von Rechtsanwältin **Elisabeth Keller-Stoltenhoff**

Auftragsdatenverarbeitung in Behörden: Was gilt es zu beachten?

Viele Behörden gehen immer mehr dazu über, ihnen anvertraute Daten (Mitarbeiter, Bürger, etc.) durch externe Dienstleister hosten oder im Rahmen von IT-Projekten verarbeiten zu lassen. Dies geschieht insbesondere dann, wenn die Leistungen durch eigene Mitarbeiter nicht erbracht werden können, da sie entweder besonders kostenintensiv oder besonders komplex sind oder einem schnellen Innovationszyklus unterliegen. Dies gilt in erster Linie für IT-Dienstleistungen.

Im Rahmen der Beratungstätigkeit der IT-Recht-Kanzlei stellte sich oft heraus, dass die Behörden nur sehr unzulänglich die durch das Bundesdatenschutzgesetz geforderten Auflagen bei der Auftragsdatenverarbeitung umsetzten. Dabei ist die Änderung und Verschärfung des Bundesdatenschutzgesetzes zu den Pflichten des Auftraggebers im Rahmen von Auftrags-datenverarbeitung bereits vor zwei Jahre in Kraft getreten.

Dieser Beitrag soll den Behörden helfen zu erkennen, wann Auftragsdatenverarbeitung vorliegt und darstellen, welche Maßnahmen in diesem Fall zu ergreifen sind.

Grundsätzlich gilt: Entschließt sich eine Verwaltung einen externen Dienstleister mit Tätigkeiten, die auch die Erhebung, Verarbeitung und Nutzung personenbezogener Daten beinhalten, zu beauftragen, müssen verschiedene rechtliche, technische und organisatorische Voraussetzungen des Datenschutzes erfüllt werden. Das Bundesdatenschutzgesetz (BDSG) regelt in seinem § 11 die sog. Auftragsdatenverarbeitung. Die Datenschutzgesetze der Länder enthalten ähnliche Vorschriften. Diese Vorschriften stellen formale, technisch-organisatorische und rechtliche Anforderungen auf, die eine öffentliche Stelle beachten muss, wenn sie personenbezogene Daten von einer anderen – öffentlichen oder nichtöffentlichen – Stelle erheben, verarbeiten oder nutzen lassen will.

Diese Anforderungen wurden durch die Änderung des Bundesdatenschutzgesetzes mit Wirkung vom 1. September 2009 präzisiert und zum Teil strenger gestaltet. Das Gesetz schreibt ausdrücklich vor, welche inhaltlichen Vorgaben in dem schriftlich zu erteilenden Auftrag in jedem Falle enthalten sein müssen. Je nach Konstellation können noch weitere Anforderungen in den Auftrag aufgenommen werden. Außerdem ist der Auftraggeber verpflichtet, sich vor Beginn der Datenverarbeitung und regelmäßig während der Durchführung des Auftrages beim Auftragnehmer von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen.

Werden dem Auftragnehmer personenbezogene Daten zu diesem Zweck überlassen, findet datenschutzrechtlich gesehen keine Übermittlung statt, da der Auftragnehmer nicht Dritter ist. Gegenüber den Bürgerinnen und Bürgern bleibt der Auftraggeber (also die Behörde, um deren Aufgabe es geht) voll dafür verantwortlich, dass mit ihren personenbezogenen Daten rechtmäßig umgegangen wird. Der Auftraggeber bleibt Herr der Daten. Dies setzt voraus, dass der Auftraggeber einen schriftlichen Auftrag erteilen muss, der Auftragnehmer nur im Rahmen der Weisungen seines Auftraggebers tätig werden darf und dass der Auftraggeber die erforderlichen Maßnahmen zur

Datensicherheit vorgeben muss. Der Auftraggeber hat das Recht und die Pflicht, sich jederzeit bei Kontrollen ein Bild zu machen, ob der Auftragnehmer korrekt arbeitet.

