Benedikt Buchner

# Verschlüsselte Daten

Externe Dienstleistungen wie Datenarchivierung oder Cloud-Speicherung werfen zahlreiche (datenschutz)rechtliche Fragen auf. Zwar ist eine Auftragsdatenverarbeitung durch externe Dienstleister zunächst einmal datenschutzrechtlich privilegiert. Probleme stellen sich aber insbesondere, wenn die verarbeiteten Daten zusätzlich unter die Schweigepflicht nach § 203 StGB fallen oder der externe Dienstleister in einem Drittstaat tätig ist. Fraglich ist, inwieweit in solchen Konstellationen eine Verschlüsselung der verarbeiteten Daten weiterhilft. Lässt eine solche Verschlüsselung den Personenbezug der Daten entfallen, wäre der datenschutzrechtliche Anwendungsbereich von vornherein nicht eröffnet; auch käme es nicht zu einer Offenbarung von Privatgeheimnissen i.S.d. § 203 StGB.

## Relative und absolute Theorie

Soweit die Frage, ob bzw. für wen verschlüsselte Daten einen Personenbezug aufweisen, bislang überhaupt diskutiert worden ist, wird hierfür regelmäßig auf den Streit zwischen absoluter und relativer Theorie verwiesen.[1]

Nach der **relativen Theorie** gilt ein subjektiver Beurteilungsmaßstab. Für die Bestimmbarkeit einer Person (und damit die Personenbezogenheit bestimmter Daten) soll es danach ausschließlich auf die Kenntnisse und Möglichkeiten der datenverarbeitenden Stelle selbst ankommen. Diese muss einen Personenbezug mit den ihr normalerweise zur Verfügung stehenden Hilfsmitteln und ohne unverhältnismäßigen Aufwand durchführen können, ein mögliches Zusatzwissen Dritter bleibt dagegen unberücksichtigt.[2] Daten können daher unter der relativen Theorie je nach individuellem Kenntnisstand für die eine Stelle personenbezogen sein, für die andere Stelle hingegen nicht. Für verschlüsselte Daten heißt dies, dass diese Daten zwar im Verhältnis zu all denjenigen einen Personenbezug aufweisen, die Inhaber des entsprechenden Schlüssels sind und damit die Daten auch wieder entschlüsseln, d.h. lesbar machen können. Im Verhältnis zu denjenigen, die keine Möglichkeit der Entschlüsselung haben, weisen die verschlüsselten Daten einen solchen Personenbezug hingegen nicht auf.

Nach der **absoluten** Theorie gilt demgegenüber ein objektiver Beurteilungsmaßstab. Die Bestimmbarkeit einer Person soll danach nicht nur nach den Kenntnissen und Möglichkeiten der datenverarbeitenden Stelle selbst zu beurteilen sein.[3] Vielmehr soll es für die Annahme eines Personenbezugs auch ausreichen, dass irgendein Dritter das hierfür nötige Zusatzwissen besitzt. Da dieses Zusatzwissen im Falle einer Verschlüsselung jedenfalls für den Schlüssel-Inhaber verfügbar ist, können nach der absoluten Theorie verschlüsselte Daten niemals und gegenüber niemandem ihren Personenbezug verlieren und unterfallen daher stets dem datenschutzrechtlichen Anwendungsbereich.[4]

## Datenschutzrichtlinie und Art. 29-Datenschutzgruppe

Für ein absolutes Verständnis des Personenbezugs wird insbesondere die Datenschutzrichtlinie als Argument herangezogen. Nach deren Erwägungsgrund 26 sollen bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden, „die vernünftigerweise entweder von dem Verantwortlichen für die Datenverarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen."

Die Art. 29-Datenschutzgruppe hat allerdings für verschlüsselte Daten eine differenzierte Sichtweise eingenommen. In ihrer Stellungnahme zum Begriff „personenbezogene Daten" hat sich die Datenschutzgruppe u.a. ausführlich mit der Konstellation auseinandergesetzt, dass verschlüsselte Daten weitergegeben werden.[5] Unstreitig ist, dass diese verschlüsselten Daten dabei zunächst einmal für denjenigen personenbezogen sind, der im Besitz des Schlüssels ist.

Was hingegen den Empfänger der Daten angeht, soll es für die Frage, ob die verschlüsselten Daten auch für diesen noch einen Personenbezug aufweisen, auf die dem Empfänger zur Verfügung stehenden Mittel ankommen, die zur Identifizierung „vernünftigerweise eingesetzt werden könnten". Daher nimmt die Datenschutzgruppe etwa dann eine Bestimmbarkeit der betroffenen Personen an, wenn die Möglichkeit besteht, dass der Datenempfänger Zugang zu dem für die Verschlüsselung verwendeten Schlüssel erhält. Ebenso sollen etwa die Risiken externer Hacking-Angriffe zu berücksichtigen sein und die Wahrscheinlichkeit, dass eine Person in der übermittelnden Organisation den Schlüssel preisgibt.

Entscheidend ist daher aus Sicht der Art. 29-Datenschutzgruppe letztlich die Sicherheit der Verschlüsselung. Ist diese gewährleistet, sind verschlüsselte Daten lediglich für die Stelle personenbezogen, die Inhaberin des Schlüssels ist, nicht hingegen für die Stellen, die diese verschlüsselten Daten zwar auch erhalten, aber nicht im Besitz des Schlüssels sind.[6] Eine sichere Verschlüsselung vorausgesetzt, wäre nach dieser Sichtweise also auch in den eingangs genannten Konstellationen eine Datenverarbeitung durch externe Auftragnehmer möglich.

1 Vgl. Stiemerling/Hartung, CR 2012, 60, 63 f.; Schröder/Haag, ZD 2011, 147, 151.
2 In diesem Sinne etwa Gola/Schomerus, BDSG, § 3 Rn. 10.
3 Pahlen-Brandt, DuD 2008, 34; Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rn. 13.
4 Vgl. Stiemerling/Hartung, CR 2012, 60, 64.
5 Stellungnahme 4/2007 (WP 136), S. 21 ff.
6 A.a.O., S. 22.