Piltz, K&R 2016, S. 709, 712; Lissner, DSITRB, S. 401, 406 ff.; Schmitz/Dall'Amri, ZD, 2016, S. 427 ff.; als Alternativen werden z. B. diskutiert, die Weitergabe durch Art. 28, 29 DSGVO zu rechtfertigen oder die Verarbeitung als einen einheitlichen Vorgang anzusehen im Sinne von Art. 4 Nr. 2 DSGVO.

d) Neue Pflichten für Auftragsverarbeiter

Auftragsverarbeiter müssen künftig wesentlich mehr Pflichten erfüllen als bisher. Sie müssen z. B.

- einen „Vertreter" in der EU bestellen, wenn sie ihren Sitz außerhalb und keine Niederlassung innerhalb der EU haben, Art. 27 Abs. 1 DSGVO,
- bei Erfüllung der Voraussetzungen Verfahrensverzeichnisse führen, Art. 30 Abs. 2 DSGVO,
- mit der Aufsichtsbehörde zusammenarbeiten, Art. 31 DSGVO,
- eigenverantwortlich angemessene technisch-organisatorischen Maßnahmen der Datensicherheit umsetzen, Art. 32 Abs. 1 DSGVO,
- bei Erfüllung der Voraussetzungen einen betrieblichen Datenschutzbeauftragten bestellen, Art. 37 Abs. 1 DSGVO,
- die allgemeinen Einschränkungen bei dem Transfer von Daten in ein Drittland beachten, Art. 44 ff. DSGVO.

Die Umsetzung der nach Art. 32 DSGVO erforderlichen technisch-organisatorischen Maßnahmen kann der Auftragsverarbeiter gemäß Art. 28 Abs. 5 DSGVO durch die Einhaltung von sogenannten genehmigten Verhaltensregeln nach Art. 40 DSGVO oder im Rahmen eines genehmigten Zertifizierungsverfahrens nachweisen, Art. 42 DSGVO. Hier bleibt abzuwarten, wie dieser Nachweis in der Praxis erbracht werden kann und ob die bereits heute bestehenden Zertifizierungen ausreichen.[15]

Unternehmen, die als Auftragsverarbeiter tätig werden, müssen sich auf diese neuen Anforderungen einstellen und z. B. Prozesse zur Gestaltung der Verfahrensverzeichnisse einführen. Hier bleibt abzuwarten, ob in der Praxis ein Verfahrensverzeichnis für alle Auftragsverarbeitungen genügt oder für jeden Kunden/Auftraggeber ein separates Verzeichnis zu erstellen ist. Der Aufwand wird jedenfalls größer. Zudem ist zu erwarten, dass Auftraggeber in ihren Auftragsverarbeitungsverträgen diese Anforderungen auch entsprechend als Verpflichtungen des Auftragnehmers aufnehmen werden.

e) Erweiterte Haftung

Nach der DSGVO haftet zudem künftig auch der Auftragsverarbeiter direkt für Verstöße, Art. 82 Abs. 2 DSGVO. Da der Auftragsverarbeiter auf Weisung des Auftraggebers handelt, werden die Haftungsrisiken allerdings entsprechend verteilt. Sofern der Auftragsverarbeiter nachweisen kann, dass ihn keine Schuld trifft, haftet er nicht bzw. seine Haftung wird reduziert. Nutzt der Auftragsverarbeiter hingegen abweichend von den Vereinbarungen die Daten für eigene Zwecke, haftet er künftig als Verantwortlicher, Art. 28 Abs. 10 DSGVO („Exzeß" des Auftragsverarbeiters).

Es empfiehlt sich auf beiden Seiten eine geeignete Dokumentation der eigenen Tätigkeiten/Pflichten. Es sollten jedenfalls konkrete Bestimmungen im Vertrag z. B. für den Fall von rechtswidrigen Weisungen oder dem Umfang der Angemessenheit der technisch-organisatorischen Maßnahmen vereinbart werden. Nur so ist klar geregelt, wann ein Haftungsfall eintritt und wer haftet. Daneben werden Auftragsverarbeiter durch z. B. Freistellungsklauseln oder Haftungsbeschränkungen versuchen, ihre Haftung vertraglich zu reduzieren. Dies wird Verhandlungssache sein.

Der Auftragsverarbeiter muss unabhängig davon künftig zusätzlich eigene Pflichten aus der DSGVO erfüllen, wie z. B. die Einhaltung der angemessenen technisch-organisatorischen Maßnahmen. Hier haftet er künftig – wie auch der Auftraggeber für sein eigenes Tun – nach Art. 83 DSGVO, der bei Verstößen gegen die DSGVO Bußgelder bis zu € 20 Mio. oder 4 % des weltweiten Jahresumsatzes des letzten Geschäftsjahres vorsieht.

f) Beiderseitige Pflicht: Abschluss des Vertrags

Art. 28 Abs. 3 DSGVO verlangt den Abschluss eines Vertrages, der zwar bestimmte Inhalte aufweisen muss, aber grundsätzlich individuell verhandelt werden kann. Insofern ist es möglich, auftraggeber- und auftragnehmerfreundliche Vertragsvarianten zu entwickeln. Geplant ist zudem, dass die Europäische Kommission oder andere zuständige Stellen Musterverträge erstellen, die alternativ genutzt werden können, Art. 28 Abs. 3 DSGVO. Diese existieren allerdings noch nicht.

Der Abschluss soll künftig bereits per „Rechtsakt" möglich sein. Daher ist auch eine Vereinbarung in Allgemeinen Geschäftsbedingungen, die allein den Auftragsverarbeiter bindet, grundsätzlich ausreichend. Zudem ist künftig die elektronische Form anerkannt. Die Verträge können somit ab 2018 auch online oder per E-Mail abgeschlossen werden, Art. 28 Abs. 9 DSGVO.

g) Inhalt des Vertrags

Art. 28 Abs. 3 DSGVO regelt, welche Inhalte in dem Vertrag geregelt werden müssen.[16] Es müssen als **Mindestinhalte** u. a. Vereinbarungen über den Gegenstand

15 Siehe Hofmann, ZD-Aktuell 2016, 05324; Bergt, DSRITB 2016, S. 483

16 Siehe dazu auch Schmitz/Dall'Amri, ZD, 2016, S. 427, 431

und die Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien der Betroffenen und die Pflichten und Rechte des Verantwortlichen aufgenommen werden. Dazu kommen weitere Anforderungen, die teilweise neu sind, teilweise aber auch bereits nach § 11 BDSG erforderlich waren.

Anpassungsbedarf bereits abgeschlossener Verträge kann sich insbesondere in folgenden Bereichen ergeben, da diese im Vergleich mit § 11 BDSG abweichende Anforderungen normieren:

