Republik Österreich
Datenschutzbehörde

Zertifizierungen gemäß DSGVO

Dr. Matthias Schmidl
Stv. Leiter der Österreichischen Datenschutzbehörde

Grundlagen für Zertifizierungen DSGVO

dsb
Republik Österreich
Datenschutz behörde

DSGVO	Inhalt/Vorgabe
Art. 42	Zertifizierung
Art. 43	Zertifizierungsstellen
Art. 57 Abs. 1 lit. n bis q	Aufgaben der Aufsichtsbehörden
Art. 58 Abs. 2 lit. h und Abs. 3 lit. e und f	Befugnisse der Aufsichtsbehörden
Art. 70 Abs. 1 lit. e	Aufgaben des EDSA (Leitlinien)

Sonstige Grundlagen

- **Leitlinien 1/2018** (des EDSA) betreffend Zertifizierungen und Zertifizierungskriterien gemäß Art. 42 und 43 DSGVO (dzt. nur auf Englisch verfügbar)
- **Leitlinien 4/2018** (des EDSA) betreffend die Akkreditierung von Zertifizierungsstellen gemäß Art. 43 DSGVO (dzt. nur auf Englisch verfügbar)
- (künftige) **Verordnung der Datenschutzbehörde** über die Akkreditierung von Zertifizierungsstellen (ZeStAkk-V)

Was ist eine Zertifizierung? - 1

- Art. 42 Abs. 1 DSGVO:

Verfahren**, die dazu dienen, **nachzuweisen**, dass die **DSGVO** bei **Verarbeitungsvorgängen** von **Verantwortlichen** und **Auftragsverarbeitern eingehalten wird

- Es wird auf die gesamte DSGVO abgestellt und nicht bloß auf Teilaspekte
- Aber: Keine Definition von „Zertifizierung“

Was ist eine Zertifizierung? - 2

- Definition gemäß International Standards Organisation (ISO):

*Die Ausstellung einer **schriftlichen Bestätigung** einer **unabhängigen Stelle**, dass das betreffende Produkt, Service oder System bestimmten Anforderungen entspricht.*

Was ist eine Zertifizierung? - 3

- Zertifizierung = widerlegbare Vermutung, dass Vorgaben der DSGVO eingehalten werden
- Zertifizierung = Konformitätsbescheinigung, die von einer unabhängigen Stelle nach Durchführung eines festgelegten Verfahrens ausgestellt wird
- Zertifizierung = Nachweis ≠ Beweis
- Art. 83 Abs. 2 lit. j DSGVO: Berücksichtigung bei der Bemessung von Geldbußen
- **Fokus**: Schutz von Grundrechten von Personen (und nicht bloß Datensicherheit)

Was kann zertifiziert werden?

- Gegenstand einer Zertifizierung wird durch Art. 42 Abs. 1 DSGVO festgelegt: „**Verarbeitungsvorgänge** von **Verantwortlichen und Auftragsverarbeitern**“
- Fokus: Nachweis der Übereinstimmung mit der **DSGVO:**

a) Vorliegen personenbezogener Daten

b) technische Systeme zur Verarbeitung

c) Hintergrundabläufe von Verarbeitungsvorgängen

- Datenschutzbeauftragte bzw. ganze Unternehmen können daher nicht gemäß DSGVO zertifiziert werden!
- Zertifizierungen werden nur **temporär** (3 Jahre) erteilt

Wer nimmt eine Zertifizierung vor? - 1

- „unabhängige Stelle“ (gemäß ISO-Definition)
- Art. 42 Abs. 5: (Datenschutz-)Aufsichtsbehörde
- Art. 43 Abs. 1 DSGVO: **Zertifizierungsstellen**
- Akkreditierung durch:

a) (Datenschutz-)Aufsichtsbehörden oder

b) Nationale Akkreditierungsstelle gemäß VO (EG) Nr. 765/2008

- **Österreich**: Akkreditierung erfolgt nur durch Datenschutzbehörde (§ 21 Abs. 3 DSG)
- Zertifizierung wird aufgrund von Kriterien erteilt, die von Aufsichtsbehörde(n) oder dem EDSA genehmigt wurden; EDSA: Europäisches Datenschutzsiegel

