DSGVO:
Verantwortliche und Auftragsverarbeiter

RA Dr Markus Frank, LLM

SEC4YOU Workshop 23.2.2018

FRANKLAW
OFFICE@FRANK-LAW.AT

RA Dr Markus Frank

Schwergewicht: Datenschutz-, Wirtschafts- und Immobilienrecht, Wien

Seit Anfang 2016: Überwiegende Tätigkeit in der umfassenden Beratung bei der Umsetzung der DSGVO-Anforderungen / Entwicklung und Einführung von Daten-Schutz-Management-Systemen

Ausbildner für DS-Recht bei Kursen für Personenzertifizierung zum „Information-Security Manager“ (CIS) seit 15 Jahren

EU-Data Protection and Privacy Rights (Zertifikat HELP - European Programme for Human Rights Education for Legal Professionals)

Jahrelange Erfahrung mit anderen Management-Systemen (Umwelt)

Dr. Markus FRANK, LL.M.
Neustiftgasse 3/5
A-1070 Wien
Tel: +43 1 523 44 02
Email: office@frank-law.at
Web: www.frank-law.at

FRANKLAW
OFFICE@FRANK-LAW.AT

Definitionen: Verantwortlicher und Auftragsverarbeiter

„Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke UND Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art 4 Abs 7 DSGVO).

„Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet (Art 4 Abs 8 DSGVO).

Folgen des Nicht-Abschlusses eines Vertrages

Unterlassung des Abschlusses

- eines Auftragsverarbeiter-Vertrages (Art 28) oder
- eines Vertrages mit dem gemeinsam Verantwortlichen (Art 26)

⇒ Verstoß gegen Verpflichtung zum Vertragsabschluss: Bußgeld bis zu € 10 Mio. oder 2 % des weltweiten Jahresumsatzes (Art 83 Abs 4 lit. a DSGVO)

FRANKLAW
OFFICE@FRANK-LAW.AT

Judikatur der Datenschutzbehörde zu DSG 2000 (ALT)

Webhosting: Das bloße Speichern fremder Daten ist ein Überlassen von Daten für die Erbringung eines Werks (Dienstleistung), wenn der Hoster über das Speichern im Sinne der Vermietung von Speicherplatz hinaus Leistungen wie die Erstellung einer Website (Webdesign) oder Service und Instandhaltung des gespeicherten Datenbestands übernimmt. Auch durch bloßes Speichern erfolgt Auftragsverarbeitung, wenn man den Weisungen eines für die Verarbeitung Verantwortlichen untersteht (Datenschutzkommission, GZ K120.819/006-DSK/2003).

Die Qualifikation eines Rechtsträgers als „Auftraggeber“ oder Dienstleister “ muss sich zunächst an den tatsächlichen Verfügungsverhältnissen orientieren.
Die … stellt nur den Zugang zu einem Datenbestand über das Internet zur Verfügung und nimmt die Entgeltverrechnung für den Zugang vor. Sie hat keine Verfügungsgewalt über den Inhalt der über ihr Internetportal dargebotenen Daten. Das ist entscheidend für die Rechtsstellung als Auftraggeber einer Datenanwendung. … ist daher im Hinblick auf diesen Datenbestand als datenschutzrechtlicher Dienstleister zu sehen.
Allfällige Weiterverwendungsrechte der … beziehen sich nicht auf die Darbietung der Daten unter dieser Bezeichnung auf der Webseite der Beschwerdegegnerin und wären als gesonderter Vertragsgegenstand zu qualifizieren. (K121.217/0021-DSK/2006)

Judikatur der Datenschutzbehörde zu DSG 2000 (ALT)

SWIFT ist Dienstleister für die Abwicklung der Überweisungsaufträge zwischen Bankinstituten durch eine Nachrichtenübermittlung. Jedoch ist eine Weiterleitung der Daten in die USA dazu nicht erforderlich. Diesbezüglich ist SWIFT deshalb Auftraggeber im Sinn von Art 2 lit d der Richtlinie 95/46/EG zu. (K121.245/0009-DSK/2007)

