Aktenzeichen

0321/00-60-21-00-00

Deutsche Rentenversicherung
Bund

Deutsche Rentenversicherung Bund 10704 Berlin

Bundesministerium für Wirtschaft und Energie
Frau Ministerialrätin
Sabine Maass
Scharnhorststraße 34 - 37
10115 Berlin

Ansprechpartner:
Ralph Pankow
Telefon 030 865-89240
Telefax 030 865-89435
E-Mail ralph.pankow@drv-bund.de

Datum 01.11.2016

Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz);
Beteiligung von Ländern, kommunalen Spitzenverbänden, Fachkreisen und Verbänden (§ 47 Abs. 1 der Gemeinsamen Geschäftsordung der Bundesministerien - GGO);
Ihr Schreiben vom 18. Oktober 2016, Ihr Az.: 161202/12

Sehr geehrte Frau Maass,
sehr geehrte Damen und Herren,

wir danken Ihnen für die Übersendung des Referentenentwurfs des eIDAS-Durchführungsgesetzes und nehmen die Gelegenheit zur Stellungnahme gerne wahr.

Das vorliegende Artikelgesetz ergänzt die seit dem 17. September 2014 beziehungsweise seit dem 1. Juli 2016 in den Mitgliedsstaaten der EU und den assoziierten Staaten unmittelbar geltenden Vorschriften der Verordnung (EU) Nr. 910/2014 (eIDAS-VO). Mit dem eIDAS-Durchführungsgesetz werden eIDAS-konforme Konkretisierungen und Ausgestaltungen auf nationaler Ebene geregelt. Die Deutsche Rentenversicherung ist mit dem bei ihr betriebenen Trust-Center und den von ihr angebotenen Online-Diensten von den Neuregelungen jedenfalls partiell betroffen.

1. Art. 1 eIDAS-DurchführungsG-E: VertrauensdiensteG (VDG)

Das Vertrauensdienstegesetz wird das Signaturgesetz (SigG) ersetzen (vgl. Artikel 11 Abs. 1 Nr.1 eIDAS-Durchführungsgesetz), es legt

Aufsichtsstellen fest und präzisiert die Vorschriften der eIDAS-VO, wobei es sich weitgehend an die bekannten eIDAS-konformen Vorschriften des SigG anlehnt. Zum Entwurf des Vertrauensdienstegesetzes (VDG-E)haben wir folgende Anmerkungen:

1.1 Fehlende Übereinstimmung von Inhaltsübersicht und Normenapparat

Die Inhaltsübersicht nennt ab der Überschrift zu § 16 Vorschriften, die sich im Normenapparat nicht wiederfinden. So findet sich unter § 16 VDG-E nicht die angekündigte Vorschrift zu „Zeitraum und Verfahren zur langfristigen Datensicherung“, sondern die Vorschrift über „Benannte Stellen nach Art. 30 Absatz 1 der Verordnung (EU) Nr. 910/2014“. Die Vorschrift über das „Qualifizierte elektronische Siegel“ findet sich nicht unter § 20 VDG-E, sondern bereits unter § 17 VDG-E. In der Inhaltsübersicht werden weiterhin die §§ 22 bis 24 genannt, obwohl der Normenapparat bereits bei § 21 VDG-E – „Übergangsvorschriften“ – endet.

1.2 Art. 1 § 7 VDG-E: Datenschutz

Im Referentenentwurf vom 27. Juni 2016 (damals noch § 3 VDG-E) hieß es: „Eine **Datenerhebung bei Dritten** ist nur mit Einwilligung der betroffenen Person zulässig.“ Nunmehr heißt es „**Datenverarbeitung**“.

Zwar könnte im Hinblick auf die Begriffsbestimmung in der (EU)-Datenschutzgrundverordnung (EU-DS-GVO) bewusst der Ausdruck der „Verarbeitung“ gewählt worden sein. Das Wort "Verarbeitung" umfasst jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe mit personenbezogenen Daten (Art. 4 Nr. 2 EU-DS-GVO). Verarbeitung schließt das Erheben oder das Erfassen ein, umfasst gleichzeitig aber auch das Weitergeben beim Verantwortlichen oder an andere Personen oder Stellen (zum Beispiel an einen IT-Dienstleister zum Zwecke der Back-up-Sicherung oder Vernichtung).