Oft besteht aber bei Behörden Unkenntnis darüber, dass Auftragsdatenverarbeitung im Sinne des §11 BDSG vorliegt. In diesem Fall kann die Behörde gemäß § 43 BDSG mit Geldbußen bis 50.000 € durch die Datenschutzbehörden belegt werden. Hierzu kommen peinliche Erwähnungen in der Presse und in Datenschutzberichten, verbunden mit dem Verlust des Vertrauens der Bürger, dass ihre Daten bei der öffentlichen Hand sicher und gesetzeskonform geschützt sind.

Jeder Behörde ist daher gut beraten, durch einen internen oder externen Datenschutzbeauftragten ermitteln zu lassen,

- in welchen Fällen in der Behörde Auftragsdatenverarbeitung vorliegt,
- ob in diesen Fällen mit den Dienstleistern den Datenschutzbestimmungen entsprechende Vereinbarungen abgeschlossen wurden,
- ob der Auftragnehmer nur im Rahmen der Weisungen des Auftraggebers tätig werden darf,
- ob der Auftraggeber die erforderlichen Maßnahmen zur Datensicherheit vorgegeben hat
- und ob der Auftraggeber die Einhaltung dieser technischen und organisatorischen Maßnahmen durch den Auftragnehmer zumindest zu Beginn der Auftragsdaten-verarbeitung überprüft hat.

1. Wann liegt Auftragsdatenverarbeitung vor?

Auftragsdatenverarbeitung liegt vor und damit der Anwendungsbereich des § 11, wenn personenbezogene Daten im Auftrag der verantwortlichen Stelle – also des Auftraggebers – durch eine andere Stelle erhoben, verarbeitet oder genutzt werden sollen.

1.1 Was ist ein personenbezogenes Datum?

Daten sind gemäß § 3 Abs. 1 BDSG **personenbezogen** , wenn sie Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) enthalten. Das heißt sie sind eindeutig einer bestimmten natürlichen Person direkt oder mittelbar zuordbar.

Beispiele für personenbezogene Daten:

- Ernst Keller hat blaue Augen.
- Erika Schmidt besitzt einen VW Golf.
- Der erste Kanzler der Bundesrepublik Deutschland war gebürtiger Kölner.
- Klaus Buranj ist am 01.01.1960 geboren.

Im ersten Beispiel wird die Angabe hat blaue Augen der Person Ernst Keller zugeordnet. Die Angabe hat blaue Augen wird dadurch zu einem personenbezogenen Datum. (Im Regelfall wird die Gesamtinformation *Ernst Keller hat blaue Augen*. als personenbezogenes Datum angesehen.)

Im zweiten Beispiel ist *besitzt einen VW Golf* das personenbezogene Datum. Ein personenbezogenes

Datum muss also nicht zwangsläufig ein körperliches Merkmal der Person sein. Es genügt ein Bezug zwischen der Person und einer Sache, einer anderen Person, einem Ereignis, einem Sachverhalt.

1.2 Abgrenzung zwischen Auftragsdatenverarbeitung und Funktionsübertragung

Nicht immer, wenn der Auftragnehmern mit personenbezogene Daten in Berührung kommt, liegt Auftragsdatenverarbeitung im Sinne des § 11 BDSG vor. Es kann sich auch um sogenannte Funktionsübertragung handeln. Diese Abgrenzung ist nicht immer leicht, daher soll hier zunächst ein kleiner Exkurs zur Abgrenzung von Auftragsdatenverarbeitung und Funktionsübertragung erfolgen.

1.2.1 Auftragsdatenverarbeitung

Bei der **Datenverarbeitung im Auftrag** wird nicht die Aufgabe selbst, zu deren Zweck die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten erfolgt, ausgelagert, sondern lediglich der zur Aufgabenerledigung erforderliche **Umgang mit den personenbezogenen Daten**. Der in Anspruch genommenen Serviceeinrichtung wird der Umgang mit den Daten nach Weisung und unter materieller Verantwortung des Auftraggebers übertragen. **Die datenschutzrechtliche Verantwortung für die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten verbleibt beim Auftraggeber.** Er schreibt die technischen und organisatorischen Maßnahmen zur Datensicherheit beim Auftragnehmer vor.

