Datenschutzbehörde
Barichgasse 40-42
1030 Wien

per E-Mail: dsb@dsb.gv.at
begutachtungsverfahren@parlament.gv.at

Zl. 13/1 20/29

GZ: D056.151 2020-0.159.543
Verordnung der Datenschutzbehörde über die Anforderungen an die Akkreditierung einer Zertifizierungsstelle (Zertifizierungsstellen-Akkreditierungs-Verordnung – ZeStAkk-V)

Referent: Dr. Günther Leissler, Rechtsanwalt in Wien

Sehr geehrte Damen und Herren!

Mit dem vorliegenden Verordnungsentwurf soll gem § 21 Abs 3 DSG in Präzisierung des Art 43 DSGVO per datenschutzbehördlicher Verordnung ein datenschutzspezifisches Zertifizierungsverfahren zur Verleihung von Datenschutzsiegel und Datenschutzprüfzeichen etabliert werden.

Der Österreichische Rechtsanwaltskammertag (ÖRAK) dankt für die Übersendung des Entwurfs und erstattet dazu folgende

S t e l l u n g n a h m e :

Berufsspezifische Bedenken:

Durch den in der Verordnung vorgeschlagenen § 4 wird die Legitimation zur Antragstellung zur Akkreditierung als Zertifizierungsstelle ausschließlich juristischen Personen im Sinne des Pkt 4.1.1 der ISO/IEC 17065:2012 vorbehalten. Eine Einschränkung auf den hier gewählten Begriff der juristischen Person ist den zur Zertifizierung einschlägigen Artikeln der DSGVO fremd (und steht die Einschränkung des § 4 im Übrigen auch nicht im Einklang mit der Begriffsdefinition des § 2 Z 5, 6 der vorgeschlagenen Verordnung). Die Folge dieser Formulierung wäre, dass vielen Angehörigen der Berufsgruppe der Rechtsanwälte der Weg zur Akkreditierung als Zertifizierungsstelle aufgrund dieser formaljuristischen Einschränkung verwehrt wäre, gleichwohl sie das in § 6 geforderte Fachwissen unzweifelhaft aufweisen (zumal gemäß den Erläuterungen zu § 6 Abs 1 eine Personenmehrheit zulässig ist, dh das

geforderte Fachwissen auch von Einzelanwälten mit entsprechendem Fachpersonal erbracht werden kann). Diese Beschränkung ist sohin nicht sachgerecht und würde deren Beibehaltung verfassungsrechtlichen Bedenken begegnen. Zu den nicht berufsspezifischen Bedenken siehe im Folgenden.

Die im vorgeschlagenen § 5 propagierten Unabhängigkeitsregelungen sind untauglich. Sie besagen, dass die mit dem Zertifizierungsverfahren betrauten Personen und die für die Zertifizierungsentscheidung verantwortliche Person vom Zertifizierungswerber fachlich, persönlich, wirtschaftlich, organisatorisch und rechtlich unabhängig zu sein hat. Da im Zeitpunkt der Akkreditierung die Zertifizierungswerber nicht bekannt sind (bzw noch nicht existieren), kann diese Unabhängigkeit nicht geprüft bzw erfüllt werden. § 5 ist in dieser Form daher nicht anwendbar. Aber auch inhaltlich erscheint die Regelung überbordend. Deren Beschreibung eines Abhängigkeitsverhältnisses, das die Unabhängigkeit und Integrität des Zertifizierungsinhabers in Frage stellt (vgl § 5 Abs 2), ist im Wesentlichen das Abstellen auf eine Spekulation. Derartiges könnte in Anlassfällen auf Einzelbasis geprüft werden, nicht aber kann dies zum generellen Akkreditierungsparameter erhoben werden. Diese breite Umschreibung würde es Rechtsanwälten verunmöglichen, ihre Mandanten zu zertifizieren, Unternehmen dürften ihre Kunden nicht zertifizieren, der TÜV dürfte keine im technischen Bereich agierenden Unternehmen zertifizieren, usw. Denn all diese Akteure stehen zueinander in dem spekulativen Naheverhältnis des § 5 Abs 2. Diese Bestimmung ist aus der Sicht des ÖRAK grundsätzlich zu überarbeiten.

