oesterreichs energie.

GENERALSEKRETARIAT

Datenschutzbehörde
Barichgasse 40-42
1030 Wien
Per E-Mail an: dsb@dsb.gv.at

Kontakt	DW	Unser Zeichen	Ihr Zeichen	Datum
DI Ursula Tauschek	223	TA/Ha – 05/2020	D056.151	25.06.2020

Stellungnahme zum Entwurf einer Verordnung der Datenschutzbehörde über die Akkreditierung einer Zertifizierungsstelle (Zertifizierungsstellen-Akkreditierungs-Verordnung – ZeStAkk-V)

Sehr geehrte Damen und Herren,

Oesterreichs Energie bedankt sich für die Gelegenheit, zum Entwurf über die Akkreditierung einer Zertifizierungsstelle (Zertifizierungsstellen-Akkreditierungs-Verordnung – ZeStAkk-V) Stellung nehmen zu dürfen.

Zu den einzelnen Punkten des Entwurfes der Datenschutzbehörde nehmen wir, wie folgt, Stellung:

Zu § 1: Allgemeine Bestimmungen
Hier ist unklar, ob ISO 17065:2012 vollinhaltlich oder nur bei jenen Punkten umgesetzt werden soll, auf die im Verordnungsentwurf verwiesen wird.

Während § 1 ZeStAkk-V davon spricht, dass die Verordnung *„in Ergänzung der Vorgaben der […] ISO/IEC 17065:2012 […] die Voraussetzungen für die Akkreditierung von Zertifizierungsstellen […]“* regelt, referenzieren die §§ 4 Abs.1, Abs. 2, 5, Abs. 3 Z 8, 6, Abs. 1, Abs. 9, 7, Abs. 1, Abs. 2, Abs. 4, 8, Abs. 2 – 4, Abs. 6, 9, Abs. 2, 10, Abs. 2, 11, Abs. 1, Abs. 3, Abs. 6, 12, 14, Abs. 2, 15, Abs. 1, 16, Abs. 1, Abs. 4, 18, Abs. 1, 19 auf konkrete Regelungen der ISO/IEC 17065:2012.
Insbesondere enthält ISO/IEC 17065:2012 auch zahlreiche Verweise auf andere internationale Normen, sodass eine Abgrenzung in dieser Hinsicht sinnvoll erschiene.

Zu § 2: Begriffsbestimmung
In die Begriffsbestimmung sollten ebenfalls folgende Begriffe aufgenommen werden:

- Inhaber von Zertifizierungsverfahren
- Zertifizierungsprogramm
- Sachverständige
- mit Zertifizierungsverfahren betraute Personen.

Zu § 3: Akkreditierung
Die Formulierung *„wird diese ermächtigt“* ist irreführend. Eine Akkreditierung ist keine Ermächtigung im staatswissenschaftlichen Sinn, sondern bloß die formelle Anerkennung durch eine nationale Akkreditierungsstelle (hier: Datenschutzbehörde), dass Akkreditierungswerber die für sie geltenden Anforderungen an Qualifikation und Ausstattung erfüllen und diese damit als kompetent gelten.

Durch die Formulierung *„wird diese ermächtigt“* wird an mehreren Stellen des Entwurfs sichtbar, dass die Autoren von einer von der Datenschutzbehörde abgeleiteten Befugnis ausgehen. Dies entspricht jedoch nicht den Tatsachen und steht auch im Widerspruch mit den Erläuterungen zu § 3 ZeStAkk-V.

Sinnvoll wäre es, sich bei der Formulierung an der Nomenklatur der Akkreditierung Österreich zu orientieren: https://www.bmdw.gv.at/Services/Akkreditierung.html.

Zu § 4 Abs. 1: Akkreditierungsverfahren
Im Entwurf wird eine Beschränkung der Akkreditierungsfähigkeit auf juristische Personen vorgenommen.

Der Verweis auf ISO/IEC 17065:2012 überzeugt nicht, weil die Datenschutzbehörde nicht verpflichtet ist, sich an der Norm zu orientieren. Auch das Argument in den Erläuterungen, wonach nur so eine Zertifizierungsstelle für ihre Tätigkeit rechtlich verantwortlich gemacht werden könne, geht ins Leere.

Die Aktivlegitimation im Akkreditierungsverfahren sollte auf alle Formen der natürlichen oder juristischen Rechtspersönlichkeit ausgeweitet werden.

Zu § 5 Abs. 3 und 4: Unabhängigkeit
In diesem Absatz wird zwar auf das Erfordernis der Unabhängigkeit verwiesen, ohne aber klar darzulegen, welche Gründe einer Unabhängigkeit entgegenstehen. Klar ist nur, dass es lt. Abs. 3 zwischen der Zertifizierungsstelle und dem Zertifizierungswerber keine Vertragsbeziehung gem. Art 26 Abs.1 bzw. Art 28 Abs. 3 DSGVO geben darf. Ansonsten wird in diesem Absatz auf die ISO/IEC-17065:2012 Bezug genommen, die öffentlich nicht einsehbar ist. Auch in den Erläuterungen steht keine weitere diesbezügliche Information. Hier wäre eine Präzisierung wünschenswert. Weiters sollte generell klargestellt werden, ob sich das Hindernis nur auf die konkret zu zertifizierende Datenverarbeitung bezieht oder generell.

Zum Zeitpunkt der Akkreditierung kann nicht gesagt werden, wer Zertifizierungswerber ist. Dementsprechend kann ein Akkreditierungswerber auch nicht nachweisen, dass die entscheidungsbefugten Personen in keiner „personellen, organisatorischen oder finanziellen Verflechtung zu den Zertifizierungswerbern“ stehen.

