chancen der digitalisierung

Überblick Rechtliche Aspekte des cloudcomputing

rechtliche herausforderungen Cloudcomputing

Vertrags- und Haftungsrecht

- Absicherung, dass Cloudanbieter entsprechende wirksame technische Maßnahmen gegen das Ausfallen der IT trifft. SLA
- Haftung bei Ausfällen. Ist der Haftende solvent genug? Versicherung

Lizenzrecht

- SPLA – Lizenzen
- Lizenzbestimmungen des einzelnen SW – Hersteller z.B. Oracle DB

Datenschutzrecht

- SW und Daten auf (irgendwelchen) Servern des Cloud Computing Anbieters
- wo Server stehen ist für die Funktionsfähigkeit des Cloud Computing grundsätzlich irrelevant, aber nicht für dessen rechtlich Zulässigkeit. (BDSG Kundendaten)

Steuer- Handelsrecht

- Buchhaltungsdaten dürfen seit 2010 auf ausländischen Servern gespeichert werden. Verfahren muss detailliert offengelegt und durch Finanzbehörde genehmigt werden.

Quelle: Dirk Fromm, Dirk Heuß Unternehmensberatung

Cloud computing
datenübertragung in die usa

- BDSG :Keine Übermittlung personenbezogener Daten außerhalb EWR
- USA gelten per se nicht als anerkanntes sicheres Drittland
- Safe Habor (Datenschutzabkommen der EU mit den USA).
- Kündigung im letzten Jahr durch den EUGH-Begründung „Patriot Act“
- Folgen: US-Unternehmen dürfen keine personenbezogenen Daten von europäischen Unternehmen erfassen, verarbeiten oder speichern.
- Nachfolgevereinbarung "EU-US-Privacy Shield„ Vorstellung am 02.02.2016
- strenge Auflagen für US Unternehmen.
- Durchsetzung über US-Recht möglich.
- Die USA sichert zu, dass transferierte Daten keiner "unterschiedslosen Massenüberwachung" unterzogen werden.
- Kontrolle durch das US-Handelsministerium.

Quelle: Dirk Fromm, Dirk Heuß Unternehmensberatung

Wir bieten Datenschutz über unsere Multi-cloud-Lösungen inklusive!

Derzeit ist für unsere Kunden in unseren Cloudlösungen enthalten:

Datenschutz nach BDSG:

- Vor Vertragsabschluss muss die besonderer Berücksichtigung der Eignung des Auftragnehmers nachgewiesen werden -§11, Abs. 2 BDSG; die beinhaltet:
- die Bestellungsurkunde des Datenschutzbeauftragten.
- Die Qualifizierungsnachweise des Datenschutzbeauftragten.
- Auf Wunsch die technischen und organisatorischen Maßnahmen zur RZ-Sicherheit (TOM).
- Wir schließen mit unseren Partnern / Kunden einen Vertrag ADV ab.
- Kundenservice!

Nach EU-DSGVO ändert sich hier Nichts!

- Art. 24 Abs. 1 EU-GDGVO regelt die Berücksichtigung der Eignung des Auftragnehmers.
- Art. 24 ff. die Datenverarbeitung im Auftrag – Inhaltlich sind die Ansprüche hier noch etwas höher als im BDSG!

Quelle: Dirk Fromm, Dirk Heuß Unternehmensberatung

Was ändert sich durch die EU-DSGVO?

- Die EU-DSGVO ist am 14.04.2016 veröffentlicht worden.
- Die kann bereits jetzt alternativ zum BDSG eingesetzt werden (Übergangsfrist).
- Am 14.05.2018 ersetzt sie ALLE bisherigen deutschen Datenschutzgesetze!
- Jedes EU-Land kann in einem angemessenen Umfang schärfere Bestimmungen erlassen.
- Die vorgegebenen Standards dürfen NICHT unterschritten werden.
- Geldbußen von bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs! (Art. 82 Abs. 5 EU-DSGVO).

