Erläuterungstext zum Entscheidungskreis

Autor: Martin Leiter, AK AV
Version 002 vom 15.4.2020
Update 003 vom 16.2.2021 (Anpassung an den aktuellen Entscheidungskreis)

Der Entscheidungskreis soll eine Hilfestellung bieten, um einschätzen zu können, ob eine vom Verantwortlichen und der betroffenen Person verschiedene Entität (diese wird in der Folge als „Dienstleister“ bezeichnet, weil diese im Normalfall auf Basis eines Dienstleistungsvertrages für den Verantwortlichen tätig wird) ein „Auftragsverarbeiter“ des Verantwortlichen im Sinne des Art 4 Z 8 ist und daher der Abschluss einer Auftragsverarbeitervereinbarung erforderlich ist.

In weiterer Folge sollen die beschriebenen Schritte des Entscheidungskreises näher erläutert werden.

Schritt 1 – Personenbezug

Handelt es sich bei den Informationen, die Gegenstand der Verarbeitung sind, um personenbezogene Daten im Sinne der DSGVO?
Nur wenn dies der Fall ist, kann es sich überhaupt um Auftragsverarbeitung handeln. Die Verarbeitung von nicht personenbezogenen Daten (z.B. statistische Aussagen oder andere Informationen, die sich nicht auf eine einzelne bestimmte oder bestimmbare Person beziehen, findet nicht unter dem Regime der DSGVO statt und kann daher auch keine Auftragsverarbeitung sein.
„Person“ bedeutet in diesem Zusammenhang immer „natürliche Person“. Das bedeutet, dass die Verwendung von Daten zu juristischen Personen in der Regel ebenfalls nicht datenschutzrelevant ist.
Achtung: oft bilden Aussagen zu juristischen Personen auch Verhältnisse von natürlichen Personen ab, z.B. von Eigentümern und Ansprechpartnern. Ist dies der Fall, ist Personenbezug gegeben[1].

Schritt 2 – Vertragsgegenstand

Hat der Vertrag zwischen dem Verantwortlichen und dem Dienstleister die Verarbeitung personenbezogener Daten zum Inhalt?
Nur wenn dies der Fall ist (und es sich bei der Verarbeitung nicht um eine bloße Nebentätigkeit[2] handelt) liegt Auftragsverarbeitung vor. Das bedeutet, dass die Verarbeitung

[1] EuGH C-92/09 und C-93/09 vom 9.11.2010: hier hatte der EuGH die Anwendbarkeit von Datenschutzrecht bejaht, wenn EU-Beihilfen an juristische Personen, die den Namen von natürliche Personen enthalten, wiederum 30-70% des Gesamteinkommens der hinter der juristischen Person stehenden natürlichen Person ausmachen.

[2] Vgl dazu Kotschy in Datenschutz - eine Standortbestimmung (Teil I) in RdW 8/2018: *„Wenn eine gekaufte Ware laut Kaufvertrag vom Verkäufer an den Käufer zuzustellen ist, erhebt sich bei der Heranziehung eines Spediteurs die Frage, ob dieser ,,Auftragsverarbeiter" hinsichtlich der übermittelten Lieferdaten ist oder ,,Dritter". Dasselbe gilt zB für die Durchführung von Zahlungen eines Unternehmens an eine natürliche Person (zB die Mitarbeiter) im Wege eines Kreditinstituts. Vieles spricht dafür, dass der Spediteur oder das Kreditinstitut als ,,Dritter" zu sehen ist, da im Mittelpunkt der bedungenen Leistung nicht die Verarbeitung von Daten, sondern Transport und Zustellung der Ware oder Transfer von Geldmitteln steht. (…) Wenn die Verarbeitung von personenbezogenen Daten nicht im Vordergrund des Auftrags steht und/oder keinen umfangreichen Teil der Leistung des Beauftragten ausmacht, wird davon auszugehen sein, dass die Mitwirkung eines ,,Dritten" vorliegt und nicht ,,Auftragsverarbeitung".*

personenbezogener Daten (auch) Gegenstand des Auftrages, d.h. der dahinterstehenden zivilrechtlichen Vereinbarung sein muss.
Achtung: da auch das „Vernichten“ eine Verarbeitung ist, wird in der Regel auch die Datenvernichtung (z.B. die physische Vernichtung von Datenträgern durch einen Dienstleister) idR als Auftragsverarbeitung betrachtet.

