

1


KT | KNYRIM.TRIEB
RECHTSANWÄLTE

DSGVO-Zertifizierung
IT-Rechtstag 2020

Dr. Rainer Knyrim

Rechtsanwalt und Partner
Knyrim Trieb Rechtsanwälte OG

2


 | **KNYRIM.TRIEB**
RECHTSANWÄLTE

Inhalt

1. Definition und Vorteile einer DSGVO-Zertifizierung, Abgrenzung
2. Das DSGVO-Zertifizierungssystem
3. Die Zertifizierungsstellen-Akkreditierungs-VO
4. Usecase: Ihr Weg zum Datenschutzzertifikat
5. Ein Blick in die Zukunft: Wie geht es weiter?

www.kt.at 3

3

 | **KNYRIM.TRIEB**
RECHTSANWÄLTE

ISO | EuroPriSe | TÜV | IAPP | DSGVO-Zertifizierung

DATENSCHUTZZERTIFIKATE

www.kt.at 4

4

Notwendigkeit einer Abgrenzung

PRIVATE ZERTIFIKATE



- keine Beschränkung des Zertifizierungsgegenstandes
- keine Prüfung der Kriterien
- (oft) keine Akkreditierung der Zertifizierungsstellen
- **kein Nachweis nach DSGVO**

DSGVO-ZERTIFIKATE

- Nur Verarbeitungsvorgänge
- Produkte und Dienstleistungen nur mittelbar
- Genehmigung der Kriterien → Bindungswirkung der Behörde
- Akkreditierung der Zertifizierungsstellen
- **Nachweis nach DSGVO**
- Aufsicht durch die DSB

5

ZERTIFIZIERUNG - WOZU?

6

Wirkung datenschutzrechtlicher Zertifizierung

- Art **24** Abs 3 DSGVO – **Verantwortlichkeit**
- Art **32** Abs 3 DSGVO – **TOMs**
- Art **46** Abs 3 DSGVO – geeignete Garantien für den **Datentransfer**
- Art **83** Abs 2 DSGVO – gebührende Berücksichtigung bei **Geldbußen**
- **Wettbewerbsvorteil** und **Kosteneffizienz**

7

Zertifizierungsgegenstand



VERARBEITUNGSTÄTIGKEITEN



COOKIES



CLOUD



WEBSHOP

8

KT | **KNYRIM.TRIEB**
RECHTSANWÄLTE

**KEINE
DSGVO-ZERTIFIZIERUNG
VON PROZESSEN
(ARBEITSABLÄUFE)**

www.kt.at

9

9

KT | **KNYRIM.TRIEB**
RECHTSANWÄLTE

Entwurf einer Verordnung der Datenschutzbehörde über die
Anforderungen an die Akkreditierung einer Zertifizierungsstelle

ZESTAKK-V

www.kt.at

10

10

Das DSGVO-Zertifizierungssystem

- Zertifizierungskriterien
- Inhaber von Zertifizierungskriterien (Programmeigner)
- Zertifizierungsstelle
- Zertifizierungsanforderungen
- Zertifizierungswerber
- Zertifizierungsinhaber
- Zertifikat, Siegel, Prüfzeichen
- Zertifizierungsprogramm

11

Inhalt der Zertifizierungsstellen-Akkreditierungs-Verordnung

§ 1	Allgemeine Bestimmungen	§ 11	Evaluierung
§ 2	Begriffsbestimmungen	§ 12	Bewertung
§ 3	Akkreditierung	§ 13	Zertifizierungsentscheidung
§ 4	Akkreditierungsverfahren	§ 14	Konformitätszeichen
§ 5	Unabhängigkeit	§ 15	Zertifizierungsverzeichnis
§ 6	Fachwissen	§ 16	Überwachungsverfahren und Aufzeichnungen
§ 7	Organisationsstruktur, Interessenkonflikte, Vertraulichkeit	§ 17	Beendigung, Einschränkung, Aussetzung, Widerruf
§ 8	Zertifizierungsverfahren	§ 18	Beschwerdeverfahren
§ 9	Zertifizierungsvereinbarung	§ 19	Anforderungen an ein Managementsystem
§ 10	Änderung von Zertifizierungsanforderungen		