Ausschließlich begrüßt wird, dass gem § 6 Abs 2 die juristische Fachkenntnis durch ein Studium zu belegen ist (gleichwohl die in § 6 Abs 1 vorgeschlagene Einschränkung auf das Datenschutzrecht, auf das TKG und auf die Dienste der Informationsgesellschaft nicht nachvollziehbar ist – man denke alleine an das komplexe, Gesundheitsdaten regulierende Medizinrecht). Nicht nachvollziehbar ist, dass das juristische Studium gem § 6 Abs 4 durch eine fünfjährige Berufspraxis ersetzt werden kann. In extensio kann gem § 6 Abs 4 iVm 6 der vorgeschlagenen Verordnung eine Person die Zertifizierungsentscheidung treffen, die ausschließlich eine entsprechende Berufspraxis aufweist. In einem Rechtsgebiet, das mittlerweile eine Dichte an höchstgerichtlichen Entscheidungen (auch des EuGHs) aufweist und das von Strafdrohungen vieler Millionen Euro geprägt ist, ein Datenschutzsiegel durch Personen vergeben zu lassen, die keine einschlägige rechtswissenschaftliche Ausbildung aufweisen müssen, ist außerhalb jeglichen rechtspolitischen Verhältnisses. In dem Verordnungsentwurf ist aufzunehmen, dass jedenfalls die Person, welcher die Entscheidung über die Zertifizierung zukommt, zwingend ein rechtswissenschaftliches Studium oder eine gleichwertige Auslandsbildung aufweisen muss.

Zu § 4 Abs 3 Z 8 findet sich in den Erläuterungen der Hinweis, dass eine risikobasierte Haftpflichtversicherung Voraussetzung ist, während sich dies im Verordnungstext nicht findet. Dass sich diese Vorgabe nicht in der Verordnung findet, sondern in den Erläuterungen, ist befremdlich, es sollte umgekehrt sein. Zudem ist jede Versicherung risikobasiert. Gemeint ist wohl eine Mindestversicherungssumme. Angesichts des Schadenspotentials fehlerhafter Zertifizierungen sollte sich diese an den Vorgaben des § 21a RAO zu orientieren haben.

<u>Nicht berufsspezifische Bedenken</u>:

In genereller Betrachtung fällt auf, dass die vorgeschlagene Verordnung in weiten Teilen auf die ISO/IEC 17065:2012 referenziert und damit unter Inanspruchnahme dynamischer Verweisungen ihren Normgehalt auf eine internationale Normierungsrichtlinie auslagert. So etwa verweist § 4 Abs 3 Z 8 zum Nachweis der Abdeckung finanzieller Verbindlichkeiten auf diese Normierungsrichtlinie. Auch wird die Antragstellung auf einen juristischen Personenbegriff der ISO/IEC 17065:2012 beschränkt, welcher der österreichischen Rechtsordnung fremd ist (vgl § 4 Abs 1). Ebenso werden Aufzeichnungspflichten (§ 6 Abs 9) und Pflichten der Strukturierung, Konfliktminimierung und der Vertraulichkeit auf diese Richtlinie ausgelagert (sämtliches: § 7). An mannigfacher Stelle der Verordnung finden sich sinngleiche Verweise auf die ISO/IEC 17065:2012.

Eine Verordnung stellt die Präzisierung eines Gesetzes dar. Sie bildet also einen Bestandteil der parlamentarisch legitimierten Gesetzgebung. Nichts anderes gilt für die Präzisierung einer unionsrechtlichen Verordnung, wie der DSGVO. Dem ÖRAK ist der Gedanke der Verwaltungseffizienz natürlich nicht fremd. Nicht aber darf dies dazu führen, dass der normative Gehalt einer Verordnung nicht durch die Verordnung selbst, sondern durch beständigen Verweis auf eine Normierungsrichtlinie geschaffen wird. Dies ist aber im vorliegenden Verordnungsentwurf der Fall. Der ÖRAK regt im Lichte der hieraus resultierenden Verfassungswidrigkeit eine grundlegende Überarbeitung des Verordnungsentwurfs dahingehend an, dass die Verweise auf die ISO/IEC 17065:2012 auf das sachgerechte Ausmaß beschränkt werden.

Wien, am 24. Juni 2020

DER ÖSTERREICHISCHE RECHTSANWALTSKAMMERTAG

Dr. Rupert Wolff
Präsident