Neue Möglichkeiten der Zertifizierung durch die DSGVO

Sebastian Meissner,
Head of EuroPriSe Certification Authority, EuroPriSe GmbH

ZertiVer 2017 – 5. Dezember 2017, art'otel Köln

Kurze Vorstellung von EuroPriSe

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

2009 – 2013: ULD betreibt EuroPriSe und agiert als Zertifizierungsstelle

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

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

Juni 2017: 10. Geburtstag des European Privacy Seals

Die relevanten §§ im Überblick

- Förderung von Zertifizierungsverfahren
  - Artikel 42 Abs. 1 S. 1 DSGVO:
    Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission ***fördern*** die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen.
- Nachweis von DSGVO-Compliance
  - Artikel 42 Abs. 1 S. 1 DSGVO:
    Gefördert werden Zertifizierungsverfahren, die dazu dienen, nachzuweisen, dass die ***DSGVO*** bei Verarbeitungsvorgängen ***eingehalten*** wird.
  - Noch ungeklärt: Relevanz nationalen Rechts, erlassen auf Grundlage von ***Öffnungsklauseln*** (z. B. Art. 88 DSGVO).

Die relevanten §§ im Überblick

- Wer kann ein Zertifikat erhalten?
  - Artikel 42 Abs. 1 S. 1 DSGVO:
    Gegenstand einer Zertifizierung können Verarbeitungsvorgänge von ***Verantwortlichen*** und von ***Auftragsverarbeitern*** sein.
- Ist eine Zertifizierung verpflichtend?
  - Artikel 42 Abs. 3 DSGVO:
    Die Zertifizierung muss ***freiwillig zugänglich*** sein.
- Macht Zertifizierung für KMUs Sinn?
  - Artikel 42 Abs. 1 S. 2 DSGVO:
    Den besonderen ***Bedürfnissen von*** Kleinstunternehmen sowie ***KMU wird Rechnung getragen***.

Die relevanten §§ im Überblick

- Was kann zertifiziert werden?
  - Artikel 42 Abs. 1 S. 1 DSGVO:
    Verarbeitungsvorgänge von Verantwortlichen und von Auftragsverarbeitern.
  - Erwägungsgrund 100:
    Den betroffenen Personen soll ein rascher Überblick über das Datenschutzniveau einschlägiger ***Produkte und Dienstleistungen*** ermöglicht werden.
  - Was heißt das nun konkret für die Zertifizierbarkeit (gem. Art. 42 f. DSGVO) von
    - IT-basierten ***Diensten***: (+)
    - IT-***Produkten***: sehr wahrscheinlich (+) wg. EG 100
    - ***Datenschutzmanagementsystemen***: (?) noch nicht geklärt
    - ***Personen*** (insbes. DSBs): (-)

Die relevanten §§ im Überblick

- Wer erteilt die Zertifizierung?
  - Artikel 42 Abs. 5 S. 1 DSGVO:
    Eine (akkreditierte) ***Zertifizierungsstelle oder*** die ***zuständige Aufsichtsbehörde***.
- Wer akkreditiert die Zertifizierungsstellen?
  - Artikel 43 Abs. 1 S. 2 DSGVO:
    Die Mitgliedstaaten stellen sicher, dass diese Zertifizierungsstellen akkreditiert werden von:
    - der ***zuständige***n ***Aufsichtsbehörde***; ***und/oder***
    - der ***nationale***n ***Akkreditierungsstelle***
  - ***§ 39 BDSG n.F.***: Erteilung der Befugnis durch die zuständige Aufsichtsbehörde auf der Grundlage einer Akkreditierung durch die DAkkS (→ AG Zertifizierung)

