Verfahren heißen jetzt Verarbeitungstätigkeiten – Teil 3

Zusammenfassung: Da in den Beschreibungen der Verarbeitungstätigkeiten bzw. den Prozessbeschreibungen auch Hinweise auf einen möglichen Datenexport enthalten sein müssen, muss geklärt werden, ob, und wenn ja, basierend auf welcher Rechtsgrundlage, diese Datenübermittlungen erfolgen. Außerdem sollten Hinweise auf Löschungen vorhanden sein. Daher ist ein generisches Löschkonzept zu erstellen. Auf dessen Basis wird dann für den Fachbereich oder gar für die einzelne Verarbeitungstätigkeit ein spezifisches Löschkonzept erstellt und in der Prozessbeschreibung erläutert.

Internationale Übermittlung: Auf den ersten Blick antworten bei der Aufnahme der Beschreibungen der Verarbeitungstätigkeiten viele Prozessverantwortliche auf die Frage, ob Daten international weitergegeben werden, mit einem erstaunten „Nein, natürlich nicht!“ Bei näherem Überlegen stellt sich dann doch immer wieder heraus, dass sehr wohl Übermittlungen in Drittstaaten, auch außerhalb der EU, stattfinden. Das ist beispielsweise schon der Fall, wenn assoziierten Unternehmen außerhalb der EU ein Zugriff auf einen SharePoint gewährt wird und dabei auch die Namen und Kontaktdaten der Verfasser oder Ansprechpartner für Rückfragen aufgeführt sind. Werden Daten zum Abruf bereitgehalten, handelt es sich um eine Übermittlung.

Innerhalb der EU: Übermittlungen innerhalb der EU, also innerhalb des Geltungsbereichs der EU-DSGVO sind unkritisch. Zwar muss die Berechtigung zur Übermittlung generell vorliegen, aber davon wird hier einfach einmal ausgegangen. Dann gibt es hier keine weiteren Einschränkungen. Zur Datenübermittlung genügt ein Vertrag über Datenverarbeitung im Auftrag, wie man ihn innerhalb Deutschlands auch abschließen kann. Klartext: Übermittlungen, die innerhalb Deutschlands erlaubt wären, sind auch innerhalb der EU mir derselben Vertragsgrundlage grundsätzlich erlaubt. Auch die Pflichten im Zusammenhang mit dem Vertrag sind dieselben. Neu ist, dass Verantwortlicher und Auftragsverarbeiter nicht mehr über- und untergeordnet, sondern gleichrangig sind. Doch das soll an anderer Stelle näher erklärt werden.

Außerhalb der EU in assoziierten Ländern und EWR: Die EU hat mit einer ganzen Reihe von Staaten Abkommen geschlossen, die ein einheitliches Datenschutzniveau zwischen dem jeweiligen Drittland und der EU sicherstellt. Dazu gehören beispielsweise die Schweiz und Norwegen, für die nun jedoch die Erneuerung der Abkommen nach den Standards der EU-DSGVO bevorstehen. Bis zum 24.Mai 2018 können Daten, die innerhalb der EU weitergegeben werden dürfen, auch in diese Staaten weitergegeben werden. Ab dem 25. Mai 2018 kann eine Datenweiterleitung in das Drittland weiterhin erlaubt sein, vorausgesetzt, das betreffende Land hat seine Datenschutzgesetzgebung an die Standards der EU-DSGVO angepasst. Nur dann sind nämlich die Voraussetzungen weiter gegeben, unter denen das betreffende Land ein sicheres Drittland ist. Beide Länder haben erklärt, dies tun zu wollen.

Datenübermittlung in die USA per Privacy Shield: Nachdem im Oktober 2015 das Safe Harbor Abkommen durch den Europäischen Gerichtshof kassiert wurde, fanden sich zahlreiche Unternehmen plötzlich in der misslichen Lage, keine gültige Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA mehr zu haben. Schon beinahe hektisch verhandelten in der Folge die USA und die EU über ein Nachfolgeabkommen. Dieses wurde mit Privacy Shield ins Leben gerufen. Wenn mit einem US-amerikanischen Unternehmen Datenaustausch erfolgen soll, muss das Unternehmen sich den Regeln des Privacy-Shield-Abkommens unterwerfen. Unternehmen, die dem Abkommen beitreten, verpflichten sich zur Einhaltung angemessener Datenschutzregeln und zu deren Veröffentlichung, sodass damit eine Durchsetzbarkeit nach US-amerikanischem Recht gewährleistet wird. Betroffene sollen sich ferner direkt bei selbstverpflichteten US-Unternehmen beschweren können sowie sich mit diesen gerichtlich auseinandersetzen können. Diese haben die Pflicht, Datenschutzverstöße abzustellen. Überwacht werden selbstverpflichtete US-Unternehmen von der Federal Trade Commission (FTC).

Basis Standardvertragsklauseln: Findet ein Austausch von personenbezogenen Daten mit einem Unternehmen statt, mit dem ein Vertrag nach den so genannten Standardvertragsklauseln (SCC) geschlossen wurde, ist dies derzeit noch eine weitere legale Möglichkeit, Daten zu übermitteln. Derzeit noch – diese Einschränkung muss gemacht werden, weil ein Verfahren gegen die Gültigkeit dieser Standardvertragsklauseln als verbindliches Regelwerk für die einzelnen nationalen Aufsichtsbehörden beim EuGH anhängt. Solange der EuGH diese Klauseln nicht einschränkt oder gar kippt, sind entsprechende Verträge eine weitere mögliche Rechtsgrundlage zum Datentransfer in die USA.

