TeleTrusT
Pioneers in IT security.

Informationstag "Ersetzendes Scannen"

Berlin, 19.04.2013

"RESISCAN durch Dritte – Rechtliche Anforderungen an die Beauftragung"

RA Karsten U. Bartels LL.M., HK2 Rechtsanwälte

Meine Punkte

Leistungsvertrag

Auftragsdatenverarbeitung

HK2
Rechtsanwälte

Darf ich (selbst) ersetzend scannen?

Verbot aus Vertrag oder Gesetz?

Datenschutzgesetz, StGB (Urkunden), Berufsrecht, …

HK2
Rechtsanwälte

Darf ich Dritte mit dem ersetzenden Scannen beauftragen?

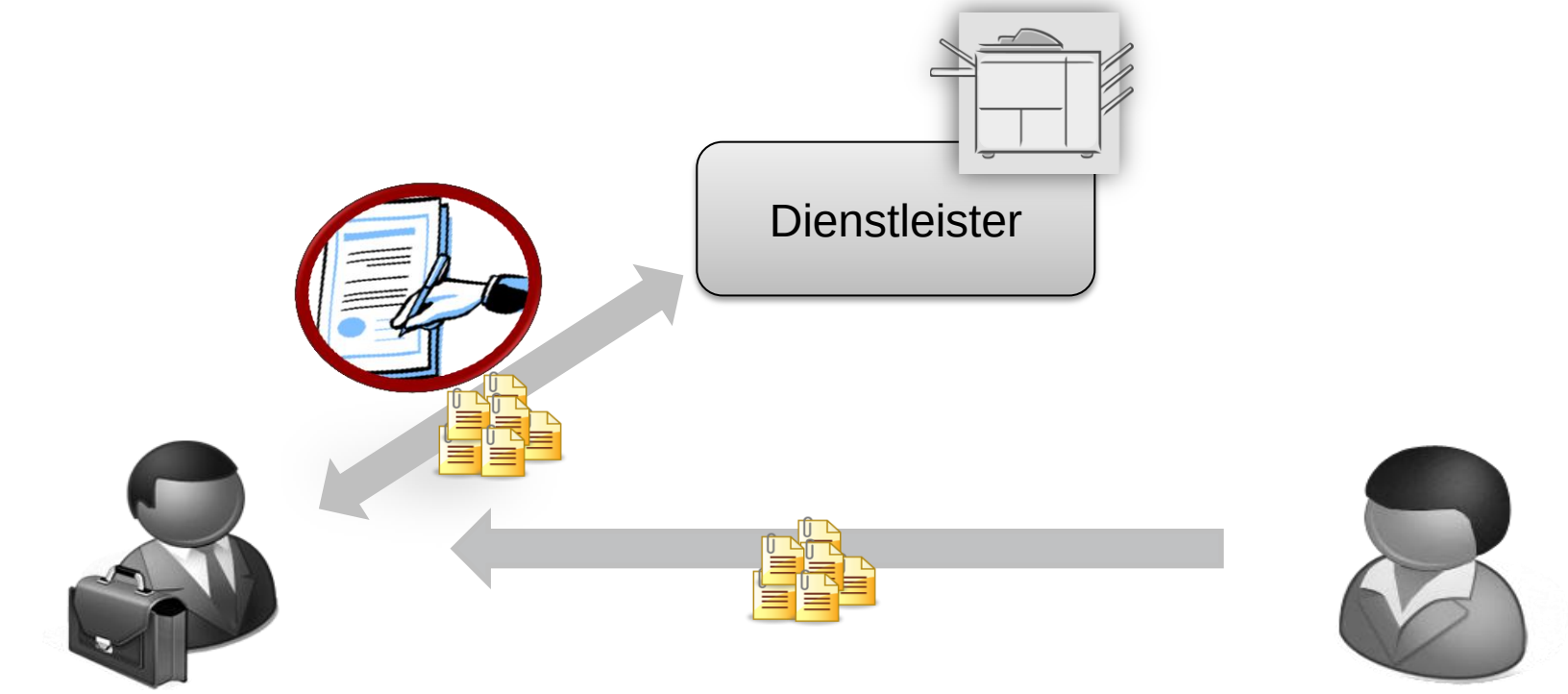
Datenschutzgesetz, StGB (Geheimnisverrat), …

HK2
Rechtsanwälte

Sollte ich ersetzend scannen
und dies outsourcen?

