Maximilian Eibl, Martin Gaedke. (Hrsg.): INFORMATIK 2017,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 751

Anforderungen des künftigen europäischen Datenschutzrechts an die vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln

Stephan Blazy[1], Susan Gonscherowski[2] und Annika Selzer[3]

Abstract:[4] Der Wunsch der Bevölkerung nach effektiven Selbstschutzmechanismen für ihre elektronische Kommunikation wird – auch vor dem Hintergrund der anlasslosen Massenüberwachungen durch Geheimdienste – immer lauter. Für den Schutz der E-Mail-Kommunikation, die einen Großteil der Kommunikation im Internet ausmacht, bestehen durch Verfahren der Ende-zu-Ende-Verschlüsselung bereits seit Jahren solche effektiven Schutzmechanismen. Problematisch ist jedoch, dass – obwohl die Verfahren zur Ende-zu-Ende-Verschlüsselung seit vielen Jahren wohlverstanden werden und von allen gängigen E-Mail-Programmen genutzt werden können – diese Verfahren nicht laientauglich ausgestaltet sind, so dass nur eine geringe Zahl an Internetnutzern ihre E-Mail-Kommunikation bisher durch Ende-zu-Ende-Verschlüsselung schützt. U. a. wird es im Zusammenhang mit der E-Mail-Verschlüsselung als problematisch empfunden, den öffentlichen Verschlüsselungsschlüssel des gewünschten Kommunikationspartners aufzufinden. Dieser Beitrag skizziert die hier genannten Probleme und stellt rechtliche Anforderungen an eine Lösung zur Verbesserung des Auffindens von Verschlüsselungsschlüsseln selbst sowie an E-Mail-Provider.

Keywords: Datenschutz, E-Mail-Provider, Haftung, Verschlüsselung, Verzeichnisdienste

1 Wunsch der Bevölkerung nach effektivem Schutz der Online-Kommunikation

Im Jahr 2013, deckte Edward Snowden anlasslose Massenüberwachungen der Online-Kommunikation durch Geheimdienste, allen voran die Geheimdienste der USA, Australien, Neuseeland, Kanada und Großbritannien (Auch als „Five Eyes“ bezeichnet), auf. Die Aufdeckung von Ausspähprogrammen löste bei einem großen Anteil der Bevölkerung Unbehagen aus. Konsequenterweise wird der Wunsch nach effektiven

[1] Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung (Provet), Pfannkuchstr. 1, 34109 Kassel, s.blazy@uni-kassel.de.
[2] Unabhängiges Landeszentrum für Datenschutz (ULD), Holstenstraße 98, 24103 Kiel, sgonscherowski@datenschutzzentrum.de.
[3] Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Rheinstraße 75, 64295 Darmstadt, annika.selzer@sit.fraunhofer.de.
[4] Dieser Beitrag entstand im Rahmen des Projekts „Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln (VVV)“ (https://keys4all.de), das vom Bundesministerium für Bildung und Forschung (BMBF) auf Grundlage des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt“ unter dem Förderkennzeichen 16KIS0354K gefördert wird.

doi:10.18420/in2017_74

Schutzmechanismen gegen anlasslose Massenüberwachungen durch Geheimdienste immer lauter.

Für den Schutz der E-Mail-Kommunikation, die einen Großteil der Kommunikation im Internet ausmacht, bestehen durch Verfahren der Ende-zu-Ende-Verschlüsselung bereits seit Jahren solche effektiven Schutzmechanismen [HSW16a, HSW16b].

1.1 Funktion digitaler Zertifikate im Kontext von Ende-zu-Ende-Verschlüsselung

Möchte der Sender eine Information verschlüsselt an den Empfänger senden, so benötigt der Sender den öffentlichen Schlüssel des Empfängers in Form eines digitalen Zertifikats (im Folgenden wird zur besseren Lesbarkeit nur von *Zertifikaten* gesprochen). Ein digitales Zertifikat bescheinigt die Vertrauenswürdigkeit eines öffentlichen Schlüssels und enthält neben dem öffentlichen Schlüssel i. d. R.[5] auch personenbezogene Daten wie z. B. den Namen und die E-Mail-Adresse des Zertifikatinhabers. Mit dem öffentlichen Schlüssel wird die Information verschlüsselt, d. h. in einen Geheimtext überführt, dann an den Empfänger versandt und mit Hilfe seines privaten Schlüssels wieder in den Klartext versetzt bzw. entschlüsselt. Die Sicherheit des Verfahrens hängt dabei auch vom verantwortungsvollen Umgang mit dem privaten Schlüssel ab, der - im Gegensatz zum öffentlichen Schlüssel - nur der Person bekannt sein darf, welcher der private Schlüssel gehört [WB16, HSW16a, HSW16b].

1.2 Fehlende Laientauglichkeit als Hemmschuh der E-Mail-Verschlüsselung

Problematisch ist, dass – obwohl die Verfahren zur Ende-zu-Ende-Verschlüsselung seit vielen Jahren wohlverstanden werden und von allen gängigen E-Mail-Programmen genutzt werden können – diese Verfahren jedoch nicht laientauglich ausgestaltet sind, so dass nur eine geringe Zahl an Internetnutzern ihre E-Mail-Kommunikation bisher durch Ende-zu-Ende-Verschlüsselung schützt [HSW16a, HSW16b].

