REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817. 463/0002-DSR/2016
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundeskanzleramt

Per Mail:
i11@bka.gv.at

Betrifft: Entwurf einer Verordnung des Bundeskanzlers, mit der die Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung – SVV) und die Verordnung des Bundeskanzlers über die Feststellung der Eignung des Vereins „Zentrum für sichere Informationstechnologie - Austria (A-SIT)“ als Bestätigungsstelle erlassen werden

Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner **229. Sitzung am 29. April 2016 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Allgemeines

Den Erläuterungen ist zu entnehmen, dass mit der Verordnung (EU) Nr. 910/2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. Nr. L 257/73 vom 28. August 2014 (so genannte "eIDAS-VO") nunmehr ua die Rechtsvorschriften jener Richtlinie gestärkt und erweitert werden sollen, indem eine gemeinsame Grundlage für eine sichere elektronische Interaktion zwischen Bürgern, Unternehmen und öffentlichen Verwaltungen geschaffen wird. Dadurch wird die Effektivität öffentlicher und privater Online-Dienstleistungen, des elektronischen

Geschäftsverkehrs und des elektronischen Handels in der Union erhöht. Zudem wird der Bereich der elektronischen Identifizierung angesprochen.
Die Durchführung der unmittelbar anwendbaren eIDAS-VO erfordert ua eine Anpassung jener innerstaatlichen Rechtsvorschriften, die das Thema elektronische Signaturen bislang regeln, wobei anstelle des aufzuhebenden SigG ein neues Signatur- und Vertrauensdienstegesetz (SVG) erlassen wird, das die Grundlage für das vorliegende Vorhaben bildet. Aufgrund der Aufhebung des Signaturgesetzes (SigG), war auch die Signaturverordnung 2008 (SigV 2008) aufzuheben. Die zur Durchführung des SVG erforderlichen Bestimmungen sollen mit der Signatur- und Vertrauensdiensteverordnung (SVV) erlassen werden. Mit dem Erlass der SVV wird von der Verordnungsermächtigung des § 17 SVG Gebrauch gemacht.

2) Datenschutzrechtlich relevante Bestimmungen:

Vorbemerkung

Der Datenschutzrat hält fest, dass seitens des informierten Vertreters des BKA in der Sitzung des Datenschutzrates angemerkt wurde, dass die eIDAS-VO die Anforderungen an den qualifizierten Vertrauensdiensteanbieter abschließend regelt und daher nicht präzisiert werden kann.

Da bis zum Ende der Begutachtungsfrist des Signatur- und Vertrauensdienste-gesetzes (SVG) keine Sitzung des Datenschutzrates stattfinden konnte, konnte der Datenschutzrat nicht fristgerecht zum Gesetzesentwurf Stellung nehmen. Allerdings wurde zum gegenständlichen Gesetzesentwurf ein Schreiben des Vorsitzenden des Datenschutzrates mit diversen datenschutzrechtlichen Fragestellungen verfasst. Vor dem Hintergrund des inhaltlichen Zusammenhangs des Gesetzesentwurfes mit den gegenständlichen Verordnungen ergeben sich zu diesem Verordnungsentwurf folgende datenschutzrechtliche Anmerkungen.

Zu Artikel 1 der Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung – SVV)

Zu § 2:

Gemäß § 2 Abs. 4 darf ein qualifizierter VDA im Rahmen der bereitgestellten qualifizierten Vertrauensdienste **nur zuverlässiges Personal beschäftigen**; nachdem

nach Verurteilungen wegen relevanter einschlägiger Straftaten die Zuverlässigkeit nicht gegeben ist, sollte klargestellt werden, ob der VDA **nur bei der Einstellung** des Personals oder auch **während der Dauer des Arbeitsverhältnisses** überprüfen muss, ob derartige Straftaten begangen wurden. Fraglich erscheint hierbei auch**, wie lange** strafrechtlich relevante Daten beim VDA zu diesem Zweck **gespeichert** werden.

Zu § 3:

Im Zusammenhang mit dem **Erfassen der Daten des Lichtbildausweises** nach § 3 sollte geregelt werden, **wie lange** diese Daten zu dokumentieren bzw. zu speichern sind.

Zu § 5:

Hinsichtlich der **Zertifikatsdatenbank** regelt § 5 Abs. 1, dass die Abfrage unentgeltlich und **ohne Identifikation** möglich sein muss. § 5 Abs. 3 sieht jedoch vor, dass die Zertifikatsdatenbank **vor unbefugtem Abruf** ausreichend geschützt sein muss. Unklar erscheint dabei, wie eine Datenbank, die ohne Identifikation abgefragt werden kann, vor **unbefugtem** Abruf geschützt werden soll. Dies sollte näher dargelegt oder klarer formuliert werden.

Weiters sollte nach Ansicht des Datenschutzrates verständlicher geregelt werden, welche **Datenarten** in der Zertifikatsdatenbank abrufbar sind und ob darüber hinaus auch weitere Daten – die für die Öffentlichkeit nicht abrufbar sind – für Zwecke der Zertifikationsdatenbank verarbeitet werden. Fraglich erscheint in diesem Zusammenhang auch, ob nicht mehr abrufbare Daten – etwa nach einem Widerruf – weiterhin gespeichert werden.

9. Mai 2016
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt