Sicher verschickt

Briefpost DSGVO-konform verschlüsseln

Schwammige Formulierungen in der DSGVO verpflichten möglicherweise zum Verschlüsseln von Briefpost. Für Unternehmen, Behörden und Bürger bedeutet das erheblichen Aufwand.

Von Jan Mahn und Merlin Schumacher

Die Datenschutzgrundverordnung gilt als vage und unpräzise formuliert. Kritiker bemängeln seit Jahren, dass das Gesetzeswerk, das in nationales Recht überführt werden musste, aufgrund unklarer Rechtsbegriffe zu viel Spiel für Interpretationen lasse und die Gerichte noch auf Jahre beschäftigen würde.[1]

Nimmt man den Gesetzestext wörtlich, seien Behörden und Großunternehmen, die eine Webseite betreiben und dort ihre Postadresse angeben, dazu verpflichtet, eingehende Briefe auch verschlüsselt anzunehmen. Was für digitale Kontaktformulare gelte, gelte auch für analoge Post.

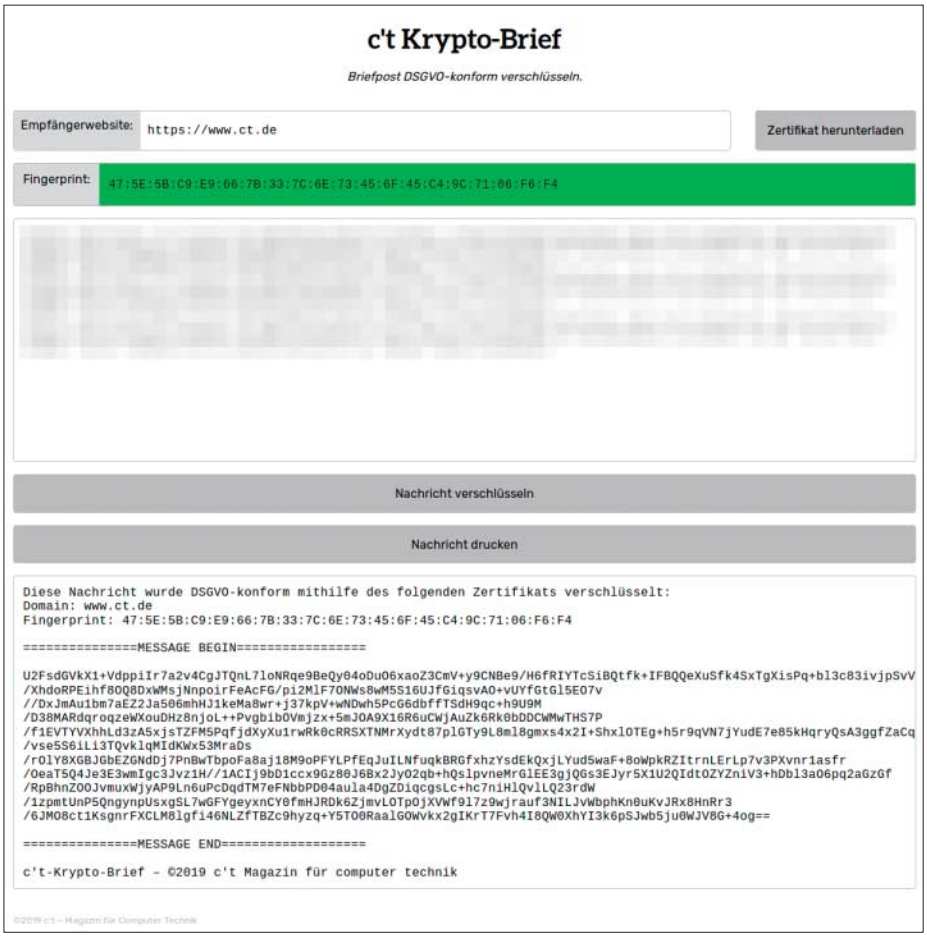
Davon ist zumindest der deutsch-griechische Netzaktivist Protos Munichion überzeugt und begründet das mit der sogenannten Technologieneutralität. Munichion arbeitet auch in Deutschland als Rechtsanwalt und berät Online-Händler und Behörden. Auf die Schwachstelle in der DSGVO stieß er, nachdem er für eine Stadtverwaltung die Datenschutzerklärung für die Homepage ausgearbeitet hatte. Ein Behördenmitarbeiter aus der IT-Abteilung stellte ihm nach der Einrichtung eines SSL-Zertifikats für das Online-Kontaktformular die entscheidende Frage: „Gilt das mit der Verschlüsselung jetzt eigentlich auch für die eingehende Post?“ Munichion ging der Sache nach, las den DSGVO-Text und befragte den zuständigen Landesdatenschutzbeauftragten. Festlegen wollte sich niemand, grundsätzlich widersprach aber auch niemand.