Dieser Umstand resultiert vor allem aus folgenden drei Problemen:

1. Nur wenige Personen verfügen über ein kryptographisches Schlüsselpaar zur E-Mail-Verschlüsselung, da dieser Prozess bisher für Laien nicht einfach und intuitiv genug ausgestaltet wurde bzw. der Bezug von S/MIME-Zertifikaten i.d.R. kostenpflichtig ist.

2. Personen, die über ein kryptographisches Schlüsselpaar verfügen, haben Schwierigkeiten das Zertifikat ihres Kommunikationspartners aufzufinden.

[5] Bei den Daten, die ein Zertifikat neben dem öffentlichen Schlüssel enthält, handelt es sich häufig um personenbezogene Daten wie z. B. Name und E-Mail-Adresse des Zertifikatinhabers. Es ist jedoch grundsätzlich auch möglich, dass das Zertifikat neben dem öffentlichen Schlüssel lediglich pseudonymisierte Daten wie z. B. eine pseudonyme E-Mail-Adresse enthält. Dieser Fall steht jedoch nicht im Fokus dieser Ausarbeitung.

3. Weil regelmäßige Kommunikationspartner entweder kein Schlüsselpaar besitzen oder dieses nicht einfach auffindbar ist, wird kein Bedarf gesehen, selbst Kryptographie-Software zu installieren und Schlüsselpaare zu erzeugen.

Dem ersten Problem begegnet u. a. die im Jahr 2016 gestartete Initiative „Volksverschlüsselung" des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT),[6] indem privaten Endnutzern nach einer Identifizierung kostenfrei ein X.509-Zertifkat für die E-Mail-Verschlüsselung (S/MIME) ausgestellt wird. Dem zweiten Problem[7] begegnet seit 2016 das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Forschungsprojekt „Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln" (VVV), welches im Folgenden Unterkapitel näher vorgestellt werden soll und an welches in den darauf folgenden Kapiteln datenschutzrechtliche Anforderungen formuliert werden sollen.[8]

1.3 Verzeichnisdienste als „Telefonbuch" für Verschlüsselungsschlüssel

Damit der Sender eine Information verschlüsselt an den gewünschten Empfänger schicken kann, benötigt der Sender das Zertifikat des Empfängers. Zertifikate können in so genannten Verzeichnisdiensten abgelegt werden, die eine Art „Telefonbuch" für Verschlüsselungsschlüssel darstellen. Der Sender einer Information kann in einem solchen Verzeichnisdienst – zum Beispiel durch die Eingabe der E-Mail-Adresse des Empfängers – nachschauen, ob sein gewünschter Kommunikationspartner sein Zertifikat in dem Verzeichnisdienst hinterlegt hat. Die Nutzung von Verzeichnisdiensten stellt Nutzer in der Praxis jedoch vor Probleme. So stellen S/MIME-Verzeichnisdienste i. d. R. „isolierte Insellösungen" dar, d. h. sie sind nicht miteinander verbunden und jeder Nutzer kann in seinem E-Mail-Client nur einen einzigen Verzeichnisdienst einstellen. Ist in diesem Verzeichnisdienst das Zertifikat des gewünschten Kommunikationspartners nicht auffindbar, so wird das Zertifikat nicht automatisch in allen weiteren bekannten Verzeichnisdiensten gesucht. Dies ist in etwa vergleichbar mit der Reichweite gedruckter Telefonbücher für einzelne Städte im Gegensatz zu der Onlinevariante eines Telefonbuches, in dem Telefonnummern weltweit gesucht werden können. Beim PGP-Standard (im Folgenden kurz PGP) stellt sich wiederum das Problem, dass Verzeichnisdienste zwar untereinander synchronisiert werden, dieser Umstand jedoch u. a. dazu führt, dass ein Zertifikat nicht mehr manuell durch den Nutzer gelöscht werden oder korrigiert werden kann bzw. nicht (gut) überprüfbar ist, ob eine Veröffentlichung tatsächlich von dem Berechtigten selbst autorisiert wurde oder welches der veröffentlichten Zertifikate (noch) aktuell ist. Diese wenig praktikablen Lösungen sollten durch ein für PGP und S/MIME einheitliches und benutzerfreundliches Verfahren zum Auffinden von Zertifikaten abgelöst werden. Genau dies hat sich das Projekt „Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln" (VVV) zum Ziel

[6] Vgl. https://www.volksverschluesselung.de/, besucht am 27.2.2017.
[7] Es ist davon auszugehen, dass das dritte Problem automatisch durch das Beheben der ersten beiden Probleme gelöst wird.
[8] Vgl. https://keys4all.de/, besucht am 27.2.2017.

gesetzt. Im Fokus steht die Entwicklung eines Verfahrens, mit dem jeder Sender einen vertrauenswürdigen und benutzerfreundlichen Zugang zu den Zertifikaten seines gewünschten Kommunikationspartners erhält. Hierfür stellt der E-Mail-Anbieter des Empfängers einen Verzeichnisdienst bereit, der über dessen Domänenadresse gefunden werden kann. Der Anbieter stellt weiterhin sicher, dass die darin gespeicherten Zertifikate mit einer von ihm bereitgestellten E-Mail-Adresse verknüpft sind. Teil der Entwicklung ist die Erweiterung einer E-Mail-Anwendung, mit der die Zertifikate des Nutzers veröffentlicht und die Zertifikate der Kommunikationspartner automatisch ermittelt werden können [HSW16a, HSW16b].

