Verfahren heißen jetzt Verarbeitungstätigkeiten – Teil 1

Zusammenfassung: Auch wenn bisher schon Verfahrensbeschreibungen vorliegen, müssen diese an die neuen Anforderungen des europaweit gültigen Datenschutzes nach EU-DSGVO bis 25. Mai 2018 angepasst werden. Jeder Verantwortliche muss künftig Beschreibungen der Verarbeitungstätigkeiten vorliegen haben. Neu ist auch, dass auch Auftragsverarbeiter solche BVTs führen müssen. Dabei sind neben den Personendaten von Vertretern des Verantwortlichen (das Unternehmen ist Verantwortlicher, die Geschäftsführung gehört zu den Vertretern des Verantwortlichen) auch Datenschutzbeauftragte einzutragen. Die Zwecke sind genau zu definieren, dazu müssen Datenschutzbeauftragte frühzeitig in die Prozessplanung eingebunden werden. (Teil 2 folgt).

Der Praxisfall: Alles neu macht der Mai 2018. Seit Mai 2016 ist sie in Kraft, ab dem 25. Mai 2018 erlangt die EU-DSGVO Gültigkeit. Das liegt an der zweijährigen Übergangsfrist, die diese europäische Verordnung vorsieht. Waren bisher die Verfahrensbeschreibungen schon das Herzstück des betrieblichen Datenschutzes, wird das künftig mit den Verarbeitungstätigkeiten, wie sie jetzt heißen, erst recht so sein. Bis zum 25. Mai 2018 sind die vorliegenden Verfahrensbeschreibungen (VB) in in Beschreibungen der Verarbeitungstätigkeiten (BVT) umzuwandeln. Dabei sind einige neue Anforderungen zu beachten, die von Datenschutzbeauftragten einige Änderungen verlangen. Die Zeit läuft. Wer bisher beispielsweise schon 80 Verfahren beschrieben hatte, muss, sofern mit der Anpassung erst jetzt gestartet wird, jeden Monat zehn Verarbeitungstätigkeiten prüfen und umschreiben. Das ist ein ehrgeiziges Unterfangen – die Praxis droht den Datenschutz zu überholen.

Wer hat`s zu führen? Jeder Verantwortliche! „Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen“ (Artikel 30 EU-DSGVO). Die EU-DSGVO verlangt die Beschreibung der Verarbeitungstätigkeiten (BVT) **erst ab einer Beschäftigtenzahl von 250**, aber nur, wenn bei der Verarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen vorliegt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien eingeschlossen wird. Aus langjähriger Erfahrung kann ich hier sagen, dass diese Voraussetzungen in keinem Unternehmen vorliegen dürften – die Grenze von 250 Beschäftigten wird in der Praxis keine oder nur äußerst selten Anwendung finden. Klartext: Jeder Verantwortliche (jedes Unternehmen) muss ran.

Besser von Prozessen als von Verarbeitungstätigkeiten sprechen: Der Begriff Verarbeitungstätigkeiten ist nicht glücklich gewählt. Alleine schon ein Blick in die englischsprachige Fassung der EU-DSGVO (DPGR) zeigt, dass dort von „processes“ die Rede ist. Die deutsche Übersetzung hätte demzufolge „Prozesse“ lauten sollen, zumal in den Unternehmen dieser Begriff eh schon geläufig ist. Kein Mensch spricht von der Verwaltung von Verarbeitungstätigkeiten, sondern von Prozessmanagement. Leider hat hier der Datenschutz wieder den Stempel des Exoten abbekommen. Daher wird in den folgenden Beiträgen zu den BVTs eher von Prozessen als von Verarbeitungstätigkeiten die Rede sein.

