Das Prinzip Verantwortung

Es ist vielleicht das wichtigste, das Kernelement des gesamten Datenschutzrechts: das Konzept des „Verantwortlichen" oder, in der Diktion des früheren BDSG, der „verantwortlichen Stelle". Den Verantwortlichen trifft die Pflicht zur Gewährleistung des Schutzes der verarbeiteten Daten vor Missbrauch, Verfälschung und Verlust, er ist zuständig für die Erfüllung der Betroffenenrechte und muss die gesamte Verarbeitung rechtskonform gestalten und organisieren – von der Prüfung der Rechtsgrundlage über die Information potentiell Betroffener, die Dokumentation der Verarbeitungstätigkeit und die Meldung von Datenschutzvorfällen bis zur fristgerechten Löschung der erhobenen Daten.

Mit der „gemeinsamen" Verantwortung hat die Datenschutz-Grundverordnung dieses klare Prinzip ein wenig aufgeweicht – denn geteilte Verantwortung resultiert in der Praxis leicht nicht in halber, sondern in aufgelöster Verantwortung. So verständlich die Motive des Verordnungsgebers sind, so problematisch ist daher die Umsetzung in der Praxis, zumal darunter Transparenz und Verständlichkeit für die Betroffenen nicht leiden dürfen.

Demgegenüber ist die Übermittlung von Daten an Dritte konsequent an hohe Hürden gebunden: Sofern sie nicht gesetzlich geboten oder zur Vertragserfüllung erforderlich ist, benötigt sie die Einwilligung der Betroffenen: Schließlich müssen diese wissen, wenn (und vor allem: wohin) sich die Verantwortlichkeit verlagert.

Das Konstrukt der Auftragsverarbeitung erlaubt dabei die Verarbeitung durch Dritte ohne einen Wechsel der Verantwortlichkeit: Über den Auftragsverarbeitungsvertrag wird der verarbeitende Dritte so über Vereinbarungen und Weisungen des Auftraggebers gebunden, dass dieser seinen datenschutzrechtlichen Pflichten als Verantwortlicher nachkommen kann.

Aber auch die Auftragsverarbeitung hat ihre praktischen Herausforderungen: Die zunehmende Zahl an digitalen Dienstleistungen, die in wachsendem Umfang in „der Cloud" erbracht werden, führen zu Vertragswerken mit langen Listen von Unterauftragnehmern. Um seiner Verantwortung gerecht zu werden, muss der Verantwortliche die Durchsetzung seiner Weisungen sicherstellen und sich regelmäßig davon überzeugen, dass vertragliche Vereinbarungen und erteilte Weisungen sowohl von den Auftragsverarbeitern als auch von deren Unterauftragnehmern eingehalten werden.

In der Praxis unterbleibt diese Prüfung oft oder wird aufgeschoben. Da es sich bei sehr vielen dieser Online-Dienste inzwischen um von den Entwicklern des Dienstes eingebundene, geradezu „atomare" Cloud-Services handelt, wie z. B. kontext-sensitive Hilfen, nachgeladene Schriften oder ein Ticketsystem zur Unterstützung des Supports, in denen – wenn überhaupt – nur in geringem Umfang personenbezogene Daten anfallen und verarbeitet werden, steht der Aufwand einer Prüfung des Dienstleisters oft in keinem Verhältnis zum erreichbaren Datenschutz-Gewinn. In solchen Fällen helfen allerdings auch Zertifizierungen des Dienstleisters nur begrenzt – so sagen beispielsweise Sicherheitszertifizierungen nach ISO 27001 nichts darüber aus, ob der Dienst erhaltene IP-Adressen auch tatsächlich unverzüglich löscht oder Tickets von ggf. irrtümlich eingefügten personenbezogenen Daten bereinigt.

Ines Geissler, *Ulrich Pordesch*, *Annika Selzer* und *Thomas Wilmer* stellen in diesem Heft ein abgestuftes und in konkreten Prüffragen ausgearbeitetes Vorgehen zur Prüfung von Auftragsverarbeitern in der Cloud vor, das sich konsequent am mit der Verarbeitung verbundenen Risiko für die Rechte und Freiheiten der Betroffenen ausrichtet. Ein Vorgehen, das hoffentlich Schule macht – und Unternehmen und Behörden dabei helfen kann, dem verbreiteten Vollzugsdefizit bei Datenschutzprüfungen von Auftragsverarbeitern abzuhelfen.

Dirk Fox