3/2020
49 – 72

FAQ-Special!
Corona & Arbeitsrecht
Viktoria Haidinger

# DATENSCHUTZ KONKRET

**Recht | Projekte | Lösungen**

Chefredaktion: Rainer Knyrim

## Information und Transparenz

### Auskunftsanspruch über die Logik einer Datenverarbeitung
*Andreas Zavadil*

### Information & Transparenz (Teil 1)
*Ursula Illibauer*

### Strafrechtliche Folgen eines Missbrauchs des Auskunftsrechts (Teil 2)
*Célia Chausse und Georg Kudrna*

### Der jö Bonus Club ist kein Pricing-Tool, sondern ein Kundenbindungsprogramm
*Interview mit Ulrike Kittinger, Geschäftsführerin Ö-Bonus Club*

### Datenschutzzertifikate in greifbarer Nähe?
*Gerald Trieb und Maximilian Kröpfl*

### Sommerrodeln und Datenschutz
*Martin Knoll*

### Checkliste Homeoffice und COVID-19
*Hans-Jürgen Pollirer*

ISSN 2313-5409

dako.manz.at

MANZ

Österreichische Post AG PZ 18Z041356 P Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

Gerald Trieb/Maximilian Kröpfl
Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte/Rechtsanwaltsanwärter ebendort

# DSGVO-Datenschutzzertifikate in greifbarer Nähe?

**Eine Besprechung des Entwurfs der Zertifizierungsstellen-Akkreditierungs-VO.** Datenschutzzertifizierung nach DSGVO rückt in greifbare Nähe! Ende April hat die DSB ihren Entwurf für eine Verordnung über die Anforderungen an die Akkreditierung einer Zertifizierungsstelle (Zertifizierungsstellen-Akkreditierungs-Verordnung; kurz: ZeStAkk-V)[1] zur Begutachtung ausgesendet.[2] Mit einer finalen Fassung der V ist wohl nicht vor Herbst zu rechnen, da die Begutachtungsfrist bis 26. 6. 2020 läuft und im Anschluss der allenfalls überarbeitete Entwurf vom Europäischen Datenschutzausschuss genehmigt werden muss.[3] Dennoch bekommen wir ein gutes Bild davon, was die datenschutzrechtliche Zertifizierung in Zukunft bereithalten wird. In Bezug auf einzelne Vorgaben und Anforderungen sind Änderungen wünschenswert.

## Ecosystem datenschutzrechtlicher Zertifizierung

Um die Transparenz zu erhöhen und die Einhaltung der DSGVO zu verbessern, sollen nach der europäischen Vorstellung von Eigenverantwortung und Rechenschaftspflicht Zertifizierungsverfahren sowie Datenschutzsiegel und Prüfzeichen eingeführt werden. Diese sollen betroffenen Personen, der Öffentlichkeit und Marktteilnehmern einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.[4]

Den **Rahmen** datenschutzrechtlicher Zertifizierung bilden **Art 42 und 43 DSGVO**. Während Art 42 Zertifizierungskriterien und den Zertifizierungszeitraum schematisch regelt, findet man in Art 43 die Anforderungen an die Zertifizierungsstelle, an das Akkreditierungsverfahren und an das Zertifizierungsverfahren. In Spezifizierung dieser generellen Vorgaben zieht die DSB mit Referenz auf Art 43 Abs 1 lit b DSGVO die internationale Norm **ISO/IEC 17065:2012**[5] heran, obwohl § 21 Abs 3 DSG[6] ausschließlich die DSB als Akkreditierungsstelle vorsieht, was nach Art 43 Abs 1 lit a DSGVO zulässig ist. Diese ISO-Norm beschreibt Anforderungen an Stellen, die Produkte, Prozesse oder Dienstleistungen zertifizieren;[7] in unserem Fall die **Datenverarbeitung**, die auch immer Gegenstand einer Zertifizierung ist.[8] Dennoch nimmt die DSB im Verordnungsentwurf an zahlreichen Stellen auf diese ISO-Norm Bezug und regelt in zusätzlicher Spezifikation[9] der schon recht umfangreichen Anforderungen dieser Norm mit der ZeStAkk-V weitere, entsprechende Anforderungen an datenschutzrechtliche Zertifizierungsstellen. Eine Zertifizierung eines Verantwortlichen oder Auftragsverarbei-