Falls die Datenverarbeitung bei Dritten bzw. die Datenverarbeitung **durch** Dritte gemeint sein sollte, also mit anderen Worten das Outsourcing oder die Auftragsverarbeitung, sehen wir hinsichtlich der Umsetzung des Satz 2 jedoch große Schwierigkeiten. Denn eine Da-

tenverarbeitung im Auftrag wäre unmöglich. Auch Wartung und Support technischer Komponenten des Trustcenterbetriebes müssen als Datenverarbeitung im Auftrag gestaltet werden, wenn nicht verhindert werden kann, dass der Dienstleister personenbezogene Daten zur Kenntnis nehmen kann.

In der Rentenversicherung wird ein Trustcenter betrieben. Dieses erbringt zurzeit für drei Rentenversicherungsträger – Vertrauensdiensteanbieter - technische Dienstleistungen und verarbeitet hierfür personenbezogene Daten im Auftrag. Die Unterstützung, die das Trustcenter der Deutschen Rentenversicherung für die Träger der Deutschen Rentenversicherung (§ 125 Abs. 1 SGB VI) als Datenverarbeitung im Auftrag leistet (vgl. auch § 36a Abs. 4 SGB I), wäre nach dem heutigen Stand des Referentenentwurfs unzulässig.
Für alle Personen, für die ein Signaturzertifikat ausgestellt wird (wurde), wäre eine Einwilligung für diese Verarbeitung durch den Dritten (Trustcenter) erforderlich.

Die Einwilligung – also eine ausdrücklich vorher erteilte Zustimmung – ist als Grundlage für die Verarbeitung personenbezogener Daten aber unzureichend. Denn eine Einwilligung kann jederzeit mit Wirkung für die Zukunft zurückgenommen werden. Das bedeutet, dass die Verarbeitungspraxis ab dem Zeitpunkt einer Einwilligungsrücknahme geändert werden müsste. Für jeden Vertrauensdiensteanbieter entstünden dabei unkalkulierbare Risiken für die Gestaltung der Arbeitsprozesse.

Vorliegend sollte daher statt des Begriffes „Datenverarbeitung“ der Begriff „Datenerhebung“ verwendet werden, wie dies ursprünglich vorgesehen war. Denn mutmaßlich soll weiterhin nur die Datenerhebung von Daten bei Dritten verhindert werden, d.h. das Beschaffen von Daten ohne Wissen und Wollen der betroffenen Personen. Es ist nicht praktikabel, jegliche Verarbeitung durch Dritte von der Einwilligung jedes einzelnen abhängig zu machen.

1.3 Art. 1 § 9 VDG-E: Deckungsvorsorge

Unter bestimmten Bedingungen kann die beschriebene Mindesthöhe der „Deckungsvorsorge“ von 250.000,- EURO zu niedrig angesetzt sein. Im Hinblick auf Artikel 13 der eIDAS-VO ist eine Begrenzung des Haftungsumfangs qualifizierter Vertrauensdiensteanbieter nicht

erkennbar. Die Begründung zu § 9 VDG-E weist selbst darauf hin, dass Art. 24 Absatz 2 Buchst. c der eIDAS-VO auch den Abschluss einer „angemessenen Haftpflichtversicherung“ vorsieht. Sofern die Haftung z.B. auch Produktionsausfallkosten beim Nutzer qualifizierter Dienste umfassen soll, kann die genannte (Mindest-) Deckungssumme sehr schnell erschöpft sein.

1.4 § 12 VDG-E: Unterrichtung über Sicherheitsmaßnahmen und Rechtswirkungen

In § 12 Abs.1 Satz1 Nr. 1 VDG-E muss es „Vertrauensdienste“ statt „Vertrauensdiensten“ heißen.