Schritt 3 – Weiterleitung

Werden die Daten von Dienstleister nur weitergeleitet, ohne dass er selbst beauftragt ist, in die Daten Einsicht zu nehmen?
Hier wird geprüft, ob sich durch den Einsatz des Dienstleisters der „Kreis der Wissenden“ erweitert. Ist dies nicht der Fall und wird durch eine bloße Weiterleitung von Daten dieser Kreis nicht erweitert (auch nicht auf den Dienstleister selbst), dann liegt keine Auftragsverarbeitung vor.
Achtung: ist der „Weiterleitungs-Dienstleister“ auch mit Wartungsarbeiten beauftragt, im Rahmen derer er z.B. im Störungsfall personenbezogene Daten verarbeiten darf, ist er jedenfalls Auftragsverarbeiter.

Schritt 4 – Normen, Judikatur

Gibt es Sondervorschriften für die konkrete Verarbeitungssituation?
In einigen Fällen regeln eigene Normen oder Verhaltensregeln nach Art 40 DSGVO die datenschutzrechtliche Zuständigkeit und damit auch insbesondere in bestimmten Zusammenhängen den „Verantwortlichen“ nach Art 4 Z 7 DSGVO, z.B. für die Ausübung des Gewerbes der Adressverlage und Direktmarketingunternehmen gem. § 151 GewO 1994. In diesen Verhaltensregeln wird auch die datenschutzrechtliche Rollenverteilung zwischen Direktmarketingunternehmen und Kunden bei der Verwendung von Marketingadressen festgelegt.
In anderen Fällen existiert Rechtsprechung der Datenschutzbehörde zur Frage der Auftragsverarbeitung, beispielsweise zur Tätigkeit von Rechtsanwälten[3], Steuerberatern[4], Inkassounternehmen[5] oder Kreditauskunfteien[6].

Schritt 5 – Zwecke

Wer legt die Zwecke der Verarbeitung fest?
Jede Verarbeitung von Daten geschieht zu einem Zweck („Warum“ werden die Daten verarbeitet?), dh es soll mit der Verarbeitung ein Ziel erreicht werden. Dieser Zweck kann die Steuerung einer anderen Tätigkeit sein, wie z.B. der Versand eines Poststückes, oder die Herstellung eines Zustandes oder die Unterstützung eines anderen Vorhabens z.B. der Überweisung von Gehältern an Mitarbeiter.
Oft haben Verarbeitungen mehrere Zwecke, z.B. dienen Kundendatenbanken einerseits dem Zweck, Kunden mit Waren oder Leistungen bedienen und diese abrechnen zu können, aber auch dem Zweck, Marketingmaßnahmen zu steuern. Klarerweise muss es für jeden dieser Zwecke eine (ggfs unterschiedliche) Rechtgrundlage geben.
Wenn nun der Dienstleister (ggfs gemeinsam mit dem Verantwortliche) über einen dieser Zwecke entscheiden kann oder gar bereits entschieden hat (z.B. die von ihm verwendeten Daten für eigene Marketingzwecke verwenden darf), so handelt es sich beim Dienstleister (jedenfalls im Rahmen dieser Tätigkeit) NICHT um einen Auftragsverarbeiter.
Achtung: wenn der Dienstleister kein Auftragsverarbeiter iSd Art 28 DSGVO ist, ist zwar der Abschluss einer entsprechenden Vereinbarung nicht erforderlich, es bedarf aber für diese

[3] K121.810/0013-DSK/2012, DSB-D122.215/0004-DSB/2014, DSB-D122.299/0003-DSB/2015
[4] DSB-D122.767/0001-DSB/2018
[5] K121.155/0015-DSK/2006, K121.330/0004-DSK/2008
[6] DSB-D122.304/0012-DSB/2015 (zu den errechneten Scorewerten)

Verwendung einer Rechtsgrundlage nach Art 6 DSGVO. Überdies kann der Abschluss einer Geheimhaltungsvereinbarung geboten sein.