Die relevanten §§ im Überblick

- Wer kann akkreditiert werden?
  - Artikel 43 Abs. 2 DSGVO:
    Zertifizierungsstellen dürfen nur dann akkreditiert werden, wenn sie
    - ihre ***Unabhängigkeit und*** ihr ***Fachwissen*** hinsichtlich des Gegenstands der Zertifizierung nachgewiesen haben;
    - sich verpflichtet haben, die (genehmigten) ***Kriterien einzuhalten***;
    - ***Verfahren für*** die ***Erteilung***, die regelmäßige ***Überprüfung und*** den ***Widerruf*** der Zertifizierung festgelegt haben;
    - ***Verfahren und Strukturen*** festgelegt und transparent gemacht haben, mit denen sie (zertifizierungsrelevanten) ***Beschwerden*** nachgehen; und
    - nachgewiesen haben, dass ihre Aufgaben und Pflichten ***nicht*** zu einem ***Interessenkonflikt*** führen.

Die relevanten §§ im Überblick

- Nach welchen Kriterien wird zertifiziert?
  - Artikel 42 Abs. 5 S. 1 DSGVO:
    Eine Zertifizierung wird anhand der von der zuständigen Aufsichtsbehörde oder durch den Ausschuss ***genehmigten Kriterien*** erteilt.
  - Konkret sind also zwei Optionen denkbar:
    - Genehmigung von Kriterien, die die zuständige Aufsichtsbehörde bzw. der Ausschuss selbst erarbeitet hat;
    - Genehmigung von Kriterien, die durch andere Stakeholder (z. B. akkreditierte Zertifizierungsstellen) erarbeitet worden sind.
  - Erwägungsgrund 166, S. 2: ***Delegierte Rechtsakte*** sollten [durch die EU-Kommission] insbesondere in Bezug auf die für Zertifizierungsverfahren geltenden Kriterien erlassen werden (vgl. Art. 43 Abs. 8 DSGVO).

Die relevanten §§ im Überblick

- Welches Verfahren ist vorgesehen?
  - Artikel 42 Abs. 3 DSGVO:
    Die Zertifizierung muss über ein ***transparentes Verfahren*** zugänglich sein.
  - Art. 43 Abs. 2 lit. c DSGVO:
    Zu akkreditierende Zertifizierungsstellen müssen ***Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf*** der Zertifizierung festlegen.
  - Art. 43 Abs. 5 DSGVO:
    Die Zertifizierungsstellen ***teilen den*** zuständigen ***Aufsichtsbehörden die Gründe*** für die Erteilung oder den Widerruf der beantragten Zertifizierung ***mit***.

Die relevanten §§ im Überblick

- Welche Mitwirkungspflichten treffen den Antragsteller?
  - Artikel 42 Abs. 6 DSGVO:
    Der Verantwortliche / Auftragsverarbeiter
    - stellt der Zert.stelle bzw. der zuständigen Aufsichtsbehörde ***alle*** für die Durchführung des Zertifizierungsverfahrens ***erforderlichen Informationen*** zur Verfügung ***und***
    - gewährt ihr den in diesem Zusammenhang ***erforderlichen Zugang zu seinen Verarbeitungstätigkeiten***.
  - Relevante ***Dokumentation***:
    Verfahrensverzeichnis, Datenschutzerklärung, PIA, ADV-Verträge, Einwilligungserklärungen etc.
  - Zugang zu Verarbeitungstätigkeiten:
    Ermöglichung einer ***technische***n ***Überprüfung*** (remote und/oder vor Ort („on-site visit“)).

Die relevanten §§ im Überblick

- Wie lange ist eine Zertifizierung gültig?
  - Artikel 42 Abs. 7 S. 1 DSGVO:
    Die Zertifizierung wird für eine ***Höchstdauer von drei Jahren*** erteilt ***und kann verlängert werden***, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden.
  - Artikel 42 Abs. 7 S. 2 DSGVO:
    Die Zertifizierung wird gegebenenfalls durch die Zert.stelle oder die zuständige Aufsichtsbehörde ***widerrufen***, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden.
  - Artikel 58 Abs. 2 lit. h DSGVO:
    Jede Aufsichtsbehörde hat die Befugnis, Zertifizierungen zu widerrufen oder die ***Zert.stelle anzuweisen***, eine ***Zertifizierung zu widerrufen / nicht zu erteilen***.