12

KT | **KNYRIM.TRIEB**
RECHTSANWÄLTE

Funktionsweise und Zusammenspiel
ECOSYSTEM

www.kt.at13

13

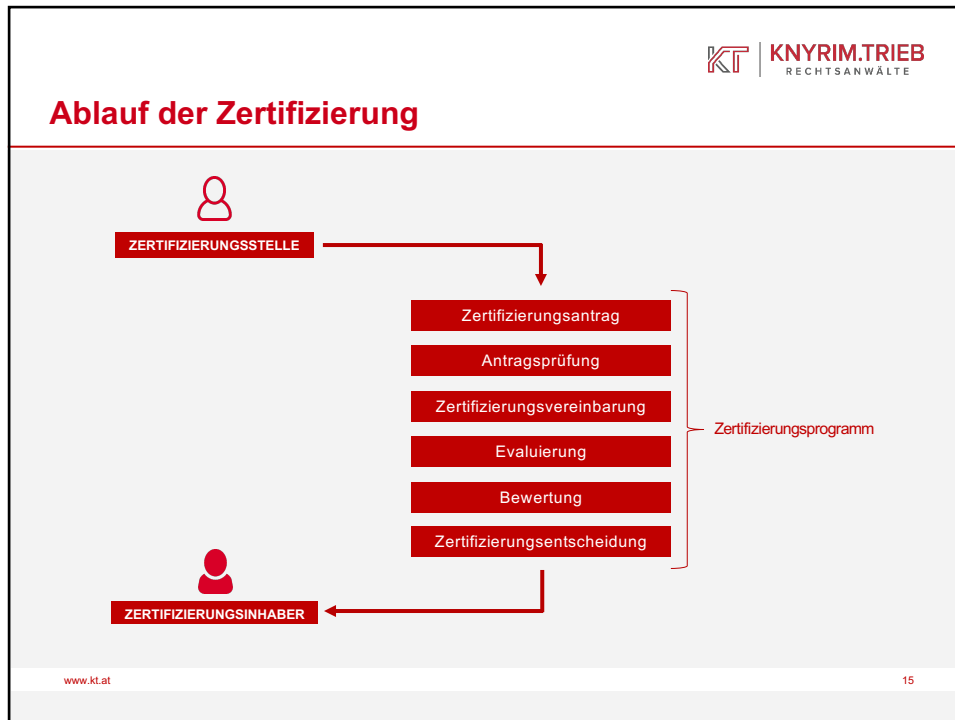
KT | **KNYRIM.TRIEB**
RECHTSANWÄLTE

Ecosystem DSGVO-Zertifizierung

```
graph TD; dsb((dsb)) -- Akkreditierung --> ZP[Zertifizierungsprogramm]; ZP --> ZS[Zertifizierungsstelle]; ZS -- Lizenzvertrag --> ZK[Zertifizierungskriterien]; ZK -- Genehmigung --> dsb; ZS <--> |Zertifizierung| ZW[Zertifizierungswerber];
```