Schritt 6 – Mittel

Wer bestimmt die wesentlichen Mittel der Verarbeitung?
Jede Verarbeitung wird geprägt durch ihre „Mittel", dh die „Art und Weise, wie ein Ergebnis oder Ziel erreicht wird". Der Begriff „Mittel" bezeichnet nicht nur die technischen Methoden für die Verarbeitung personenbezogener Daten, sondern auch das „Wie" der Verarbeitung; dazu gehören Fragen wie „Welche Daten werden verarbeitet?", „Welche Dritte haben Zugang zu diesen Daten?", „Wann werden Daten gelöscht?" usw. [7].
Wer über die wesentlichen Mittel der Verarbeitung entscheidet, ist selbst Verantwortlicher, kann aber seinem Auftragsverarbeiter Spielräume bei der Auswahl der Mittel einräumen. Dieser Spielraum kann betreffend den Einsatz technischer Mittel sehr weit sein, z.B. beim externen Marketing, wo der Auftragsverarbeiter je nach zivilrechtlicher Vereinbarung über die eingesetzten Mittel entscheidet.
Entscheidet der Verantwortliche nicht allein über die technischen Mittel, so sollte er doch vollständig darüber informiert sein. Wenn ein Dienstleister dagegen Einfluss auf den Zweck hat, ist er selbst Verantwortlicher (s.o.).

Schritt 7 - Nutzungsrecht

Darf der Dienstleister die Daten zu eigenen Zwecken nutzen?
Hat der Dienstleister ein Recht Daten zu nutzen, d.h. zu eigenen bzw. von ihm definierten Zwecken für sich oder einen Dritten zu verwenden, ist er für diesen Verarbeitungsvorgang nicht Auftragsverarbeiter, sondern selbst Verantwortlicher – vgl. dazu oben unter Schritt 5 – Zwecke.
Das gilt nicht für die Nutzung eines anonymisierten Datenbestandes oder für statistische Auswertungen, beispielsweise im zur Verbesserung der Produkte des Dienstleisters, dies deshalb, weil anonymisierte Daten (d.h. solchen, die auf keinen Fall einer bestimmten oder bestimmbaren Person zugeordnet werden können) nicht dem Datenschutzrecht unterliegen.
Achtung: das bedeutet nicht, dass der Dienstleister auch zivilrechtlich die Befugnis hat, solche (anonymisierten) Auswertungen durchzuführen. Ob dies gestattet ist oder nicht, sollte sich aus dem Dienstleistungsvertrag erschließen.

Schritt 8 - Betroffenenrechte

Wer steht der betroffene Person Rede und Antwort?
Zentrales Element der Verpflichtungen des Verantwortlichen ist die Wahrnehmung der Rechte der betroffenen Personen. Das bedeutet, dass es die Verpflichtung des Verantwortlichen darstellt, betroffene Personen zu informieren, Auskunft aus Datenbeständen zu erteilen sowie insbesondere über Datenlöschungen und –sperren zu entscheiden.
Der Verantwortliche kann vertraglich den Auftragsverarbeiter beauftragen, hier bestimmte Standardschritte durchzuführen, z.B. im Namen des Verantwortlichen Auskünfte zu erteilen[8].
Kann der Dienstleister dagegen eigenständig entscheiden, wie im Falle einer Anfrage einer betroffenen Person mit dieser umgegangen wird, dh etwa bestimmen, welche Daten offengelegt werden und welche Daten antragsgemäß gelöscht werden oder nicht, so spricht das dafür, dass es sich beim Dienstleister nicht um einen Auftragsverarbeiter, sondern um einen eigenständigen Verantwortlichen handelt, weil ihm eine Befugnis zukommt, über die Verarbeitung von Daten selbst zu entscheiden.

Schritt 9 - Eindruck

[7] WP 167 der Art 29 –Datenschutzgruppe vom 16.2.2010

[8] Ist dies der Fall und kann der Dienstleister für den Verantwortlichen gegenüber den betroffenen Personen agierten, verbleibt das Risiko für nicht rechtskonformes Verhalten bestraft zu werden, selbstverständlich weiterhin beim Verantwortlichen.

Welchen Eindruck erweckt der Dienstleister nach außen?
Schließlich ist der Eindruck wichtig, den der Auftragsverarbeiter auf betroffenen Verkehrskreise, insbesondere betroffene Personen macht: tritt der Auftragsverarbeiter nach außen hin so auf, als wäre er hinsichtlich des Datenbestandes verfügungs- oder entscheidungsberechtigt, so kann sich daraus ergeben, dass er selbst Verantwortlicher ist, oder zumindest von der Datenschutzbehörde als solcher betrachtet und zur Verantwortung gezogen wird[9].
Aus dem Prinzip von Treu und Glauben und aus dem Transparenzgebot ergibt sich, dass der Verantwortliche in gebührender Weise offenzulegen ist, insbesondere damit betroffenen Personen ihre sich aus dem Datenschutzrecht ergebenden Rechte geltend machen können.

[9] Allenfalls in Form einer „gemeinsamen Verantwortung“ nach Art 26 DSGVO