In § 12 Abs. 2 VDG-E wird ausgeführt, dass, wenn „eine Person, die einen qualifizierten Vertrauensdienst nutzen will, [über die Bedingungen der Dienstenutzung sowie über Sicherheitsmaßnahmen und Rechtswirkungen] bereits zu einem früheren Zeitpunkt nach Art. 24 Absatz 2 Buchst. d der Verordnung (EU) 910/2014 sowie nach § 12 Abs. 1 unterrichtet worden ist“, eine erneute Unterrichtung unterbleiben kann.

Diese Formulierung ist sehr generell gehalten und könnte dazu führen, dass ggf. Änderungen eines Sachverhalts ggf. nicht oder verspätet bekannt werden.

Wir regen daher an, vor dem letzten Halbsatz des § 12 Abs. 2 VDG-E folgenden Zusatz in die Vorschrift aufzunehmen:

„sofern keine Änderungen eingetreten sind“.

1.5 § 13 VDG-E: Widerruf qualifizierter Zertifikate

Ihre zu der Norm des § 13 Abs. 1 Nr. 2 VDG-E gestellte Frage, ob ein Widerruf bei Website-Zertifikaten üblich/möglich/sachgerecht ist (Kommentar JZ7 in der übermittelten Datei), beantworten wir wie folgt:

„Die Sperrung („Widerruf“) von Webseitenzertifikaten wird zum Beispiel im Fall der Kompromittierung des verwendeten Schlüsselmaterials für sachgerecht gehalten.“

1.6 § 15 VDG-E: Beendigungsplan; auf Dauer prüfbare Vertrauensdienste

In § 15 Absatz 1 Satz 1 Nr. 2 am Ende VDG-E müsste es heißen: „die ausgestellten Zertifikate **„zu“** widerrufen“.

1.7 § 16 VDG-E: Benannte Stellen nach Art. 30 Absatz 1 der Verordnung (EU) 910/2014

Gemäß der Anlage 1, Abschnitt 1, Nr. 2 der Signaturverordnung (SigV) vom 16.November 2001 veröffentlicht die Bundesnetzagentur (BNetzA) bisher als zuständige Behörde jährlich den sogenannten „Algorithmenkatalog“, in dem zur Erzeugung qualifizierter elektronischer Signaturen geeignete kryptographische Verfahren veröffentlicht werden. Es ist für uns nicht nachvollziehbar, inwieweit diese Tätigkeit künftig noch zu dem Aufgabenbereich der im VDG genannten Stellen – Bundesamt für Sicherheit in der Informationstechnologie (BSI) und Bundesnetzagentur (BNetzA) – gehört. Besteht die Regelung aus der Signatur-Verordnung, die in § 21 VDG-E aufgehoben werden soll, ggf. weiter ? Im Sinne der technischen Interoperabilität, der Sicherheitseigenschaften und damit auch im Hinblick auf eine einheitliche Rechtswirkung wäre es zu begrüßen, wenn hier weiterhin Standards zu geeigneten kryptographischen Verfahren normiert würden. Der eIDAS-VO haben wir dazu nichts entnehmen können. In der Begründung zu § 16 Absatz 1 VDG-E heißt es lediglich, dass das BSI die Korrektheit der Implementierung sicherstellen soll.

2. Art. 10: Folgeänderungen

Auffällig ist bei den unter Art. 10 erfassten Gesetzesänderungen, dass die genannten Folgeänderungen sich regelmäßig nur auf die qualifizierte elektronische Signatur beziehen. Das „qualifizierte elektronische Siegel“ (§ 17 VDG-E) wird regelmäßig nicht genannt. Eine Prüfung, in welchen der von den Gesetzesänderungen erfassten Fälle auch die Anwendung des qualifizierten elektronischen Siegels in Betracht zu ziehen ist, wäre daher zu begrüßen.

Mit freundlichen Grüßen

Dr. Wolfgang Binne