REUNTEC
INFORMATIONSSICHERHEIT

Datenschutz und Datensicherheit – Update 2017

Datenschutz-Zertifizierungen im Blickwinkel der DS-GVO

Wiesbaden, 23. März 2017

Dipl.-Math. Petra Nietzer

Datenschutz-Auditorin (DSZ)
IT-Security-Auditorin (TÜV)
Geprüfte Datenschutzbeauftragte (bfz/FH)

Inhalt

VORGABEN DER DS-GVO
ÜBERBLICK DER NACHWEISMÖGLICHKEITEN
AUSBLICK

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Vorgaben der DS-GVO

- Fundstellen in der DS-GVO
  - 20 Treffer für „nachweis“
  - 19 Treffer für „sicherstellen“
  - 65 Treffer für „gewährleisten“
  - 77 Treffer für „zertifi“

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Vorgaben der DS-GVO

- Vielfältige Pflichten des Verantwortlichen
  - Rechenschaftspflicht :
    „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können“.
  - Vielfältige Nachweispflichten:
    - „muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat“
    - „Maßnahmen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“
    - …

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Vorgaben der DS-GVO

- Zertifizierung als Möglichkeit der Erfüllung der Pflichten:
  - Art. 24 Verantwortung des für die Verarbeitung Verantwortlichen
    „Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen“

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Vorgaben der DS-GVO

- Zertifizierung als Möglichkeit der Erfüllung der Pflichten:
  - Art. 28 Auftragsverarbeiter:

    „Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.“

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Vorgaben der DS-GVO

- Zertifizierung als Möglichkeit der Erfüllung der Pflichten:
  - Art. 32 Sicherheit der Verarbeitung

    „Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.“

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Vorgaben der DS-GVO

- Zertifizierung für wen möglich?
  - für die „zur Einhaltung durch die unter diese Verordnung fallenden Verantwortlichen oder Auftragsverarbeiter“
  - für Verantwortliche und Auftragsverarbeiter, die nicht unter diese Verordnung fallen
    - im Rahmen der Übermittlung an Drittländer
    - im Rahmen der Übermittlung an internationale Organisationen
    - zum Nachweis geeigneter Garantien gem. Art. 46 Abs. 2 f

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Vorgaben der DS-GVO

- Nutzen einer Zertifizierung
  - Möglichkeit des Nachweises der Einhaltung der Vorgaben der DS-GVO
- Trotz Zertifikat
  - Verantwortlicher und Auftragsverarbeiter weiterhin verantwortlich für die Einhaltung der Vorgaben der DS-GVO
  - Keine Beeinflussung der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörden

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Vorgaben der DS-GVO

- Anforderungen an eine Zertifizierung
  - Freiwillig
  - Zugänglich über ein transparentes Verfahren

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Vorgaben der DS-GVO

- Wer kann Zertifikate nach DS-GVO erteilen?
  - akkreditierte Zertifizierungsstellen
    - Akkreditierung erfolgt durch
      - zuständige Aufsichtsbehörde oder
      - nationalen Akkreditierungsstelle (in Deutschland die DAkkS)
  - zuständige Aufsichtsbehörden

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Vorgaben der DS-GVO

- Bedingungen für eine akkreditierte Zertifizierungsstelle
  - Nachweis von Unabhängigkeit und Fachwissen
  - Zertifikatserteilung nur bei Einhaltung der genehmigten Kriterien (für das Zertifikat)
  - Prozesse für
    - Zertifikatserteilung,
    - Überprüfung,
    - Widerruf
  - Prozesse für Beschwerden und Umsetzungsverletzung der Zertifikatsnehmer
  - Kein Interessenskonflikt bei der Ausübung der Aufgaben und Pflichten

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Vorgaben der DS-GVO

- Bedingungen für ein Zertifikat
  - Einhaltung der durch Aufsichtsbehörde oder Ausschuss vorgegebenen Kriterien
  - Max. 3 Jahre Gültigkeit
  - Verlängerungsmöglichkeit
  - Widerruf durch Aufsichtsbehörde möglich

- Veröffentlichung durch den Ausschuss
  - in einem Register

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Nachweismöglichkeiten

- Bisherige Zertifizierungsverfahren oft keinen oder nicht ausreichenden Fokus auf Datenschutz
  - Abzielen auf Schutz von Geschäftsprozessen vs. Schutz von Personen

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Beispiel 1 IT-Sicherheit ≠ Datenschutz: Technische Maßnahme

- Verschlüsselung ist nützlich
  - für IT-Sicherheit
  - und Datenschutz

- „Wir verschlüsseln“ – nicht ausreichend
  - Klären: wegen welcher Gefährdungen?
  - Werden Geschäftsprozesse/-Daten geschützt oder Personen(-daten)?
  - Risiken für Personen gehen auch vom eigenen Unternehmen aus

