BUNDESARBEITSKAMMER

PRINZ-EUGEN-STRASSE 20-22
1040 WIEN
www.arbeiterkammer.at
erreichbar mit der Linie D

DSB
Republik Österreich
Datenschutzbehörde
Barichgasse 40-42
1030 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel **501 65**	Fax **501 65**	Datum
GZ:D056.151 2020-0.159.543	BAK/KS/ GSt/DZ/BE	Daniela Zimmer Filiz Yurdakul	DW 12722	DW 12693	10.06.2020

Verordnung der Datenschutzbehörde über die Anforderungen an die Akkreditierung einer Zertifizierungsstelle (Zertifizierungsstellen-Akkreditierungs-Verordnung-ZeStAkk-V)

Die Bundesarbeitskammer (BAK) bedankt sich für die Übermittlung des Entwurfs und nimmt dazu wie folgt Stellung.

Zum Inhalt der Verordnung

Die vorliegende Verordnung regelt die Voraussetzungen für die Akkreditierung von Zertifizierungsstellen gemäß Art 58 Abs 3 lit e DSGVO. Zertifizierungsverfahren und Datenschutzsiegel sollen betroffenen Personen „einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienste ermöglichen“ (EG 100 DSGVO).

Neben branchenspezifischen Verhaltensregeln gemäß Art 40 DSGVO stellt die Zertifizierung ein weiteres Instrument der Selbstregulierung dar. In Österreich fungiert die Datenschutzbehörde – gemäß § 24 Abs 3 des Datenschutzgesetzes (DSG) – als einzige nationale Akkreditierungsstelle gemäß Art 43 Abs 1 DSGVO.

Zertifizierungsstellen sind befugt, Zertifizierungswerbern die Bestätigung von datenschutzkonformen Datenverarbeitungen zu erteilen. Die Konformitätsbescheinigung dient als Nachweis dafür, dass die DSGVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird.

Zusammenfassende Bewertung: Die BAK erhebt gegen den Entwurf keinen Einwand, erlaubt sich aber, im Folgenden einige Anregungen zu geben, die der Klarstellung und Transparenz gegenüber interessierten Betroffenen dienen.

Anmerkungen

Zu § 4 Abs 1 (Akkreditierungsverfahren): Um akkreditiert zu werden und die Funktion einer Zertifizierungsstelle auszuüben, bedarf es eines schriftlichen Antrages an die Datenschutzbehörde als zuständige Aufsichtsbehörde. Im Akkreditierungsverfahren ist nicht angeführt, ob im Falle einer Absage ein neuerlicher Antrag möglich ist und wenn ja, in welchem Zeitraum.

Zu § 4 Abs 6 (Akkreditierungsverfahren): Es wird begrüßt, dass der maximale Geltungszeitraum für Akkreditierungen nach der DSGVO nicht undifferenziert übernommen wird. Die vorgenommene Unterscheidung in einen grundsätzlichen Zeitraum von fünf Jahren, von dem zugunsten von 3 Jahren abgewichen werden kann, erscheint zweckmäßig. Auf diese Weise kann darauf geachtet werden, ob Zertifizierungsverfahren auch in Hinblick auf Prüfschema und Technik noch der Marktentwicklung entsprechen. Der kürzere Zeitraum ist vorgesehen, wenn sich „der Gegenstand der Akkreditierung auf die Verarbeitung besonderer Kategorien personenbezogener Daten bezieht". Weitere Ausnahmen für „heikle" Datenanwendungen wären sachgerecht (bei Verarbeitungen, die allgemein einer Folgenabschätzung unterliegen, bei massenhaft verarbeiteten Daten, strafrechtsrelevanten Daten etc).

Zu § 6 Abs 4 (Fachwissen): Die juristischen und technischen Fachkenntnisse können auch in Form einer mindestens fünfjährigen einschlägigen Berufserfahrung nachgewiesen werden. Hier wäre es wünschenswert, die einschlägige Berufserfahrung näher zu konkretisieren.

Zu § 8 Abs 1 (Zertifizierungsverfahren): Die Zertifizierung erfolgt auf Grundlage eines Antrags des Zertifizierungswerbers an die Zertifizierungsstelle; es wird nicht ausgeführt, ob und wann im Falle einer Absage ein erneuter Antrag vom Zertifizierungswerber möglich ist.

Zu § 13 Abs 2 lit 4 (Zertifizierungsentscheidung): Die schriftliche Bescheinigung im Falle der Zertifizierung hat folgende Angaben zu enthalten: Den Geltungsbereich der Zertifizierung und eine aussagekräftige Beschreibung des Zertifizierungsgegenstandes. „Aussagekräftige Beschreibung" ist etwas vage formuliert. Außerdem ist in den Erläuterungen zu § 4 Abs 3 Z 2 angeführt, dass klar ersichtlich sein muss, welche konkreten Verarbeitungsvorgänge Gegenstand der Zertifizierung sind und welche Komponenten bewertet werden. Die Formulierung „konkrete Verarbeitungsvorgänge" sollte auch im Normtext verwendet werden.

Zu § 15 (Zertifizierungsverzeichnis): Die Zertifizierungsstelle hat eine Zusammenfassung der Bewertungsberichte in geeigneter Form zu veröffentlichen und auf Anfrage bereitzustellen. Ziel der Zertifizierung ist es, Betroffenen einen raschen Überblick über das Datenschutzniveau eines Produktes oder Dienstes zu ermöglichen. Vor diesem Hintergrund sollte ein zentrales Zertifizierungsverzeichnis bei der Datenschutzbehörde eingerichtet und für jedermann abrufbar sein. Sollten Interessierte doch nur an die Verzeichnisse einzelner

Zertifizierungsstellen verwiesen werden, muss der Zugang zu den Infos für Betroffene möglichst leicht sein (zB durch einen gut auffindbaren Link-Hinweis in der Datenschutzerklärung des Verantwortlichen auf den bei der Zertifizierungsstelle veröffentlichten Bewertungsbericht).

Unterzeichner	Bundeskammer für Arbeiter und Angestellte
Datum/Zeit-UTC	23.06.2020 19:31
Prüfhinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.