Michael Knopp

Muss die Wirkung von Verschlüsselung neu gedacht werden?

Aus Datenschutzperspektive ist man häufig bereits erleichtert, wenn verantwortliche Stellen für die Kommunikation oder bei der Speicherung personenbezogener Daten überhaupt Verschlüsselungstechniken einsetzen. Im vorausgegangenen Beitrag haben Ulrich Pordesch und Roland Steidle dargestellt, dass jedoch selbst bei technisch fehlerfrei angewendeter Verschlüsselungstechnik mit Blick auf den langfristigen Schutz Vorsicht geboten sein kann. Die vorliegende Replik wählt einen etwas anderen Betrachtungsansatz, um die datenschutzrechtliche Wirkung von Verschlüsselung darzustellen.

1 Einleitung

Das Einbinden von Dienstleistern in den IT-Betrieb oder die Weitergabe von personenbezogenen Daten an Dienstleister richtig zu gestalten ist heute eines der praxisrelevantesten Themen des Datenschutzrechts. In vielen Fällen bietet die Gestaltung als Auftragsdatenverarbeitung eine praktikable Lösung, doch sobald Bezüge zu Standorten außerhalb des Anwendungsbereichs der europäischen Datenschutzrichtlinie bestehen, Berufsgeheimnisse betroffen sind oder der Vertragsschluss zur Auftragsdatenverarbeitung sich als schwierig erweist, trifft dieses Modell auf Grenzen.

Die Konstellationen und die Arten der betroffenen Dienstleistungen sind vielfältig. Eine einfache Konstellation ist die Nutzung von fremden Speicherkapazitäten, bspw. auch von Cloud-Storage-Diensten. Ein anderes Beispiel ist die Nutzung eines externen E-Mail-Providers. In diesen Fällen, in denen der Dienstleister oder Dritte keinen Zugriff auf die Daten benötigen, bietet sich die Verschlüsselung der Daten als Ansatz an.

Aus Datenschutzsicht könnte dies eine einfache Lösung sein, da so der Zugriff des Dienstleisters ausgeschlossen wird. Bei genauem Hinsehen ergeben sich jedoch mehrere Fragestellungen, die eine differenziertere Betrachtung erfordern. Die erste betrifft die rechtliche Einordnung der Weitergabe verschlüsselter Daten: Ist diese ohne weiteres zulässig? Wie sind verschlüsselte personenbezogene Daten rechtlich einzuordnen? Handelt es sich noch um personenbezogene Daten und wenn ja, kann der Personenbezug von der Schlüsselinhaberschaft abhängig sein?

Michael Knopp, Jurist

Berater bei der Secorvo Security Consulting GmbH. Schwerpunkte: Datenschutz und Rechtsfragen im Kontext der IT-Sicherheit.

E-Mail: michael.knopp@secorvo.de

Verbunden hiermit ist die Frage, ob weiterhin eine Auftragsdatenverarbeitung vorliegt oder ob die Weitergabe als solche gestaltet werden muss. Hierdurch gewinnt die Thematik ihre praktische Relevanz.

2 Einordnung der Verschlüsselung

Eine Datenverschlüsselung ist eine technische Sicherheitsmaßnahme.[1] Als solche hat sie in verschiedener Form Eingang in gesetzliche Regelungen gefunden.

Das Bundesdatenschutzgesetz erwähnt Verschlüsselungstechniken lediglich in dem Anhang zu den in § 9 BDSG geforderten technischen und organisatorischen Maßnahmen. Die Verwendung dem Stand der Technik entsprechender Verschlüsselungsverfahren wird als eine Maßnahme zur Zugangs-, Zugriffs- und Weitergabekontrolle ausdrücklich benannt. Dieser Einordnung folgt auch die Legaldefinition im Landesdatenschutzgesetz von Schleswig-Holstein (§ 2 Abs. 2 Nr. 8): „*Verschlüsseln [ist] das Verändern personenbezogener Daten derart, dass ohne Nutzung des Geheimnisses die Kenntnisnahme vom Inhalt der Daten nicht oder nur mit einem unverhältnismäßigen Aufwand möglich ist.*“[2]