Um Rechtssicherheit herzustellen, entschied sich Munichion dazu, einen Präzedenzfall zu schaffen. Als Gegner wählte er seine griechische Heimatgemeinde – dort verfügte er über eine Zulassung als Rechtsanwalt. Munichion rief das SSL-Zertifikat der Webseite der Gemeinde ab, kopierte den öffentlichen Schlüssel heraus und verschlüsselte damit einen Bauantrag für ein Wochenendhaus. Das Bauamt weigerte sich erwartungsgemäß, einen verschlüsselten Bauantrag auf dem Postweg entgegenzunehmen, Munichion verpasste dadurch eine Frist für Fördergelder und zog wie geplant vor Gericht.

Der Fall ging durch alle Instanzen und landete vor dem höchsten griechischen Verwaltungsgericht in Athen. Die Richter gaben Munichion grundsätzlich Recht, verwiesen den Fall aber an den Europäischen Gerichtshof und verlangten die Klärung von zwei Grundsatzfragen: Erstreckt sich die Pflicht für Postempfänger, verschlüsselte Kommunikation zu ermöglichen, auch auf den analogen Postweg? Und könnten solche Organisationen sogar verpflichtet sein, Briefe ausschließlich verschlüsselt anzunehmen? Eine solche Pflicht ginge weit über das hinaus, was Munichion erreichen wollte.

Die Entscheidung der Luxemburger Richter hätte Folgen für die gesamte Europäische Union und würde auch für Deutschland gelten – bis dahin dürften aber noch einige Monate vergehen. In einer ersten Stellungnahme während des Verfahrens stellte ein Sprecher des Gerichts aber bereits klar, dass Munichions Rechtsauffassung grundsätzlich richtig sei. Es gehe vor allem um die Frage, ob unverschlüsselte Briefe ganz verboten werden könnten.

Auch die Europäische Konferenz der Verwaltungen für Post und Telekommu-



Mit dem c’t-Krypto-Brief können Sie Ihre Post rechtssicher verschlüsseln.

nikation (CEPT) zeigte sich von der Entscheidung überrascht, aber begeistert: „Es ist richtig und wichtig, dass der Brief im 21. Jahrhundert noch Beachtung findet und moderne Verschlüsselungsmethoden auch auf dem Papier ankommen“, teilte CEPT-Pressesprecherin Élodie Germinal gegenüber c’t mit.

Erwägungsgründe und vage Begriffe

Die Argumentation stützt sich auf Artikel 2 und 5 der DSGVO. Artikel 2 regelt den Geltungsbereich der Verordnung: „Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten.“ Die Rede ist explizit nicht etwa von Computersystemen oder elektronischer Datenverarbeitung. Folgen die Luxemburger der Einschätzung, gilt die DSGVO damit auch für alle Poststellen von Behörden und großen Unternehmen, die irgendeine Form der Automation einsetzen – also zum Beispiel maschinelle Brieföffner, Förderbänder oder automatische Scan-Systeme, die in vielen Poststellen zu finden sind.

Artikel 5 regelt dann, wie Datenverarbeitung erfolgen muss. Absatz 1, Satz f fordert: „Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung […] durch geeignete technische und organisatorische Maßnahmen.“ Was eine geeignete technische Maßnahme ist, schreibt der Gesetzgeber nicht. Betreiber von Webseiten leiten aus der Formulierung die Pflicht ab, verschlüsselten Verkehr über HTTPS zu ermöglichen, wenn ein Kontaktformular angeboten wird. Eine wesentlich deutlichere Formulierung findet sich in den sogenannten Erwägungsgründen. Das sind Zusätze zum Gesetz, die während des Gesetzgebungsverfahrens festgehalten wurden und die Intentionen der Gesetzgeber erläutern sollen. Erwägungsgrund 15 unterstützt Munichions Ansicht: „Um ein ernsthaftes Risiko einer Umgehung der Vorschriften zu vermeiden, sollte der Schutz natürlicher Personen technologieneutral sein und nicht von den verwendeten Techniken abhängen.“

