Auftragsverarbeitung

DSGVO *Unternehmen und Behörden lagern ihre Lohnbuchhaltung oder die IT aus. Auftragsverarbeitung liegt im Trend. Für Betriebs- und Personalräte wird damit die Ausübung ihrer Rechte nicht einfacher.*

VON **BRUNO SCHIERBAUM**

DARUM GEHT ES

1. Die Datenverarbeitung außer Haus erfreut sich immer größerer Beliebtheit.

2. Das Verarbeiten personenbezogener Daten durch Externe bedarf immer einer rechtlichen Grundlage.

3. Die Auftragsverarbeitung lässt die Beteiligungsrechte von Betriebs- und Personalräten unberührt.

Entscheidende Kennzeichen der Auftragsverarbeitung sind die alleinige Entscheidung des Verantwortlichen über die Verarbeitung personenbezogener Daten und die Weisungsgebundenheit des Auftragsverarbeiters. Letztgenannter darf nach Art. 29 der Datenschutzgrundverordnung (DSGVO) personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen, also des Auftraggebers, verarbeiten. Der Verantwortliche hat die entsprechenden Weisungen zu dokumentieren, Art. 28 Abs. 3 a DSGVO. Im Rahmen von Auftragsverarbeitung agiert der Auftragsverarbeiter lediglich als verlängerter Arm des Auftraggebers, denn dieser ist für die Verarbeitung personenbezogener Daten verantwortlich und somit »Herr der Daten«.[1]

Privilegierte Auftragsverarbeiter

Auch nach dem Inkrafttreten der DSGVO bedarf die Auftragsverarbeitung weiterhin eines schriftlichen Vertrags. Auftragsdatenverarbeitung nach dem BDSG-alt bedeutete, dass eine vertragliche Regelung zwischen Auftraggeber und Auftragnehmer als Voraussetzung für die Weiterleitung personenbezogener Daten ausreichte und es keiner weiteren Zulässigkeitsprüfung vor einer Weitergabe von Daten an den Auftragnehmer bedurfte.

Diese Weiterleitung stellte nach dem alten BDSG keine Übermittlung dar. Auftragsdatenverarbeitung war insoweit ein Privileg, da der Auftragnehmer kein »Dritter« war und somit auch keine »Übermittlung« personenbezogener Daten stattfand. Ob dieses Privileg der Auftragsverarbeitung nach der DSGVO auch gegeben ist, ist umstritten, denn eine Definition des Begriffs der Übermittlung ist nicht vorhanden. So wird die Auffassung vertreten, dass bei einer Auftragsverarbeitung sowohl eine Zulässigkeitsprüfung nach Art. 6 DSGVO vorgenommen werden muss, wobei beim Beschäftigtendatenschutz zusätzlich der § 26 BDSG-neu hinzuzuziehen ist und es darüber hinaus noch einen Vertrag zur Auftragsverarbeitung geben muss.[2]

1 Vgl. Paal/Pauly (Hrsg.), DSGVO – BDSG, Art. 28 Rn. 2

2 Vgl. zur Diskussion Wedde, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG-neu, Art. 28 Rn. 5 ff.

Bestimmte Vorgaben der DSGVO deuten jedoch auf eine Privilegierung hin. So macht beispielsweise die Definition des Dritten in Art. 4 Nr. 10 DSGVO deutlich, dass der Auftragsverarbeiter eine Sonderstellung einnimmt. Dritter ist danach jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer dem Auftragsverarbeiter und die Personen, die unter unmittelbarer Verantwortung des Auftragsverarbeiters befugt sind, personenbezogene Daten zu verarbeiten.

Die Artikel-29-Datenschutzgruppe stellt fest: »Die Rechtmäßigkeit der Datenverarbeitungstätigkeit des Auftragsverarbeiters wird somit durch den von dem für die Verarbeitung Verantwortlichen erteilten Auftrag bestimmt.«[3] Man kann davon ausgehen, dass eine vertragliche Regelung, dessen Mindestumfang in Art. 28 Abs. 3 DSGVO festgelegt ist, für die rechtmäßige Weitergabe personenbezogener Daten durch den Verantwortlichen an den Auftragsverarbeiter ausreicht.