Bonitätsauskünfte: Der Bereitsteller eines Zugangsportals für Bonitätsdatenbanken ist Dienstleister für den, der die Bonitätsdaten zur Verfügung stellt. Die Einsichtnahme von Kunden des Bereitstellers ist Übermittlung der Daten an diese Kunden, die damit verantwortliche Auftraggeber für eine allfällige Weiterverwendung der Daten werden. (K121.339/0007-DSK/2008)

Dienstleister war auch, wer (Gesundheits-)Daten im Auftrag eines Verantwortlichen erhoben und bloß auf Papier festgehalten hat. (K210.583/0009-DSK/2008)

Ein Bestattungsunternehmen war Dienstleister hinsichtlich der Verarbeitung von Daten für Friedhofsverwaltung und Gebühreninkasso. Auftraggeber war die katholische Kirche in Österreich weil die Pfarre, der der Friedhof gehört, ihr zugerechnet wird. Die Pfarre ist zwar eigene Körperschaft, aber nicht als eigener Auftraggeber ins von der Datenschutzkommission geführte Datenverarbeitungsregister (DVR) eingetragen. (K121.842/0008-DSK/2012)

DSGVO: Auftragsverarbeitung?

Definition „Verantwortlicher“: … entscheidet über die Zwecke UND Mittel der Verarbeitung von personenbezogenen Daten.

ABER:

Dem Verantwortlichen wird üblich nicht bekannt, wie etwa ein Infrastruktur-Betreiber (z.B. UPC, Dropbox, Youtube, Appstore etc.) ihre Angebote technisch umsetzen -> Er entscheidet daher nicht über die „Mittel“ der Verarbeitung. -> Dennoch Auftragsdatenverarbeitung?

Art 29 Gruppe, WP 169, Opinion 1/2010 on the concepts of „controller“ and „processor“:

Ein Auftragsverarbeiter könnte „aufgrund allgemeiner Weisungen tätig sein, die in erster Linie die Zwecke betreffen und in Bezug auf die Mittel nicht zu sehr ins Detail gehen.“(WP 169, Seite 16).

Es ist sogar „durchaus möglich, dass ausschließlich der Auftragsverarbeiter über die technischen und organisatorischen Mittel entscheidet.“ (WP 169, Seite 17).

=> Eine Auftragsverarbeitung kann also auch dann vorliegen, wenn der Verantwortliche zwar über den Zweck entscheidet, bei den Mitteln aber nur einige wesentliche Aspekte vorgibt. Die nähere Ausgestaltung dieser Mittel hinsichtlich technischer oder organisatorischer Fragen kann dem Auftragsverarbeiter vorbehalten bleiben. (s. auch Bernhard Horn in Knyrim, DSGVO, S. 156 f)

FRANKLAW
OFFICE@FRANK-LAW.AT

Haftung des Verantwortlichen / Auftragsverarbeiters für Bußgeld oder Schadenersatz

Haftung für Bußgeld (Art 83 DSGVO):

- Verantwortlicher + Auftragsverarbeiter!
- Jeder nach seinem Verschulden und dem Grad seiner Verantwortung

Haftung für Schadenersatz gegenüber Betroffenen (Art82 DSGVO):

- Verantwortlicher + Auftragsverarbeiter!
- Solidarische Haftung bei gemeinsamer Verantwortung
- Auftragsverarbeiter haftet neben dem Verantwortlichen nur für Verletzung seiner eingeschränkten DSGVO-Pflichten (z.B. für Daten-Sicherheit gemäß Art 32, nicht aber etwa für Einhaltung der Datenschutz-Grundsätze gemäß Art 5, etwa Datenminimierung).

FRANKLAW
OFFICE@FRANK-LAW.AT

Weitere Beispiele: Infrastrukturbetreiber als Auftragsverarbeiter?

