Verfahren heißen jetzt Verarbeitungstätigkeiten – Teil 2

Zusammenfassung: Bei der Beschreibung der Verarbeitungstätigkeiten gilt es auch, die betroffenen Personen und die diese betreffenden Daten zu beschreiben. Kurz: Um wen geht es und was wird verarbeitet? Gleiches gilt für die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen. Kurz: wer bekommt die Daten oder wer könnte sie bekommen? Hier muss sehr sorgfältig vorgegangen werden, denn die BVT bildet bei Betroffenenanfragen die Grundlage für die Ermittlung der Daten, die im jeweiligen Prozess gespeichert und gegebenenfalls weitergegeben wurden. Unsauberes Arbeiten kann sich hier bei Fehlern in der Betroffeneninformation bitter rächen.

Der Praxisfall: Anfrage einer Aufsichtsbehörde an ein mittelständisches Unternehmen, ob Daten in die USA übermittelt werden und wenn ja, auf welcher Rechtsgrundlage das geschieht. Ein Blick in die Verfahrensbeschreibungen, dort unter der Rubrik „Übermittlung in Drittländer“ brachte zunächst eine Fehlanzeige. Zur Sicherheit befragte der Datenschutzbeauftragte noch einmal die IT. Dort stellte sich dann heraus, dass zwar (im Selbstverständnis der IT) „keine Daten übermittelt werden“, aber ein von allen Standorten (auch USA) aus erreichbares zentrales Datenaustauschsystem vorgehalten wurde, in dem auch die Namen und Kontaktdaten der Verfasser der veröffentlichten Beiträge, Damit lag der Tatbestand der Übermittlung vor, die entsprechenden Angaben in den Verfahrensbeschreibungen wurde ergänzt. Jetzt sind sie aktuell, bei der Überführung in die Verarbeitungstätigkeiten kann zumindest in diesem Bereich nichts mehr schiefgehen.

Betroffene Personen: In den Verfahrensbeschreibungen nach BDSG und anderen relevanten datenschutzrechtlichen Vorschriften waren „folgende Angabe zu machen: (5.) eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien“. Derr Wortlaut der EU-DSGVO ist nahezu identisch. Hier wird in Art. 30 Abs. 1c „eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten“ eingefordert. Statt von „betroffenen Personengruppen“ im BDSG spricht die EU-DSGVO von „Kategorien betroffener Personen“. Die alte Formulierung war schwammiger – was genau sind „betroffene Personengruppen“? Gut, in einem Verfahren, bei dem Beschäftigtendaten verarbeitet werden, konnte die „betroffene Personengruppe“ zunächst einmal aus Beschäftigten bestehen. Genauso konnten Leiharbeitnehmerinnen und Leiharbeitnehmer beteiligt sein. Oder es konnten Bewerberinnen und Bewerber sein, bei Assessements auch die „betreuenden Dienstleister“.

Kategorien betroffener Personen: Die wichtigsten Personenkategorien dürften sich unter Beschäftigten, Bewerbern, Kunden, Lieferanten, Patienten usw. finden. Wie das vorhergehende Beispiel zeigt, kann das aber immer noch weiter unterteilt werden, was vor allem dann von Bedeutung ist, wenn bei Kunden zwischen B2B- und B2C.Kunden zu unterscheiden ist, oder wenn zu Beschäftigten bzw. Arbeitnehmern auch noch Leiharbeitnehmerinnen oder selbstständige Dienstleister mit demselben Aufgabenspektrum dazukommen. Es empfiehlt sich daher, diese Kategorien so exakt wie möglich zu beschreiben. Sonst kann es geschehen dass eine ganze Gruppe vergessen wird. Damit wäre die Beschreibung der Verarbeitungstätigkeit unvollständig.