▸ Technischer Support

Früher war die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen eindeutig als Datenverarbeitung im Auftrag zu qualifizieren, in der DSGVO allerdings nicht mehr. Da aber im Rahmen von Wartung und Fernzugriffen eine Kenntnisnahme personenbezogener Daten durch externe Dienstleister nicht ausgeschlossen werden kann, handelt es sich dabei um einen Vorgang mit personenbezogenen Daten. Hauptanliegen der DSGVO ist gerade deren Schutz. Ob Systemwartung als eine »Offenlegung« durch »Übermittlung« oder »Verbreitung« einzuordnen ist, ist für die Praxis irrelevant, denn eine der genannten Verarbeitungsformen kommt zum Tragen. Das heißt, diese Form der »Kenntnisnahme« personenbezogener Daten kann als Auftragsverarbeitung qualifiziert werden. Diese Auffassung vertritt die Datenschutzkonferenz in ihrem Arbeitspapier zur Auftragsverarbeitung.[4] Hierzu gibt es aber auch andere Meinungen.[5] Ist man der Ansicht, es liegt keine Auftragsverarbeitung vor, wird man eine Zulässigkeitsprüfung nach Art. 6 DSGVO beziehungsweise beim Beschäftigtendatenschutz unter Hinzuziehung des § 26 BDSG-neu vornehmen müssen. Eine datenschutzgerechte Absicherung wird aber auch in diesem Fall eine vertragliche Regelung erforderlich machen, da es insbesondere um die Geheimhaltungspflicht der beim externen Dienstleister beschäftigten Personen geht.[6]

Auswahl des Auftragsverarbeiters

Ist eine Verarbeitung im Auftrag eines Verantwortlichen vorgesehen, arbeitet dieser nach Art. 28 Abs. 1 DSGVO nur mit Auftragsverarbeitern zusammen, die hinreichende Garantien bieten. So muss der Auftragsverarbeiter garantieren, dass

- geeignete technische und organisatorische Maßnahmen durchgeführt werden (Art. 32 DSGVO),
- die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und
- der Schutz der Rechte der Betroffenen gewährleistet wird (Art. 12 – 23 DSGVO).

Vor der Auftragsvergabe muss der Verantwortliche die Prüfung der Geeignetheit des Auftragsverarbeiters prüfen oder, anders ausgedrückt, muss der Auftragsverarbeiter geeignete Garantien nachweisen. Nach § 28 Abs. 5 DSGVO kann der Auftragsverarbeiter diese Garantien durch die Einhaltung genehmigter Verhaltensregeln von genehmigten Zertifizierungen nachweisen.

Der Erwägungsgrund 81 macht deutlich, dass der Verantwortliche nur die Auftragsverarbeiter heranziehen darf, die insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen hinreichende Garantie dafür bieten, dass technische und organisatorische Maßnahmen getroffen werden, die den Anforderungen der DSGVO genügen.[7] Neben der Einhaltung der DSGVO durch den Auftragsverarbeiter sind auch die Rechte der Betroffenen/Beschäftigten zum Beispiel auf Auskunft, Berichtigung oder Einschränkung der Verarbeitung zu beachten. Die Vorschrift zur Auftragsverarbeitung verlangt also die Auswahl eines tauglichen Auftragnehmers. Darauf muss der Verantwortliche nicht nur bei der erstmaligen Auswahl achten, sondern für die gesamte Zeitdauer des Auftragsverhältnisses.

Vertragliche Regelung

Ein Vertrag, für dessen Abschluss der Auftraggeber verantwortlich ist, muss schriftlich erfolgen und Regelungen in Bezug auf die Unter-

AUFTRAGS-VERARBEITER

Ein Auftragsverarbeiter ist nach der Definition des Art. 4 Nr. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

VERANTWORTLICHER

Ein Verantwortlicher ist nach Art. 4 Nr. 7 DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

3 Vgl. Artikel-29-Datenschutzgruppe, WP 169, 31
4 DSK-Kurzpapier Nr. 13, Art. 28 DSGVO, 3; Schmidt/Freund, Perspektiven der Auftragsdatenverarbeitung, in: ZD 1/2017, 14; Däubler/Wedde/Weichert/Sommer, aaO., Art. 28 Rn. 28; Müthlein, ADV 5.0, in: RDS 2/2016, 83
5 Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DSGVO/BDSG, 2018, Art. 28 Rn. 77
6 Vgl. hierzu: Wedde, in: Däubler/Wedde/Weichert/Sommer, aaO., Art. 28 Rn. 28 f.
7 Vgl. Erwägungsgrund 81 Satz 1

auftragsverhältnisse enthalten. Der Abschluss des Vertrags ist auch in elektronischer Form möglich. Unterauftragsverhältnisse können etwa bei Vernichtung von Datenträgern oder bei Fernwartung durch andere Stellen gegeben sein. Ein Vertrag muss nach den Vorgaben des Art. 28 Abs. 3 DSGVO bestimmte Mindestinhalte haben.

