it.sec
security for your information

Datenschutzzertifizierung – Datenschutzmanagementsystem

Bernhard C. Witt
Senior Consultant für Datenschutz und Informationssicherheit

DIN NIA 27 AK 1 & 5 ad hoc Meeting „Datenschutzmanagementsystem“
15. Juli 2016, Bonn

Bernhard C. Witt

- **Senior Consultant** für Datenschutz und Informationssicherheit bei der it.sec GmbH & Co. KG, verantwortlich für Datenschutz & IT Governance, Risk & Compliance Management
- Industriekaufmann, Diplom-Informatiker
- geprüfter fachkundiger Datenschutzbeauftragter (UDIS)
- zertifizierter ISO/IEC 27001 Lead Auditor (BSi)
- CRISC (ISACA)
- Lehrbeauftragter an der Universität Ulm (seit 2005)
- Autor der Bücher „IT-Sicherheit kompakt und verständlich“ (2006) und „Datenschutz kompakt und verständlich“ (2008 & 2010)
- Mitglied im Leitungsgremium des GI-Fachbereichs Sicherheit – Schutz und Zuverlässigkeit (seit 2009), deren stellvertretender Sprecher seit 11/2013
- Mitglied im Leitungsgremium der GI-Fachgruppe Management von Informationssicherheit (seit 2007), deren Sprecher von 02/2009 – 11/2013
- Mitglied im Leitungsgremium der GI-Fachgruppe Datenschutz-fördernde Technik (seit 2012)
- Mitglied im DIN-Arbeitsausschuss „IT-Sicherheitsverfahren“ AK 1 & 4 (seit 2011)

Zur it.sec:
- Seit 1996 Dienstleister zur Informationssicherheit
- Penetrationstests
- IT-Forensik
- IT GRC Management

Anforderungen der EU-DS-GVO (1)

- Die zum 25. Mai 2018 verbindlich innerhalb der EU in Kraft tretende EU-Datenschutz-Grundverordnung schreibt in Art. 5 Abs. 2 vor, dass die **Einhaltung der** in Abs. 1 definierten **Grundsätze** für die Verarbeitung personenbezogener Daten **nachgewiesen** werden müssen, um eine Geldbuße nach Art. 83 Abs. 5 von bis zu 20 Mio. € bzw. 4 % des weltweiten Jahresumsatzes vermeiden zu können
- Darüber hinaus werden **zahlreiche weitere Nachweispflichten** in der EU-DS-GVO eingefordert, die wiederum nach Art. 83 Abs. 4 mit einer Geldbuße von bis zu 10 Mio. € bzw. 2 % des weltweiten Jahresumsatzes geahndet werden können
- Die Erfüllung dieser Nachweispflichten setzt insoweit faktisch die **Einrichtung eines Datenschutzmanagementsystems** voraus – dieses kann aber auch aus einer systematischen Zusammenstellung verteilt vorliegender Quellen über einen spezifischen „View“ erfüllt werden

Anforderungen der EU-DS-GVO (2)

- In der EU-DS-GVO erfolgt nach Art. 32 Abs. 1 lit. b sowie Abs. 2 eine Orientierung auf die **Gewährleistung von**
  - **Vertraulichkeit**
  - **Integrität**
  - **Verfügbarkeit**
- Die Ausrichtung der Schutzvorkehrungen basiert auf einem **risikobasierten Ansatz** (nach Art. 24 Abs. 1 unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung auf die Rechte & Freiheiten natürlicher Personen)
- Die Maßnahmen (nach Stand der Technik!) sind nach Art. 24 Abs. 1 erforderlichenfalls zu **überprüfen und aktualisieren**
- Zudem sind Verfahren zur regelmäßigen **Überprüfung, Bewertung & Evaluierung der Wirksamkeit dieser Maßnahmen** nötig

→ **Ausrichtung des Datenschutzmanagementsystems auf ISO/IEC 27001 & 27009 sinnvoll!**

Anforderungen der EU-DS-GVO (3)