Binding Corporate Rules (BCR): Diese stellen eine dritte Möglichkeit der legalen Datenübermittlung in die USA dar. BCR erfordern

eine komplexe Vorbereitung. Sie sind nur mit Genehmigung der federführenden Aufsichtsbehörde gültig. BCR müssen mehrere Bedingungen erfüllen:

- Genehmigung durch eine Aufsichtsbehörde
- Verpflichtung aller Mitarbeiter der Unternehmensgruppe auf die BCR
- Die Mitarbeiter müssen die Einhaltung der BCR umsetzen
- Die Rechte und Freiheiten der Betroffenen müssen entsprechend den Anforderungen der EU-DSGVO geachtet werden.
- Erfasst sind auch Vertriebs- und Kooperationspartner sowie Dienstleister

In Art. 47 Abs. 2 DSGVO sind die Bedingungen für rechtsgültige BCR aufgelistet. Die Tendenz hinsichtlich der Zahl der Unternehmen, die BCR umsetzen, nimmt zu.

Prüfpflicht unabhängig von der Listung bei Privacy Shield: Selbst wenn ein Unternehmen sich vordergründig den Regeln des Privacy Shield unterworfen hat, muss das noch lange nicht heißen, dass sich dort alle Prozesse konform zu den Datenschutzbestimmungen der EU-DSGVO abspielt. So sind etliche Fälle bekannt, wo schon ein einfacher Blich auf die Homepage zeigt, dass das betreffende Unternehmen sich mutmaßlich nicht an die unterzeichneten Regeln hält. Wenn auf der Homepage beispielsweise noch davon die Rede ist, dass das betreffende Unternehmen sich konform zu Safe Harbor verhält, was aber schon mehrere Jahre nicht mehr rechtskräftig ist, muss das ganze Vorhaben kritisch hinterfragt werden. Die Vermutung liegt nahe, dass es sich um keine ernsthafte Beteiligung am europäischen Datenschutz handelt. Angesicht der ab 25. Mai 2018 drohenden höheren Bußgelder ist in eine genaue Prüfung dringend zu empfehlen.

Datenübermittlung in andere außer-EU-Länder: Werden Daten in außereuropäische Länder, aber nicht in die USA übermittelt, können derzeit nur die Standardverträge oder BCR verwendet werden.

Was gehört nun in die BVT? In den Beschreibungen der Verarbeitungstätigkeiten sind die Kategorien der betroffenen Personen, der Daten, der außer-EU-Unternehmen als Verantwortliche und die jeweilige Rechtsgrundlage aufzunehmen.

Hinweise auf Löschung: Das Verzeichnis der Verarbeitungstätigkeiten soll, wenn möglich, auch die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien enthalten. In der Vergangenheit hatten etliche Unternehmen auf ihrer Homepage das so genannte öffentliche Verfahrensverzeichnis stehen. Dort waren auch Hinweise auf eine Löschung der Daten anzugeben. Zumeist fand man den lapidaren Satz, wonach die Löschung der Daten „entsprechend den gesetzlichen Aufbewahrungsfristen“ erfolge.

Generisches Löschkonzept erforderlich: Diese Angaben dürften angesichts der verschärften Vorgaben zur Löschung personenbezogener Daten nach DSVO nicht mehr genügen. Dafür sollte ein generisches Löschkonzept erarbeitet werden, das dann für die einzelnen Fachbereiche im Unternehmen zu spezifizieren ist. Zu diesem Thema wird es in der nächsten Zeit einen eigenen Praxistipp geben. Nur so viel sei hier schon gesagt: Es ist eher selten, dass die tatsächliche Aufbewahrung von Daten im Unternehmen sich nach den gesetzlichen Aufbewahrungsfristen richtet. Oft werden personenbezogene Daten länger aufbewahrt. Daher sollten im generischen Löschkonzept die Möglichkeiten der Datenhaltung aufgezeichnet werden. Daten können solange aufbewahrt werden, wie ihre gesetzliche Aufbewahrungsdauer es erfordert. Auf der anderen Seite gibt es auch eine prozessuale Aufbewahrungsdauer.

Richtiges Löschen: Stimmen gesetzliche Fristen und die Proessanforderung an die Aufbewahrung der Daten überein, ist alles recht einfach, dann ist zu löschen, wenn die Frist abgelaufen ist. Ist die gesetzliche Aufbewahrungsfrist länger, sind die Daten nach Ende der Prozesserfordernis für weiterem Zugriff zu sperren. Ist die Prozessanforderung an die Aufbewahrung der Daten länger als die gesetzliche Frist es fordert, muss eine gute Begründung diese Anforderung untermauern. Auf alle Fälle ist die Löschung unmittelbar im Anschluss an den Ablauf der Aufbewahrungsfrist vorzunehmen.

Löschkonzept für Verarbeitungstätigkeiten: Ist das generische Löschkonzept erstellt, muss ein Löschkonzept für den Geschäftsbereich bzw. die jeweilige Verarbeitungstätigkeit erarbeitet werden. Hier muss der Fachbereich für die einzelnen Datenkategorien Aufbewahrungsfristen und Löschregeln definieren. Diese Löschhinweise sollten dann in die Beschreibung der Verarbeitungstätigkeit einfließen.

Im Teil vier dieser Reihe von Praxistipps folgen Hinweise für die Darstellung der technischen und organisatorischen 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.