Wer nimmt eine Zertifizierung vor? - 2

- Akkreditierung einer Zertifizierungsstelle erfolgt durch DSB; Akkreditierungsdauer: max. 5 Jahre
- Zertifizierungsstelle muss Nachweis erbringen, dass die Vorgaben des Art. 43 Abs. 2 DSGVO eingehalten werden
- Nähere Präzisierung erfolgt durch ZeStAkk-V der DSB
- Grundlage: **ISO 17065/2012** (siehe auch LL 4/2018)

Rolle des Aufsichtsbehörden

- Aufsichtsbehörden können selbst zertifizieren (Art. 42 Abs. 5 DSGVO)→ **gilt nicht für Österreich**
- Akkreditierung von Zertifizierungsstellen bzw. Widerruf einer Akkreditierung
- Genehmigung von Zertifizierungskriterien
- Anweisung an Zertifizierungsstellen, Zertifizierungen zu widerrufen bzw. keine Zertifizierungen zu erteilen
- Verhängung von Geldbußen gegen Zertifizierungsstellen, wenn Pflichten nicht eingehalten werden

Vorteile einer Zertifizierung

- Anscheinsbeweis, dass DSGVO eingehalten wird → Publizitätswirkung
- Kann in Verwaltungsstrafverfahren mildernd berücksichtigt werden
- Vorteil bei internationalem Datentransfer (Art. 46 Abs. 2 lit. f DSGVO)

Weiterführende Informationen

- Website der DSB: www.dsb.gv.at
- Website des EDSA: https://edpb.europa.eu/
- Newsletter der DSB: erscheint vierteljährlich und kann unter dsb@dsb.gv.at bestellt werden
- Leitlinien zur DSGVO: Abrufbar auf der Website der Art. 29-Gruppe (erreichbar über DSB-Website bzw. EDSA-Website)

Literatur und weiterführende Informationen zu Zertifizierungen

- *Kröpfl,* Datenschutzrechtliche Zertifizierungen, in *Jahnel (Hrsg.),* Datenschutzrecht. Jahrbuch 19 (2019), 163 ff
- *Strohmaier*, Vom zertifiziert richtigen Verhalten, in *Knyrim* (Hrsg.), Datenschutz-Grundverordnung (2016), 247 ff

Literatur und weiterführende Informationen zur DSGVO

dsb
Republik Österreich
Datenschutz behörde

Stand: Oktober 2018 (alphabetische, nicht vollständige Aufzählung):

- *Ehmann/Selmayr,* Datenschutz-Grundverordnung (Kommentar)
- *Feiler/Forgó*, EU-Datenschutz-Grundverordnung (Kommentar)
- *Gantschacher/Jelinek/Schmidl/Spanberger* (Hrsg.), Kommentar zur Datenschutz-Grundverordnung
- *Gola* (Hrsg.), Datenschutz-Grundverordnung (Kommentar)
- *Kühling/Buchner* (Hrsg.), Datenschutz-Grundverordnung (Kommentar)
- *Knyrim* (Hrsg.), Datenschutz-Grundverordnung (Praxishandbuch)
- *Paal/Pauly* (Hrsg.), Datenschutz-Grundverordnung (Kommentar)
- *Pollirer/Weiss/Knyrim/Haidinger*, DSGVO (Textausgabe)
- *Sydow* (Hrsg.), Europäische Datenschutzgrundverordnung (Kommentar)

Literatur und weiterführende Informationen zum DSG

dsb
Republik Österreich
Datenschutz behörde

Stand: Oktober 2018 (alphabetische, nicht vollständige Aufzählung):

- *Bergauer/Jahnel,* DSGVO und DSG (Textausgabe)
- *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl,* DSG (Kommentar)
- *Jelinek/Schmidl/Spanberger,* Datenschutzgesetz (Kommentar)
- *Knyrim*, DatKomm
- *Pollirer/Weiss/Knyrim/Haidinger*, DSG (Textausgabe mit Erläuterungen)

Republik Österreich
Datenschutzbehörde

Danke für Ihre Aufmerksamkeit!