



Aktiv voran: Neue Möglichkeiten der Zertifizierung für Unternehmen und Verwaltung durch die DSGVO: Teil 2

Sebastian Meissner,
Head of EuroPriSe Certification Authority, EuroPriSe GmbH
Sommerakademie am 18.09.2017 in Kiel



Kurze Vorstellung von EuroPriSe

S. 2 Aktiv voran: Neue Möglichkeiten der Zertifizierung für Unternehmen und Verwaltung durch die DSGVO

2016: EU-DSGVO tritt in Kraft: Erstmals EU-Regelungen zu DS-Zertifizierungen (inkl. Möglichkeit eines Europäischen Datenschutzsiegels)

25. Mai 2018:

EU-DSGVO gilt unmittelbar: EuroPriSe strebt EU-weit gültige Akkreditierung als Zert.stelle für ein Europäisches DS-Siegel an

2014: Betreiberwechsel: ULD → EuroPriSe GmbH
Advisory Board mit DS-Experten aus diversen EU-Staaten

2009 - 2013: ULD betreibt EuroPriSe und agiert als Zertifizierungsstelle

2007 - 2009: EuroPriSe startet als von der EU-Kommission mit 1.3 Mio. Euro gefördertes Projekt mit DS-Aufsichtsbehörden aus DE (ULD), FR (CNIL) und ES (APDCM): Spezifizierung von Zertifizierungskriterien & Verfahren → Pilotzertifizierungen

Juni 2017: 10. Geburtstag des European Privacy Seals

Zertifizierung: Die europäische Perspektive

S. 3 Aktiv voran: Neue Möglichkeiten der Zertifizierung für Unternehmen und Verwaltung durch die DSGVO

Was sagt die DSGVO hierzu?

-  Artikel 42 Abs. 1 DSGVO:
Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern **insbesondere auf Unionsebene** die Einführung von datenschutzspezifischen Zertifizierungsverfahren [...].
-  Artikel 42 Abs. 5 DSGVO:
Eine Zertifizierung [...] wird [...] anhand der durch die zuständige Aufsichtsbehörde [...] oder [...] **durch den Ausschuss** genehmigten Kriterien erteilt. Werden die Kriterien vom Ausschuss genehmigt, kann dies zu einer gemeinsamen Zertifizierung, dem **Europäischen Datenschutzsiegel**, führen.

Zertifizierung: Die europäische Perspektive

S. 4 Aktiv voran: Neue Möglichkeiten der Zertifizierung für Unternehmen und Verwaltung durch die DSGVO

Was sagt die DSGVO hierzu?

-  Artikel 43 Abs. 3 S. 1 DSGVO:
Die **Akkreditierung von Zertifizierungsstellen** [...] erfolgt anhand der Kriterien, die von der [...] zuständigen Aufsichtsbehörde oder [...] von dem **Ausschuss** genehmigt wurden.
-  Artikel 70 Abs. 1 S. 2 lit. o) DSGVO:
Hierzu nimmt der **Ausschuss** von sich aus oder gegebenenfalls auf Ersuchen der Kommission insbesondere folgende Tätigkeiten wahr:
Akkreditierung von Zertifizierungsstellen und deren regelmäßige Überprüfung gemäß Artikel 43 [...].

Zertifizierung: Die europäische Perspektive

S. 5 Aktiv voran: Neue Möglichkeiten der Zertifizierung für Unternehmen und Verwaltung durch die DSGVO

- 🕒 **Warum ist ein europäischer Ansatz wichtig?**
 - 🕒 Gerade wenn Zertifizierungen überwiegend von privaten Zertifizierungsstellen erteilt werden sollten - wofür vieles spricht -, ist ein europäischer Ansatz besonders wichtig.
 - 🕒 Anderenfalls droht folgendes Worst-Case-Szenario:
 - 🕒 Herausbildung einer Vielzahl von Siegeln unterschiedlicher Qualität in den einzelnen Mitgliedstaaten der EU;
 - 🕒 Abwärtsspirale in Sachen Kosten und Qualität;
 - 🕒 Nachhaltige Beschädigung der Glaubwürdigkeit von Datenschutzzertifizierungen insgesamt.
 - 🕒 Europäischer Ansatz = Grundidee der Verordnung:
„Die Vorschriften zum Schutz [...] von natürlichen Personen bei der Verarbeitung pb. Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden“ (Erwägungsgrund 10 Abs. 2 DSGVO).