Verantwortlicher oder Auftragsverarbeiter? Neu ist in der EU-DSGVO auch, dass zwischen Verantwortlichen und Auftragsverarbeitern unterschieden wird. Im Art. 30 Abs. 1 EU-DSGVO stehen die Anforderungen an die BVT bei Verantwortlichen, in Abs. 2 die an die Auftragsverarbeiter. Das ist insofern von Bedeutung, weil die Auftragnehmer bei der Auftragsdatenverarbeitung (jetzt Auftragsverarbeiter), bislang ja nicht als Verantwortliche eingestuft wurden (ADV war Privilegierung bei der Datenverarbeitung) und daher nach dem Wortlaut des BDSG nicht verpflichtet waren, die Verfahrensbeschreibungen für die im Auftrag erfolgte Verarbeitung von personenbezogenen Daten vorzunehmen. Dass dies zumeist in den Verträgen über Auftragsdatenverarbeitung vorgegeben war, steht auf einem anderen Blatt. Fest steht, dass dies nun ab dem 25. Mai 2018 verpflichtend ist.

Daten zu Verantwortlichen in den BVTs: Zunächst sind Namen und Kontaktdaten des Verantwortlichen zu nennen. Das waren bisher die verantwortliche Stelle sowie die Leiter oder andere Personen. Entsprechend sind in den neuen BVTs auch die eventuell gemeinsam Verantwortlichen sowie des Vertreters des Verantwortlichen aufzuführen. Da es vor allem in größeren Unternehmen hier immer wieder zu Wechseln kommen kann, empfiehlt es sich, die BVTs mit einem Vorblatt (oder einer zentralen Datei) zu versehen, wo die aktuell Verantwortlichen benannt sind. So müssen nicht bei jeder Umfirmierung oder bei jedem Wechsel in der Geschäftsführung alle BVTs neu ausgedruckt werden.

Datenschutzbeauftragter ist zu nennen: Neu ist außerdem, dass in der EU-DSGVO gefordert wird, dass der „etwaige“ Datenschutzbeauftragte in der BVT zu benennen ist. Dafür ist der Leiter IT herausgefallen, der in den Verfahrensbeschreibungen (VB) des BDSG noch zu

benennen war. Dennoch ist diese Information für Datenschutzbeauftragte wichtig, vor allem für externe Datenschutzbeauftragte, die nicht ständig vor Ort sind und Veränderungen bei der IT-Leitung nicht immer gleich mitbekommen. Werden dann Beschreibungen der Verarbeitungstätigkeiten aufgenommen und dort steht nach einem möglichen Wechsel der IT-Leitung noch der alte Name, dann sagen das die Gesprächspartner sofort und die erforderlichen Schritte können gemacht werden (Gespräch mit dem neuen IT-Leiter, Aufnahme oder Anpassung der technischen und organisatorischen Maßnahmen usw.)

Zweck der Verarbeitung: Dieses Thema ist nicht neu. Schon in den Verfahrensbeschreibungen nach § 4e BDSG waren die Zwecke anzugeben. Dennoch lohnt sich eine erneute Betrachtung der bisher schon gemachten Angaben, erstens weil die Erlaubnistatbestände, die eine Verarbeitung personenbezogener Daten zulassen, in der EU-DSGVO an die technische und gesellschaftliche Entwicklung angepasst wurden und zweitens künftig eine Zweckänderung während einer laufenden Verarbeitungstätigkeit nur mit erheblichem Aufwand vorgenommen werden kann. Es ist davon auszugehen, dass die Aufsichtsbehörden bei möglichen Kontrollen oder bei der rechtlich gebotenen Einsichtnahme in die BVTs genau auf die dort angegebenen Zwecke achten werden. Dass in der Folge die Realität der Verarbeitung mit den in der BVT angegebenen Zwecken genau abgeglichen wird, davon ist auszugehen.

Keine „Vorratszwecke“: Andererseits sollten in der Verarbeitungstätigkeit auch nur die Zwecke angegeben werden, die aktuell benötigt werden. Nach dem Motto „Vielleicht können wir das ja auch noch für den einen oder anderen Zweck brauchen“ einfach zusätzliche Zwecke quasi auf Vorrat anzugeben, obwohl sie aktuell nicht vorgesehen sind, ist umgekehrt auch nicht statthaft, wenn es hierfür noch nicht einmal vage Absichten gibt. Ein Prozess kann zwar durchaus auf eine Entwicklung über einen längeren Zeitraum angelegt sein, aber dann muss es konkrete Pläne geben.