REUNTEC INFORMATIONSSICHERHEIT

Beispiel 2 IT-Sicherheit ≠ Datenschutz: Schutzbedarfskategorien

- Schutzbedarfskategorien mit Fokus auf finanzielle Auswirkungen und Prozessbeeinträchtigung

NORMAL	HOCH	SEHR HOCH
Möglicher finanzielle Schaden <= 50.000 EUR Höchstens unerhebliche Beeinträchtigung der Unternehmensprozesse. Ausfallzeit von mehr als 24h sind hinnehmbar.	50.000 EUR < Möglicher finanzielle Schaden <= 500.000 EUR. Erhebliche Beeinträchtigung der Unternehmensprozesse. Ausfallzeiten dürfen höchstens 24h betragen	Möglicher finanzielle Schaden > 500.000 EUR. Beeinträchtigung der Unternehmensprozesse mit Ausfallzeiten > 2h nicht tolerierbar.

REUNTEC INFORMATIONSSICHERHEIT

Beispiel 2 IT-Sicherheit ≠ Datenschutz: Schutzbedarfskategorien

- Schutzbedarfskategorien personenbezogene Daten

NORMAL	HOCH	SEHR HOCH
Betroffene sind in ihrer gesellschaftlichen Stellung oder wirtschaftlichen Verhältnissen beeinträchtigt. Begrenzte Schadensauswirkung, Schäden sind leicht durch eigene Aktivitäten zu heilen	Betroffene sind in ihrer gesellschaftlichen Stellung oder wirtschaftlichen Verhältnissen erheblich beeinträchtigt. Schadensauswirkungen für Betroffene sind beträchtlich	Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen. Schadensauswirkung haben für den Betroffenen ein unmittelbar existenziell bedrohliches, katastrophales Ausmaß

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Nachweismöglichkeiten

- Große Auswahl in der Zertifizierungslandschaft
  - Trusted Cloud
  - DQS Gütesiegel Datenschutz
  - ISIS12
  - Standard Datenschutzmodell
  - DSZ Datenschutz Zertifizierungsgesellschaft
  - ULD, TÜV, GoodPriv@cy, ePrivacy,…

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Nachweismöglichkeiten

- SDM
  - Anwendungsbereich: Einzelne Verfahren
  - Erprobungsfassung von der Konferenz der Datenschutzbehörden zustimmend zur Kenntnis genommen (Nov. 2016).
    - Erprobung durch Aufsichtsbehörden und Verantwortliche
    - Fortentwicklung des Standards durch Arbeitsgremium der Konferenz
  - Grundidee: Rechtliche Vorgaben in angemessene technische und organisatorische Maßnahmen umsetzen
  - Kernelemente des SDM
    - 7 Schutzziele
    - 3 Schutzbedarfsabstufungen
    - 3 Verfahrenskomponenten
  - Maßnahmenkatalog in Arbeit

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Nachweismöglichkeiten

- DSZ Datenschutz Zertifizierungsgesellschaft
  - Datenschutzstandard DS-BVD-GDD-01
    - Entwickelt aus den Verbänden GDD e.V. und BvD e.V.
    - öffentlicher Standard
    - Fokus: Auftragsverarbeitung gem. §11 BDSG
    - Nutzen: Verlässlichkeit für Auftragsdatenverarbeiter und verantwortliche Stellen
  - Befürwortung durch LDI NRW

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Nachweismöglichkeiten

- DSZ Datenschutz Zertifizierungsgesellschaft
  - Vorbereitungen zur Überführung von BDSG zur DS-GVO
    - Bereits erfolgt: Anpassung des Standards an Vorgaben der DS-GVO
    - Schaffung von Prozessen zur Erfüllung der Voraussetzungen für eine Zertifizierungsstelle
  - Plan:
    - Akkreditierung der dsz GmbH gemäß DS-GVO

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Ausblick

- DS-GVO unterstützt Zertifizierungen ausdrücklich
  - Zertifizierungen für Produkte und Dienstleistungen dienen der Transparenz für Verantwortliche und Betroffene hinsichtlich des Datenschutzniveaus
  - Doch: es besteht keine Pflicht für eine Zertifizierung

Datenschutz-Zertifizierungen

REUNTEC INFORMATIONSSICHERHEIT

Ausblick

- Festlegung für Zertifikatkriterien durch die Aufsichtsbehörden abwarten
  - Erst nach Verabschiedung des DS-AnpUG-EU möglich
- Anpassung der bestehenden Zertifikate an die Kriterien
- Akkreditierung von Zertifizierungsstellen für das Zertifikat

- Auswahl der geeigneten Gütesiegel/Zertifikate und Umsetzung durch Verantwortliche

Fragen? Anregungen?

Vielen Dank für
Ihre Aufmerksamkeit

REUNTEC – Angewandte Informationssicherheit
Inhaberin Dipl.-Math. Petra Nietzer

Prinz-Karl-Weg 4 | 86159 Augsburg
www.reuntec.com

Petra Nietzer
nietzer@reuntec.com | 0821 / 420888-55