Außerhalb des Datenschutzrechts stellt die Verwendung von Verschlüsselungsverfahren in einigen Regelungen eine gesetzliche Sicherheitsanforderung dar. Beispiele sind § 5 Abs. 3 Nr. 1 De-Mail-G, § 87a Abs. 1 S. 2 AO oder § 3 Abs. 1 S. 4 PassDEÜV, in denen für bestimmte Datenübertragungen eine Verschlüsselung vorgeschrieben wird.[3]

Die gesetzliche Forderung nach Verschlüsselung wird begleitet durch den strafrechtlichen Schutz von Verschlüsselungsverfahren. § 202a StGB stellt unter Strafe, sich unbefugt Zugang zu Daten zu verschaffen, die besonders gegen unberechtigten Zugang

1 Ernestus in Simitis, BDSG, 8. Aufl. 2014, § 9 Rn. 165, 173; Hartung/Storm in Hilber, Handbuch Cloud Computing, Teil 4 Rn. 117;

2 Eine ähnliche Definition findet sich im Landesdatenschutzgesetz von Mecklenburg-Vorpommern.

3 Weitere Beispiele bei Bergt, CR 2014, 726 (728).

gesichert sind. Unter die gemeinten Zugangssicherungen fallen auch Verschlüsselungsverfahren.[4]

Wie aber sind verschlüsselte Daten im Datenschutzrecht einzuordnen? Mit der Antwort auf diese Frage ist die Anwendbarkeit des Datenschutzrechts verbunden.

Denn die Einordnung verschlüsselter Daten wird häufig unter dem Aspekt der Personenbeziehbarkeit behandelt.[5] Wenn die Verschlüsselung gezielt eingesetzt wird, um Identifikationsmerkmale zu verschlüsseln, ist dieser Ansatz richtig.

Werden Daten zur Speicherung oder zur Übermittlung verschlüsselt, verhindert die Verschlüsselung – ihre Funktionsfähigkeit und Eignung vorausgesetzt – lediglich den Zugriff aller Personen, die nicht über den verwendeten Schlüssel verfügen. An dem Personenbezug der verschlüsselten Daten ändert sich nichts – wie z. B. beim Verschließen eines Dokumentes in einem Tresor.

2.1 Anonymisierung und Pseudonymisierung

Unwidersprochen wird die Feststellung bleiben, dass es sich bei verschlüsselten personenbezogenen Daten für den Schlüsselinhaber weiterhin um personenbezogene Daten handelt. Hierin liegt ein Unterschied zu anonymisierten Daten. Selbst für die verantwortliche Stelle oder den Anwender des Anonymisierungsverfahrens wäre nach einer Anonymisierung der Personenbezug nur mit unverhältnismäßig großem Aufwand wieder herstellbar.

Auch eine Pseudonymisierung liegt weder im herkömmlichen Wortsinn noch nach der Definition des § 3 Abs. 6a BDSG vor, denn es werden eben gerade nicht die identifizierenden Merkmale so ersetzt, dass nur die Stelle im Besitz der Zuordnungsregel die Daten auf eine Person beziehen kann.[6] Die Situation ist nur insoweit vergleichbar, als dass nur die Besitzer der Zuordnungsregel oder des verwendeten Schlüssels die Daten personenbezogen bzw. überhaupt verwenden können, Dritte hingegen nicht. Pseudonyme Daten können allerdings weiter bspw. zur Verknüpfung mit Daten zu demselben Pseudonym genutzt werden. Bei verschlüsselten Dateien ist dies dagegen nicht möglich.

Die Regelungen zur Anonymisierung oder Pseudonymisierung – soweit vorhanden – sind also nicht anwendbar.

2.2 Personenbezug für Dritte

Für Dritte, die den Schlüssel nicht besitzen, wird jedoch häufig davon ausgegangen, es handele sich für diese nicht um personenbezogene Daten.[7] Voraussetzung hierfür ist allerdings bereits, dass ein relatives Verständnis des Personenbezuges zugrunde gelegt wird.[8]

Doch was ist hieraus datenschutzrechtlich zu folgern? Nur personenbezogene Daten fallen unter den Anwendungsbereich des Datenschutzrechts. Wenn verschlüsselte Dateien für Dritte nicht personenbezogen sind, dürften sie dann ohne weitere Einschränkung an Dritte weitergegeben werden?

