whitepaper

Was gehört alles in einen Auftragsverarbeitungsvertrag und was eher nicht?

Einleitung

Sowohl im Internet, als auch im realen Leben kursieren verschiedene Auftragsverarbeitungsvertrags (AV-Vertrag)-Vorlagen, die sich inhaltlich alle sehr ähnlich sind. Hierbei gibt es nach meiner Erkenntnis ca. 5 Muster, die in Deutschland Verwendung finden. In manchen übersandten AV-Verträgen wurden aber Änderungen in diese Musterverträge eingepflegt, die es in sich haben, oder Wichtiges wurde weggestrichen, so dass Sie mit Hilfe dieses Whitepapers erkennen können sollen, was in einen Auftragsverarbeitungsvertrag gehört und worauf Sie bei einer Prüfung eines solchen Vertrages achten sollten.

Wichtiger Hinweis

- In diesem Whitepaper wird nicht die Frage behandelt, wann der Abschluss eines AV-Vertrags überhaupt erforderlich ist. Dieses Whitepaper soll vielmehr eine Hilfe bei der Prüfung und Anpassung von AVV sein, setzt also die erfolgte Prüfung des Vorliegens eines AV-Verhältnisses im Sinne von Art. 28 DSGVO voraus. Dies ist nicht Gegenstand dieses Whitepapers.

- Bei der Ausgestaltung eines Vertrages kommt es natürlich immer darauf an, welche der beiden Seiten man vertritt. Die nachfolgende Übersicht schlägt sich auf keine von beiden Seiten.

- Natürlich kann dieses Whitepaper die individuelle Vertragsprüfung und im Zweifelsfall die Einholung von Rechtsrat nicht ersetzen. Dieses Whitepaper erhebt auch nicht den Anspruch einer wissenschaftlichen Abhandlung, sondern möchte eine praxistaugliche Hilfe für rechtliche Laien bieten.

Gegenstand der Datenverarbeitung

In diesem Teil ist konkret und individuell zu beschreiben, was der Auftragsverarbeiter eigentlich machen soll:

Welche Tätigkeit führt er im Hinblick auf die Datenverarbeitung aus, für welche Dauer (auch die Angabe „unbefristet“ ist hier natürlich möglich) und zu welchem Zweck erfolgt die Datenverarbeitung?

An dieser Stelle erfolgt in einigen Mustern ein Verweis auf die dem AV-Vertrag zugrunde liegende Leistungsvereinbarung, also quasi den „Haupt-“ oder „Rahmenvertrag“ zwischen den Parteien. Voraussetzung für den bloßen Verweis ist, dass dieser Hauptvertrag auch tatsächlich konkrete Angaben Daten zur Datenverarbeitung durch den Auftragsverarbeiter enthält, weil ansonsten der Verweis ins Leere läuft. Dies ist etwa der Fall, wenn der Hauptvertrag lediglich Konditionenvereinbarungen enthält.

Enthalten sein müssen im Vertrag (egal ob über den Verweis oder direkt im AV-Vertrag) immer:

- Die vom Auftragsverarbeiter erbrachten Leistungen
- Der Zweck der Datenverarbeitung
- Die Arten der personenbezogenen Daten
- Die Empfängerkategorie der betroffenen Personen

Hierbei sollten Sie möglichst konkret sein. Ein Dritter, zum Beispiel die Aufsichtsbehörde, sollten dem Vertrag ohne Weiteres entnehmen können, was Aufgabe des Auftragsverarbeiters ist und welche Daten er dafür erhält.

TIPP: Da man im Falle eines Falles aber den AV-Vertrag der Aufsichtsbehörde vorlegen muss und im Falle eines Verweises auf einen etwaigen Hauptvertrag auch diesen vorlegen muss, sollten man gut abwägen, ob man dies auch tatsächlich will. Die Aufsichtsbehörde könnte so Kenntnis von Details erlangen, welche besser im Unternehmen bleiben würden.