Unterauftragsverhältnisse

Der Auftragsverarbeiter muss nicht zwingend alle Datenverarbeitungstätigkeiten mit eigenen Mitteln durchführen. In Art. 28 Abs. 2 und 4 DSGVO werden die Bedingungen für die Beauftragung weiterer Unterauftragsnehmer genannt. Danach darf der Auftragsverarbeiter keine weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch nehmen. Spätere beabsichtigte Änderungen in Bezug auf das Hinzuziehen oder das Ersetzen anderer Auftragsverarbeiter sind dem Verantwortlichen vorher mitzuteilen. Er kann gegen derartige Änderungen Einspruch erheben. Darf der Auftragsverarbeiter einen Unterauftrag erteilen, sind dem Unterauftragnehmer die gleichen Pflichten schriftlich aufzuerlegen, die auch den Hauptauftraggeber treffen. Dabei müssen insbesondere hinreichende Garantien geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden und die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der (Haupt-)Auftragnehmer gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragnehmers.

Standardvertragsklauseln

Der Vertrag zur Auftragsverarbeitung kann nach Art. 28 Abs. 6 DSGVO auf sogenannten Standardvertragsklauseln beruhen. Diese enthalten datenschutzrechtliche Mindeststandards und orientieren sich an die in Art. 28 Abs. 3 DSGVO verankerten Inhalte eines Vertrags zur Auftragsverarbeitung. Diese Klauseln können durch die EU-Kommission oder die Aufsichtsbehörde (im Rahmen des Kohärenzverfahrens) festgelegt werden. Die derzeit bekannten Muster der Standardvertragsklauseln entsprechen nicht den Vorgaben der DSGVO.[8]

Kontrolle vor Ort

Damit der Verantwortliche Kontrollen durchführen kann, sind ihm alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung zu stellen. Zudem muss der Auftragsverarbeiter ermöglichen und dazu beitragen, dass Überprüfungen – einschließlich Inspektionen – die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden sollen, auch stattfinden können. In dem Vertrag zur Auftragsverarbeitung ist dieses Recht auf Prüfung/Inspektion zu verankern. Neben den genannten Personen sollte im Vertrag vor allem auch der Datenschutzbeauftragte des Verantwortlichen, aber auch der Betriebs- oder Personalrat benannt werden. Denn deren Informations- und Überwachungsrecht kann nicht durch Auftragsverarbeitung eingeschränkt werden, was auch für weitere Rechte nach dem BetrVG beziehungsweise PersVG gilt.

Datenverarbeitung im Konzern

In Konzernen oder Unternehmensverbünden ist vielfach ein arbeitsteiliges Zusammenwirken der verschiedenen Unternehmen zu beobachten. Dieses wird unter anderem mit dem Begriff Shared Services bezeichnet. So kann ein Unternehmen eines Konzerns als gemeinsames Rechenzentrum fungieren oder in der Unternehmenszentrale eines Konzerns finden die Personalverwaltung und Lohnbuchhaltung statt. Diese Datenverarbeitungen werden grundsätzlich als Auftragsverarbeitung zu betrachten sein, so dass zwischen den einzelnen Unternehmen jeweils eine vertragliche Regelung zur Auftragsverarbeitung erfolgen muss.[9]

Es gibt aber die Möglichkeit, dass auch im Rahmen von Unternehmensgruppen ein arbeitsteiliges Zusammenwirken möglich ist und dass alle Beteiligten gemäß Art. 26 DSGVO »gemeinsam Verantwortliche« sind. Dieses bedarf aber einer gleichberechtigten und gemeinsamen Festlegung der Zusammenarbeit. Jedes beteiligte Unternehmen muss dann »Herr der Daten« sein. Es ist in diesem Zusammenhang aber auch erforderlich, dass im Rahmen einer Vereinbarung in transparenter Form festlegt wird, wer welche Verpflichtung gemäß der DSGVO hat. Dieses gilt insbesondere hinsichtlich der Wahrnehmung der Rechte der

