Verfahren heißen jetzt Verarbeitungstätigkeiten – Teil 4

Zusammenfassung: Da in den Anforderungen an die Beschreibung der Verarbeitungstätigkeiten auch die Auftragsverarbeiter einen aktiven Part spielen, werden im vorliegenden Praxistipp deren Anforderungen an die Beschreibungen der Verarbeitungstätigkeiten näher beleuchtet. Wichtig ist die Empfehlung, im eigenen Interesse etwas mehr zu dokumentieren, als der Gesetzgeber fordert, weil ansonsten in einigen Fällen (wie Betroffenenanfragen, Vorliegen einer Folgenabschätzung) aufwändige Nacharbeiten erforderlich werden könnten. Das Thema findet mit diesem Praxistipp nach nunmehr vier Teilen seinen Abschluss.

Kaum Änderungen bei bislang korrektem Datenschutz: Wer das Thema Datenschutz bislang schon ernst genommen hatte und die erforderlichen Tätigkeiten ausgeführt und dokumentiert hatte, der hat mit der Umstellung auf die DSGVO nur verhältnismäßig wenig Arbeit. Wer jedoch den Datenschutz bislang aus welchen Gründen auch immer vernachlässigte, der muss jetzt richtig ranklotzen. Das Beispiel der Beschreibung der Verarbeitungstätigkeiten von Auftragsverarbeitern zeigt dies besonders schön. Schon alleine um die teilweise umfangreichen vertraglichen Vorgaben bei der Auftragsverarbeitung zu erfüllen, bot es sich schon in der Vergangenheit an, die entsprechenden Verfahren als Auftragnehmer (Auftragsverarbeiter) zu beschreiben. Sonst wäre eine datenschutzkonforme Behandlung der Tätigkeiten kaum möglich gewesen.

BVT für Auftragsverarbeiter: Ein neuer Begriff für den Auftragnehmer bei der Auftragsdatenverarbeitung wurde mit der DSGVO ebenfalls geschaffen. Dieser heißt nun Auftragsverarbeiter, die Übersetzung von „processor“, dem Originalbegriff in der Verhandlungssprache Englisch. Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung (Art. 30 Abs. 2 DSGVO). Ein Verzeichnis zu allen Kategorien – so gilt es erst einmal Kategorien von Tätigkeiten der Verarbeitung zu identifizieren.

Neue Definition Auftragsverarbeiter: Die DSGVO versteht unter „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Dabei unterliegt zwar der Auftragsverarbeiter noch der Weisungsbefugnis des Verantwortlichen, die Weisungsgebundenheit ist – anders als im BDSG – nicht mehr entscheidendes Kriterium für das Vorliegen einer Auftragsverarbeitung. Man erinnert sich: Lag bei einer Verarbeitung durch einen Auftragnehmer keine Möglichkeit der Weisungsbindung vor, etwa bei arbeitsmedizinischer Betreuung (ein Arzt ist neben den geltenden Gesetzen nur seinem Gewissen und den standesrechtlichen Vorgaben verpflichtet, nicht den Weisungen eines Auftraggebers), so handelte es sich nicht um Auftragsdatenverarbeitung, sondern um Funktionsübertragung. Insofern hat der Gesetzgeber das Privileg der Auftragsverarbeitung ausgeweitet.

Funktionsübertragung gibt es nicht mehr: Die bisherige Unterteilung von Verarbeitung im Auftrag eines anderen in weisungsgebundene Auftragsdatenverarbeitung und die besonderen rechtlichen Bedingungen unterliegende Funktionsübertragung fällt weg. Anders ausgedrückt: Die Funktionsübertragung gibt es schon noch, sie läuft nun aber auch nach den Regeln der Datenverarbeitung im Auftrag ab. Demzufolge müssen auch Steuerberater und andere freiberuflich Tätige, für die bislang die Beschreibung der Verarbeitungstätigkeiten bei Funktionsübertragung anders geregelt war, die BVT nun anfertigen.

Auftragsverarbeiter müssen jetzt auch BVT der Auftragsverarbeitung beschreiben: Anders als bisher, als nur die verantwortliche Stelle die Verfahren der Auftragsdatenverarbeitung im Verfahrensverzeichnis zu beschreiben hatte, müssen nun die Auftragsverarbeiter auch die processing activities (Verarbeitungstätigkeiten) beschreiben.

Verbindliche Inhalte: Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

- den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, ein-

schließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO

Verkürzte BVT der Verantwortlichen: Vergleicht man die Anforderungen an die Beschreibung der Verarbeitungstätigkeiten für Verantwortliche (Art. 28 Abs. 1) mit denen für Auftragsverarbeiter, stellt man fest, dass letzter eine verkürzte Fassung der BVT des Verantwortlichen darstellen, allerdings aus der Sicht der Auftragsverarbeiter. Neu auch hier die Angabe des Datenschutzbeauftragten, der übrigens dann europaweit von Auftragsverarbeitern gestellt werden muss, wenn dies die Verantwortlichen im Vertrag über die Auftragsverarbeitung einfordern. Dieses Vorgehen ist Unternehmen, die einen Datenschutzbeauftragten bestellt haben, dringend zu empfehlen, denn das erleichtert die Zusammenarbeit zwischen Verantwortlichem und Auftragsverarbeiter erheblich.