Die EU-DS-GVO sieht ausdrücklich vor, dass entsprechende **Nachweise auch durch Vorlage eines geeigneten Zertifikats** nach einem von den zuständigen Aufsichtsbehörden genehmigten Zertifizierungsverfahren erbracht werden können hinsichtlich:

- Erfüllung der Pflichten des Verantwortlichen zu **Sicherstellung & Nachweis**, dass die Verarbeitung **unter Einhaltung der EU-DS-GVO** erfolgt (Art. 24 Abs. 3)
- Nachweis von **Data Protection by Design / Default** (Art. 25 Abs. 3)
- Hinreichende Garantien für **geeignete technische & organisatorische Maßnahmen des Auftragsverarbeiters** (Art. 28 Abs. 5)
- **Angemessenheit getroffener Schutzvorkehrungen** (Art. 32 Abs. 3)
- **Geeignete Garantien in einem Drittland** zusammen mit rechtsverbindlichen & durchsetzbaren Verpflichtungen des Verantwortlichen oder Auftragsverarbeiters (Art. 46 Abs. 2 lit. f)

Anforderungen der EU-DS-GVO (4)

- Im Rahmen der EU-DS-GVO nutzbare Zertifikate müssen nach Art. 43 Abs. 1 von einer **Zertifizierungsstelle** stammen, die ak-kreditiert wurde durch:
  - eine zuständige Aufsichtsbehörde gemäß Art. 55 & 56 oder
  - die nationale Akkreditierungsstelle nach EU-Verordnung 765 / 2008 (in Deutschland: DAkkS) im Einklang mit EN ISO/IEC 17065:2012 („Conformity assessment – Requirements for bodies certifying products, processes and services“) und den Kriterien, die von der zuständigen Aufsichtsbehörde gemäß Art. 55 & 56 bzw. durch den Ausschuss (nach Art. 64 Abs. 1 lit. c) genehmigt & veröffentlicht wurden
- Die Akkreditierung wird auf bis zu 5 Jahre erteilt und kann unter den gleichen Bedingungen verlängert werden
- Durch delegierte Rechtsakte oder Durchführungsrechtsakte kann die EU-Kommission weitere Details festlegen

Anforderungen der EU-DS-GVO (5)

- Derartige **Zertifizierungsstellen müssen** nach Art. 43 Abs. 2
  - **unabhängig** sein & **einschlägiges Fachwissen** zur Zufriedenheit der zuständigen Aufsichtsbehörde nachweisen
  - Verfahren zu **Erteilung, regelmäßige Überprüfung und Widerruf der Zertifizierungen** festlegen
  - **transparente Beschwerdeverfahren** aufweisen
  - **frei von Interessenkonflikten** zur Zufriedenheit der zuständigen Aufsichtsbehörde sein
- Der **Aufwand zum Aufbau eines geeigneten** (zustimmungsfähigen) **Zertifizierungsstandards** ist ausgesprochen **hoch**
  → m.E. nur im Rahmen des ISO-Normenwerks sinnvoll
  → allerdings ist auch Erweiterung bei ISO/IEC 27006 nötig
- Bisher nur ein Standard bekannt, der EU-DS-GVO bereits berücksichtigt: ADCERT (angelehnt an ISO/IEC 27001); ansonsten viele noch in Anpassung (7 derzeit auf EU-DSRL ausgerichtet)

Bernhard C. Witt
bcwitt@it-sec.de

Vielen Dank!

it.sec GmbH & Co. KG
Einsteinstr. 55
D-89077 Ulm

USt Id Nr.: DE 225547544
Steuernummer: 88012/53709
Amtsgericht Ulm: HRA 3129

vertreten durch den **Geschäftsführer Dipl. Ing. (FH) Holger Heimann**.

Haftender Komplementär:
it.sec Verwaltungs GmbH
Amtsgericht Ulm: HRB 4593
Einsteinstr. 55
D-89077 Ulm

tel: +49 (0) 731 20589-0
mailto:info@it-sec.de
http://www.it-sec.de