BUNDESGESETZBLATT

FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2016 **Ausgegeben am 1. August 2016** **Teil II**

208. 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

Artikel 1

Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung – SVV)

Auf Grund des § 17 des Signatur- und Vertrauensdienstegesetzes (SVG), BGBl. I Nr. 50/2016, wird – hinsichtlich §§ 3 bis 5 im Einvernehmen mit dem Bundesminister für Justiz – verordnet:

Gebühren für Aufsichtstätigkeiten

§ 1. (1) Von den Vertrauensdiensteanbietern (VDA) sind für Leistungen im Rahmen der Aufsichtstätigkeit folgende Gebühren zu entrichten:

1.	Analyse der Konformitätsbewertungsberichte gemäß Art. 17 Abs. 4 lit. b iVm Art. 20 Abs. 1 und Art. 21 Abs. 1 Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (im Folgenden: eIDAS-VO), ABl. Nr. L 257 vom 28.08.2014 S. 73, in der Fassung der Berichtigung ABl. Nr. L 257 vom 29.01.2015 S. 19 im Sinne § 3 Abs. 1 Z 1 SVG	2 500 Euro;
2.	Durchführung von Überprüfungen der qualifizierten VDA gemäß Art. 17 Abs. 4 lit. e iVm Art. 20 Abs. 2 erster Fall eIDAS-VO	
	a) bei Überprüfungen aufgrund sicherheitsrelevanter Anlässe	4 500 Euro;
	b) bei Überprüfungen ohne sicherheitsrelevante Anlässe	1 000 Euro;
3.	Verleihung des Qualifikationsstatus an VDA und die von ihnen erbrachten Dienste sowie Entzug dieses Status gemäß Art. 17 Abs. 4 lit. g iVm Art. 20 und 21 eIDAS-VO	700 Euro;
4.	Erteilung von Auflagen gemäß Art. 17 Abs. 4 lit. j eIDAS-VO	700 Euro;
5.	Überprüfung des Vorliegens und der ordnungsgemäßen Anwendung von Vorschriften über Beendigungspläne (§ 9 SVG) gemäß Art. 17 Abs. 4 lit. i iVm Art. 24 Abs. 2 lit. h eIDAS-VO	1 500 Euro;
6.	Weiterführung der Zertifikatsdatenbank durch die Aufsichtsstelle (§ 9 SVG):	
	pro Jahr und Zertifikat, das in der Zertifikatsdatenbank geführt wird	1 Euro;
	jedoch insgesamt pro Jahr nicht mehr als	5 000 Euro;
7.	Führung der Vertrauensliste bei der Aufsichtsstelle (§ 14 Abs. 1 SVG):	
	pro aufgenommenen VDA und Jahr	300 Euro.

(2) Die Gebühren sind von der Aufsichtsstelle mit Bescheid vorzuschreiben.

(3) Wenn sich die Aufsichtsstelle bei der Aufsicht

1. einer Bestätigungsstelle oder

2. nichtamtlicher Personen oder Einrichtungen als Sachverständiger bedient,

sind die Gebühren nach § 53a AVG dem betroffenen VDA als Barauslage im Sinne des § 76 AVG vorzuschreiben.

(4) Zur Finanzierung der notwendigen Kosten der Aufsichtsstelle und der RTR-GmbH, die nicht durch Gebühreneinahmen gemäß Abs. 1 abgedeckt sind, ist der RTR-GmbH aus dem Bundeshaushalt jährlich per 30. Jänner ein Kostenersatz in der Höhe von 115.000 Euro zu leisten. Sofern sich die Anzahl der zu beaufsichtigenden VDA nach dem Inkrafttreten dieser Verordnung erhöht, sind die Kosten für dadurch notwendige zusätzliche Tätigkeiten der Aufsichtsstelle und der RTR-GmbH, die nicht durch Gebühreneinahmen gemäß Abs. 1 abgedeckt sind, bis zu einem Betrag von zusätzlich jährlich 60.000 Euro zu ersetzen. Der Kostenersatz vermindert oder erhöht sich ab dem Jahr 2017 in jenem Maße, in dem sich der von der Bundesanstalt Statistik Österreich verlautbarte Verbraucherpreisindex 2005 oder der an seine Stelle tretende Index des Vorjahres verändert hat. Die RTR-GmbH hat dem Bundeskanzler jährlich bis zum 30. April des Folgejahres über die Verwendung dieser Mittel zu berichten und einen Rechnungsabschluss vorzulegen.