Prozesse noch besser planen und modellieren Durch die EU-DSGVO müssen Datenschutzbeauftragte noch intensiver in die organisationsinternen Prozesse eingebunden werden als dies früher der Fall war. Nur wer Prozesse sauber plant, kann schon zu Beginn der Verarbeitungstätigkeit genau angeben, für welche Zwecke die personenbezogenen Daten im Verlauf des Prozesses benötigt werden. Dies stellt auch weitere Anforderungen an eine genaue und strukturierte Prozessplanung. Das ist aber kein Fehler, sondern wird der Strukturierung der Unternehmensabläufe sehr zugute kommen. Auch hier wieder ein Beispiel, wie guter Datenschutz ein Unternehmen voranbringen kann.

Verarbeitungstätigkeiten prüfend begleiten: Aus dem bisher Gesagten folgt, dass der Datenschutz schon in der Planung eines Prozessablaufs eingebunden werden sollte. Je früher Datenschutz beachtet und eingebunden wird, desto stringenter werden die Prozessabläufe geplant. Wenn die BVT fertiggestellt ist, sollte ein Folgetermin zur Überprüfung der Einhaltung der Prozessabläufe vereinbart werden. Hier werden mit großer Wahrscheinlichkeit Abweichungen von den ursprünglich vorgesehenen Abläufen zu erkennen sein, denn Prozesse sind dynamisch und können sich immer wieder ändern. Diese Änderungen müssen dann auch auf Konformität mit den Vorgaben des Datenschutzrechts geprüft werden. In der Folge sollten in regelmäßigen Abständen die BVT auf Vollständigkeit und Aktualität geprüft werden. Bei Bedarf sind dann auch die erforderlichen Anpassungen vorzunehmen.

Rechtsgrundlagen angeben: Es genügt jedoch nicht alleine, die Zwecke der geplanten Verarbeitungstätigkeit abzugeben. Vielmehr sollte auch geprüft werden, ob für jeden Zweck der Verarbeitung eine Rechtsgrundlage vorhanden ist. Hier sind die EU-DSGVO und das Datenschutz-Anpassungs- und-Umsetzungs-Gesetz (DSAnpUG-EU) zu Rate zu ziehen. Dann gelten weiter die ca. 300 vorrangigen nationalen Gesetze, in denen Regelungen zum Datenschutz, abweichend von der EU-DSGVO (nur verschärfend!) enthalten sind (beispielsweise der Sozialdatenschutz in den Büchern des SGB).

Erfordernis der Folgenabschätzung prüfen: Wenn die Rechtsgrundlagen nicht eindeutig geklärt sind, ist in jedem Fall sofort zu prüfen. ob eine formale Folgenabschätzung nach Art. 35 EU-DSGVO vorzunehmen ist. Da dies – anders als bisher – nicht mehr vorrangig eine Aufgabe des Datenschutzbeauftragten ist, sondern des „Verantwortlichen“, hat in diesem Fall der Verantwortliche die Initiative zu ergreifen. Dazu muss er zuerst informiert werden – und kann seinerseits den Datenschutzbeauftragten, der ja in Deutschland wie zuvor geregelt ist, hinzuziehen und ihm diese Aufgabe übertragen.

Dokumentieren: Die BVTs sind schriftlich anzufertigen und revisionssicher aufzubewahren, damit sie bei möglichen Kontrollen vorgelegt werden können.

Hinweis: Mit DATSIS liegt bei der HäckerSoft GmbH eine Software vor, die bei der Anfertigung der BVT nach den neuen Vorgaben eine große Unterstützung ist.

Nähere Informationen unter

info@haeckersoft.de oder unter www.datsis.de

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.