Folgt man diesem Ansatz, ist allerdings schwer zu erklären, wie die mit einer Verschlüsselung verbundenen Risiken datenschutzrechtlich bewertet oder bewältigt werden sollen.[9] Was ist die Konsequenz, wenn das Verschlüsselungsverfahren einen Fehler aufweist, der samt Verfahren zur Fehlerausnutzung publik wird? Was ist die Folge, wenn das Verschlüsselungsverfahren gebrochen wird, der Schlüssel in die Hände des Dritten fällt oder auf andere Weise die Verschlüsselung wirkungslos wird?

Wie Pordesch/Steidle richtig feststellen, existiert keine datenschutzrechtliche Kategorie ‚verschlüsselte Daten'. Für das Datenschutzrecht existieren bloß personenbezogene oder nicht personenbezogene Daten. Wie aber soll dies nun für Daten beurteilt werden, die der Dritte plötzlich oder nach längerer Zeit mit geringem Aufwand entschlüsseln kann? Werden die Daten schon mit der Schwächung des Verschlüsselungsverfahrens wieder personenbezogen oder erst, wenn buchstäblich der Schlüssel im Schloss gedreht wird? Immerhin ist die Entschlüsselung für unbefugte Dritte weiterhin strafbar (§ 202a StGB).[10] Andererseits stellt das Datenschutzrecht bei der Bestimmbarkeit des Betroffenen auf die Größe der Wahrscheinlichkeit ab, mit der die Herstellung des Personenbezugs möglich ist und berücksichtigt dabei alle dem Dritten vernünftigerweise zur Verfügung stehenden Mittel.[11] Wäre die unberechtigte Entschlüsselung eine Erhebung personenbezogener Daten, die datenschutzrechtlich sogar gerechtfertigt sein kann? Oder wird die vorangegangene Dateiweitergabe nachträglich zur Übermittlung?

Die Alternative bei einem allein am Personenbezug orientierten Ansatz wäre, die verschlüsselten Daten weiterhin gegenüber jedermann als personenbezogen zu betrachten.[12] Hier käme eine eher objektive Auffassung des Personenbezugs zum Tragen. Die Konsequenz wäre, dass für jede Weitergabe eine Rechtsgrundlage erforderlich wäre. Doch wie soll eine Einwilligung in eine Übermittlung für den eigentlich nicht vorgesehenen Fall der Entschlüsselung aussehen?[13] Wie soll der Empfänger seine datenschutzrechtliche Verantwortung wahrnehmen, wenn er keinen Zugriff hat und eventuell gar nicht weiß, um welche Art von Daten es sich handelt?

In Betracht kommt natürlich die Gestaltung der Weitergabe als Auftragsdatenverarbeitung. Für den E-Mail-Provider eines Ein-Mann-Steuerbüros scheidet das aber bspw. aus. Das Erbringen der Telekommunikationsdienstleistungen ist hier keine

4 Fischer, Strafgesetzbuch, 61. Aufl. 2014, § 202a Rn. 9a, 11a.

5 S. bspw. Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Version 2.0, Stand 9.10.2014, S. 12, abrufbar unter https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf; Kroschwald, Verschlüsseltes Cloud Computing, ZD 2014, 75 ; Stiemerling/Hartung, Dateschutz und Verschlüsselung, CR 2012, 60 (62 ff).

6 A.A. Art. 29 Datenschutzgruppe, WP 136, III 3, S. 21, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf

7 Kroschwald, s. Fn. 5, 77 f m.w.N.; Jotzo, Der Schutz personenbezogener Daten in der Cloud, 2013, S. 67 f.

8 Zur Darstellung der Diskussion um ein relatives oder objektives Verständnis des Personenbezugs Damann in Simitis, s. Fn. 1, § 3 23 ff.