Die relevanten §§ im Überblick

- Welche Befugnisse hat die Aufsichtsbehörde, wenn Zertifizierungen durch Zert.stellen erteilt werden?
  - Artikel 58 Abs. 2 DSGVO:
    Jede Aufsichtsbehörde hat die Befugnis,
    - lit c: eine ***Überprüfung der*** nach Artikel 42 Absatz 7 ***erteilten Zertifizierungen*** durchzuführen;
    - lit h: Zertifizierungen zu widerrufen oder die ***Zert.stelle anzuweisen, eine Zertifizierung zu widerrufen / nicht zu erteilen,*** wenn die Voraussetzungen nicht (mehr) vorliegen.
  - Erleichtert wird die Ausübung dieser Befugnisse durch die Pflicht der Zert.stellen, den zuständigen Aufsichtsbehörden die Gründe für die Erteilung der beantragten Zertifizierung mitzuteilen.

Die relevanten §§ im Überblick

- Welche Vorteile bringt eine genehmigte Zertifizierung aus rechtlicher Sicht?
  - Ein genehmigtes Zert.verfahren kann als Gesichtspunkt herangezogen werden, um die ***Erfüllung der Pflichten*** des Verantwortlichen/Auftragsverarbeiters ***nachzuweisen***.
  - Dieser Aspekt wird in folgenden §§ der DSGVO adressiert:
    - Artikel 24 Abs. 3 DSGVO
      (Verantwortung des für die Verarbeitung Verantwortlichen)
    - Artikel 25 Abs. 3 DSGVO
      (Datenschutz durch Technikgestaltung / Voreinstellungen)
    - Artikel 28 Abs. 5 DSGVO
      (Auftragsverarbeiter)
    - Artikel 32 Abs. 3 DSGVO
      (Sicherheit der Verabeitung)

Die relevanten §§ im Überblick

- Welche Vorteile bringt eine genehmigte Zertifizierung aus rechtlicher Sicht (Forts.)?
  - Artikel 83 Abs. 2 lit. j DSGVO:
    Bei der ***Entscheidung über*** die Verhängung / Höhe einer ***Geldbuße*** wird Folgendes gebührend berücksichtigt:
    Einhaltung von genehmigten Zert.verfahren nach Art. 42.
  - Erwägungsgrund 78, letzter Satz DSGVO:
    Datenschutz durch Technik/Voreinstellungen sollte **bei öffentlichen Ausschreibungen** Rechnung getragen werden.
  - Artikel 42 Abs. 4 DSGVO:
    Eine ***Zertifizierung mindert nicht die*** Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung und berührt nicht die Aufgaben und ***Befugnisse der Aufsichtsbehörden***.

Die relevanten §§ im Überblick

- Kann eine genehmigte Zertifizierung einen Drittstaatentransfer legitimieren?
  - Artikel 46 Abs. 2 lit. f DSGVO:
    Geeignete Garantien für einen Drittstaatentransfer können in einem genehmigten ***Zertifizierungsmechanismus*** gemäß Artikel 42 ***zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen*** des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland bestehen.
  - Art. 42 Abs. 2 S. 1 DSGVO:
    Nachweis, dass Verantwortliche oder Auftragsverarbeiter, die nicht unter den räumlichen Anwendungsbereich der DSGVO fallen, ***geeignete Garantien*** bzgl. der Übermittlung personenbezogener Daten an Drittländer bieten.