Erbringung von qualifizierten Vertrauensdiensten

§ 2. (1) Werden die Einrichtungen eines qualifizierten VDA organisatorisch oder technisch getrennt geführt, so ist durch Sicherheitsmaßnahmen sicherzustellen, dass die Übertragung der Daten zwischen den Teileinrichtungen nicht zu einer Kompromittierung der qualifizierten Vertrauensdienste führt.

(2) Die technischen Einrichtungen eines qualifizierten VDA sind so zu gestalten, dass deren Funktionen und Anwendungen, die zu den bereitgestellten qualifizierten Vertrauensdiensten gehören, von anderen Funktionen und Anwendungen getrennt sind und eine Beeinflussung ausgeschlossen ist. Dies muss sowohl für den regulären Betrieb, für besondere Betriebssituationen und außerhalb des Betriebs sichergestellt sein. Besondere Betriebssituationen wie beispielweise eine Wartung sind zu dokumentieren.

(3) Ein qualifizierter VDA hat geeignete Vorkehrungen zu treffen, die seine Einrichtungen zur Erbringung von qualifizierten Vertrauensdiensten vor unbefugtem Zutritt schützen.

(4) Ein qualifizierter VDA darf im Rahmen der bereitgestellten qualifizierten Vertrauensdienste nur zuverlässiges Personal beschäftigen. Die Zuverlässigkeit ist jedenfalls bei Personen nicht gegeben, die wegen einer mit Vorsatz begangenen strafbaren Handlung zu einer Freiheitsstrafe von mehr als einem Jahr oder wegen strafbarer Handlungen gegen das Vermögen oder gegen die Zuverlässigkeit von Urkunden und Beweiszeichen zu einer Freiheitsstrafe von mehr als drei Monaten verurteilt wurden. Verurteilungen, die nach den Bestimmungen des Tilgungsgesetzes 1972 getilgt sind oder der beschränkten Auskunft unterliegen, bleiben außer Betracht.

(5) Das Personal eines qualifizierten VDA muss in Hinblick auf die zu erfüllenden Aufgaben über ausreichendes Fachwissen in folgenden Bereichen verfügen:

1. allgemeine EDV-Ausbildung,
2. Sicherheitstechnologie, Kryptographie, elektronische Signatur und Public Key Infrastructure,
3. technische Normen, insbesondere Evaluierungsnormen,
4. Hard- und Software,
5. Vorschriften für die Sicherheit und den Schutz personenbezogener Daten sowie
6. Anwendung von Verwaltungs- und Managementverfahren.

(6) Auf Verlangen der Aufsichtsstelle hat der qualifizierte VDA Auskunft über das erforderliche Fachwissen des Personals zu geben. Das erforderliche Fachwissen des Personals kann insbesondere durch

1. Absolvierung einer einschlägigen Höheren Technischen Lehranstalt (HTL),
2. einer einschlägigen Fachhochschule,
3. eines einschlägigen Studiums oder durch
4. eine fachlich einschlägige Tätigkeit in der Dauer von zumindest drei Jahren

erworben werden.

(7) Werden die Signatur- oder Siegelerstellungsdaten beim qualifizierten VDA oder bei der Produktion der Signatur- oder Siegelerstellungseinheit erzeugt, so muss vom qualifizierten VDA sichergestellt werden, dass die Signatur- oder Siegelerstellungsdaten nur in den alleinigen Verfügungsbereich des Signators oder des Siegelerstellers gelangen. Davor muss die Möglichkeit der Verwendung der Signatur- oder Siegelerstellungsdaten ausgeschlossen sein. In jedem Fall hat sich der qualifizierte VDA darüber zu vergewissern, dass die Signatur- oder Siegelerstellungsdaten des Signators oder des Siegelerstellers und die Signatur- oder Siegelvalidierungsdaten des entsprechenden Zertifikats in komplementärer Weise anwendbar sind.