8 Vgl. Wedde, in: Däubler/Wedde/Weichert/Sommer, aaO., Art. 28 Rn. 106 f.

9 Vgl. Moos/Schefzig/Arning (Hrsg.), Die neue DSGVO, 2018, 257

Mit Augenmaß

Ruchhöft / Wilke
Mobiles Arbeiten
Handlungshilfe für Betriebsräte
Reihe: AiB-Stichwort
2017. 99 Seiten, kartoniert
€ 14,90
ISBN: 978-3-7663-6659-7

www.bund-verlag.de/6659

BUND VERLAG
kontakt@bund-verlag.de
Info-Telefon: 069/79 50 10-20

Betroffenen und der Informationspflichten nach Art. 13 und 14 DSGVO. In Bezug auf das Konstrukt, der »gemeinsam Verantwortlichen« muss neben einer vertraglichen Regelung auch die Rechtmäßigkeit der Datenübermittlung von einem zum anderen Unternehmen gemäß Art. 6 DSGVO, bei sensiblen Daten nach Art. 9 DSGVO und bei Beschäftigtendaten nach § 26 BDSG-neu gestaltet werden. Die Rechtmäßigkeit der Übermittlung muss geprüft werden, denn aus Art. 26 DSGVO leitet sich keine privilegierte Verarbeitung ab.

Auftragsverarbeitung in Drittländern

Die DSGVO unterscheidet nicht zwischen Auftragsverarbeitern innerhalb oder außerhalb der EU. Die Privilegierung gilt auch für Verarbeiter in Drittländern, das heißt der Abschluss eines Vertrags nach Art. 28 DSGVO – aber auch die zusätzlichen Voraussetzungen für den Datentransfer in Drittländer nach Art. 44 ff. DSGVO – müssen erfüllt sein, um rechtmäßig zu handeln.[10]

Das heißt natürlich nicht, dass die Verarbeitung personenbezogener Daten im Rahmen der Auftragsverarbeitung in Drittländern unbegrenzt möglich ist. Die Zulässigkeit von Auftragsverarbeitung setzt voraus, dass das durch die DSGVO vorgeschriebene angemessene Datenschutzniveau uneingeschränkt garantiert wird und die betroffenen Personen rechtlich ebenso gestellt sind wie bei einer Verarbeitung innerhalb der EU.[11]

Haftung und Bußgeld

Die Haftungsregeln für den Auftragsverarbeiter sind gegenüber dem alten Datenschutzrecht verschärft worden. Nach Art. 82 DSGVO haften der Verantwortliche und der Auftragsverarbeiter gegenüber dem Betroffenen grundsätzlich gemeinsam für Datenschutzverstöße, an dem beide beteiligt sind. Das bedeutet, dass der Betroffene seinen gesamten Schaden vom Verantwortlichen und Auftragsverarbeiter verlangen kann.[12]

Dieses gilt für materielle und immaterielle Schäden. Wenn sich der Auftragsverarbeiter zum Verantwortlichen »aufschwingt« und zum Beispiel über die Zwecke und Mittel der Verarbeitung bestimmt, haftet er als Verantwortlicher.[13] Auch die strengen Bußgeldfolgen können nicht nur den Verantwortlichen, sondern auch den Auftragsverarbeiter treffen. Bußgelder können nach Art. 83 Abs. 4a DSGVO in Höhe von bis zu 10.000.000 Euro oder zwei Prozent des weltweiten Jahresumsatzes des Vorjahres verhängt werden. Behörden und sonstige öffentliche Stellen müssen keine Bußgelder fürchten (§ 43 Abs. 3 BDSG-neu).

