

Kleine Anfrage

der Abgeordneten Gisela Piltz, Hans-Joachim Otto (Frankfurt), Christoph Waitz, Dr. Max Stadler, Christian Ahrendt, Hartfrid Wolff (Rems-Murr), Jens Ackermann, Dr. Karl Addicks, Uwe Barth, Rainer Brüderle, Angelika Brunkhorst, Ernst Burgbacher, Patrick Döring, Jörg van Essen, Ulrike Flach, Otto Fricke, Horst Friedrich (Bayreuth), Hans-Michael Goldmann, Miriam Gruß, Dr. Christel Happach-Kasan, Elke Hoff, Birgit Homburger, Dr. Heinrich L. Kolb, Gudrun Kopp, Jürgen Koppelin, Heinz Lanfermann, Sibylle Laurischk, Harald Leibrecht, Ina Lenke, Sabine Leutheusser-Schnarrenberger, Michael Link (Heilbronn), Markus Löning, Horst Meierhofer, Patrick Meinhardt, Jan Mücke, Burkhardt Müller-Sönksen, Detlef Parr, Cornelia Pieper, Frank Schäffler, Marina Schuster, Carl-Ludwig Thiele, Florian Toncar, Dr. Daniel Volk, Dr. Claudia Winterstein, Dr. Volker Wissing, Dr. Guido Westerwelle und der Fraktion der FDP

Planungen der Bundesregierung zur Einführung von De-Mail

Die Bundesregierung plant die Einführung eines De-Mail-Dienstes, mit dem neben bereits bestehenden Möglichkeiten der verschlüsselten und mithin sicheren elektronischen Kommunikation eine Infrastruktur für sicheren Mail-Versand geschaffen werden soll. Über De-Mail sollen Bürgerinnen und Bürger im Rahmen der Weiterentwicklung von E-Government-Anwendungen sicher mit Behörden kommunizieren können.

Die Förderung der rechtssicheren, datensicheren und zuverlässigen elektronischen Kommunikation zwischen Behörden und Unternehmen sowie Bürgerinnen und Bürgern ist für die Informationsgesellschaft von erheblicher Bedeutung.

Allerdings ist bislang nicht hinreichend klar, warum der Staat hier eine eigene Infrastruktur aufbauen muss statt auf bestehende Möglichkeiten zurückzugreifen. Der im Aufbau von De-Mail liegende Eingriff in marktwirtschaftliche, aber auch technische Entwicklungen muss genau geprüft werden.

Datensicherheit und Datenschutz sind unabdingbare Voraussetzung für das Vertrauen der Bürgerinnen und Bürger sowie Unternehmen in E-Government. Nur wenn Datenschutz und Datensicherheit groß geschrieben werden, werden E-Government-Anwendungen auch von den Nutzern angenommen. Daher müssen beim Projekt De-Mail diese Aspekte besonders gewürdigt werden.

Die EU-Dienstleistungsrichtlinie führt erfreulicherweise zu einem Schub bei der Entwicklung von E-Government in der Bundesrepublik Deutschland. In Bund, Ländern und Kommunen wird mit Hochdruck daran gearbeitet, die Voraussetzungen zur Umsetzung der Richtlinie zu schaffen. Hierbei muss jedoch das Augenmerk auch darauf liegen, den Zugang zu Behörden mittels elektronischer Kommunikation so einfach wie möglich zu gestalten. Neue Hürden aufzubauen,

indem ein neues System genutzt werden soll, laufen diesem Zweck jedoch zuwider.

Wir fragen die Bundesregierung:

1. Aus welchen Gründen hält die Bundesregierung es für erforderlich, statt auf schon verfügbare sichere elektronische Kommunikationsmöglichkeiten zurückzugreifen, einen neuen E-Mail-Service „De-Mail“ zu schaffen?
2. Welche Gründe sprechen gegen die Nutzung von schon vorhandenen E-Mail-Strukturen unter Hinzuziehung sicherer Verschlüsselungsmethoden?
3. In welchem Verhältnis soll De-Mail zur im Rahmen der Einführung des elektronischen Personalausweises geplanten Funktionalität des elektronischen Identitätsnachweises stehen?
4. Warum ist es erforderlich, neben der Einführung des elektronischen Identitätsnachweises eine eigene technische Infrastruktur für elektronische Kommunikation aufzubauen statt bestehende Strukturen mittels Verschlüsselungstechnologien in Verbindung mit dem neuen Personalausweis oder anderen derartigen Karten zu nutzen?
5. Wie bewertet die Bundesregierung es aus datenschutzrechtlichen Aspekten, dass alle Bürgerinnen und Bürger, die an De-Mail teilnehmen möchten, ihre bestehende E-Mail-Adresse bekannt geben müssen, um diese dann mit dem Zusatz De-Mail für die Kommunikation mit Behörden nutzen zu können, insbesondere vor dem Hintergrund, dass viele Menschen gerade zum Schutz ihrer persönlichen Daten anonyme oder kryptische Adressen verwenden?
6. Ist aus datenschutzrechtlichen Gründen vorgesehen, dass unter dem System De-Mail auch neue E-Mail-Adressen kreiert werden können?
7. Werden die den De-Mail-Adressen zugrunde liegenden E-Mail-Adressen der teilnehmenden Bürgerinnen und Bürger, falls ja, an welcher Stelle, gespeichert?
8. Werden die De-Mail-Adressen der Bürgerinnen und Bürger generell oder in bestimmten Fällen mit Melderegisterdaten in Verbindung gebracht, abgeglichen, verknüpft oder im Melderegister gespeichert?
9. Soll die Kommunikation mit dem nach der EU-Dienstleistungsrichtlinie erforderlichen einheitlichen Ansprechpartner oder mit Behörden generell ausschließlich über De-Mail möglich sein, bzw. ist geplant, eine Umstellung auf die ausschließliche Nutzung dieses Dienstes zu welchem Zeitpunkt vorzunehmen?
10. Falls ja, welche Kosten entstehen hierdurch bei Unternehmen im In- und Ausland?
11. Welche Überlegungen hat die Bundesregierung dahingehend angestellt, dass mit der Erforderlichkeit einer Teilnahme am De-Mail-System für die Kommunikation mit Behörden statt der Weiternutzung bestehender sicherer elektronischer Kommunikationswege die Teilnahme an E-Government-Services erschwert statt erleichtert wird?
12. Welche Kosten entstehen für den einzelnen Nutzer von De-Mail, z. B. für die Erlangung der Adresse, Speicherplatz auf den Servern u. a. im virtuellen Dokumentensafe etc.?
13. Ist geplant, dass allen Bürgerinnen und Bürgern automatisch De-Mail-Adressen zugewiesen werden, ggf. bei Ausstellung des elektronischen Personalausweises?