Der vorliegende Beitrag befasst sich mit dem eben skizzierten einheitlichen und benutzungsfreundlichen Verfahren zum Auffinden von Zertifikaten (im Folgenden: VVV-Lösung) aus datenschutzrechtlicher Sicht. Zunächst werden die relevanten unionsgesetzgeberischen Neuerungen vorgestellt (Kapitel 2). Den Schwerpunkt der rechtlichen Betrachtung bildet sodann die Aufstellung datenschutzrechtlicher Vorgaben an die Lösung sowie an E-Mail-Provider, die diese Lösung anbieten wollen (Kapitel 3). Dies erfolgt auf Grundlage der Datenschutz-Grundverordnung (DSGVO). Der Beitrag endet mit einer Zusammenfassung (Kapitel 4).

2 Neue Regelungen des Unionsrechts

Ab 25. Mai 2018 stellt die DSGVO den allgemeinen Rechtsrahmen für die Verarbeitung personenbezogener Daten in der EU dar. Jeder E-Mail-Provider[9] – als Verantwortlicher i. S. d. Art. 4 Abs. 7 DSGVO – muss bestimmten Verpflichtungen nachkommen, wenn er im Rahmen der Bereitstellung eines E-Mail-Accounts personenbezogene Daten verarbeiten will. Dazu zählen Informationspflichten gegenüber Betroffenen, Nachweispflichten gegenüber den Aufsichtsbehörden sowie Vorsorgepflichten zur Eindämmung von Sicherheitsrisiken. Kommt ein Provider diesen Verpflichtungen nicht hinreichend nach, hat dies regelmäßig einen Gesetzesverstoß zur Folge, der mit einem nicht unerheblichen Bußgeld sanktioniert werden kann.

Der von der EU-Kommission eingebrachte Entwurf einer Verordnung über Privatsphäre und elektronische Kommunikation (e-Privacy-VO-E) wird die Richtlinie für Datenschutz in der elektronischen Kommunikation aus dem Jahr 2002 ersetzen und die DSGVO bereichsspezifisch ergänzen [Ro17b]. Die Notwendigkeit einer regulatorischen Überarbeitung der Richtlinie resultiert aus einschneidenden wirtschaftlichen und vor allem technischen Entwicklungen. So ist die Nutzung klassischer Kommunikationsdienste, wie die Festnetztelefonie, in den vergangenen Jahren zunehmend in den Hintergrund getreten. Demgegenüber hat sich eine rasante Verbreitung neuer, internetbasierter Kommunikationsformen vollzogen zu denen etwa VoIP-Telefonie oder Over-The-Top-Dienste zählen. Diese Entwicklung hat dazu geführt, dass die elektronische Kommunikation nicht mehr vollumfänglich vom derzeitigen

[9] Im Folgenden „Provider“ genannt.

(europäischen-) Rechtsrahmen erfasst wird, was durch den e-Privacy-VO-E ausgeglichen werden soll.

3 Datenschutzrechtliche Einordnung der VVV-Lösung

Die im VVV-Projekt entwickelte Anwendung stellt dem Nutzer über eine Anwendung die Zertifikate der Kommunikationspartner zur Verfügung. Die im Zertifikat aufgeführten Daten wie Name, Vorname sowie eventuell weitere Angaben, etwa Anschrift oder E-Mail-Adresse – PGP erlaubt gar das Einfügen von Gesichtsbildern – stellen personenbezogene Daten dar. Beabsichtigt der Provider nun im Rahmen einer Public-Key-Infrastruktur (PKI) diese Zertifikate zu verwalten und zu verteilen, sind die einschlägigen datenschutzrechtlichen Regelungen zu beachten, die im Folgenden diskutiert werden sollen.

Über die o. g. Anwendung können Inhalte über die Anwendung in Verzeichnisse veröffentlicht und auch aus elektronischen Verzeichnissen abgerufen werden. Es handelt sich entsprechend um einen Telemediendienst, der es dem Nutzer ermöglicht ein Zertifikat in einem Verzeichnis eines E-Mail-Übertragungsdienstes bereitzustellen. E-Mail-Übertragungsdienste gehören zur Kategorie interpersoneller Kommunikationsdienste, wie sie in Art. 2 Abs. 5 im Entwurf der Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation[10] definiert sind. Dieser Definition folgt auch der Entwurf der e-Privacy-VO.