9 Teilweise werden verschlüsselte Daten als „potentiell personenbezogen" betrachtet, im Fall des Versagens der Verschlüsselung würden aus den zuvor anonymen Daten personenbezogene Daten. Die ex ante anonyme Weitergabe würde dann zur nachträglich rechtswidrigen Übermittlung (Damann in Simitis, s. Fn.1, § 3 Rn. 36 ff.).

10 Eine solche Strafbarkeit stellt allerdings bei einer internationalen Weitergabe verschlüsselter Dateien nicht durchgängig und für jeden Dateibesitzer eine Hürde dar.

11 Zu dem diesbezüglichen Verständnis der Personenbeziehbarkeit und den diesbezüglichen Streitständen s. Karg, in diesem Heft; Buchner, DuD 2013, 804.

12 Art. 29 Datenschutzgruppe, WP 136, III 3, S. 23; so auch Helmschrott, Verschlüsselung der Daten beseitigt nicht datenschutzrechtliche Anforderungen, abrufbar unter http://www.rbi-law.de/blog/verschluesselung-von-daten-beseitigt-nicht-datenschutzrechtliche-anforderungen/;

13 Verlangt wird bspw. eine umfassende Information über Verschlüsselung als Teil der Sicherheitsmaßnahmen (Taeger in Taeger/Gabel, BDSG, 2. Aufl. 2013, § 4a Rn. 15). In diesem Fall wird aber dann wohl nur in die Datenverwendung der verantwortlichen Stelle eingewilligt und die Information über die verschlüsselte Weitergabe als notwendig für eine informierte Einwilligung gesehen.

Auftragsdatenverarbeitung; nicht jede Dienstleistung ist auch als Auftragsdatenverarbeitung abbildbar.

Anhand der schwer zu beantwortenden Fragen wird deutlich, dass Ansätze, die am Personenbezug der verschlüsselten Daten gegenüber Dritten ansetzen, keine adäquaten Lösungen liefern, da hierbei das Wesen oder die Funktion der Verschlüsselung missachtet wird.

3 Zulässigkeit der Weitergabe

Es bietet sich jedoch eine andere Betrachtungsweise an, die strikt von der verantwortlichen Stelle ausgeht, die die Verschlüsselung vornimmt. Denn neben dem Personenbezug der betrachteten Daten ist die Anwendbarkeit des Datenschutzrechts an das Vorhandensein eines Adressaten geknüpft. Für diese verantwortliche Stelle, die regelmäßig auch Schlüsselinhaberin sein wird, handelt es sich, wie bereits festgestellt, auch nach der Verschlüsselung beim Umgang mit der verschlüsselten Datei weiter um ein Verarbeiten oder Nutzen personenbezogener Daten.

Gibt die verantwortliche Stelle personenbezogene Daten an Dritte weiter, so handelt es sich gewöhnlich um eine Übermittlung oder eine Auftragsdatenverarbeitung. Wie sieht dies aber mit verschlüsselten Daten aus, zu denen der Empfänger keinen Schlüssel besitzt? § 3 Abs. 4 Nr. 3 BDSG definiert die Übermittlung als Bekanntgabe gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an Dritte. Durch die Verschlüsselung fehlt es an einer Bekanntgabe gegenüber den Dritten, da diese wenigstens zum Zeitpunkt der Weitergabe keinen Zugriff auf die personenbezogenen Daten erlangen.

Doch selbst wenn dieser Zustand konstant wäre, könnten verschlüsselte Daten nicht beliebig – ohne weitere Kontrollen und zeitlich unbegrenzt – an Dritte weitergegeben werden. Auch wenn keine Übermittlung vorliegt, so handelt es sich doch weiter um Speicherungen von Daten der verantwortlichen Stelle bei Dritten.[14] Damit ist die verantwortliche Stelle auch weiterhin in Verantwortung, bspw. mit Entfallen des Zweckes oder der Erforderlichkeit die Löschung der Daten vorzunehmen oder vornehmen zu lassen, § 35 Abs. 2 BDSG, oder allgemein die internen Löschfristen auch auf die verschlüsselt gespeicherten Daten anzuwenden. Auch die Auskunftsrechte Betroffener würden sich bspw. weiterhin auch auf die verschlüsselten Daten in den Händen Dritter erstrecken. Aus Sicht der verantwortlichen Stelle bleibt das Datenschutzrecht anwendbar.