Kategorien betroffener Daten: In den meisten Fällen dürfte es sich hier zum einen um so genannte Stammdaten und zum anderen um dazukommende prozessspezifische Daten handeln. Betrachte man beispielsweise Verarbeitungstätigkeiten aus dem Bereich der Personalverwaltung, so sind einige Stammdaten in jedem nahezu jedem Personalprozess vorhanden, ergänzt um die Daten, die spezifisch für die Verarbeitungstätigkeiten sind. Betrachtet man beispielsweise die Verarbeitungstätigkeit „Lohnpfändungen“, so sind hier naturgemäß die erforderlichen Stammdaten wie Name, Adresse usw. im Prozessablauf enthalten. Hinzu kommen dann noch die Daten, die durch die konkrete Lohnpfändung erforderlich werden.

Kategorien von Empfängern: In Art. 30 Abs. 1d EU-DSGVO fordert der Gesetzgeber als eine der Pflichtangaben beim Verzeichnis der Verarbeitungstätigkeiten „die Kategorien von Empfängern (zu nennen), gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen“. Diese zu kategorisieren ist zunächst nicht weiter schwierig. Zu beachten ist, dass hier nicht von „Dritten“ die Rede ist, als logische Konsequenz daraus müssen auch interne Stellen oder Auftragsverarbeiter berücksichtigt werden.

Interne Stellen: Solange personenbezogene Daten ausschließlich von denjenigen Personen verarbeitet werden, die direkt bei der Verarbei-

tungstätigkeit beteiligt sind, ist relativ leicht zu prüfen, ob die Datenschutzbestimmungen der EU-DSGVO eingehalten werden. Allerdings gibt es auch interne Stellen, an die personenbezogene Daten weitergeleitet und dort auch verarbeitet werden. Ein klassisches Beispiel ist Controlling. Hier müssen zwangsläufig Prozesse geprüft werden, bei denen auch personenbezogene Daten betroffen sind. Somit sind zunächst die internen Stellen zu ermitteln, wenn die Kategorien von Empfängern in das Verzeichnis der Verarbeitungstätigkeiten eingetragen werden.

Konzerninterne Stellen: Was beim Verzeichnis von Verarbeitungstätigkeiten oft vergessen wir, ist die Weiterleitung von personenbezogenen Daten an Schwesterunternehmen im selben Konzern. Insbesondere dann, wenn sich die verbundenen Unternehmen dieselben Räumlichkeiten teilen, wird die Weiterleitung von Daten an eine Kollegin, die in einem Büro über den Flur arbeitet, rein rechtlich aber beim verbundenen Unternehmen beschäftigt ist, nicht als Weiterleitung an einen Empfänger im Sinne der hier untersuchten Stellen erkannt. Daher werden solche Weiterleitungen bei den Beschreibungen der Verarbeitungstätigkeiten oft übersehen. Erschwerend kann hinzukommen, dass sich die Empfänger, obwohl konzernintern, in einem Drittland befinden. Faktisch ist das aber eine Offenlegung von personenbezogenen Daten an andere Empfänger, und diese muss hier mit aufgelistet werden.

Konzerninterne Stellen in Drittländern: Wenn konzerninterne Schwesterunternehmen oder das Mutterunternehmen nicht als eigene Stelle betrachtet werden, dann dürfte auch die gesonderte Betrachtung des Falles, dass sich diese verbundene Organisation in einem Drittland außerhalb der EU befindet, vermutlich auch eher unter den Tisch fallen. Das kann spätestens dann problematisch werden, wenn personenbezogene Daten dorthin übermittelt werden und „übersehen“ wird, dass dafür eine belastbare Rechtsgrundlage vorhanden sein muss. Basiert eine derartige Übermittlung noch auf einem Safe Harbor Abkommen, dann muss sehr rasch reagiert werden, denn dieses Abkommen ist vom EuGH für ungültig erklärt worden. Selbst das Nachfolgeabkommen Privacy Shield steht auf tönernen Füßen, denn auch gegen dieses ist eine Klage beim EuGH eingereicht worden. Experten rechnen auch hier damit, dass dieses Abkommen kassiert wird. Bleiben noch die Standardverträge der EU-Kommission, aber die sind sehr umfangreich und von daher nicht einfach anzuwenden.