Die europäische Perspektive

- 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.
  - Datenschutzkonferenz im Kurzpapier Nr. 9 zur DSGVO: „Ein Wildwuchs zahlreicher unterschiedlicher Zert.verfahren sollte gerade mit Blick auf ein einheitliches europäisches Datenschutzniveau im Interesse aller Beteiligten vermieden werden.“

Die europäische Perspektive

- Für welche Zertifizierungskunden ist ein europäischer Ansatz (besonders) wichtig?
  - Letztlich profitiert jede Organisation, die ein Zertifikat erwirbt, davon, wenn dieses überall in der EU anerkannt / gültig ist.
  - Besonders wichtig ist dieser Aspekt aber für folgende Organisationen, die ein Siegel erweben 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***.

Die europäische Perspektive

- Was sagt die DSGVO dazu?
  - Artikel 42 Abs. 1 S. 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 von der zuständigen Aufsichtsbehörde oder ***durch den Ausschuss*** genehmigten Kriterien erteilt. Werden die Kriterien vom Ausschuss genehmigt, kann das zu einer gemeinsamen Zertifizierung, dem ***Europäischen Datenschutzsiegel***, führen.

Die europäische Perspektive

- Was sagt die DSGVO dazu (Forts.)?
  - 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 ggf. auf Ersuchen der Kommission insbesondere folgende Tätigkeiten wahr: ***Akkreditierung von Zert.stellen*** und deren regelmäßige Überprüfung gemäß Artikel 43.

    Gegenwärtig ist noch unklar, ob und unter welchen Umständen der Ausschuss selbst akkreditieren wird.

EuroPriSe und 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 (Prio1).
  - **Genehmigung** der aktuellen Version **des EuroPriSe-Kriterienkatalogs** für IT-Produkte und IT-basierte Dienste zum frühestmöglichen Zeitpunkt, vorzugsweise **durch den Europäischen Datenschutzausschuss** (Prio2).
  - Summa summarum: EuroPriSe möchte möglichst bald als eine EU-weit anerkannte **Zertifizierungsstelle für ein Europäisches Datenschutzsiegel** tätig werden.

EuroPriSe und die DSGVO

- Bietet EuroPriSe bereits Zertifizierungen an, die Compliance mit der DSGVO nachweisen?
  - 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.

    WICHTIGE KLARSTELLUNG: Hierbei handelt es sich nicht um ein genehmigtes Zertifizierungsverfahren gem. Art. 42 f. DSGVO – ein solches ist frühestens ab dem 25. Mai 2018 möglich.

EuroPriSe und 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

EuroPriSe und 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***.
  - Formale Anfrage über die gegenwärtige Präsidentschaft (CNIL) bei WP29 bzgl. ***Genehmigung der EuroPriSe-Kriterien*** für Produkte und Dienste ***durch den Ausschuss***.
  - ***Akkreditierung auf nationaler Ebene*** in einem ersten Schritt (sobald möglich).
  - ***Workshops / Pilotverfahren*** mit interessierten Kunden und Datenschutzaufsichtsbehörden sowie Gedankenaustausch mit anderen Zertifizierungsstellen.

Relevante Aktivitäten wichtiger Stakeholder

- Was machen WP29, KOM, DAkkS et al.?
  - Die deutschen Aufsichtsbehörden diskutieren in der ***„AG Zertifizierung“*** zusammen mit der DAkkS über die künftigen Modalitäten von Zertifizierung/Akkreditierung.
  - Die ***Artikel 29-Gruppe*** erarbeitet ***„Guidelines“*** zum Thema Zertifizierung, die im Februar 2018 verabschiedet werden sollen (→ Abstimmung auf EU-Ebene).
  - Die Europäische Kommission wird ggf. ***delegierte und Durchführungsrechtsakte*** gem Art. 43 Abs. 8 + 9 DSGVO erlassen.
  - Aktuelle Aktivitäten der KOM:
    - Durchführung einer Studie zu Zertifizierung (läuft);
    - Multistakeholder Expert Group (Arbeit aufgenommen in 10/17).

Kontakt

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