Erkennungsmerkmale für Auftragsdatenverarbeitung:

- Fehlende Entscheidungsbefugnis des Auftragnehmers,
- **Weisungsgebundenheit des Auftragnehmers bezüglich dessen, was mit den Daten geschieht,**
- **Umgang nur mit Daten, die der Auftraggeber zur Verfügung stellt; es sei denn, der Auftrag ist auch auf die Erhebung personenbezogener Daten gerichtet,**
- Ausschluss der Verarbeitung oder Nutzung der Daten zu eigenen Zwecken des Auftragnehmers,
- **keine (vertragliche) Beziehung des Auftragnehmers zum Betroffenen,**
- Auftragnehmer tritt (gegenüber dem Betroffenen) nicht in eigenem Namen auf.

1.2.2 Funktionsübertragung

Bei der **Funktionsübertragung** wird dagegen auch die der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zugrunde liegende Aufgabe ganz oder teilweise abgegeben. Die in Anspruch genommene Serviceeinrichtung erbringt - über die technische Durchführung des Umgangs mit personenbezogenen Daten hinaus - materielle Leistungen mit Hilfe der überlassenen Daten. Sie handelt hierbei eigenverantwortlich, auch im Sinne des Datenschutzrechts.

Erkennungsmerkmale für Funktionsübertragung:

- **Weisungsfreiheit des Dienstleisters bezüglich dessen, was mit den Daten geschieht,**
- **Überlassung von Nutzungsrechten an den Daten,**
- **eigenverantwortliche Sicherstellung von Zulässigkeit und Richtigkeit der Daten durch den Dienstleister, einschließlich des Sicherstellens der Rechte von Betroffenen (Benachrichtigungspflicht, Auskunftsanspruch),**
- Handeln des Dienstleisters (gegenüber dem Betroffenen) im eigenen Namen,
- **Entscheidungsbefugnis des Dienstleisters in der Sache.**

Liegt aber tatsächlich Auftragsdatenverarbeitung vor, gilt es Folgendes zu beachten:

2. Art des Auftrags

Der Umfang und die Zeitdauer des Auftrags spielen keine Rolle. Bei dem Auftrag handelt es sich nicht um einen Auftrag im Sinne des § 662 BGB – also um einen Auftrag zur unentgeltlichen Geschäftsbesorgung des Auftragnehmers - , sondern um einen Auftrag zur Verarbeitung von personenbezogenen Daten. Was unter „Verarbeitung“ zu verstehen ist, ergibt sich aus § 3 Abs. 4 BDSG.

Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

- Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,
- Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
- Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
- die Daten an den Dritten weitergegeben werden oder
- der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
- Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
- Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten

Also liegt immer dann ein Auftrag im Sinne des § 11 BDSG vor, wenn ein Auftragnehmer im Rahmen der vertraglichen Leistungen personenbezogene Daten der Mitarbeiter des Auftrag-gebers oder von anderen Dritten transferiert, speichert oder inhaltlich umgestaltet.

Um einen Auftrag gemäß § 11 BDSG handelt es sich zum Beispiel um folgende Leistungsvereinbarungen:

- Hosting auf Daten auf fremden Rechnern, Cloud Computing
- Outsourcing des Rechenzentrums (ganz oder teilweise).
- Papier- und Aktenvernichtung sowie die Vernichtung von Datenträgern.
- Externe Rechnungsbearbeitung / Buchhaltung.
- Datenmigration durch externe Dienstleister
- Arbeiten an Datenbanken im Rahmen von IT-Projekten
- Mitarbeiterbefragung, Versand von Newslettern durch externe Dienstleister.