Zertifizierung: Die europäische Perspektive

S. 6 Aktiv voran: Neue Möglichkeiten der Zertifizierung für Unternehmen und Verwaltung durch die DSGVO

- 📌 Für welche Zertifizierungskunden ist ein europäischer Ansatz (besonders) wichtig?
 - 📌 Letztlich profitiert jede Organisation, die ein Datenschutzsiegel erwirbt, davon, wenn dieses nicht nur in einem Land, sondern überall in der EU eingesetzt werden kann / gültig ist.
 - 📌 Besonders wichtig ist dieser Aspekt aber für folgende Organisationen, die ein Siegel erwerben wollen:
 - 📌 Unternehmen mit Niederlassungen in mehr als einem Mitgliedstaat der EU;
 - 📌 Unternehmen, die personenbezogene Daten im Auftrag ihrer Kunden verarbeiten, und deren Kunden aus mehr als einem Mitgliedstaat der EU stammen.

DSGVO: Ziele und bisherige / geplante Aktivitäten von EuroPriSe

S. 7 Aktiv voran: Neue Möglichkeiten der Zertifizierung für Unternehmen und Verwaltung durch die DSGVO

- 🕒 Welche Ziele verfolgt EuroPriSe vor dem Hintergrund des Art. 42 f. DSGVO?
 - ✅ Erwerb einer EU-weit gültigen Akkreditierung zum frühestmöglichen Zeitpunkt, wobei die Erteilung der Akkreditierung vorzugsweise durch den Europäischen Datenschutzausschuss erfolgen soll;
 - ✅ Genehmigung der aktuellen Version des EuroPriSe-Kriterienkatalogs für IT-Produkte und IT-basierte Dienstleistungen durch den Ausschuss zum frühestmöglichen Zeitpunkt;
 - ✅ Summa summarum: EuroPriSe möchte möglichst bald als eine EU-weit anerkannte Zertifizierungsstelle für ein Europäisches Datenschutzsiegel tätig werden.

- 🕒 Welche Ziele verfolgt EuroPriSe vor dem Hintergrund des Art. 42 f. DSGVO?
 - ✅ EuroPriSe setzt auch weiterhin auf die Zertifizierung von IT-Produkten und IT-basierten Dienstleistungen.
 - ✅ Explizite Erwähnung von Produkten und Dienstleistungen in Erwägungsgrund 100 DSGVO: Einführung von Zertifizierungsverfahren, „die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte + Dienstleistungen ermöglichen“.
 - ✅ Eine auf bestimmte Technologien (Cloud, Mobile Apps) oder Branchen (Telekommunikation, Gesundheit) zugeschnittene Zertifizierung erscheint als weniger sinnvoll, da es in der Praxis regelmäßig zu Überlappungen zwischen diesen Technologien und Branchen kommt.

DSGVO: Ziele und bisherige / geplante Aktivitäten von EuroPriSe

S. 9 Aktiv voran: Neue Möglichkeiten der Zertifizierung für Unternehmen und Verwaltung durch die DSGVO

- 📌 Was hat EuroPriSe bisher getan, um sich auf Art. 42 f. DSGVO vorzubereiten?
 - 📌 Seit Inkrafttreten der DSGVO: **Dialog mit wichtigen Stakeholdern** (z.B. EU-Kommission, WP29, LDI NRW als für die EuroPriSe GmbH zuständige Aufsichtsbehörde + ULD).
 - 📌 Juli 2016: EuroPriSe moderiert den Workshop zum Thema **Zertifizierung** beim ersten **FabLab** der **Art. 29-Gruppe** (WP29) zur DSGVO in Brüssel.

Aufbauend auf den Ergebnissen dieses Workshops erarbeitet die WP29 zur Zeit **Guidelines zum Thema Zertifizierung / Akkreditierung**, die noch in 2017 veröffentlicht werden sollen.

DSGVO: Ziele und bisherige / geplante Aktivitäten von EuroPriSe

S. 10 Aktiv voran: Neue Möglichkeiten der Zertifizierung für Unternehmen und Verwaltung durch die DSGVO

📌 Was hat EuroPriSe bisher getan, um sich auf Art. 42 f. DSGVO vorzubereiten?