4 Relevante Vorgaben des Entwurfs der e-Privacy-VO

Art. 15 e-Privacy-VO-E befasst sich mit der Regelung öffentlich zugänglicher Verzeichnisse. Was unter einem öffentlich zugänglichen Verzeichnis im Sinne des Verordnungsentwurfes zu verstehen ist, beschreibt Art. 4 Abs. 3 lit. d e-Privacy-VO-E. Hiernach handelt es sich um ein Verzeichnis der Endnutzer elektronischer Kommunikationsdienste in gedruckter oder elektronischer Form, das veröffentlicht oder der Öffentlichkeit bzw. einem Teil der Öffentlichkeit zugänglich gemacht wird, auch mithilfe eines Verzeichnisauskunftsdienstes. Die in derartigen Verzeichnissen gespeicherten Informationen umfassen etwa Telefonnummern, E-Mail-Adressen oder andere Kontaktangaben der Endnutzer.[11] Sie erfüllen mithin die Funktion eines (elektronischen) Telefonbuchs. Die Hinterlegung des einem Endnutzer zugeordneten Zertifikats in ein providerseitiges Verzeichnis und die Möglichkeit der öffentlichen Abfrage dieser Information mit dem Zweck der Kontaktaufnahme, erfüllt ebenfalls diese (Auskunfts-)Funktion und fällt damit in den Anwendungsbereich des

[10] Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über den Kodex für die elektronische Kommunikation, COM(2016) 590 final- 2016/0288 (COD).
[11] S. Erwägungsgrund 30 des Verordnungsentwurfs.

Verordnungsentwurfs.

Die im Entwurf exemplarisch aufgeführten Angaben wie Telefonnummer und E-Mail-Adresse repräsentieren ein eindeutiges Kommunikationsmedium. Zwar stellt der Versand einer Ende-zu-Ende-verschlüsselten E-Mail in Relation zu einer unverschlüsselten E-Mail eine signifikante Veränderung der Kommunikationsform dar, die sich nicht allein in der technischen Absicherung der informationellen Selbstbestimmung, sondern zudem in der gefühlten kommunikativen Selbstbestimmung und damit dem kommunikativen Verhalten selbst äußert. Für eine Auslösung des Anwendungsbereichs des Art. 15 e-Privacy-VO-E auf VVV spricht das erklärte Bestreben des europäischen Gesetzgebers neuartige, bisher ungeregelte, internetbasierte Kommunikationsdienste zu regulieren.

Dies hätte zu Folge, dass die Provider von den Nutzern als Betroffene (natürliche Personen) gem. Art. 15 Abs. 1 e-Privacy-VO-E die ausdrückliche Einwilligung in die Aufnahme des mit VVV etablierten Verzeichnisdienstes einzuholen verpflichtet sind. Neben der Aufnahme erstreckt sich die Einwilligung auch auf die Suchfunktionalitäten von VVV, über die der Nutzer im Vorhinein aufzuklären ist. Erst dann darf das Zertifikat der Nutzer via VVV an andere Kommunikationspartner übermittelt werden. Für die Anforderungen, denen die Einwilligung genügen muss, verweist Art. 9 Abs. 1 e-Privacy-VO-E auf die einschlägigen Bestimmungen der DSGVO. Juristische Personen haben bezüglich der Aufnahme ihrer Zertifikate in das Verzeichnis gem. Art. 9 Abs. 3 e-Privacy-VO-E lediglich ein Widerspruchsrecht. Den Nutzern von VVV – unabhängig ob sie nun natürliche oder juristische Personen sind – wird darüber hinaus nach Art. 15 e-Privacy-VO-E das Recht eingeräumt ihre Zertifikate kostenlos auf ihre Richtigkeit hin zu überprüfen und ggf. zu löschen.[12]

5 Relevante Vorgaben der DSGVO

Die folgenden Unterabschnitte thematisieren die Rechtmäßigkeit der Verarbeitung, die Datenminimierung, die Datenrichtigkeit, die Löschung, die Informationspflichten, die Datensicherheit, die Haftung der Provider sowie die Rechenschaftspflichten als rechtliche Anforderungen der Datenschutz-Grundverordnung an die VVV-Lösung.

5.1 Rechtmäßigkeit der Verarbeitung

Die Zertifikate des Nutzers werden vom Provider z. B. auf seinem eigenen Server oder dem Server eines Unterauftragnehmers gespeichert und bei entsprechenden Anfragen an die jeweiligen Kommunikationsteilnehmer übermittelt. Diese Verwaltung der Zertifikate beim Provider stellt eine Verarbeitung i. S. d. Art. 4 Nr. 2 DSGVO dar und muss für eine

[12] Zur Problematik des Löschungsanspruchs s. Punkt 3.2.4 in Bezug zur DSGVO.