- Beauftragung eines Callcenters für Kundensupport oder Kundengewinnung.
- Datenabgleichen der Verwaltungsbehörden durch externe Dienstleister
- Zugriff von Ermittlungsbehörden auf Internet- und Telefonverbindungsdaten durch externe Dienstleister
- Speicherung von Bewegungsdaten über Mautsysteme durch externe Dienstleister

Oft übersehen wird § 11 Absatz 5 des BDSG. Durch diese Vorschrift liegt auch dann Auftragsdatenverarbeitung im Sinne von § 11 BDSG vor, wenn im Rahmen der Wartung und Pflege ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. (Beispiele):

- Wartung von Servern und Computern mit Hilfe eines Remotezugriffs
- Parametrisierung oder Pflege von Software (Updates etc.), über die Zugriff auf personenbezogene Daten möglich ist
- Systemmigrationen

3. Welche Pflichten hat die öffentliche Verwaltung als Auftraggeberin

Oft übersehen öffentliche Verwaltungen, dass § 11 BDSG eine Vorschrift ist, die den Auftraggeber und nicht den Auftragnehmer zur Handlung zwingt. Der Auftraggeber hat die inhaltliche Gestaltung der Aufttragsdatenverarbeitung durch den Auftragnehmer nach Maßgabe des § 11 BDSG vorzugeben und zu kontrollieren.

Vernachlässigt der Auftraggeber diese Pflicht, drohen (wie oben bereits erwähnt) gemäß § 43 BDSG Geldbußen bis 50.000 €, die die Datenschutzbehörden verhängen und peinliche Erwähnung in Datenschutzberichten.

Welche Pflichten hat nun die Behörde, wenn eine Auftragsdatenverabeitung vorliegt?

Diese müssen schriftlich geregelt werden. Der Vertrag sollte gemäß § 11 BDSG **insbesondere** (!) im Einzelnen festlegen:

- den Gegenstand und die Dauer des Auftrags
- den Umfang, die Art und den Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen
- die nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen
- die Berichtigung, Löschung und Sperrung von Daten
- die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers

- mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen
- den Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags

Der Vertrag kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde geschlossen werden.

Wichtig ist, dass der Auftraggeber sich gemäß § 11 Abs.4 Satz 4 BDSG*vor Beginn* der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen durch Kontrollen überzeugt. Das Ergebnis ist zu dokumentieren.

Eine Erleichterung verschafft hier § 43 Abs.1, Nr.2b BDSG, da nur ordnungswidrig handelt, wer sich gemäß § 11 Absatz 2 Satz 4 nicht **vor Beginn** der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt. Erfolgt danach keine Kontrolle mehr, handelt die Behörde also zumindest nicht ordnungswidrig.

Eine Behörde sollte daher für die Auftragsdatenverarbeitung Musterverträge erarbeiten und alle Beteiligten dahingehend so schulen, dass sie

- erkennen können, dass ein Fall von Auftragsdatenverarbeitung vorliegt,
- einen Vertrag auf Grund des Musters mit dem Auftragnehmer abschließen können,
- und wissen, welche technischen und organisatorischen Maßnahmen sie zu fordern und wie zu überwachen haben.

Daher kann zur Sicherung der Umsetzung der datenschutzrechtlichen Vorgaben und zur Vermeidung von Bußgeldern und Imageschäden Behörde nur geraten werden, einen Mitarbeiter zum Datenschutzbeauftragten zu ernennen und entsprechend zu schulen oder einen Berater für Datenschutz oder einen Datenschutzbeauftragten hinzuzuziehen. Der externe Datenschutzbeauftragte hat den Vorteil, dass er im Zweifel für mögliche Versäumnisse (mangelhafte Umsetzung der Vorschriften) und fehlerhafte Beratung haftet.

4. Fazit

Entschließt sich eine Verwaltung einen externen Dienstleister mit Tätigkeiten, die auch die Erhebung, Verarbeitung und Nutzung personenbezogener Daten beinhalten, zu beauftragen, müssen verschiedene rechtliche, technische und organisatorische Voraussetzungen des Datenschutzes erfüllt werden. Das Bundesdatenschutzgesetz (BDSG) regelt in seinem § 11 die sog. Auftragsdatenverarbeitung. Die Datenschutz-gesetze der Länder enthalten ähnliche Vorschriften. Diese Vorschriften stellen formale, technisch-organisatorische und rechtliche Anforderungen auf, die eine öffentliche Stelle beachten muss, wenn sie personenbezogene Daten von einer anderen – öffentlichen oder nichtöffentlichen – Stelle erheben, verarbeiten oder nutzen lassen will.

Autor:
RAin Elisabeth Keller-Stoltenhoff
Rechtsanwältin