»Es ist richtig und wichtig, dass moderne Verschlüsselungsmethoden auch auf dem Papier ankommen.«

Geeignete Maßnahme

Die Idee, analoge Post mit dem öffentlichen Schlüssel des SSL-Zertifikats eines Webseitenbetreibers zu verschlüsseln, ist in jedem Fall eine geeignete Maßnahme, die Sicherheit der Übertragung sicherzustellen. Nur der Inhaber des zugehörigen privaten Schlüssels, also der Webseitenbetreiber, ist in der Lage, den Inhalt wieder zu entschlüsseln. Der Aufwand zum Entschlüsseln ist überschaubar. Das Problem des Schlüsseltauschs, bei jeder Form von Verschlüsselung der kritische Moment, ist durch das etablierte HTTPS bereits gelöst und erprobt. Alternativ können Sie Ihre Nachricht per PGP verschlüsseln, wenn Sie den Schlüssel des Empfängers kennen. Leider ist PGP bislang bei den wenigsten Ämtern eine Option. Eventuell kann man auch eine De-Mail schreiben, ob das Amt in der Lage ist diese zu empfangen, ist fraglich [2].

Damit Sie die sichere Kommunikation bereits vor der endgültigen Entscheidung der Luxemburger Richter des EuGH ausprobieren können, haben wir eine Webseite vorbereitet, die Ihnen als Versender die meiste Arbeit abnimmt – siehe ct.de/yv3y.

Geben Sie dafür zunächst die URL des Empfängers in Form von `https://www.beispiel.de/` ein. Klicken Sie dann auf „Zertifikat herunterladen“. Die Anwendung lädt nun das Zertifikat der Website herunter und zeigt Ihnen den SHA1-Fingerprint des Zertifikats zur Validation an. Wenn Sie die Empfänger-URL in Ihrem Browser abrufen, können Sie über die Zertifikatsinformationen prüfen, ob der Fingerprint übereinstimmt.

Der Verschlüsselungsvorgang passiert nur in Ihrem Browser, lediglich das Beschaffen des Zertifikats erfolgt über einen externen Server, da der Download des Zertifikats innerhalb eines Webbrowsers nicht möglich ist. Geben Sie nach dem Zertifikats-Download Ihre Nachricht an den Empfänger ein und klicken Sie auf „Nachricht verschlüsseln“. Die JavaScript-Bibliothek CryptoJS verschlüsselt dann Ihre Nachricht mit Hilfe des öffentlichen Schlüssels. Im unteren Feld sehen Sie nun die verschlüsselte Nachricht. Die können Sie nun mittels des „Nachricht drucken“-Knopfs zu Papier bringen lassen. Anschließend verfahren Sie mit dem Ausdruck wie mit normaler Briefpost.

Der Anwalt Protos Munichion hat die Gesetzeslücke in der DSGVO aufgedeckt.

Ungeklärte Fragen

Ungeklärt ist bis dato noch, wie man mit Dokumenten verfährt, die eine eigenhändige Unterschrift verlangen. Auch die Übersendung von Formularen ist ein schwieriger Fall. Eventuell ist es hier nötig, das Dokument einzuscannen, in einen Base64-kodierten Datenstrom umzuwandeln, zu verschlüsseln und auszudrucken. Auch wie Menschen ohne Computer in Zukunft rechtssicher mit Behörden Kontakt aufnehmen können, ist noch offen. Bis zum endgültigen Urteil sollten Sie mit dem Einsatz der Verschlüsselung noch warten. Insbesondere dann, wenn wie bei Protos Munichion der Verlust von Fördergeldern oder anderes Ungemach droht. *(mls@ct.de)* c't

Literatur

[1] Holger Bleich, Holpriger DSGVO-Start, Erste Auswirkungen des neuen EU-Datenschutzes, c’t 13/2018, S. 16
[2] Tim Gerber, Unerreichbar, Wie die Justiz den elektronischen Rechtsverkehr behindert, c't 7/2018, S. 30

***c’t-Krypto-Brief:* ct.de/yv3y**