rechtliche Legitimation einen Tatbestand des Art. 6 Abs. 1 UAbs. 1 erfüllen [PP17]. Hat der Nutzer einen Account bei einem E-Mail-Provider, der auch VVV-Dienste unterstützt, liegt als Rechtsgrundlage der Datenverarbeitung bereits ein Vertrag mit dem Provider i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO vor [Ro17a]. Das Hochladen des **eigenen** Zertifikats mit einem vom Provider bereitgestellten Verfahren, kann in diesem Fall als konkludente Vertragserweiterung angesehen werden, auf welche die Verarbeitung gestützt werden kann.[13] Hiervon ist auch auszugehen, wenn die Erbringung des E-Mail-Dienstes mit einer entsprechenden VVV-Erweiterung kostenlos ist. Im Rahmen der Vertragserweiterung sollte der Provider dem Betroffenen demnach alle Umstände der Datenverarbeitung hinreichend bekannt machen, bevor dieser sein Zertifikat via VVV publiziert. Hierzu ist es empfehlenswert den Vorgang des Schlüsselhochladens in einem eindeutig informierenden, bspw. Opt-in gestalteten Verfahren, vorzunehmen und die Umstände im Vertrag zu integrieren.

Die Verarbeitung personenbezogener Daten Dritter, z.B. in Form eines signierten Schlüssels ist jedoch nicht vertraglich erfasst [Mo11]. Der Provider hat sicherzustellen, dass der jeweilige Schlüssel auch vom Inhaber der korrespondierenden E-Mail-Adresse stammt und der Inhaber den zugehörigen privaten Schlüssel nutzen kann.

5.2 Datenminimierung

In den in Art. 5 DSGVO normierten Grundsätzen der Datenverarbeitung ist in lit. c die Datenminimierung festgeschrieben. Hiernach muss die Verarbeitung personenbezogener Daten dem Zweck angemessen, erheblich sowie auf das notwendige Maß begrenzt sein [PP17]. Der Grundsatz der Datenminimierung ist als solcher nicht neu, trat er doch bisher im Gewand Erforderlichkeit in Art. 6 Abs. 1 lit. c DSRL in Erscheinung. Die demgegenüber abzugrenzende Datensparsamkeit des BDSG ist strenger gefasst und hinterfragt bereits die Zweckbestimmung, wohingegen die Datenminimierung die bereits zweckgebundene Datenverarbeitung auf ein erforderliches Maß zu reduzieren sucht [Ro17a] [Ro03]. Dies wird etwa dann relevant, wenn der Betroffene nachweisen muss, dass er tatsächlich der Inhaber des Zertifikats ist, den er in das Verzeichnis des Providers hochzuladen beabsichtigt. Die damit verbundene Authentifizierung des Nutzers erfordert regelmäßig die Angabe personenbezogener Daten. Unter Berücksichtigung der Datenminimierung sollte der Provider in diesem Fall die Verifizierung des Zertifikats, soweit dies möglich und sinnvoll ist, anhand von Daten vornehmen, die ihm bereits aus dem bestehenden Vertragsverhältnis mit dem Betroffenen bekannt sind. Hierunter fällt bspw. die E-Mail-Adresse des entsprechenden Accounts. Von darüber hinausgehenden Angaben sollte abgesehen werden.

[13] S. aber unabhängig vom Vorliegen eines bestehenden Vertrags die Erforderlichkeit der Einwilligung in die Aufnahme des Verzeichnisdienstes i. S. d. Art. 15 e-Privacy-VO-E. Zur technischen Umsetzung der Einwilligung im Rahmen des Projekts VVV vgl. den im selben Kapitel erschienenen Beitrag zu Verfahren zur vertrauenswürdigen Verteilung von Verschlüsselungsschlüsseln.

5.3 Datenrichtigkeit

Gem. Art. 15 Abs. 1 Satz 2 e-Privacy-VO-E muss der Provider eine Überprüfung, Berichtigung und Löschung personenbezogener Daten ermöglichen. Korrespondierend hierzu hat jeder Betroffene nach Art. 16 DSGVO das Recht, fehlerhafte oder unvollständige personenbezogene Daten unverzüglich vom Provider berichtigen zu lassen [Ro17a]. Diese Norm konkretisiert den in Art. 5 Abs. 1 lit. d DSGVO normierten Grundsatz der Datenrichtigkeit. Hiernach sind die personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neusten Stand zu halten. Ein Zertifikat ist für den Inhaber nutzlos, wenn er nicht korrekt durch den Provider übernommen wird. Eine Entschlüsselung der empfangenen E-Mails wäre dann nicht mehr möglich. Die Aktualität eines Zertifikats stellt hier ein besonderes Problem dar. Erfolgt keine Synchronisation mit anderen Servern (PGP) und auch kein Abgleich mit Revocationlists (S/MIME), sollte der Provider in Zusammenarbeit mit dem Kunden/Inhaber des Zertifikats ein nutzerkontrolliertes Löschen bzw. Aktualisieren des Zertifikats ermöglichen. Denn obwohl ein abgelaufenes Zertifikat i. d. R. funktionsfähig bleibt, stellt sich für den verschlüsselnden Kommunikationspartner (nicht Zertifikatinhaber) die Frage, ob das Zertifikat tatsächlich weiter verwendet werden soll. Die Verteilung eines abgelaufenen Zertifikats durch einen Provider stellt sowohl die Vertraulichkeit der Nachrichten als auch die Integrität des Zertifikats selbst in Frage. In der Folge hat auch der Provider ein Interesse an der Aktualität der im Umlauf befindlichen Zertifikate. Es erscheint ratsam dem Nutzer in einem standardisierten Verfahren rechtzeitig auf den Ablauf des Zertifikats hinzuweisen.