Aufgaben für die Belegschaftsvertretung

Die Beteiligungsrechte des Betriebs- oder Personalrats sind bei der Auftragsverarbeitung genauso zu beachten, wie bei einer Datenverarbeitung »im eigenen Hause«.[14] Wäre das nicht der Fall, könnte jeder Arbeitgeber durch das Auslagern seiner Datenverarbeitung die Beteiligung der Arbeitnehmervertretung umgehen. So hat diese einen Informationsanspruch und zusätzlich ein Überwachungsrecht hinsichtlich bestehender betrieblicher oder dienstlicher Vereinbarungen und Gesetze, wozu auch die DSGVO, das BDSG-neu beziehungsweise das jeweilige Landesdatenschutzgesetz gehören. Vor der Auslagerung der Datenverarbeitung ist der Betriebs- oder Personalrat über die eingesetzte Hard- und Software, die gespeicherten personenbezogenen Daten, die Auswertungen, die zugriffsberechtigten Personen mit Art und Umfang des Zugriffs, die Schnittstellen, die Löschfristen und über die Datenschutz- und Datensicherungsmaßnahmen zu informieren[15], außerdem über die Umsetzung der Grundsätze der Datenverarbeitung nach Art. 5 DSGVO und über das Ergebnis einer Datenschutzfolgenabschätzung.

Ist die im Rahmen der Auftragsverarbeitung eingesetzte Hard- und Software zur Leistungs- oder Verhaltenskontrolle geeignet – wovon auszugehen ist -, ist das Mitbestimmungsrecht zu beachten.[16] In diesem Fall empfiehlt es sich, eine Betriebs- oder Dienstvereinbarung abzuschließen. Der Arbeitgeber hat dafür Sorge zu tragen, dass diese Vereinbarung dann auch durch den Auftragsverarbeiter eingehalten wird. Dieses sollte sowohl in der Vereinbarung selbst oder in dem Vertrag zur Auftragsverarbeitung vereinbart werden. ◁

Bruno Schierbaum,
BTQ Niedersachsen GmbH
schierbaum@btq.de
www.btq.de

VERTRAG »AUFTRAGSVERARBEITUNG«

Mindestinhalt nach Art. 28 DSGVO:

- Gegenstand, Dauer, Art, Zweck der Verarbeitung
- Art der personenbezogenen Daten
- Kategorien der betroffenen Personen
- Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen
- Verpflichtung zur Vertraulichkeit der beim Auftragsverarbeiter Beschäftigten oder Verschwiegenheitspflicht
- Einhaltung der technischen und organisatorischen Maßnahmen (TOMs) nach Art. 32
- Einhaltung der Vorgaben zum Einsatz von Unterauftragsverhältnissen
- Unterstützung des Auftraggebers bei Umsetzung der TOMs, damit dieser Betroffenenrechten nachkommen kann
- Unterstützung des Auftraggebers bei TOMs, Unterrichtung von Aufsichtsbehörden, Information der Betroffenen bei Pannen, Datenschutzfolgenabschätzung
- Rückgabe/Löschung der personenbezogenen Daten nach Abschluss
- dem Verantwortlichen sind alle erforderlichen Informationen zur Auftragsverarbeitung zur Verfügung zu stellen und Überprüfungen zu ermöglichen
- Information an Verantwortlichen bei vermutetem Datenschutzverstoß

10 Vgl. Schmidt/Freund, aaO., 16; Hartung/Büttgen, Die Auftragsverarbeitung nach der DSGVO, in: DuD 9/2017, 533; Kühling/Buchner (Hrsg.), DSGVO, 2018, Art. 28 Rn. 104; Wedde, in: Däubler/Wedde/Weichert/Sommer, aaO., Art. 28 Rn. 8; Datenschutzkonferenz, Kurzpapier Nr. 13, aaO., Art. 28 DSGVO, 1
11 Däubler/Wedde/Weichert/Sommer, aaO., Art. 28 Rn. 26
12 Vgl. Schmitz/von Dall'Armi, Auftragsdatenverarbeitung in der DSGVO – das Ende der Privilegierung, in: ZD 9/2016, 427 ff (432)
13 Schwartmann/Jaspers/Thüsing/Kugelmann, aaO., Art. 28 Rn. 171
14 Ausführlich dazu Wedde, Beschäftigtendaten außer Haus, in: CuA 3/2018, 30 ff.
15 Vgl. BVerwG 8.11.1989 – 6 P 7.87, in: RDV 3/1990, 144
16 Das BetrVG enthält in § 87 Abs. 1 Nr. 6 und das BPersVG in § 75 Abs. 3 Nr. 17 ein entsprechendes Mitbestimmungsrecht. Die Landespersonalvertretungsgesetze enthalten ebenfalls entsprechende Mitbestimmungsrechte.