Verschlüsselung ist jedoch keine unfehlbare Sicherheitsmaßnahme.[15] Vor allem durch die Weiterentwicklung der verfügbaren Rechenkapazitäten verlieren ein zum Zeitpunkt der Verschlüsselung als Stand der Technik akzeptiertes Verfahren und eine empfohlene Schlüssellänge als Sicherheitsmaßnahme in der Regel mit der Zeit ihren Sicherheitswert. Daneben stehen mögliche unentdeckte Implementierungsfehler des Verfahrens oder Fragen der sicheren Schlüsselaufbewahrung. Die spannende datenschutzrechtliche Frage im Kontext des Umgangs mit verschlüsselten Daten ist, wie mit diesem Umstand umzugehen ist.

Auch wenn die verschlüsselten personenbezogenen Daten bei Dritten abgelegt werden, handelt es sich aus Sicht der verantwortlichen Stelle immer noch um eine eigene Speicherung. Aus diesem Grund hat die verantwortliche Stelle auch bezüglich der aus der Hand gegebenen verschlüsselten personenbezogenen Daten weiterhin die Pflicht aus § 9 BDSG, die im Verhältnis zum angestrebten Schutzzweck angemessenen technischen und organisatorischen Maßnahmen zu ergreifen, die zur Wahrung der datenschutzrechtlichen Vorschriften erforderlich sind. Die Verschlüsselung kann in dieser Betrachtungsweise ihrer Funktion nach betrachtet werden, nämlich als Sicherheitsmaßnahme unabhängig von ihrer Auswirkung auf den Personenbezug.

Im Ergebnis bedeutet dies, dass die verantwortliche Stelle prüfen muss, ob die gewählte Verschlüsselung geeignet ist, Unbefugte von einem Zugriff abzuhalten oder ob ergänzende Maßnahmen erforderlich sind. Dabei ist besonders zu berücksichtigen, ob die Datei Dritten zugänglich ist und welche Kontrolle über den Zugang Dritter besteht.

4 Angemessene Datensicherheit

Das Bundesverfassungsgericht hat im Volkszählungsurteil die Feststellung getroffen, dass es keine belanglosen personenbezogenen Daten gibt und dass der Schutzbedarf bzw. die Zulässigkeit der Einschränkung des Rechts auf informationelle Selbstbestimmung immer im Verwendungskontext der Daten zu beurteilen sind.

Damit scheidet vor allem aus, personenbezogene Daten von vornherein aus dem Schutzbereich der informationellen Selbstbestimmung oder des Datenschutzrechts auszunehmen. Eine Abwägung zwischen den Betroffeneninteressen und den Interessen der Datenverwender auf Ebene der zu treffenden Sicherheitsmaßnahmen ist jedoch möglich und sogar gefordert.

Bei der Weitergabe verschlüsselter personenbezogener Daten ist diese Abwägung jedoch durchaus komplex. Gerade auch, weil die Veränderung der Abwägungskriterien (Eignung der Verschlüsselung, Risiken für den Betroffenen bei unbefugter Entschlüsselung) mit Zeitablauf zu berücksichtigen ist und die Abwägung nicht nur die Gegenwart, sondern auch zukünftige Risiken berücksichtigen muss.

Die Abwägung sollte mit den Betroffeneninteressen beginnen. Hierzu ist zuerst zu bestimmen, welche Risiken für den Betroffenen mit einem Bekanntwerden der verschlüsselten Daten verbunden sind. Sind die Daten ohnehin weitgehend öffentlich verfügbar? Handelt es sich um schnell veränderliche Daten, die nach wenigen Jahren praktisch ohne Wert sind? Befinden sich unter den Daten besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG)? Bestimmt werden muss, ob von verschlüsselten personenbezogenen Daten geringe oder schwere Risiken für den Betroffenen ausgehen und im zweiten Schritt, ob es auch nach Zeitablauf bei schweren Risiken bleibt. Wenigstens nach dem Tod der Betroffenen ist der Schutz personenbezogener Daten durch das Datenschutzrecht begrenzt,[16] doch auch zuvor kann das Risiko sinken.