📌 Dezember 2016: Fertigstellung einer neuen Version des Kriterienkatalogs für Produkte und Dienstleistungen („GDPR ready“).

Der neue Katalog wurde kurz darauf in einer Sitzung des EuroPriSe Advisory Boards diskutiert. Im Nachgang zu dieser Sitzung wurde das Dokument noch einmal ergänzt.

Die finale Version des Katalogs wurde noch in 2016 veröffentlicht und kommt seit Januar 2017 zum Einsatz.

Eine neue Version des Kommentars für EuroPriSe-Gutachter wurde im Mai 2017 fertiggestellt.

DSGVO: Ziele und bisherige / geplante Aktivitäten von EuroPriSe

S. 11 Aktiv voran: Neue Möglichkeiten der Zertifizierung für Unternehmen und Verwaltung durch die DSGVO



Kriterienkatalog: Was ist neu?

- Zusätzliche Kriterien wegen neuer rechtlicher Anforderungen eingefügt (z. B. Datenschutz-Folgenabschätzung und Recht auf Datenübertragbarkeit,)
- Änderung bestehender Kriterien wegen geänderter rechtlicher Anforderungen (z. B. Inhalt von ADV-Verträgen und erweiterte Informationspflichten).
- Streichung bisheriger Kriterien mangels Fortbestehen der zugrunde liegenden rechtlichen Anforderungen (z. B. Meldepflicht und Vorabkontrolle).
- Fragen sind jetzt zugeschnitten auf
 - IT-Produkte
 - Dienste von Auftragsverarbeitern
 - Dienste von Verantwortlichen

DSGVO: Ziele und bisherige / geplante Aktivitäten von EuroPriSe

S. 12 Aktiv voran: Neue Möglichkeiten der Zertifizierung für Unternehmen und Verwaltung durch die DSGVO

- 🕒 Was hat EuroPriSe bisher getan, um sich auf Art. 42 f. DSGVO vorzubereiten?
 - 🕒 Weitere Aktivitäten:
 - 🕒 WP29 über Technology Subgroup angefragt bzgl. Akkreditierung von EuroPriSe durch den künftigen Europäischen Datenschutzausschuss.
 - 🕒 WP29 über Technology Subgroup angefragt bzgl. Genehmigung der EuroPriSe-Kriterien für Produkte und Dienstleistungen durch den Ausschuss.
 - 🕒 Anpassung bestehender Prozesse, Verträge etc. an die Vorgaben von ISO/IEC 17065 (Anforderungen an Zertifizierungsstellen für Produkte, Prozesse + Dienste).
 - 🕒 Intensivierung von Public Relations-Aktivitäten (Vorträge im In- und Ausland etc.).

DSGVO: Ziele und bisherige / geplante Aktivitäten von EuroPriSe

S. 13 Aktiv voran: Neue Möglichkeiten der Zertifizierung für Unternehmen und Verwaltung durch die DSGVO

- 🕒 Welche weiteren Aktivitäten plant EuroPriSe, um sich auf Art. 42 f. DSGVO vorzubereiten?
 - 🕒 Formale Anfrage über die gegenwärtige Präsidentschaft (CNIL) bei WP29 bzgl. Akkreditierung von EuroPriSe durch den künftigen Europäischen Datenschutzausschuss.

Start mit den weiteren Vorbereitungen auf eine solche Akkreditierung, sobald (positives) Feedback von WP29.
 - 🕒 Formale Anfrage über die gegenwärtige Präsidentschaft (CNIL) bei WP29 bzgl. Genehmigung der EuroPriSe-Kriterien für Produkte und Dienstleistungen durch den Ausschuss.
 - 🕒 Ggf. Akkreditierung für DE in einem ersten Schritt (sobald möglich).
 - 🕒 Ggf. Workshops / Pilotverfahren mit interessierten Datenschutzaufsichtsbehörden.

Vielen Dank für Ihre Aufmerksamkeit!

Fragen beantworte ich gerne sofort oder im Nachgang zu dieser Veranstaltung.

Sie können mich erreichen unter:

EuroPriSe GmbH

Sebastian Meissner

Head of EuroPriSe Certification Authority

Joseph-Schumpeter-Allee 25

D-53227 Bonn

Tel: +49 228 763 679 - 30

Email: ca@european-privacy-seal.eu