[1] Entwurf einer V der DSB über die Anforderungen an die Akkreditierung einer Zertifizierungsstelle; http://wko.at/ooe/Branchen/Industrie/Zusendungen/DSB_ZeStAkk-V_Entwurf.pdf (Stand aller Links 8. 5. 2020). [2] Gem Art 57 Abs 1 lit p DSGVO ist die DSB als nationale Aufsichtsbehörde zur Abfassung und Veröffentlichung der Akkreditierungskriterien für Zertifizierungsstellen verpflichtet, gem § 21 Abs 3 DSG dazu auch national ermächtigt. [3] Art 43 Abs 3 DSGVO. [4] ErwGr 100 DSGVO. [5] Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren (EN ISO/IEC 17065:2012). [6] BG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) BGBl I 2017/120. [7] EN ISO/IEC 17065:2012, 6. [8] Erläut der DSB zum Entwurf der ZeStAkk-V 3, http://wko.at/ooe/Branchen/Industrie/Zusendungen/DSB_Erl%C3%A4uterungen_ZeStAkk-V_Entwurf.pdf [9] § 1 ZeStAkk-V.

ters in seiner Gesamtheit ist daher nicht möglich.[10] Vor dem Hintergrund, dass eine Prüfung der Datenverarbeitung auch die eingesetzten technischen Systeme sowie die Verarbeitungsorganisation umfasst, werden Hard- und Software sowie getroffene technische und organisatorische Maßnahmen (wie ein Datenschutz-Management-System) jedoch auch nach Ansicht der DSB zumindest mittelbar geprüft und zertifiziert.[11] Denn die kleinste Betrachtungseinheit „Datenverarbeitung" basiert in Unternehmen regelmäßig auf einem organisationsweiten Datenschutz-Management-System. Was im Kleinen zertifiziert ist, gibt auch Auskunft über die dahinter stehenden Prozesse und Anforderungen der guten datenschutzrechtlichen Praxis im Unternehmen.[12] Eine unmittelbare Zertifizierungsmöglichkeit von **Datenschutz-Management-Systemen** wäre jedoch wünschenswert und würde sich in der Praxis wohl auch großer Beliebtheit erfreuen, da auf diese Weise die gesamtheitliche Sicherstellung der Einhaltung der DSGVO *„bei Verarbeitungsvorgängen"*[13] von Verantwortlichen und Auftragsverarbeitern zertifiziert werden könnte.

Betrachtet man das Spielbrett der datenschutzrechtlichen Zertifizierung, so kann man folgende **fünf Figuren** entdecken:

- Den Inhaber der Zertifizierungskriterien,
- die akkreditierte Zertifizierungsstelle,
- den Zertifizierungswerber,
- den Zertifizierungsinhaber und
- die DSB als datenschutzrechtliche Aufsicht.

Während Inhaber der Zertifizierungskriterien und akkreditierte Zertifizierungsstelle in Personalunion bestehen können, sind die Rollen des Zertifizierungswerbers und -inhabers einander in Abhängigkeit nachgelagert.

## Mehrwert datenschutzrechtlicher Zertifizierung

Datenschutzrechtliche Zertifizierungen iSd Art 42 DSGVO können als Faktor herangezogen werden, um die **Erfüllung der Pflichten** des Verantwortlichen (Art 24 Abs 1 DSGVO) oder der zu implementierenden technischen und organisatorischen Maßnahmen (Art 32 Abs 1 DSGVO) **nachzuweisen**.

Zudem können sie auch für die verpflichtende Prüfung des Verantwortlichen herangezogen werden,[14] ob der für die Vornahme von Verarbeitungen herangezogene Auftragsverarbeiter eine rechtskonforme und sichere Verarbeitung garantieren kann. Dies auch aus **haftungstechnischen Gründen**. Die datenschutzrechtliche Zertifizierung kann somit das Outsourcing von Datenverarbeitungen an Auftragsverarbeiter (auch in Bezug auf Cloud-Dienstleistungen) erleichtern.