Ausstellung qualifizierter Zertifikate für einen Vertrauensdienst bei persönlicher Anwesenheit

§ 3. Zur Feststellung der Identität von persönlich anwesenden natürlichen Personen oder Vertretern einer juristischen Person, denen ein qualifiziertes Zertifikat ausgestellt werden soll (§ 8 Abs. 1 SVG), geeignet sind ein

1. amtlicher Lichtbildausweis oder
2. ein Nachweis, der bescheinigt, dass die Identität zumindest mit jener Verlässlichkeit geprüft wurde, wie sie bei der Zustellung zu eigenen Handen (§ 21 ZustG) einzuhalten ist.

Die Daten des Lichtbildausweises oder des anderen Nachweises (§ 8 Abs. 1 erster Satz SVG) sind zu erfassen und mit dem Antrag zu dokumentieren, sofern sie nicht schon dokumentiert wurden. Die Erfassung und Dokumentation kann auch in ausschließlich elektronischer Form erfolgen.

Qualifizierte Zertifikate

§ 4. (1) Stellt ein VDA neben qualifizierten Zertifikaten auch andere Zertifikate aus, so muss er für die Signatur oder das Siegel der qualifizierten Zertifikate gesonderte Signatur- oder Siegelerstellungsdaten verwenden.

(2) Bis zum Ablauf der Gültigkeit eines qualifizierten Zertifikats ist es zulässig, mit Ausnahme der Gültigkeitsdauer und der eindeutigen Kennung, dieselben Inhalte samt denselben Signatur- oder Siegelvalidierungsdaten neu zu zertifizieren und auf diese Weise ein neues Zertifikat auszustellen.

(3) Im Fall der Übernahme gemäß § 9 Abs. 2 SVG ist auch eine Änderung der Angaben und Inhalte des qualifizierten Zertifikats zulässig, soweit diese Änderung zur Weiterführung des qualifizierten Zertifikats erforderlich ist. Der Beginn der Gültigkeit des neu ausgestellten qualifizierten Zertifikats hat dabei unmittelbar an das Ende der Gültigkeit des bestehenden qualifizierten Zertifikats anzuschließen. In allen anderen Fällen bewirkt der Umstand, dass für Signatur- oder Siegelzwecke ausgestellte qualifizierte Zertifikate dieselben Signatur- oder Siegelvalidierungsdaten, aber unterschiedliche Inhalte aufweisen, eine Kompromittierung der betroffenen qualifizierten Zertifikate.

Zertifikatsdatenbank

§ 5. (1) Der qualifizierte VDA hat sicherzustellen, dass die Formate der Zertifikatsdatenbank (Art. 24 Abs. 2 lit. k eIDAS-VO) für deren Weiterführung durch die Aufsichtsstelle geeignet sind. Die Formate der Zertifikatsdatenbank dürfen während der Geltungsdauer des Zertifikats nicht verändert werden. Jedenfalls muss die Zertifikatsdatenbank die Feststellung zulassen, ob das Zertifikat zu einem bestimmten Zeitpunkt widerrufen war. Die Zertifikatsdatenbank muss allgemein frei zugänglich sein. Die Abfrage der Zertifikatsdatenbank muss unentgeltlich und ohne Identifikation möglich sein.

(2) Der qualifizierte VDA hat den Signatoren, den Siegelerstellern und sonstigen dazu Berechtigten geeignete Kommunikationsmöglichkeiten bekannt zu geben, mit denen diese jederzeit einen Widerruf des Zertifikats veranlassen können. Dafür muss ein Authentifizierungsverfahren vorgesehen werden. Der Widerruf eines Zertifikats muss jedenfalls auch in Papierform möglich sein.

(3) Die Zertifikatsdatenbank muss vor Fälschung, Verfälschung und unbefugtem Zugriff ausreichend geschützt sein. Es muss sichergestellt sein, dass nur befugte Personen Eintragungen und Veränderungen in der Zertifikatsdatenbank vornehmen können. Weiters darf eine Aussetzung nicht unbemerkt rückgängig gemacht werden können.