(1)Ein Webhoster (z.B. UPC) verarbeitet u.a. IP-Adressen und eindeutige Browserdaten der Seitenbesucher, um die Webseite des Seitenbetreiber (Verantwortlicher) an den Browser des Besuchers auszuliefern. Zweck der Verarbeitung für den Seitenbetreiber ist Kundenkommunikation, Selbstdarstellung, E-Commerce.

(2) Der Betreiber einer Infrastruktur zur unternehmensinternen Zusammenarbeit (z.B. Office oder Dropbox Business) verarbeitet die IP-Adressen, Nutzerdaten und Arbeitsergebnisse der Mitarbeiter des Verantwortlichen. Dadurch werden die Effektivität gesteigert und lassen sich Arbeitsprozesse komfortabel abwickeln (= Zweck des Verantwortlichen).

(3) Ein Betreiber einer Videoplattform (z.B. Youtube) verarbeitet IP-Adressen, Konsumverhalten und Interessen der Online-Zuschauer, damit die Inhalte des Content-Creator (Verantwortlichen) die Zuschauer erreichen und er damit Werbung verbreiten kann (=Zweck).

(4) Der Betreiber eines Appstores (z.B. Appstore von Apple oder Playstore von Google) vertreibt eine App (z.B. electronic banking) und erhebt Gerätekennungen, Downloadverhalten, Nutzungszeit und In-App-Kaufverhalten der App-Käufer. Der App-Store ermöglicht damit dem App-Anbieter, seine App kopiergeschützt zu vertreiben und die Attraktivität der App zu messen und zu steigern (= Zweck).

(siehe Dr. Malte Engeler, Telemedicus v. 24.11.2016, http://tlmd.in/a/3150)

Dr. Malte Engeler, Telemedicus v. 24.11.2016 (zur Rechtslage nach dt. BDSG zu Beispielen von Infrastrukturbetreibern als Dienstleister (1) – (4)):

> *Mit Blick darauf, dass in allen angeführten Beispielen die Datenverarbeitung für Zwecke der Verantwortlichen durchgeführt wird und diese sich bewusst für die technischen Mittel der jeweiligen Infrastrukturbetreiber entschieden haben, haften die Verantwortlichen für die Verarbeitungen ihrer Infrastrukturbetreiber.*

Haftung des Verantwortlichen für Handlungen des Auftragsverarbeiters?

DSGVO: Der Verantwortliche haftet mit Bußgeld und Schadenersatz

- für die weisungsgemäße Verarbeitung durch seinen Auftragsverarbeiter wie für eigene Verarbeitung (Art 24 i.V.m. Art 28 i.V.m. Art 82 und 83);.
- jedoch nicht grundsätzlich auch für Auftrags-Exzesse durch seinen Auftragsverarbeiter. Bestimmt der Auftragsverarbeiter entgegen diesen Weisungen selbst über Zwecke und Mittel der Verarbeitung, wird er selbst zum Verantwortlichen (Art 28 Abs 10 DSGVO).

DAHER:

Schließe Auftragsverarbeiter-Verträge mit Infrastrukturbetreibern mit klaren Weisungen des Verantwortlichen für die Verarbeitung!

ODER:

Prüfe alternative Auftragsverarbeiter, die bereit sind, einen solchen AV-Vertrag zu schließen!

Beispiele: Auftragsverarbeitung oder getrennt Verantwortliche

Beispiel Verantwortlicher beauftragt Rechtsanwalt:

- Unabhängigkeit des Rechtsanwalt gemäß Rechtsanwalts-Ordnung!
- RA entscheidet allein über Mittel der Verarbeitung!

-> Mandant und Rechtsanwalt sind getrennt Verantwortliche!
-> Keiner der beiden Verantwortlichen haftet datenschutzrechtlich für den anderen.