Quelle: Dirk Fromm, Dirk Heuß Unternehmensberatung

Zwingendes ereignis umsetzungsplan Kritis.
Umsetzung der europäischen cyber-richtlinie.

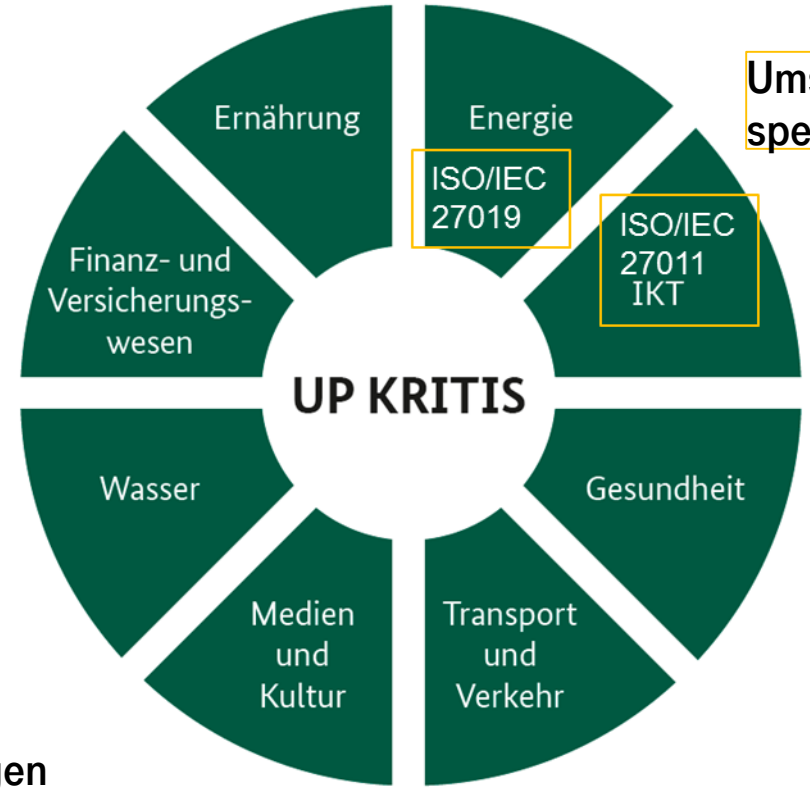
Zertifizierung nach ISO/IEC 27001

Umsetzung
IT-Sicherheitsgesetz

Software-Zertifizierung
nach ISO 27034

Anforderungen BDSG

Anforderungen
EU-DSGVO ab Mai 2018



Umsetzung branchen-spezifischer Normen

Umsetzung von
Binding
Corporate Rules

Quelle: KRITIS BUND

Das IT-Sicherheitsgesetzes und dessen Auswirkungen auf unser Kunden.

- Das IT-Sicherheitsgesetz basiert auf der Umsetzung der Cyberrichtlinie der EU.
- Danach wurden ALLE Marktteilnehmer in der EU zur Umsetzung der ISO/IEC 27001 verpflichtet Art. 14-16 der EU-Cyberrichtlinie).
- Das Gesetz wurde am 12.06.2015 im Deutschen Bundestag verabschiedet.
- Die Umsetzung wurde an das BSI übertragen und beschränkt sich derzeit nur auf die kritischen Infrastrukturen –KRITIS-Branchen (§ 2 Abs. 10 und 11 BSI-Gesetz) mit Ausnahme Telekommunikation und Telemedien (hier ist die Bundesnetzagentur zuständig).
- Es beinhaltet eine unverzügliche Meldepflicht aller IT-Angriffe (§ 8 BSI-Gesetz), dafür sind von den Unternehmen Warn- und Alarmierungskontakte zu benennen (Rechtsverordnung dazu wird noch in diesem Jahr erwartet).

Quelle: Dirk Fromm, Dirk Heuß Unternehmensberatung

Vielen Dank