Eine solche ex ante Deklaration ist in ISO/IEC 17065:2012 (natürlich) auch nicht vorgesehen. Stattdessen sollte eine Vorgabe aufgenommen werden, dass Zertifizierungsstellen durch vertragliche Regelungen entsprechende Vorkehrungen treffen.

Zu § 6: Fachwissen
Durch die mannigfaltigen Verweise der ISO 17065:2012 und der global unterschiedlichen umgesetzten und gelebten Konformitätsbewertung wäre eine Klarstellung bzw. Einschränkung wünschenswert.
Durch die Datenschutzbehörde sollten die relevanten Normen klar benannt werden.

Weiters ist die strikte Eingrenzung in Abs. 2 auf das Studium der Rechtswissenschaften nicht nachvollziehbar. Es wäre das Studium „Wirtschaftsrecht“ somit nicht erfasst. Auch wenn Abs. 4 eine Abschwächung dahingehend vorsieht, dass eine 5jährige einschlägige Berufserfahrung dem gleichzuhalten ist (die laut der Erläuterungen durch ein Dienstzeugnis nachgewiesen werden kann), empfehlen wir aus Gründen der Gleichbehandlung in Abs. 2 auch Absolventen des Studiums „Wirtschaftsrecht“ zu erfassen.

Zu § 8 Abs. 1 Z 3: Zertifizierungsverfahren
Es ist nachvollziehbar, dass Prozesse und damit in Verbindung stehende Verträge gem. Art 26 und 28 DSGVO nachgewiesen werden müssen. Dass schon bei Antragstellung Kopien dieser Verträge vorzulegen sind, erhöht aber aus unserer Sicht den bürokratischen Aufwand. Es wäre aus unserer Sicht ausreichend, eine Liste der abgeschlossenen Verträge bei Antragstellung vorzulegen und Verträge auf Anfrage zur Verfügung zu stellen.

Zu § 9: Zertifizierungsvereinbarung
Der in Abs. 2 Z 5 verankerte Zugang für die mit der Durchführung der Zertifizierung betrauten Personen zu den Betriebsstätten sollte nach unserer Auffassung lediglich nach vorheriger Ankündigung erfolgen.

In Abs. 2 Z 6 ist vorgesehen, dass in der Zertifizierungsvereinbarung ein verpflichtender Hinweis aufgenommen wird, *„dass die Zertifizierung unbeschadet der aus der DSGVO resultierenden Verpflichtung erfolgt“.*

Eine solche Klarstellung ergibt sich schon aus dem Normtext und muss deshalb nicht nochmals gesondert vereinbart oder mitgeteilt werden.

Zu § 10 Abs. 2: Änderungen von Zertifizierungsanforderungen
In Abs. 2 werden Entscheidungen des Europäischen Datenschutzausschusses (EDSA) als wirkungsrelevante Änderungen angeführt.

In der DSGVO wurde für den Europäischen Datenschutzausschuss das Instrument der Stellungnahme festgelegt. Somit stellen die Stellungnahmen und Leitlinien (sog. „graue Literatur“) des EDSA eine unverbindliche Verwaltungsmeinung dar.

Durch ein Überbinden der Verwaltungsmeinung zur wirkungsrelevanten Änderung im Gleichklang mit Änderungen der Rechtslage oder gerichtlichen Entscheidungen bzw. Erlässen der Europäischen Kommission kommt es zu einer unzulässigen Verletzung der verfassungsmäßig gewährleisteten Gewaltentrennung. Auch mangelt es den Positionen des EDSA dann am notwendigen Rechtsschutzinstrumentarium.

Zu § 16 Abs. 3 Z 1: Überwachungsverfahren
Nach dem Entwurf richtet sich die Häufigkeit der Überprüfung nach dem Zertifizierungsgegenstand, dem Ergebnis der Risikoanalyse und der Anzahl der Beschwerdefälle.

Die Datenschutzbehörde sollte ein Mindestintervall festsetzen und ggf. klarstellen, dass es zu einem kürzeren Intervall kommen kann, wenn dies durch das Ergebnis der Risikoanalyse und der Anzahl an Beschwerden geboten erscheint. Auch sollte die Datenschutzbehörde im Akkreditierungsverfahren dann vorschreiben, dass das System der Risikoanalyse dargestellt werden muss.

Zu § 18 Abs. 2 Z 1: Beschwerdeverfahren
Die Datenschutzbehörde sollte festlegen, wer befugt ist, eine Beschwerde an die Zertifizierungsstelle zu richten.

Wir danken für die Kenntnisnahme der Anliegen von Oesterreichs Energie und ersuchen um deren Berücksichtigung.

Mit freundlichen Grüßen

Mag. Dr. Michael Strugl
Präsident

Dr. Barbara Schmidt
Generalsekretärin

Über Oesterreichs Energie
Oesterreichs Energie vertritt seit 1953 die gemeinsam erarbeiteten Brancheninteressen der E-Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit. Als erste Anlaufstelle in Energiefragen arbeiten wir eng mit politischen Institutionen, Behörden und Verbänden zusammen und informieren die Öffentlichkeit über Themen der Elektrizitätsbranche.
Die rund 140 Mitgliedsunternehmen erzeugen mit rund 20.000 Mitarbeiterinnen und Mitarbeitern mehr als 90 Prozent des österreichischen Stroms mit einer Engpassleistung von über 25.000 MW und einer Erzeugung von rund 68 TWh jährlich, davon 72 Prozent aus erneuerbaren Quellen.