Laut Art. 5 Abs. 1 lit. d DSGVO sind personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich zu löschen oder zu berichtigen. Der Verarbeitungszweck eines Zertifikats liegt in der Gewährleistung der Vertraulichkeit der E-Mail-Kommunikation. Zweifel an der Aktualität und damit der Integrität eines Zertifikats gefährden die Vertraulichkeit der Kommunikation und widersprechen damit dem Zweck seiner Verarbeitung. Stellt ein Provider ein abgelaufenes Zertifikat weiter zu Verfügung und entsteht einem Nutzer dadurch ein Schaden, beispielweise durch den Verlust von Geschäftsgeheimnissen, könnte der Provider für den Schaden haften.[14]

5.4 Löschung

Art. 17 Abs. 1 DSGVO normiert den Anspruch der betroffenen Person auf Löschung ihrer sämtlichen personenbezogenen Daten. Dieses „Recht auf Vergessenwerden“ greift in den Fällen, in denen die Daten für die ursprüngliche Zweckerreichung nicht mehr notwendig sind, der Betroffene seine Einwilligung widerruft, die Befristung ausläuft, der Verarbeitung widersprochen wird bzw. diese mit der DSGVO nicht vereinbar ist

[14] Das Zertifikat enthält zwar keine Information darüber, woher es für einen konkreten Verwendungsfall heruntergeladen wurde. Die Verantwortung für den Nachweis über den ordnungsgemäßen Betrieb des Keyservers muss der Provider jedoch selbst, z. B. durch Dokumentation von Änderungen in der Datenbank, gemäß ISO- oder BSI-Grundschutzstandards erbringen.

[Ro17a]. Art. 17 DSGVO konkretisiert in der Folge ebenfalls den in Art. 5 Abs. 1 lit. d DSGVO verorteten Grundsatz der Datenrichtigkeit. Die aus diesem Recht geschaffene Möglichkeit sein Zertifikat zu löschen, ist mit den derzeit gebräuchlichen Verfahren (bei PGP) technisch nicht umsetzbar, da sich die einzelnen Keyserver untereinander synchronisieren. In der Folge müsste der Datensatz simultan auf allen dem Verbund angehörigen Servern gelöscht werden, die unter unterschiedlicher Kontrolle stehen. Das Zertifikat kann in einer derartigen Architektur lediglich für ungültig erklärt und entsprechend markiert bzw. ein zusätzliches Widerrufszertifikat veröffentlicht werden, durch den die Ungültigkeit erklärt wird. Demgegenüber erfolgt in der VVV-Lösung keine Synchronisation der Schlüsselserver untereinander und eine damit einhergehende Datenredundanz. Der Betroffene hat also zu jeder Zeit die Möglichkeit sein Zertifikat aus dem Verzeichnis zu löschen.[15]

5.5 Informationspflichten

Zu den Informationspflichten eines Providers gehören hauptsächlich Aufklärung, Auskunft und Benachrichtigung der Nutzer. Unter Umständen ergeben sich auch Informationspflichten gegenüber der zuständigen Aufsichtsbehörde. Die gesetzlichen Informationspflichten gegenüber dem Nutzer beginnen bereits vor der Datenerhebung mit dem Einholen der Einwilligung des Nutzers in die Datenverarbeitung (Art. 15 Abs. 1 Satz 1 e-Privacy-VO-E). Die Bedingungen an Freiwilligkeit und Informiertheit bestehen weiter fort, jedoch werden an verschiedenen Stellen Vereinfachungen für die Betroffenen ermöglicht. Auf die Verantwortlichen kommen damit z. T. andere Aufgaben zu. So sieht der Entwurf der e-Privacy-VO in Art. 2 Abs. 2 für die Betreiber von Verzeichnissen auch eine Einwilligung in die Freischaltung von verfügbaren Suchfunktionen vor. Die DSGVO stellt ihrerseits auf eine umfassende Informiertheit des Betroffenen ab. Die Pflichten des Verantwortlichen gegenüber dem Betroffenen gelten unabhängig davon, ob die Erhebung direkt bei der Person oder an anderer Stelle stattfindet. Jedoch erweitert Art. 14 Abs. 1 und Abs. 2 litt. a-d DSGVO in diesem Fall den Umfang der Informationspflichten im Gegensatz zu Sachverhalten bei denen die Daten bei den Betroffenen i. S. d. Art. 13 Abs. 1 und Abs. 2 litt. a-d erhoben wurden [Ma16]. Zusätzlich zu den bisherigen Informationen, wie dem Zweck der Datenverarbeitung, muss dem Nutzer verdeutlicht werden auf welcher Rechtsgrundlage die Verarbeitung stattfindet (Art. 13 Abs. 1 lit. c DSGVO). Zudem müssen die Speicherdauer bzw. Kriterien für die Festlegung der Speicherdauer mitgeteilt werden (Art. 13 Abs. 2 lit. a DSGVO). Der Verantwortliche muss außerdem über weitere Empfänger und eine beabsichtigte Übermittlung in Drittländer oder an internationale Organisationen informieren (Art. 13 Abs. 1 litt. e, f DSGVO). Die Anforderungen an eine informierte und damit in allen Teilen gültige Einwilligung umfassen auch die Aufklärung des Nutzers über sein Recht auf Auskunft, Berichtigung und Löschung der Verarbeitung sowie neuerdings das Recht auf Datenübertragbarkeit (Art. 13 Abs. 2 lit. b DSGVO).