Weiters, wenngleich unter den Voraussetzungen von Art 46 Abs 2 lit f iVm Art 42 Abs 2 DSGVO, können datenschutzrechtliche Zertifizierungen als geeignete **Garantien für den internationalen Datentransfer** herangezogen werden.[15]

**Zertifizierungen können Geldbußen reduzieren!**

Insb ist aber eine aufrechte datenschutzrechtliche Zertifizierung auch bei der Entscheidung über die Verhängung einer **Geldbuße** und über deren Betrag je nach Einzelfall gebührend zu berücksichtigen; die Zertifizierung könnte somit empfindliche Geldbußen auf ein erträgliches Maß reduzieren helfen![16]

## Zertifizierungskriterien und -anforderungen

Den Rahmen der datenschutzrechtlichen Zertifizierung bilden die Zertifizierungskriterien. Nach der Legaldefinition handelt es sich bei **Zertifizierungskriterien** um jene von der akkreditierten Zertifizierungsstelle festgelegten und gem Art 42 Abs 5 DSGVO genehmigten Kriterien, anhand derer eine Zertifizierung durchgeführt wird.[17] Grundsätzlich unterscheidet man zwischen nationalen, multinationalen und europäischen Zertifizierungskriterien.[18]

In Spezifizierung der Zertifizierungskriterien hat die Zertifizierungsstelle **Zertifizierungsanforderungen** festzulegen. Dabei handelt es sich um jene Anforderungen, die vom Zertifizierungswerber als eine Bedingung zur Feststellung oder Aufrechterhaltung der Zertifizierung zu erfüllen sind.[19]

## Akkreditierung der Zertifizierungsstelle

Zertifizierungsstelle ist jene unabhängige Stelle, die gem ZeStAkk-V von der DSB zur Konformitätsbewertung von DSGVO-Datenschutzzertifikaten akkreditiert wurde.[20] Ihre **Aufgaben** sind das Verleihen, Überwachen, Erneuern und Entziehen von datenschutzrechtlichen Zertifizierungen.[21]

Als Zertifizierungsstelle akkreditiert werden können nur juristische Personen.[22] Eine Begründung dafür bleiben auch die Erläuterungen zum Verordnungsentwurf schuldig.[23] Eine Zertifizierungsstelle hat die Zertifizierungstätigkeit unabhängig[24, 25] vertraulich,[26] unparteiisch[27] und dokumentiert[28] durchzuführen.[29] Dabei hat sie systematische, nach festgelegten Regeln durchgeführte Verfahren vorzusehen, die die initiale Konformitätsbewertung und das Überwachungsaudit regeln.[30] Darüber hinaus haben Zertifizierungsstellen sog **Beschwerdeverfahren** zu unterhalten.[31] In diesem Rahmen können Dritte die Nichtkonformität eines Zertifizierungsinhabers bei der Zertifizierungsstelle behaupten. Handelt es sich dabei um eine betroffene Person iSd Art 4 Z 1 DSGVO, so kann diese bei Vorliegen der erforderlichen Voraussetzungen statt Inanspruchnahme des Beschwerdeverfahrens bei der Zertifizierungsstelle auch Beschwerde an die DSB erheben.[32]

**Durch ein Beschwerdeverfahren kann die Zertifizierung auf dem Prüfstand stehen.**

An die **Kompetenz der Zertifizierungsstelle** stellt die DSB besonders **hohe Anforderungen**. So sind neben Kenntnissen des Datenschutzrechts[33] hinreichende Erfahrung der Anwendung technischer und organisatorischer Maßnahmen und Verfahren[34] und der für die Konformitätsbewertung maßgeblichen Bestimmungen und Normen[35] auch Kenntnisse im Telekommunikationsrecht und dem Recht der Informationsgesellschaft[36] nachzuweisen. Audito-