Auf der anderen Seite ist die Eignung des Verschlüsselungsverfahrens zu betrachten. Zuerst ist zu prüfen, ob das Verfahren überhaupt in der Gegenwart angemessen ist, die Daten ausrei-

14 Hier könnte man allerdings einwenden, dass bei einer unkontrollierten Weitergabe verschlüsselter Daten der beabsichtigte Zweck der Weiterverarbeitung fehlt, den § 3 Abs. 4 Nr. 1 BDSG als Definitionsbestandteil der Speicherung enthält. An der fortbestehenden Verantwortung der verantwortlichen Stelle würde dies jedoch nichts ändern.

15 S. hierzu Bergt, CR 2014, 726 (729 f).

16 Gola/Schomerus, BDSG, 10. Aufl. 2010, § 3 Rn. 12.

chend zu schützen. Hier ist vor allem die technische Eignung des Verschlüsselungsverfahrens zu betrachten. Dabei ist z. B. auch zu berücksichtigen, wer die Kontrolle über den Schlüssel und das Verschlüsselungsverfahren hat. Wenn der Dienstleister durch seine Kontrolle über das Verfahren auch den verwendeten Schlüssel kontrolliert, ist er durch Verschlüsselung nicht vom Zugriff ausgeschlossen.

Danach ist eine Prognose für die fortdauernde Eignung mit Zeitablauf zu stellen. Anschließend sind neben dem Verfahren selbst weitere Einflüsse zu berücksichtigen. Hierzu gehört nicht zuletzt der Umstand, dass die Verschlüsselung nicht allein durch den Aufwand schützt, der zu betreiben ist, um sie zu brechen. Dieser mag für sich bereits ausreichen, wenn er dauerhaft in keinem Verhältnis zu dem evtl. geringen oder zeitlich abnehmenden Wert der Daten steht. Die Verschlüsselung schützt jedoch wenigstens in Deutschland und weiteren Staaten[17] auch dadurch, dass ihre unbefugte Durchbrechung strafrechtlich sanktioniert ist (§ 202a StGB). Selbst wenn die Verschlüsselung mit geringem Aufwand durchbrochen werden kann, bleibt immer noch zu berücksichtigen, dass der Unbefugte zu einer illegalen Handlung bereit sein muss. Damit kann auch bereits eine schwache Verschlüsselung geeignet sein.

Außerdem ist einzubeziehen, ob die Verschlüsselung die einzige Schutzmaßnahme darstellt. Es ist ein Unterschied, ob die verantwortliche Stelle Kontrollen über den Verbleib und die Aufbewahrung der verschlüsselten Datei in der Hand behält oder die verschlüsselten Daten in einer Weise weitergibt, in der sie nicht mehr kontrollieren kann, wie sie sich verbreiten, wer Zugang erlangt oder was der empfangende Dritte mit den verschlüsselten Daten unternimmt. Bei einer Weitergabe im Rahmen von Dienstleistungsverhältnissen dürfte letzteres in der Regel nicht der Fall sein, auch nicht bei Cloud-Diensten. In der Regel wird wenigstens ein Kontrolle vermittelndes Vertragsverhältnis bestehen. Unter Umständen erfolgt die Speicherung bei dem Dritten sogar so, dass weder eine weitere Weitergabe noch ein Zugang Dritter zu befürchten sind. In diesem Fall soll oder muss die Verschlüsselung lediglich den Dritten selbst vom Zugriff ausschließen.[18] Je weniger zusätzliche Kontrollen bestehen, desto stärker muss die Verschlüsselung sein und desto geringer das von den Daten ausgehende Risiko.

Eine Weitergabe völlig ohne Kontrollvorbehalt, also ohne eine vertragliche Absicherung der Einflussnahme auf den weiteren Verbleib der verschlüsselten Daten, wird regelmäßig unzulässig sein. Allein schon, weil die Löschverpflichtung nicht umgesetzt werden kann, und weil Dritte mehr oder weniger unbeschränkt und ungehindert versuchen könnten, Zugriff zu erlangen.