Verteilung der Verantwortlichkeiten

Achten Sie darauf, dass die gesetzlich geregelten Verantwortlichkeiten zwischen den einzelnen Parteien im Vertrag ihren Niederschlag finden und nicht unterlaufen werden. Der Verantwortliche ist weisungsbefugt und bestimmt alleine (!) über die Zwecke und die Art und Weise der Datenverarbeitung (Art. 29 DSGVO). Der Auftragsverarbeiter darf spiegelbildlich Daten nur auf Weisung des Verantwortlichen verarbeiten.
Wenn diese Rollenverteilung nicht richtig auf das Ihnen vorliegende Vertragsverhältnis passt, weil der Auftragsverarbeiter eventuell auch selber über die Zwecke und / oder die Art und Weise der Datenverarbeitung entscheidet, liegt eventuell eine sog. „gemeinsame Verantwortlichkeit / Joint Controllership“ gem. Art. 26 DSGVO und kein Fall der Auftragsverarbeitung vor.
Der Auftragsverarbeiter sollte also darauf achten, dass die Formulierungen hier sorgfältig gewählt werden, um nicht Gefahr zu laufen, selbst zum Verantwortlichen zu werden. Gleichzeitig ist aber auch das „Konstruieren“ eines Auftragsverhältnisses über den AV-Vertrag, der in der Praxis anders gelebt wird, nicht möglich. Der Abgrenzung zwischen Auftragsverarbeitung und der gemeinsamen Verantwortlichkeit könnte man ein eigenes dickes Lehrbuch widmen, so dass es hierzu ein eigenes Whitepaper geben wird.

Der Auftragnehmer sollte sich im Vertrag nicht einfach Verarbeitungszwecke vertraglich ausbedingen, die über die vom Verantwortlichen vorgesehenen Zwecke hinausgehen. Natürlich hätte der Auftragsverarbeiter die Kundendaten des Verantwortlichen gern, um damit z.B. eigene Marktforschung zu betreiben. Aber: Das hat mit der im Vertrag geregelten Auftragsverarbeitung nichts mehr zu tun, weil der Auftragnehmer diesbezüglich nicht auf Weisung des Verantwortlichen tätig wird und eigene Zwecke verfolgt. Damit sollte daher im Vertrag besonders sensibel umgegangen werden.

TIPP: Sofern der Auftragsverarbeiter die Verwendung für eigene Zwecke wünscht, so ist die allenfalls möglich, wenn der Auftragsverarbeiter die Daten vollständig anonymisiert und er die Anonymisierung vertraglich garantiert (nach der Anonymisierung unterliegen die Daten nicht mehr der DSGVO, vgl. EG 26, Satz 5 DSGVO).

Technische und organisatorische Maßnahmen („TOMs“)

Der Vertrag muss den Auftragsverarbeiter dazu verpflichten, die gem. Art. 32 DSGVO geeigneten TOMs zu ergreifen. Die Auswahl der TOMs ist nach dem in der DSGVO vorherrschenden risikobasierten Ansatz vorzunehmen, und natürlich sind die vom Auftragsverarbeiter – in der Regel in einer Anlage zum Vertrag – niedergelegten TOMs konkret zu prüfen.

TIPP: Achten Sie darauf, dass hier nicht nur der Gesetzestext abgeschrieben wurde. Die TOMs sind immer (!) individuell anzupassen. In der Regel gibt der Auftragsverarbeiter, weil er näher dran ist, seine TOMs an und der Verantwortliche prüft, ob er diese für die konkrete vertragliche Konstellation als ausreichend erachtet. Für nicht ausreichende TOMs haftet der Verantwortliche!