[10] Erläut ZeStAkk-V 3. [11] Erläut ZeStAkk-V 3. [12] Wenngleich mit der Norm ISO 27701:2019 ein guter Ansatz für einen internationalen Standard vorliegt, können solche privaten Zertifikate nicht den so dringend verlangten Mehrwert einer DSGVO-Zertifizierung vermitteln. [13] Art 42 Abs 1 DSGVO. [14] Siehe Art 28 Abs 1 DSGVO. [15] Erläut ZeStAkk-V 1. [16] Art 83 Abs 2 lit j DSGVO. [17] § 2 Z 3 ZeStAkk-V. [18] *Kröpfl*, Datenschutzrechtliche Zertifizierungen, in *Jahnel* (Hrsg), Datenschutzrecht (2019) 164 (175). [19] § 2 Z 1 ZeStAkk-V. [20] § 2 Z 4 ZeStAkk-V. [21] *Europäischer Datenschutzausschuss*, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation (4. 6. 2019) Rz 27. [22] § 4 Abs 1 ZeStAkk-V. [23] Argumentiert wird bloß, dass eine Zertifizierungsstelle nur so für ihre Tätigkeit rechtlich verantwortlich gemacht werden könne. Das erschließt sich jedoch nicht, weil dies auch auf natürliche Personen zutrifft. [24] § 5 Abs 1 ZeStAkk-V. [25] § 7 Abs 2 ZeStAkk-V. [26] § 7 Abs 4 ZeStAkk-V. [27] EN ISO/IEC 17065:2012, 5.1.1. [28] EN ISO/IEC 17065:2012, 5.1.2. [29] § 7 Abs 1 ZeStAkk-V. [30] § 16 Abs 1 ZeStAkk-V. [31] § 18 Abs 1 ZeStAkk-V. [32] Erläut ZeStAkk-V 6. [33] § 6 Abs 1 Z 1 ZeStAkk-V. [34] § 6 Abs 1 Z 1 ZeStAkk-V. [35] § 6 Abs 1 Z 3 ZeStAkk-V. [36] § 6 Abs 1 Z 2 ZeStAkk-V.

ren haben entsprechende Kenntnisse und Erfahrungen aufzuweisen.[37] Jene Person, die die Zertifizierungsentscheidung trifft, muss darüber hinaus zusätzlich über mindestens fünfjährige Berufserfahrung im Datenschutzrecht und im Bereich des technischen Datenschutzes verfügen.[38] Der Nachweis durch eine Personenmehrheit ist zulässig.[39]

Die Akkreditierung der Zertifizierungsstelle ist für **fünf Jahre** aufrecht.[40] Eingeschränkt auf **drei Jahre** wird akkreditiert, wenn sich der Gegenstand der Akkreditierung auf die Verarbeitung besonderer Kategorien personenbezogener Daten[41] bezieht.[42] Damit scheint, ähnlich wie bei Überwachungsstellen nach Art 41 DSGVO, die nur in Bezug auf genehmigte Verhaltensregeln akkreditiert werden können, nicht möglich zu sein, eine Akkreditierung als Zertifizierungsstelle ohne Bezugnahme auf bestimmte Zertifizierungskriterien zu erhalten.

## Zertifizierungsverfahren

Die Zertifizierung ist eine **Konformitätsbestätigung**.[43] Ein Zertifizierungsverfahren wird anhand der Zertifizierungsanforderungen und auf Basis eines Auditplans durchgeführt. Das Ergebnis einer positiven Konformitätsbewertung ist die Erteilung einer schriftlichen Konformitätsbescheinigung (Zertifizierung) zum Nachweis dafür, dass die DSGVO bei Verarbeitungsvorgängen eingehalten wird.[44]

Das Zertifizierungsverfahren folgt einem **standardisierten Ablauf**:[45] Zunächst ist vom Zertifizierungswerber ein Antrag auf Zertifizierung an die dafür akkreditierte Zertifizierungsstelle zu richten. Die Zertifizierungsstelle prüft den Antrag, schließt eine Zertifizierungsvereinbarung ab und leitet die Evaluierung durch eigene Kräfte oder durch beauftragte Dritte[46] ein. Mit Hilfe der Evaluierung sollen ausreichende objektive Nachweise zusammengetragen werden,[47] ob die Zertifizierungsanforderungen erfüllt sind. In diesem Rahmen sind auch Informationen zu allfällig ausgegliederten Prozessen und Kopien der Auftragsverarbeiterverträge oder Vereinbarungen über die gemeinsame Verantwortlichkeit bereitzustellen.[48]

Auf der nächsten Ebene sind die zusammengetragenen Nachweise zu bewerten. Auf Basis des **Bewertungsberichts** trifft dann die oberste Leitung der Zertifizierungsstelle die Zertifizierungsentscheidung durch Abgleich, ob der Zertifizierungswerber die Zertifizierungsanforderungen einhält. Fällt die Zertifizierungsentscheidung positiv aus, so ist ein entsprechendes für drei Jahre gültiges Zertifikat auszugeben und gegebenenfalls zur Führung eines Datenschutzsiegels oder -prüfzeichens zu ermächtigen.