(4) Die Aktualisierung der Zertifikatsdatenbank muss an Werktagen, ausgenommen Samstagen, von 9 bis 17 Uhr spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes erfolgen. Außerhalb dieser Zeit hat der qualifizierte VDA jedenfalls dafür Sorge zu tragen, dass ein Verlangen auf Widerruf eines qualifizierten Zertifikats jederzeit automatisiert entgegengenommen wird und die Aussetzung spätestens innerhalb von sechs Stunden auslöst.

(5) Die Zertifikatsdatenbank muss ständig verfügbar sein. Eine durchgehende Unterbrechung der Zertifikatsdatenbank von mehr als 30 Minuten ist als Störfall zu dokumentieren. Für Wartungs- und Ausfallsituationen der Zertifikatsdatenbank ist ein Ersatzsystem bereitzustellen. Fällt auch das Ersatzsystem aus, so ist dies innerhalb eines Kalendertags der Aufsichtsstelle anzuzeigen. Die Aufsichtsstelle hat für die Wiederherstellung der Zertifikatsdatenbank innerhalb von drei Kalendertagen Sorge zu tragen.

(6) Führt die Aufsichtsstelle die Zertifikatsdatenbank gemäß § 9 Abs. 2 zweiter Satz SVG weiter, so ist Art. 24 Abs. 4 eIDAS-VO sinngemäß anzuwenden.

(7) Im Fall einer Aussetzung eines qualifizierten Zertifikats ist der Signator oder der Siegelersteller unverzüglich zu verständigen. Die Aussetzung kann aufgehoben werden. Eine aufgehobene Aussetzung hat auf die Gültigkeit des Zertifikats keinen Einfluss. Wird eine Aussetzung nicht aufgehoben, so ist das

Zertifikat zu widerrufen. Erfolgt auf Grund einer Aussetzung der Widerruf eines Zertifikats, so gilt bereits die Aussetzung als Widerruf.

(8) Werden die Signatur- oder Siegelerstellungsdaten des Signators oder des Siegelerstellers bekannt oder kommen diese außer beim Signator oder Siegelersteller als Signatur- oder Siegelerstellungsdaten oder in anderer Form ein weiteres Mal vor, so liegt eine Kompromittierung der Signatur- oder Siegelerstellungsdaten vor.

Inkrafttreten

§ 6. Diese Verordnung tritt mit dem der Kundmachung folgenden Tag in Kraft. Gleichzeitig treten die Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008), BGBl. II Nr. 3/2008, in der Fassung der Verordnung BGBl. II Nr. 401/2010, samt Anhang, die Verordnung des Bundeskanzlers über die Feststellung der Eignung des Vereins „Zentrum für sichere Informationstechnologie – Austria (A-SIT)“ als Bestätigungsstelle, BGBl. II Nr. 31/2000, und die Bestätigungsstellenverordnung (BestV), BGBl. II Nr. 299/2002, außer Kraft.

Artikel 2

Verordnung des Bundeskanzlers über die Feststellung der Eignung des Vereins „Zentrum für sichere Informationstechnologie – Austria (A-SIT)“ als Bestätigungsstelle

Auf Grund des § 7 Abs. 3 des Signatur- und Vertrauensdienstegesetzes (SVG), BGBl. I Nr. 50/2016, wird verordnet:

Eignung des Vereins „Zentrum für sichere Informationstechnologie – Austria (A-SIT)“

Die Eignung des Vereins „Zentrum für sichere Informationstechnologie – Austria (A-SIT)“, die Aufgaben einer Bestätigungsstelle nach dem Signatur- und Vertrauensdienstegesetz (SVG) und den auf seiner Grundlage ergangenen Verordnungen wahrzunehmen, wird festgestellt.

Artikel 3

Hinweis auf die Notifikation

Diese Verordnung wurde unter Einhaltung der Bestimmungen der Richtlinie (EU) 2015/1535 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (kodifizierter Text), ABl. Nr. L 241 vom 17.09.2015 S. 1, notifiziert (Notifikationsnummer: 2016/149/A).

Kern