17 § 202a StGB dient der Umsetzung verschiedener internationaler Abkommen, unter anderem der Convention on Cybercrime, so dass der strafrechtliche Schutz zwar nicht weltweit vorausgesetzt werden kann, aber nicht auf Deutschland beschränkt ist (Schönke/Schröder, Strafgesetzbuch, 29. Aufl. 2014, § 202a Rn. 1).

18 Zur Unterscheidung von Verschlüsselungsverfahren nach der Ausschlusswirkung siehe Brennscheidt, Cloud Computing und Datenschutz, 2013, S. 89 f.

5 Datenschutzrechtliche Wirkung

Die Ausgangsfrage war jedoch auch, wie sich die Verschlüsselung beispielsweise im Kontext von Cloud-Speicherdiensten oder Kommunikationsdiensten auswirkt. Folgt man dem auf die Verantwortlichkeit fokussierten Ansatz, gelangt man hier zu durchaus relevant abweichenden Ergebnissen: Da keine Übermittlung vorliegt, ist keine Rechtsgrundlage – also auch keine Einwilligung der Betroffenen in die Weitergabe der verschlüsselten Datei – erforderlich. Auch ein Auftragsdatenverarbeitungsvertrag muss aus demselben Grund nicht geschlossen werden. Die verantwortliche Stelle ist in der Gestaltung zusätzlicher vertraglicher Sicherungen des Zugriffsschutzes frei. Vor allem im Kontext der mit der Auftragsdatenverarbeitung nach deutschem Recht verbundenen Problematik der Übermittlung ins außereuropäische Ausland kann dies sehr hilfreich sein.

6 Fazit

Entgegen der herrschenden Meinung sollte die Zulässigkeitsprüfung bei der Weitergabe verschlüsselter personenbezogener Daten bei der verantwortlichen Stelle und der Erfüllung von deren fortdauernden Schutzpflichten ansetzen. Die alleinige Fokussierung auf den Personenbezug verschlüsselter Daten reicht nicht aus.

Nur so kann Verschlüsselung als das geprüft werden, was sie ist – als Schutzmaßnahme und Zugriffsschutz. Eine allgemeingültige Aussage zur Zulässigkeit der Weitergabe verschlüsselter personenbezogener Daten ist, wie dargestellt, nicht möglich. Die verantwortliche Stelle muss für jeden Fall einzeln prüfen, ob bei der verschlüsselten Weitergabe eine ausreichende Datensicherheit gewährleistet ist. Hierbei ist sowohl die Risikoabschätzung als auch die Eignungsbeurteilung für die Sicherheitsmaßnahmen mit Blick auf die entferntere Zukunft durchzuführen.

Bei personenbezogenen Daten, die auch nach Jahren noch bei ihrer Bekanntgabe schwerwiegende Beeinträchtigungen für den Betroffenen nach sich ziehen können, wird eine verschlüsselte Weitergabe nur in Betracht kommen, wenn ähnliche vertragliche Vorkehrungen wie bei einer Auftragsdatenverarbeitung getroffen werden. Dies schließt die Option einer vollständigen Rückgabe oder Löschung aller Kopien der verschlüsselten Daten ein. Eine Auftragsdatenverarbeitung liegt jedoch regelmäßig nicht vor, da der Empfänger keinen Zugriff auf die verschlüsselten Daten erhält.

Bei E-Mail-Diensten ist zusätzlich zu berücksichtigen, dass der Anbieter auch den Bestimmungen des Telekommunikationsgesetztes und dem Telekommunikationsgeheimnis unterliegt. Jenseits vom Ausreichen der Verschlüsselung kann hier davon ausgegangen werden, dass der Anbieter nicht mutwillig gegen seine gesetzlichen Vorgaben verstößt. Eine verschlüsselte Nutzung dieser Dienste bleibt daher selbst bei Berufsgeheimnissen oder besonderen Arten personenbezogener Daten in der Regel zulässig.