



BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Deutsche Telekom AG
Datenschutzbeauftragter
[REDACTED]
Friedrich-Ebert-Allee 140
53113 Bonn

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn

FON (0228) 997799- [REDACTED]

E-MAIL Referat24@bfdi.bund.de

BEARBEITET VON [REDACTED]

INTERNET www.bfdi.bund.de

DATUM Bonn, 06.05.2024

GESCHÄFTSZ. 24-193-2 II#1721

**Bitte geben Sie das vorstehende Geschäftszeichen
bei allen Antwortschreiben unbedingt an.**

BETREFF **Datenschutz in der Telekommunikation, Az. 24-193-2 II#1721**

Sehr geehrtes Telekom-Datenschutzteam,

vielen Dank für das Antwortschreiben vom 25.04.2024 zur Frage des Einsatzes von DANE.

Die Frage des Einsatzes von DANE bei Mailservern im Allgemeinen wird hier unter dem Aktenzeichen 24-193 II#6195 weiterbearbeitet. Unter dem Aktenzeichen 24-193-2 II#1721 geht es im Weiteren Speziell um den Einsatz des Email Encryption Gateways (EEGW).

Der Beschwerdeführer moniert zum EEGW, dass die Registrierungsdaten wie auch die Passwortwiederherstellungsdaten per E-Mail versendet werden und dabei unzureichend gegen Abhören oder Manipulation geschützt seien.

Nach meinem bisherigen Verständnis wird das EEGW vom Verantwortlichen zur Beantwortung von Anfragen mit höherem Schutzbedarf verwendet um ein dementsprechendes Schutzniveau zu gewährleisten. Um dies zu ermöglichen muss sichergestellt sein, dass auch das Einrichten oder Ändern von Zugangsdaten zum EEGW entsprechend geschützt ist. Mit E-Mail vom 06.10.2023 teilte der Verantwortliche mir mit, dass der Versand von Zugangsdaten nunmehr immer TLS-verschlüsselt erfolgt. Hierdurch ist jedoch lediglich sichergestellt, dass die Zugangsdaten nicht unverschlüsselt versendet werden, nicht jedoch mit welcher Gegenstelle die verschlüsselte Verbindung zustande kommt. Dies kann z.B. sichergestellt werden, indem der Verantwortliche vor Versand per DANE das Zertifikat des Empfängers abfragt und der Versand der Mail nur bei einer Verbindung mit diesem Zertifikat erfolgt.



Werden Zugangsdaten dagegen ohne Authentifizierung der Gegenstelle versendet, so erlaubt dies den Zugriff auf die personenbezogenen Daten in gleicher Weise als wenn die personenbezogenen Daten selbst ohne Authentifizierung versendet würden.

Daher habe ich folgende Fragen zur Sache:

- (1) Auf welches Schutzniveau für den Zugriff auf personenbezogene Daten zielt das EEGW ab?
- (2) Wie beurteilt der Verantwortliche das Risiko des Abfangens der Registrierungsdaten (insb. des Einmalpasswortes bei Registrierung oder Passwort zurücksetzen) beim EEGW? Hierbei bitte ich auch auf das Szenario ohne E-Mail Made in Germany einzugehen, da der Betroffene hier einen eigenen Mailserver betreibt.
- (3) Wie beurteilt der Verantwortliche alternative Wege der Zusendung des Einmalpasswortes oder der Passwortrücksetzung, etwa postalisch oder über Mobilfunk?

Ich bitte um Stellungnahme innerhalb von zwei Wochen. Für Fragen stehe ich gerne zur Verfügung.

Mit freundlichen Grüßen

Im Auftrag

██████████