Rechtsgrundlage sicherstellen: Auf alle Fälle muss für die Übermittlung personenbezogener Daten auch innerhalb eines Konzerns oder einer Unternehmensgruppe eine Rechtsgrundlage vorliegen. Was viele nicht beachten: auch das Bereitstellen von Daten zum Abruf stellt eine Datenverarbeitung dar. Wird beispielsweise ein zentraler SharePoint betrieben, über den intern verfasste technische Dokumente von einem verbundenen Unternehmen abgerufen werden können, und dort sind personenbezogene Daten angefügt (Name, Mailadresse und Telefonnummer des Verfassers), liegt schon eine Datenübermittlung in so genannte unsichere Drittstaaten vor, die mit einer entsprechenden Rechtsgrundlage abgesichert sein muss.

Öffentliche Stellen: Sodann ist eine weitere Kategorie von Empfängern die der öffentlichen Stellen. Beispiele hierfür sind Krankenkassen und Finanzbehörden im Zusammenhang mit der Personalverwaltung und der Lohn- und Gehaltsabrechnung. In aller Regel liegen bei Übermittlungen personenbezogener Daten an öffentliche Stellen einschlägige gesetzliche Regelungen zugrunde. Diese gilt es im Zusammenhang mit den Zwecken der Verarbeitung zu ermitteln und zu dokumentieren.

Nicht-öffentliche Stellen: Übermittlungen an nicht-öffentliche Stellen sind die nächste Kategorie, auf die sich die Beschreibungen der Verarbeitungstätigkeiten beziehen müssen. Hier ist zu unterscheiden zwischen nicht-öffentlichen Stellen, an die Daten zur Erfüllung eines Vertrags mit dem Betroffenen weitergeleitet werden und solchen Stellen, die als Auftragsverarbeiter tätig werden (wie schon gesagt, der Gesetzestext spricht bei den zu nennenden Empfängern nicht von Dritten, also ist die Vorgabe der Nennung der Stellen, an die weitergeleitet wird, auch für Auftragsverarbeiter anzuwenden).

Weitergabe in der Verarbeitungskette: Auch die Weitergabe von personenbezogenen Daten nach einer Anreicherung mit weiteren Informationen ist hier zu beachten. Solche Verarbeitungen sind hier ebenfalls zu ermitteln und in die Beschreibung der Verarbeitungstätigkeit aufzunehmen. Wird beispielsweise eine Agentur beim Betrieb der Homepage tätig, wo die Kunden auf dem entsprechenden Portal Änderungen bei ihren Stammdaten eingeben können, liegt ein solcher Fall möglicherweise schon vor. An dieser Stelle kommt es nicht darauf an, ob die Kunden wissen, dass sie auf der Seite eines Dritten sind oder vermuten, dass sie noch bei ihrem eigentlichen Vertragspartner verbunden sind. Entscheidend ist, dass eine andere nicht-öffentliche Stelle Daten im Rahmen der Verarbeitungstätigkeit übermittelt bekommt.

Softwarewartung kann Übermittlung an nicht-öffentliche Stellen sein: Auch bei Wartung von Software kann es sich um Übermittlung an nicht-öffentliche Stellen handeln.

Zumindest dann, wenn bei der Wartung ein Zugriff auf personenbezogene Daten im Rahmen der Wartungsarbeiten nicht ausgeschlossen werden kann. Dass es sich dabei auch um Auftragsdatenverarbeitung handelt, soll hier nicht weiter vertieft werden, kann aber eine der neuen Erkenntnisse durch die Beschreibung der Verarbeitungstätigkeit sein. Hier ist wichtig, dass diese Fälle bei der Beschreibung der Verarbeitungstätigkeit nicht vergessen werden.

Ausblick: Im Folgenden dritten Teil des Praxisbeitrags geht es unter anderem um Löschkonzepte und technische und organisatorische Maßnahmen.

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.