www.kt.at14

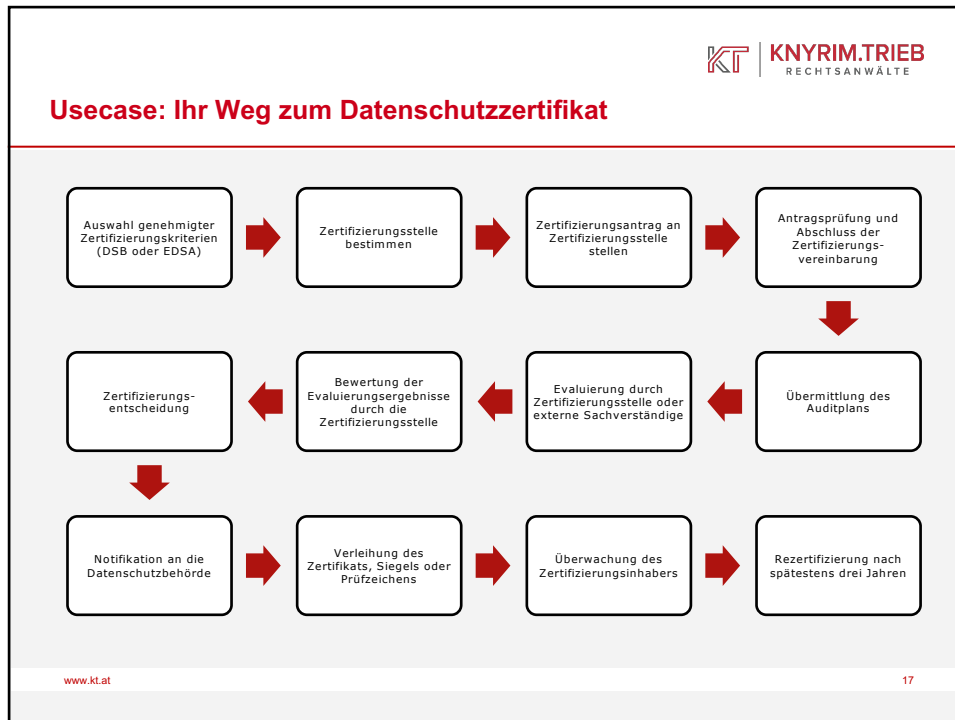
14



15



16



17


KT | **KNYRIM.TRIEB**
RECHTSANWÄLTE

DAS ECOSYSTEM DER DSGVO-ZERTIFIZIERUNG BIETET FÜR JEDEN DIE RICHTIGE ROLLE. WO SEHEN SIE SICH?

www.kt.at

18

18



Weiterführende Literatur

Gerald Trieb/Maximilian Kröpfl
Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte/Rechtsanwältin ebendorf

DSGVO-Datenschutzzertifikate in greifbarer Nähe?

Eine Besprechung des Entwurfs der Zertifizierungsstellen-Akkreditierungs-VO. Datenschutz-zertifizierung 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 ausgedent.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.

<p>Ecosystem datenschutzrechtlicher Zertifizierung</p> <p>Um die Transparenz zu erhöhen und die Einhaltung der DSGVO zu verbessern, sollen nach der europäischen Vorstellung von Eigenverantwortung und Rechenschaftspflicht Zertifizierungsverfahren sowie Datenschutzniveaus und Prüfverfahren eingeführt werden. Diese sollen betroffenen Personen, der Öffentlichkeit und Marktteilnehmern einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.⁴</p> <p>Den Rahmen datenschutzrechtlicher Zertifizierung bilden Art 42 und 43 DSGVO. Während Art 42 Zertifizierungskriterien und den Zertifizierungszeitraum</p>	<p>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 27001:2017 heran, obwohl § 21 Abs 3 DSG⁵ 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; in unserem Fall die Datenverarbeitung, die auch immer Gegenstand einer Zertifizierung ist.⁶ Dennoch nimmt die DSB in Verordnungsentwurf an zahlreichen Stellen auf diese</p>	<p>ISO-Norm Bezug und regelt in zusätzlicher Spezifikation⁷ der schon recht umfangreichen Anforderungen dieser Norm mit der ZeStAkk-V weitere, entsprechende Anforderungen an datenschutzrechtliche Zertifizierungsstellen. Eine Zertifizierung eines Verantwortlichen oder Auftragsverarbeiter</p> <p style="font-size: x-small; margin-top: 10px;">¹Entwurf einer Verordnung über die Anforderungen an die Akkreditierung einer zertifizierungsstellen, (http://dsb.dsb-nz.at/wordpress/wp-content/uploads/2019/04/20190420-ZeStAkk-V-Entwurf.pdf) (Stand: 20. April 2019). ²Entwurf, Art 13 Abs 1 lit b DSGVO) hat die DSB im Rahmen der Aufarbeitung der ZeStAkk-V und Veröffentlichung der Akkreditierungsstellen für zertifizierte Organisationen veröffentlicht, gem § 21 Abs 1 DSG. Diese auch national verbindliche, Art 43 Abs 1 DSGVO, durch die Produkte, Prozesse und Dienstleistungen zertifizieren (DSB) (http://dsb.dsb-nz.at/wordpress/wp-content/uploads/2019/04/20190420-ZeStAkk-V-Entwurf.pdf) (Stand: 20. April 2019). ³Die DSB hat im Rahmen der Aufarbeitung der ZeStAkk-V und Veröffentlichung der Akkreditierungsstellen für zertifizierte Organisationen veröffentlicht, gem § 21 Abs 1 DSG. Diese auch national verbindliche, Art 43 Abs 1 DSGVO, durch die Produkte, Prozesse und Dienstleistungen zertifizieren (DSB) (http://dsb.dsb-nz.at/wordpress/wp-content/uploads/2019/04/20190420-ZeStAkk-V-Entwurf.pdf) (Stand: 20. April 2019).</p>
---	--	--

www.kt.at 52 Doko 3 | 2020 MANZ 19

19



Weiterführende Literatur



Strohmaier in Knyrim, DatKomm – Aktualisierung erscheint Anfang 2021

www.kt.at 20

20

RA Dr. Rainer Knyrim

Knyrim Trieb Rechtsanwälte OG
1060 Wien, Mariahilfer Straße 89A
Tel. +43/1/9093070, E-Mail: kt@kt.at; www.kt.at