## Laufende Überwachung und Rezertifizierung

Mit erhaltener Zertifizierung heißt es nicht, sich in den kommenden drei Jahren ausruhen zu können. Es ist während des Zertifizierungszyklus ein **Überwachungsaudit** durchzuführen. Über die Frequenz und inhaltliche Tiefe dieses Verfahrens schweigt der Verordnungsentwurf.

Kommt während des Überwachungsaudits hervor, dass die Zertifizierungskriterien nicht vollständig eingehalten werden können, so hat die Zertifizierungsstelle die Anwendung des Zertifikats und der Datenschutzsiegel oder -prüfzeichen einzuschränken, auszusetzen oder zu beenden.[49, 50] Dem Zertifizierungsinhaber ist die **Möglichkeit zur Verbesserung** binnen gesetzter Frist zu geben.[51]

Nach Ablauf des Zertifizierungszyklus muss sich der Zertifizierungsinhaber um eine **Rezertifizierung** bemühen. Diese bedingt das Durchlaufen der kompletten Konformitätsbewertung auf Grundlage der Zertifizierungsanforderungen.

## Fazit

Der Entwurf für die ZeStAkk-V ist ein gelungener Startschuss für die in der Datenschutzbranche herbeigesehnte Möglichkeit zur datenschutzrechtlichen Zertifizierung nach DSGVO. Sie gibt einen guten ersten Einblick in die zu erwartenden Anforderungen an Zertifizierungsstellen und die Erlangung von Zertifizierungen und deren Aufrechterhaltung. **Keine Vorgaben** enthält sie jedoch für Zertifizierungskriterien, also jene Kriterien, anhand derer eine Zertifizierung durchführt wird.[52]

Vor dem Hintergrund der auch infolge der zahlreichen Bezugnahmen auf die Anforderungen nach ISO EN ISO/IEC 17065:2012 und der wohl auch damit in Zusammenhang stehenden, reservierten Haltung der Verordnungsgeber gegenüber der **Zertifizierung** von **Datenschutz-Management-Systemen** wird sich erst zeigen, ob nach dem nunmehr erfolgten Startschuss die DSGVO-Datenschutzzertifikate schnell Fahrt aufnehmen und entspechende Zertifikate bei Verantwortlichen und Auftragsverarbeitern weite Verbreitung und Anwendung werden finden können.

Dako 2020/32

[37] § 6 Abs 5 ZeStAkk-V. [38] § 6 Abs 6 ZeStAkk-V. [39] Erläut ZeStAkk-V, 4. [40] § 4 Abs 6 ZeStAkk-V. [41] Art 9 Abs 1 DSGVO. [42] § 4 Abs 6 ZeStAkk-V. [43] *Europäischer Datenschutzausschuss*, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation Rz 18. [44] Erläut ZeStAkk-V 1. [45] Erläut ZeStAkk-V 4. [46] Zu den Anforderungen an externe Sachverständige siehe § 11 Abs 4 ZeStAkk-V. [47] EN ISO/IEC 17065:2012, 3.3. [48] § 8 Abs 1 Z 3 ZeStAkk-V. [49] EN ISO/IEC 17065:2012, 7.11.1. [50] Art 42 Abs 7 DSGVO. [51] § 8 Abs 5 ZeStAkk-V. [52] § 2 Z 3 ZeStAkk-V.

## Zum Thema

### Über die Autoren

**Dr. Gerald Trieb, LL.M, ist Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte.**
**E-Mail: gt@kt.at**
**Mag. Maximilian Kröpfl ist Rechtsanwaltsanwärter bei Knyrim Trieb Rechtsanwälte.**
**E-Mail: mk@kt.at**