- **Weisungsbefugnisse**: Der Umfang der Weisungsbefugnisse ist festzulegen. Weisungen sind – dies ist neu – sowohl von dem Auftraggeber als auch von dem Auftragsverarbeiter zu dokumentieren, Art. 28, Abs. 3 lit a und 29 DSGVO. Die Dokumentation kann schriftlich oder in Textform (d.h. per E-Mail) erfolgen. Die Dokumentationspflicht gilt auch für Weisungen des Auftraggebers, die die Übermittlung von Daten in unsichere Drittländer, d.h. Länder, die kein Datenschutzniveau aufweisen, das dem der DSGVO entspricht, zum Gegenstand haben. Ohne Weisung darf der Auftragsverarbeiter mit Sitz in der EU nur dann die Daten in einem Drittland verarbeiten, wenn er dazu rechtlich verpflichtet ist. Er muss den Auftraggeber über diese Verpflichtung vorab informieren, es sei denn ein wichtiges öffentliches Interesse (wie eine Gefährdung der Strafverfolgung) verbietet ihm dies. Art. 29 DSGVO sieht zudem vor, dass der Auftraggeber auch gegenüber den Mitarbeitern des Auftragsverarbeiters und den Personen, die dem Auftragsverarbeiter unterstellt sind, Weisungsrechte hat.[17] Hier sollte der Auftragsverarbeiter sicherstellen, dass bei Einsatz von Subunternehmern entsprechende mittelbare Weisungsrechte des Auftraggebers umgesetzt werden können. Ggf. muss er die mit seinen Subunternehmern bestehenden Verträge anpassen.
- **Regelungen zur Unterstützung**: Die Parteien müssen künftig regeln, wie der Auftragsverarbeiter den Auftraggeber bei der Einhaltung von Pflichten des Auftraggebers unterstützt, Art. 28 Abs. 3 Satz 2 lit. e, f DSGVO. Dies umfasst Unterstützungsleistungen bei der Erfüllung der Pflichten des Auftraggebers, sofern Betroffene ihre Rechte nach Art. 12 ff. DSGVO geltend machen, der Umsetzung der technisch-organisatorischen Maßnahmen zur Datensicherung nach Art. 32 DSGVO, der Meldung von Datenpannen an die Aufsichtsbehörden und die Betroffenen nach Art. 33, 34 DSGVO, der Durchführung von Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO und der ggf. nötigen Konsultation mit den Aufsichtsbehörden nach Art. 36 DSGVO.
- **Einsatz von Subunternehmern**: Art. 28 Abs. 2, 3 lit. d und 4 DSGVO sieht vor, dass die Parteien zwingend in ihrem Vertrag Regelungen zur Einschaltung von Subunternehmern treffen, die vorsehen, dass der Auftragsverarbeiter die **Regelungen des Hauptvertrags** dem Subunternehmer auferlegt (inklusive der Vereinbarung hinreichender Garantien für die Einhaltung der vereinbarten technisch-organisatorischen Maßnahmen), er für die Subunternehmer haftet und der Auftraggeber **vorher zustimmt**. Diese Zustimmung kann entweder **jeweils im Einzelfall** eingeholt oder alternativ **pauschal im Vertrag** für **mehrere Subunternehmer** erteilt werden. In letzterem Fall muss der Auftragsverarbeiter vor einem Austausch oder dem Einsatz neuer Subunternehmer den Auftraggeber informieren. Der Auftraggeber muss das Recht zum Einspruch haben. Empfehlenswert ist hier Konsequenzen festzulegen, sofern es zu einer Ablehnung des Subunternehmers kommt (z.B. Kündigungsrechte oder kein Einsatz). Viele Verträge sahen hier bereits in der Vergangenheit entsprechende Regelungen vor. Die Praxis hat allerdings gezeigt, dass z.B. große Cloud-Provider den Abschluss entsprechender Regelungen aufgrund ihres Verwaltungsaufwands oftmals verweigert haben. Dies ist künftig nicht mehr so einfach vertretbar.

Weiterhin gibt es eine Reihe von Anforderungen, die nur **leicht** von den heute nach BDSG bestehenden **abweichen**. Hier muss im Einzelnen geprüft werden, ob die bestehenden Verträge diese bereits erfüllen oder Anpassungsbedarf besteht. Hier gilt für den Auftragsverarbeiter folgendes:

- Einsatz von Personen bei der Verarbeitung, die zur **Verschwiegenheit** verpflichtet sind bzw. einer **gesetzlichen Verschwiegenheit** unterliegen, Art. 28 Abs. 3 lit. b DSGVO; diese Pflicht geht über § 5 BDSG (Datengeheimnis) leicht hinaus, da sich letztere nur auf den Umgang mit Daten bezieht.
- Umsetzung der nach Art. 32 DSGVO **erforderlichen technisch-organisatorischen Maßnahmen**, Art. 28 Abs. 3 lit. c DSGVO.[18]
- **Rückgabe oder Vernichtung der Daten** nach Ende des Auftrags nach Wahl des Auftraggebers (Ausnahme: Pflicht zur Speicherung), Art. 28 Abs. 3 lit. g DSGVO.

17 Dies ergibt sich in Ableitung aus Art. 32 Abs. 4 DSGVO, der eine entsprechende Verpflichtung vorsieht.

18 Siehe dazu auch Martini in Paal/Pauly, DSGVO, Art. 28 DSGVO, Rn. 45; diese weisen zu Recht darauf hin, dass der Auftraggeber den Auftragsverarbeiter damit vertraglich zur Umsetzung der von ihm gewünschten Maßnahmen anhalten kann und es nicht nur auf die eigenverantwortliche Beurteilung durch den Auftragsverarbeiter ankommt.