[15] Jedoch sieht die VVV-Lösung nicht die Möglichkeit vor, ein Widerrufszertifikat zu veröffentlichen, so dass andere Nutzer nicht erfahren können, warum das Zertifikat gelöscht wurde. Dem Nutzer soll die Möglichkeit offen stehen, das Zertifikat zu wiederrufen, weil er lediglich nicht mehr im Verzeichnisdienst stehen möchte.

5.6 Datensicherheit

Die Provider, die Teil der VVV-Architektur sind, müssen auch für die Sicherheit der ihnen überantworteten personenbezogenen Zertifikatsinformationen Sorge tragen. Den Rahmen hierfür geben Art. 5 und 32 DSGVO vor. Art. 5 Abs. 1 lit. f DSGVO statuiert diesbezüglich den Grundsatz der Integrität und Vertraulichkeit personenbezogener Daten. Hiernach sind technische und organisatorische Maßnahmen zu ergreifen, die geeignet sein müssen, einer missbräuchlichen Verarbeitung, dem unbeabsichtigten Verlust, der Schädigung oder Zerstörung personenbezogener Daten vorzubeugen. Wie diese zu ergreifenden technischen und organisatorischen Maßnahmen im Einzelfall auszugestalten sind, konkretisiert der mit „Sicherheit der Verarbeitung" überschriebene Art. 32 DSGVO [Ro17a]. Sie haben sich an dem jeweiligen Zweck der Verarbeitung, dem Stand der Technik sowie dem Risiko der Datenverarbeitung für „Rechte und Freiheiten natürlicher Personen" zu orientieren. Neben den Datensicherheitsanforderungen der DSGVO tritt für VVV als Verzeichnisdienst im Sinne des Art. 15 e-Privacy-VO-E die Vertraulichkeit der elektronischen Kommunikationsdaten gem. Art. 5 e-Privacy-VO-E.[16]

Die vom Provider zu ergreifenden technischen und organisatorischen Maßnahmen betreffen auch den Zugriff auf die einzelnen Zertifikate, um das potenzielle Risiko eines Missbrauchs für die Betroffenen so gering wie möglich zu halten. Das von VVV vorgesehene Zugriffs- und Berechtigungskonzept schränkt die z.T. sehr undifferenzierten Suchmöglichkeiten von Zertifikaten deutlich ein. Eine Suchanfrage liefert überhaupt nur ein Ergebnis, wenn die vollständige E-Mail-Adresse eingegeben wird. Im zweiten Schritt gibt der Server nur das eine Zertifikat aus, der vom Inhaber zur Verfügung gestellt wurde. Anders als im gegenwärtigen Verfahren ist also keine Zertifikatshistorie einsehbar. Des Weiteren sind die Übertragungswege der Zertifikate und damit verbundene Abfragen vor potenziellen Sicherheitsrisiken zu schützen. Die Informationen über die unterstützten Verschlüsselungsverfahren und das korrespondierende Schlüsselverzeichnis werden durch die DNS-Betreiber verbindlich mit DNSSEC und DANE gegen Veränderung abgesichert [WF16] [Sc16].[17] Die weiteren Kommunikationsvorgänge, die in die Verantwortlichkeit des Providers fallen, sind zudem kryptografisch abzusichern und zu authentisieren.

5.7 Haftung der Provider

Art. 82 Abs. 2 DSGVO besagt: „Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende

[16] Als elektronische Kommunikationsdaten gem. Art. 4 Abs. 3 lit. a e-Privacy-VO-E gelten auch Metadaten zum Zweck der Übermittlung, Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte.

[17] In der VVV-Lösung wird mit DANE die Authentizität der vom Provider eingesetzten TLS-Zertifikate bei der verschlüsselten Kommunikation mit den Schlüsselservern abgesichert, nicht aber die Informationen zu den unterstützen Schlüsselservern. Die Informationen zu den unterstützen Schlüsselservern sind über DNSSEC-Signaturen geschützt.

Verarbeitung verursacht wurde."[18] Dabei ist es unerheblich, ob es sich um einen materiellen oder immateriellen Schaden handelt (Art. 82 Abs. 1 DSGVO). Art 82 Abs. 3 DSGVO statuiert die Verschuldenshaftung mit Beweislastumkehr, wonach der Verantwortliche oder der Auftragsverarbeiter von der Haftung des Abs. 2 befreit wird, wenn er nachweisen kann, dass er nicht für den Umstand durch den der Schaden entstanden ist verantwortlich ist.