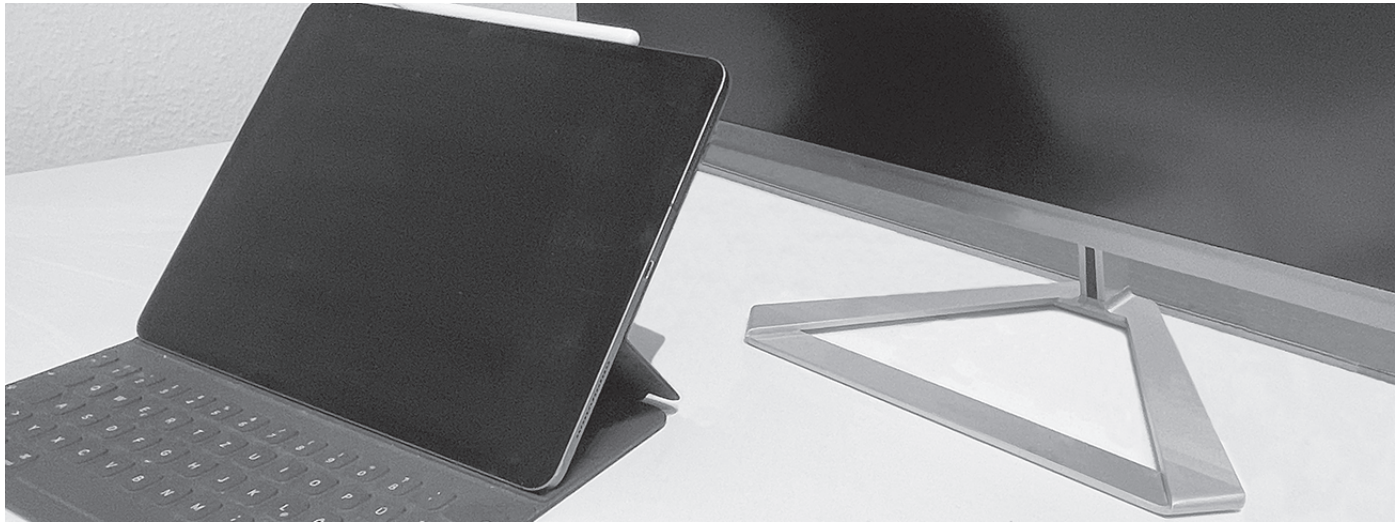
Aus meiner Praxis weiß ich, dass bei vielen Verantwortlichen fälschlicherweise angenommen wird, der Auftragsverarbeiter fülle die Anlage zu den TOMs aus, man segnet das ab, und fertig ist der AV-Vertrag. Das kann im Zweifelsfall gefährlich werden, weil der Verantwortliche für die Gewährleistung eines angemessen Schutzniveaus und damit für die Auswahl der passenden TOMs (und deren Einhaltung) genauso haftet wie der Auftragsverarbeiter.

Unterauftragsverhältnisse

Achten Sie darauf, ob bezüglich der Vereinbarung von Unterauftragsverhältnissen von der gesetzlichen Regelung in Art. 28 Abs. 2 DSGVO abgewichen wird und ob die vertragliche Ausgestaltung der Unterbeauftragung für Ihre vertragliche Konstellation passend ist: Die DSGVO bietet die Wahl:

- Verbot der Unterbeauftragung mit Ausnahme der Einzelgenehmigung durch den Verantwortlichen, oder
- allgemeine Erlaubnis der Unterbeauftragung im AV-Vertrag in Kombination mit einem Vetorecht des Verantwortlichen.

Wichtig: Sind Sie der Auftragsverarbeiter und beauftragen Sie wiederum Unterauftragsverarbeiter, haften Sie bzw. Ihr Unternehmen für deren Einhaltung der gleichen Standards, zu denen Sie sich verpflichtet haben, Art. 28 Abs. 4 DSGVO). Daher ist es für Sie zwingend, identische AV-Verträge mit Ihren Unter-Auftragsverarbeitern zu schließen. Das sollte also nicht nur als Verpflichtung im AV-Vertrag stehen, sondern auch tatsächlich gelebt werden.



Datenverarbeitung im Drittland

Im Vertrag sollte statuiert sein, dass die Datenverarbeitung in einem Drittland, also einem Nicht-EU-Mitgliedstaat, grundsätzlich untersagt ist (die EWR Staaten Norwegen, Island und Liechtenstein sind keine Drittländer, weil sie die Anwendbarkeit der DSGVO für sich beschlossen haben). Jede Verlagerung einer Verarbeitungstätigkeit (auch die durch Unterauftragnehmer) sollte an die Genehmigung durch den Verantwortlichen geknüpft werden. Außerdem sollte festgelegt werden, dass die Verlagerung in ein Drittland nur erfolgen darf, wenn hierfür eine wirksame Rechtsgrundlage gem. Art. 44-46 DSGVO vorliegt.