Beispiel Übermittlung der Zustelldaten von Waren-Verkäufer an Auslieferer:

- Auslieferer entscheidet üblich völlig selbständig über die Mittel der Verarbeitung

Beispiel: Fernwartung

Gemeinsam Verantwortliche

Beispiel: Zwei oder mehrere Verantwortliche in gemeinsamen IT-System:

- Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche (Art 26 Abs 1 DSGVO).
- Vgl. „Informationsverbundsystem“ gemäß DSG alt, wenn Verantwortliche in einem gemeinsamen IT-System auf eigene Daten Zugriff haben und auch auf solche Daten, die von anderen Verantwortlichen zur Verfügung gestellt wurden. Hingegen müssen „Gemeinsam Verantwortliche“ gemäß DSGVO nicht auch Zugriff auf die Daten der anderen haben.
- Vertrag für gemeinsam Verantwortliche: Vereinbarung in transparenter Form, wer welche Verpflichtungen gemäß DSGVO (z.B. Informationspflichten) erfüllt.

-> Solidarische Haftung aller gemeinsam Verantwortlichen: Die betroffene Person kann ihre Rechte im Rahmen dieser Vereinbarung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen (Abs 3).

Auftragsverarbeiter-Vertrag

Freier Dienstvertrag (Arbeitskraft wird zur Verfügung gestellt, keine persönliche Abhängigkeit)

Werkvertrag: Verpflichtung, ein bestimmtes Werk herzustellen. Eigene Planung, eigene Betriebsmittel, Haftung für Fehler des Werkes gegenüber Auftraggeber.

Besorgung von Aufträgen, Vollmacht, Ermächtigung

auch unentgeltlich (DSK zu GZ K121.217/0021-DSK/2006)

WICHTIG:

- Definition der Leistung bzw. des Werkes möglichst konkret beschreiben!
- Achte auf *wording*:
  - Er „schuldet“
  - Er “garantiert“
  - Er „unterstützt“ oder „berät“ oder „trägt bei“ …
- Kontrollbefugnisse detailliert klären
- Vergütung pauschal, nach Stunden, Erfolgshonorar, …
- Zurückbehaltungsrecht

FRANKLAW
OFFICE@FRANK-LAW.AT

Disclaimer

Die gegenständlichen Unterlagen sowie der darauf basierende Vortrag erheben keinen Anspruch auf Vollständigkeit. Trotz größtmöglicher Sorgfalt bei der Erstellung dieser Unterlagen kann eine Gewähr für Richtigkeit und Vollständigkeit nicht gegeben werden.

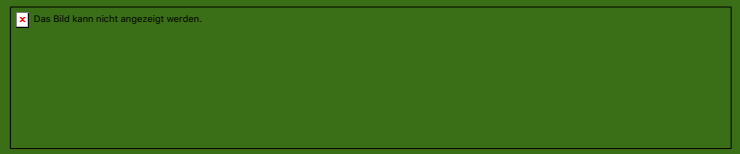
Die Unterlagen und der Vortrag können eine individuelle Beratung durch Rechtsanwälte, Steuerberater oder sonstige Spezialisten nicht ersetzen.

Eine Haftung aus der vorliegenden Präsentationsunterlage (auch als „nützlicher Link“ auf Webseiten Dritter) ist ausgeschlossen.

Die Überlassung der Präsentationsunterlage erfolgt nur für den internen Gebrauch des Empfängers bzw. des empfangenden Unternehmens. Eine Weitergabe an Dritte oder eine (auch nur auszugsweise) Veröffentlichung bedarf der vorherigen schriftlichen Zustimmung. Dies gilt auch für eine Bild- oder Ton-Aufzeichnung des Vortrags.

FRANKLAW
OFFICE@FRANK-LAW.AT

Danke für Ihre Aufmerksamkeit!



Dr. Markus Frank, Rechtsanwalt
Neustiftgasse 3/5, 1070 Wien
Tel. 01/523 44 02 (Fax 10)

FRANKLAW
OFFICE@FRANK-LAW.AT