Datenkategorien sind nicht gefordert, aber zu empfehlen: Da sich betroffene Personen künftig sowohl an die Verantwortlichen als auch an die Auftragsverarbeiter (und zwar alle!) wenden können, wenn sie eine Forderung nach Ersatz eines erlittenen Schadens haben, müssen auch die Auftragsverarbeiter ein Interesse daran haben, in den BVT die Personenkategorien und die Kategorien personenbezogener Daten aufgelistet zu haben, um im Zweifel rasch reagieren zu können. Gleiches gilt für den Fall einer Datenpanne, die als Data Breach Notification eine entsprechende Meldepflicht auslösen könnte, auch hier ist – um die Informationswege sicherzustellen – eine erweiterte Beschreibung in den BVT zu empfehlen.

Besondere Kategorien von Daten nach Art. 9 DSGVO: Werden vom Auftragsverarbeiter auch besondere Kategorien personenbezogener von Daten gemäß Art. 9 DSGVO verarbeitet, was regelmäßig mindestens im Bereich der Personaldienstleistungen oder bei Lohnabrechnung der Fall sein dürfte, ist darauf zu achten, dass in jedem Fall vor der ersten Verarbeitung die informierte Einwilligung der betroffenen Personen vorliegt. Allerdings stellt sich das oft erst während der Beschreibung der jeweiligen Verarbeitungstätigkeit heraus. Insofern empfiehlt es sich, in ein Template oder ein Formular zur Erfassung der BVT eine entsprechende Abfrage mit aufzunehmen. Normalerweise ist diese Abfrage schon in der Beschreibung des Verantwortlichen enthalten, so dass der Gesetzgeber dies nicht noch einmal explizit vom Auftragsverarbeiter fordert. Dennoch sollten auch Auftragsverarbeiter ein Interesse an dieser Information haben, denn sie haften gegenüber einer zu Schaden gekommenen betroffener Person in gleichem Maße wie die Verantwortlichen.

Allgemeine Beschreibung der TOMs: Diese Formulierung ist so allgemein gehalten, dass sie Fragen aufwirft. Vor allem, wenn die bisherigen technischen und organisatorischen Maßnahmen als Grundlage herangezogen werden. Hier gilt, dass bei bestehenden AV-Verhältnissen auch schon technische und organisatorische Maßnahmen beschrieben sind, die zunächst so lange weiterverwendet werden können, bis sich daran etwas inhaltlich oder substanziell ändert. Dann sind sie in die neue Fassung der TOMs nach Art. 32 Abs. 1 DSGVO umzuwandeln. Hier kann unter Umständen eine tabellarische Neugliederung Hilfe leisten. Auf der linken Seite stehen dabei die neuen TOMs, auf der rechten die alten, so zugeordnet, dass sie zum größten Teil den neuen Anforderungen entsprechen. Beispiel: die bisher verwendeten TOMs Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle entsprechen wohl im Wesentlichen der neuen Anforderung nach Vertraulichkeit, die alte Verfügbarkeitskontrolle (nomen est omen) der neuen Anforderung nach Verfügbarkeit.

Folgenabschätzung erforderlich oder nicht: Schließlich sollten in die BVT noch Hinweise aufgenommen werden, ob es sich um eine Verarbeitungstätigkeit handelt, bei der eine Folgenabschätzung durchzuführen ist oder nicht. Falls nicht, sollte hier die Begründung dafür notiert werden. Dies gilt für Verantwortliche und Auftragsverarbeiter in gleichem Maße. Handelt es sich um eine Tätigkeit, für die die Kriterien zutreffen, so können sich Verantwortliche und Auftragsverarbeiter bzw. deren Datenschutzbeauftragte hier auch kurzschließen. Ein Informationsaustausch kann hier unnötige Mehrarbeit vermeiden helfen.

Fazit: Die Anforderungen an die Beschreibungen der Verarbeitungstätigkeit sind erfüllbar, erfordern aber eine Struktur, um das Thema ohne allzu großen Aufwand abarbeiten zu können. Wer schon bisher Verfahrensbeschreibungen intensiv geführt hat, wird mit den neuen Verarbeitungstätigkeiten keine allzu großen Probleme haben. Wer jedoch bisher nur wenig oder gar nichts vorliegen hat, der sollte sich sputen. Spätestens ab 25. Mai 2018 gelten die neuen Anforderungen und Bußgelder ohne Einschränkung.

Eberhard Häcker, Ensdorf

Der Autor Eberhard Häcker ist Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und seit vielen Jahren als Externer Datenschutzbeauftragter und Datenschutzberater tätig. Seine Fachaufsätze erscheinen regelmäßig in unterschiedlichen Publikationen. Außerdem ist er Geschäftsführer der HäckerSoft GmbH, die unter anderem mit der Datenschutzsoftware DATSIS und der Lernplattform Optilearn (Pflichtschulungen für Datenschutzbeauftragte) am Markt aktiv ist. Sein Lieblingsprojekt ist datenschutzkabarett.de.