Sollte die Auftragsverarbeitung bei Ihnen im Unternehmen standardmäßig in Drittländer ausgelagert werden, holen Sie sich entsprechenden Rechtsrat, wenn Sie unsicher sind, wie der Vertrag an dieser Stelle auszugestalten ist.
Das Thema ist zu komplex, um es in diesem Whitepaper zu behandeln.

An dieser Stelle sei jedoch gesagt, dass mit den neuen Standardvertragsklauseln der EU (kurz SCC) recht gut gearbeitet werden kann. Hierbei gilt es jedoch zu beachten, dass die SCC für sich allein genommen nicht ausreichend sein werden. Es müssen zusätzliche Garantien mit dem Auftragsverarbeiter (Datenimporteur) vereinbart werden, die anhand eines umfassenden Transfer Impact Assessment (TIA) zu ermitteln sind. Nach dem erfolgten TIA weiß man erst, welche Jurisdiktion in dem jeweiligen Land herrscht, wie der Zugriff der Behörden auf die Daten dort ausgestaltet ist, welche grundsätzlichen Maßnahmen der Datenimporteuer bereits vorgenommen hat und welche zusätzlichen Maßnahmen hier zu vereinbaren sind.

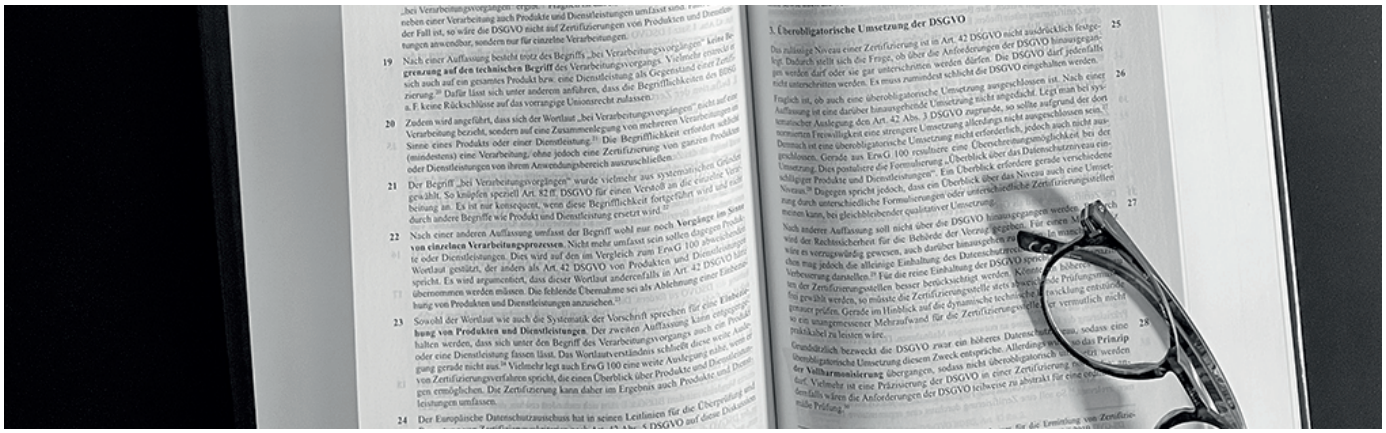
Noch im Jahr 2022 soll zudem für den EU-US Datentransfer ein neues Abkommen in Kraft treten, das sogenannte Trans-Atlantic Data Privacy Framework, welches dem vom EuGH aufgehobene EU-US Privacy Shield folgen soll. Noch sind es lediglich Absichtserklärungen, welche noch mit Leben gefüllt werden müssen. Sobald dieses Framework jedoch in Kraft ist, können voraussichtlich auch die EU-US Datentransfers wieder hierauf gestützt werden, so dass mit den großen Playern am Markt (wie z.B. Google, Microsoft, Amazon etc.) nicht mehr mit den Standardvertragsklauseln und Zusatzgarantien gearbeitet werden muss. Die weitere Entwicklung hierzu bleibt spannend.