14. Wurde durch das Bundesamt für Sicherheit in der Informationstechnologie (BSI) oder eine andere staatliche Institution bereits ein Sicherheitsprofil erstellt, das die grundlegenden Anforderungen an den allgemeinen mobilen Datenverkehr innerhalb von oder zwischen staatlichen Institutionen definiert, und wenn ja, wie ist dieser ausgestaltet worden?
15. Falls solch ein Standard noch nicht erarbeitet wurde, wann rechnet die Bundesregierung mit einer entsprechenden Vorlage?
16. Plant die Bundesregierung die Entwicklung einer eigenen Lösung für den mobilen Datenverkehr?
17. Falls ja, welche Kosten werde dafür veranschlagt, und wann soll die entsprechende Lösung verfügbar sein?
18. Welche wettbewerblichen Konsequenzen für an „De-Mail“ teilnehmende und entsprechend zertifizierte Provider erwartet die Bundesregierung?
19. Wie wird das Zertifizierungsverfahren ausgestaltet, und wer entscheidet über die Zulassung von Providern?
20. Ist geplant, neben dem üblichen Rechtsweg ein Schlichtungsverfahren für Provider einzuführen, denen die Zertifizierung für „De-Mail“ versagt wird?
21. Ist die Bundesregierung der Ansicht, dass sie angesichts des von ihr in dieser Wahlperiode massiv ausgeweiteten Telekommunikations-Überwachungsregimes sowie der verschärften Vorratsdatenspeicherungspflichten und der angestrebten erweiterten polizeilichen Ermittlungsbefugnisse im Onlinebereich durch eine Mehrheit der Bürger als vertrauenswürdiger Ansprechpartner in Angelegenheiten elektronischer Kommunikation angesehen wird?
22. Welche Funktion soll der mit De-Mail geplante virtuelle Dokumentensafe haben?
23. Wozu ist dieser erforderlich, und was spricht dagegen, Dokumente per De-Mail jeweils an den Empfänger zu schicken statt diese auf einen Server hochzuladen und dort liegen zu lassen?
24. Wie bewertet die Bundesregierung die Akzeptanz eines derartigen virtuellen Dokumentensafes bei den Bürgerinnen und Bürgern wie auch bei Unternehmen angesichts des allgemeinen Vertrauens in staatliche Datensicherheit, einmal vor dem Hintergrund aktueller Datenschutzskandale z. B. bei Meldedaten und zum anderen vor dem Hintergrund der zunehmenden Überwachungsbefugnisse und -maßnahmen von Sicherheitsbehörden?
25. Gibt es vergleichbare Systeme in anderen Staaten, insbesondere der EU, und wie sind gegebenenfalls die Erfahrungen damit?
26. Falls nein, welche Probleme könnten bei der Umsetzung der EU-Dienstleistungsrichtlinie für die Bundesrepublik Deutschland entstehen, wenn Unternehmen oder natürliche Personen aus dem EU-Ausland nicht auf dem üblichen elektronischen Kommunikationsweg an die Behörden herantreten können, sondern erst Teilnehmer von De-Mail werden müssen?
27. In welcher Weise sind Länder und Kommunen in die Entwicklung von De-Mail eingebunden?
28. Welche Kosten entstehen bei den Kommunen für die Implementierung der notwendigen technischen Infrastrukturen zur Nutzung von De-Mail durch ihre Behörden?
29. Welche Kosten entstehen insbesondere für das Vorhalten von Speicherplatz für den virtuellen Dokumentensafe?

30. Welche rechtlichen Rahmenbedingungen werden für die Nutzung von De-Mail für die Bürgerinnen und Bürger, die den Service nutzen, gelten, insbesondere im Hinblick auf Haftungsfragen bei Verlust von Passwörtern, die die Integrität z. B. des virtuellen Dokumentensafes gefährden können?
31. Welche Sicherheit für im virtuellen Dokumentsafe gespeicherten Daten gegen Datenverlust und zum Schutz von deren Vertraulichkeit und Integrität sollen im Rahmen von De-Mail getroffen werden?
32. Plant die Bundesregierung gesetzgeberische Schritte, die das Vorhaben flankieren, insbesondere im Hinblick auf die teilnehmenden Telekommunikationsprovider auf der einen, die Behörden auf der anderen Seite, und wenn ja, welche?
33. Welche Aussagen zur Zukunftssicherheit und Nachhaltigkeit von De-Mail kann die Bundesregierung vor dem Hintergrund der schnellen technischen Weiterentwicklung treffen?

Berlin, den 3. Dezember 2008

Dr. Guido Westerwelle und Fraktion