Anwendungsgrenzen des Datenschutzes

„Sind verschlüsselte Daten in der Cloud eigentlich personenbezogen?" „Für wen personenbezogen? Für den Dienstleister?" ... Die Geschichte dieses Schwerpunkthefts begann mit in einer kleinen Diskussionsrunde unter Kollegen am Kaffee-Automaten.

Die Ausgangsfrage führte uns an die Grenzen des Datenschutzes: Müssen die Stellen, die nicht entschlüsseln können, auch das Datenschutzrecht beachten? Dann begann eine Sammlung von Randbedingungen: Wer verschlüsselt, wer hat Zugang zum Schlüsselmaterial, wie wird verarbeitet? Eine vermeintlich klare Grenze zieht das BDSG für anonyme Daten. Für sie ist das Datenschutzrecht nicht einschlägig. Sind aber verschlüsselte Daten für Dritte anonym? Eher nicht, denn Ziel und Wirkung von Verschlüsselung unterscheiden sich von Anonymisierung. Ohnehin verschwimmen die klaren Grenzen für „anonym" schnell – in den vergangenen 15 Jahren haben sich sowohl die Möglichkeiten zur Deanonymisierung wie auch wissenschaftliche Maße zur Bewertung von Anonymisierungstechniken wesentlich weiterentwickelt. Als drittes Instrument gesellen sich Pseudonyme zu dieser Runde. Sie haben ‚irgendwie' Bezug zu Anonymität und Verschlüsselung. Wir erkannten schnell, dass die Ausgangsfrage zu einem sehr weiten Feld führt: den Grenzen der Anwendung des Datenschutzrechts und der ‚alten' Diskussion um die Relativität des Personenbezugs. Für den Einsatz der Instrumente in der Auftragsdatenverarbeitung und beim Cloud Computing sind diese Fragen hoch aktuell.

Die Recherchen und Diskussionen waren so interessant, dass daraus dieses Schwerpunktheft entstand. Das Verhältnis zwischen den Instrumenten Anonymisierung, Pseudonymen und Verschlüsselung stellen wir im ersten Artikel aus einer eher technischen Perspektive dar. Die weiteren Beiträge vertiefen dann einzelne Aspekte zu den drei Instrumenten.

Buchmann gibt einen Einblick in mathematische Ansätze, die die Qualität von Anonymisierung messen und verbessern können und skizziert Verfahren des Information Hiding. Anonymisierung ist in der der empirischen Sozialforschung Alltagsgeschäft. *Watteler und Kinder-Kurlanda* stellen Verfahren und Kriterien zum Umgang mit Forschungsdaten aus diesem Bereich vor.

Rechtliche Positionen zu anonymen Daten und Pseudonymen, besonders auch aus der aktuellen Diskussion um die Datenschutz-Grundverordnung, und den Anwendungsgrenzen des Datenschutzes, fasst *Karg* zusammen. Der rudimentären Regelungslage zu Pseudonymen im Datenschutzrecht widmet sich *Knopp*.

Die Motivation der Ausgangsfrage war: Muss für verschlüsselte Daten ein Vertrag zur Auftragsdatenverarbeitung geschlossen werden, wenn der Dienstleister nicht auf die Daten zugreifen kann? *Steidle/Pordesch* argumentieren in diese Richtung. Gegen die Subsumtion unter ADV wendet sich *Knopp* in seiner Replik.

Wie Verschlüsselungsmechanismen im Berechtigungsmanagement für Office 365 mit Azure RMS eingesetzt werden, beschreiben *Schäfer* und *Jendrian* in ihrem Beitrag. Erst mit diesen Details kann man bewerten, ob der Dienstleister Zugriff auf die Klardaten des Auftraggebers haben kann. Einen Ausblick auf künftige Techniken verschlüsselter Verarbeitung von Daten geben schließlich *Müller-Quade*, *Huber* und *Nilges*.

Aus der Frage in der Kaffeeküche ist ein randvolles Heft zum Thema Anonymität, Pseudonymen und Verschlüsselung entstanden. Wir glauben, dass Sie das Thema so interessant finden werden wie wir. Die Frage nach den Anwendungsgrenzen des Datenschutzes wird (leider) nicht abschließend beantwortet. Wenn wir aber die Diskussion anregen konnten, hat das Heft seinen Zweck erfüllt. Wir freuen uns auf Rückmeldungen mit Zustimmung und Gegenmeinungen, gerne auch in weiteren DuD-Beiträgen.

Volker Hammer und Michael Knopp