In Art. 5 Abs. 2 DSGVO legt der Gesetzgeber ausdrücklich fest, dass der Verantwortliche die Einhaltung der Bestimmungen aus Absatz 1 nachweisen können muss. Entsprechend dieser Gesetzeslage kann eine betroffene (natürliche) Person Schadenersatz verlangen, wenn der Provider nicht nachweisen kann, dass die Verarbeitungsgrundsätze der Verordnung eingehalten wurden.

5.8 Rechenschaftspflichten/Nachweispflichten

Zu den Nachweispflichten/Rechenschaftspflichten gegenüber der Aufsichtsbehörde zählen die Verfahrensnachweise bzw. Datenschutz-Folgenabschätzungen (Art. 35 DSGVO) und Meldungen von Verletzungen des Schutzes personenbezogener Daten gem. Art. 33 DSGVO. Mit Art. 24 DSGVO erfolgt eine Umkehrung der Beweislast. Musste der Betroffene bisher nachweisen, dass der Verantwortliche personenbezogene Daten fehlerhaft verarbeitet hat, ist es nun Sache des für die Verarbeitung Verantwortlichen. Gleiches gilt für die Einwilligung der Betroffenen in die Datenverarbeitung (Art. 7 Abs. 1 DSGVO)

6 Zusammenfassung

Als eine Möglichkeit, Ende-zu-Ende-Verschlüsselung benutzungstauglicher zu gestalten, verwies dieser Beitrag auf die Lösung des Projekts „Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln", im Rahmen dessen wenig praktikable Lösungen von Verzeichnisdiensten durch ein für PGP und S/MIME einheitliches und benutzungsfreundliches Verfahren zum Auffinden von Zertifikaten abgelöst werden sollen. Der Beitrag formulierte sodann datenschutzrechtliche Anforderungen an diese Lösung.

Die im Zertifikat häufig aufgeführten Daten wie Name und Vorname stellen personenbezogene Daten dar, deren Verarbeitung ab dem 25. Mai 2018 die Datenschutz-Grundverordnung regeln wird. Beabsichtigt also ein Provider, die Zertifikate zu verwalten und zu verteilen, sind die einschlägigen Regelungen der Datenschutz-Grundverordnung zu beachten. Dazu zählen u. a. Nachweispflichten gegenüber den Aufsichtsbehörden sowie Vorsorgepflichten zur Eindämmung von Sicherheitsrisiken.

[18] Die Haftung der e-Privacy-VO-E ist in Art. 22 geregelt und verweist auf die Ausnahmetatbestände des Art. 82 DSGVO.

Der von der EU-Kommission eingebrachte Entwurf einer Verordnung über Privatsphäre und elektronische Kommunikation wird die DSGVO darüber hinaus bereichsspezifisch ergänzen. Der Entwurf regelt für öffentliche Verzeichnisdienste, die als Telemediendienste einzustufen sind, angemessene Interventionsmöglichkeiten für den Endnutzer bereitzustellen. Dazu gehört u. a., dass der Endnutzer über die Aufnahme der Kategorien personenbezogener Daten bestimmt und seine Daten überprüfen, berichtigen und löschen kann.

Literaturverzeichnis

[HSW16a] Herfert, M.; Selzer, A.; Waldmann, U.: Selbstdatenschutz in Zeiten massenhafter E-Mail-Überwachungen, in: BvD-News 01/2016, S. 57-59, 2016.

[HSW16b] Herfert, M.; Selzer, A.; Waldmann, U.: Laientaugliche Schlüsselgenerierung für die Ende-zu-Ende-Verschlüsselung, in: DuD 2016, S. 290-294, 2016.

[KSS15] Kühling,.J.; Seidel, C.; Sivridis, A.: Datenschutzrecht, 3. Aufl., 2015.

[Ma16] Marschall, K.: Erweiterte Informationspflichten in der DSGVO: Änderungen für die Unternehmen, in: DSB S. 231-233, 2016.

[Mo11] Mommers, C.: BGH präzisiert Zulässigkeit von Deep-Links, in: DFN-Infobrief Recht 1/11, 2011.

[PP17] Paal, B.; Pauly, D.: Datenschutz-Grundverordnung, 2017.

[Ro03] Roßnagel, A. (Hrsg.): Handbuch Datenschutzrecht, 2003.

[Ro17a] Roßnagel, A. (Hrsg.): Europäische Datenschutz-Grundverordnung, 2017.

[Ro17b] Roßnagel, A. (Hrsg.): Entwurf einer E-Privacy-Verordnung – Licht und Schatten, in: ZPR 2017, S. 33, 2017.

[Sc16] Schirrmacher, D.: Haufenweise Fake-PGP-Schlüssel im Umlauf, über: https://www.heise.de/security/meldung/Haufenweise-Fake-PGP-Schluessel-im-Umlauf-3297175.html, besucht am 11.4.2017.

[WF16] Waldmann, U.; Fischer, P.: Technische Beschreibung der VVV-Lösung, 2016.

[WB16] Wolff, H.; Brink, S.: Datenschutzrecht in Bund und Ländern, 2016.