Vergütungspflicht des Verantwortlichen

Relativ beliebt ist vor allem bei großen Auftragsverarbeitern mit verhältnismäßig großer Verhandlungsmacht, im Vertrag eine Vergütung für Pflichten festzulegen, die ihnen von Gesetzes wegen obliegen (z.B. die Duldung der Ausübung der o.g. Kontrollrechte). Das ist nicht ganz unproblematisch und läuft oftmals dem Regelungszweck der DSGVO zuwider (die bayrische Aufsichtsbehörde sieht das genauso). Allerdings scheint der EuGH mit einer solchen Regelung gut leben zu können, weshalb sie auch immer öfters in AV-Verträgen anzutreffen ist.

TIPP: Sie sollten darauf achten, dass derlei Klauseln so formuliert sind, dass die gesetzlichen Pflichten nicht unterlaufen bzw. aufgeweicht werden. Mein Vorschlag in Bezug auf die Kontrollrechte: Es sollten Intervalle bzw. die Häufigkeit der Kontrollen vertraglich geregelt werden, um zu verhindern, dass hierdurch zu hohe Kosten anfallen. Denn das Argument, dass dem Auftragsverarbeiter bei der Ermöglichung von Kontrollen Kosten anfallen, lässt sich natürlich nicht von der Hand weisen.

Generell gilt: Sollte vertraglich eine Vergütung für die Erbringung der Pflichten aus dem AV-Vertrag vereinbart werden, muss die Vergütung angemessen und nicht so hoch bemessen sein, dass sie faktisch die Ausübung der Rechte des Verantwortlichen verhindert. Denn dies würde im Zweifel dazu führen, dass der AV-Vertrag nicht den Anforderungen der DSGVO entspricht, was ein entsprechendes Bußgeld nach sich ziehen kann.



Vertraulichkeitsverpflichtung des Auftragnehmers

Der Auftragnehmer muss im Vertrag zur Vertraulichkeit bei der Datenverarbeitung verpflichtet werden sowie dazu, auch seine Mitarbeiter auf Vertraulichkeit zu verpflichten.
Hiermit wird kurz gesagt vor allem die Sensibilität der Mitarbeiter in Punkto Datenschutz erhöht.

Zu Beweiszwecken empfiehlt es sich, die Vertraulichkeitsverpflichtungen der Mitarbeiter schriftlich vorzunehmen.
Die Mitarbeiter unterschreiben

- im Idealfall nach entsprechender Datenschutzschulung
- eine entsprechend vorformulierte Erklärung.

Kontrollrechte des Verantwortlichen

Dem Verantwortlichen werden in der DSGVO Kontrollrechte im Hinblick auf die Einhaltung der im Vertrag festgelegten Pflichten eingeräumt (Art. 28 Abs. 3 lit. h DSGVO). Diese Kontrollrechte sind hinsichtlich ihrer Intensität und Häufigkeit unbedingt auf die jeweilige Vertragskonstellation anzupassen. Zu den Kontrollrechten zählen unter anderem auch das Zur-Verfügung Stellen von Audit-Reports oder der Vorbehalt von Drittkontrollen. Verträge, die keinerlei Kontrollmöglichkeiten des Verantwortlichen enthalten, sollen den Anforderungen der DSGVO an einen wirksamen AV-Vertrag nicht genügen.

Fazit

Es gibt einige Fallstricke, die es beim Abschluss von AV-Verträgen zu beachten gilt. Nicht immer werden die bewährten und altbekannten Muster vollständig übernommen. Es gilt daher besonders wachsam zu sein und Klausel für Klausel zu prüfen, ob hier nicht etwas Wichtiges weggelassen oder für den Verantwortlichen Ungünstiges hinzugefügt wurde.

Gerne steht die IT-Kanzlei Lutz mit ihrer Expertise Ihnen bei der Prüfung und Erstellung von AV-Verträgen, der Vereinbarung von Standardvertragsklauseln und der generellen Beratung in datenschutzrechtlichen Fragen zur Verfügung.

IT-KANZLEI LUTZ
DATENSCHUTZ UND RECHTSBERATUNG

Stefan Lutz, LL.M.
Rechtsanwalt
Fachanwalt für IT-Recht
Externer Datenschutzbeauftragter

Kanzlei Ravensburg
Bachstrasse 3
88214 Ravensburg
T 07 51 / 27 088 53-0
www.datenschutz-rv.de
lutz@datenschutz-rv.de