Beweisrecht, Obliegenheitsverletzungen

1 ADV


Dienstleister
Verantwortliche Stelle
Personenbezogene Daten
Betroffener

Auftragsdatenverarbeitung
§ 11 BDSG / Fachgesetz / Landesrecht

HK2 Rechtsanwälte

- Erforderliche Regelungen in Schriftform
  - Gegenstand und die Dauer des Auftrags
  - Umfang, Art und Zweck der vorgesehenen Datenverwendung
  - Weisungsrechte des Auftraggebers
  - Kontrollrechte und Kontrollpflichten des Auftraggebers
  - Regelungen von Subunternehmerverhältnissen
  - Festlegung der „TOM“ (z.B. gem. § 9 BDSG)
  - Datenrückgabe-, Löschungspflichten

- Zusätzliche Regelungen
  - Vertragsstrafen

Technische und organisatorische Maßnahmen (z.B. gem. § 9 BDSG)

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- „Trennungskontrolle“

Prüfpflichten

Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

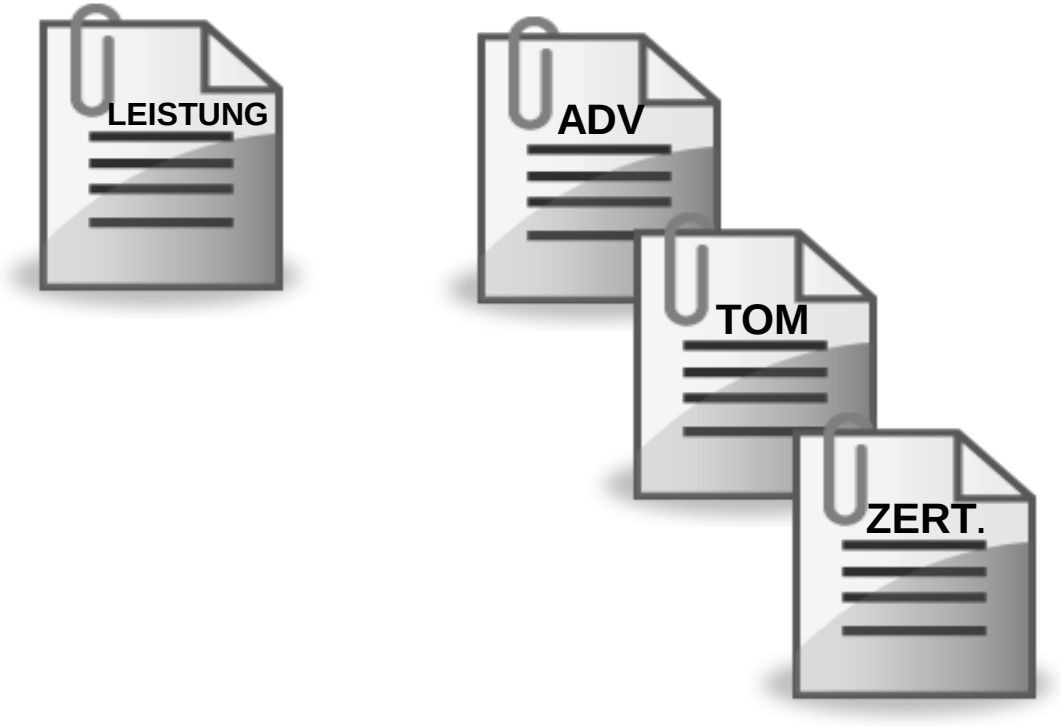
(§ 11 Abs. 2 S.4 BDSG)

- Persönliche Prüfung nicht erforderlich
- Verhältnis zum TR-Zertifikat

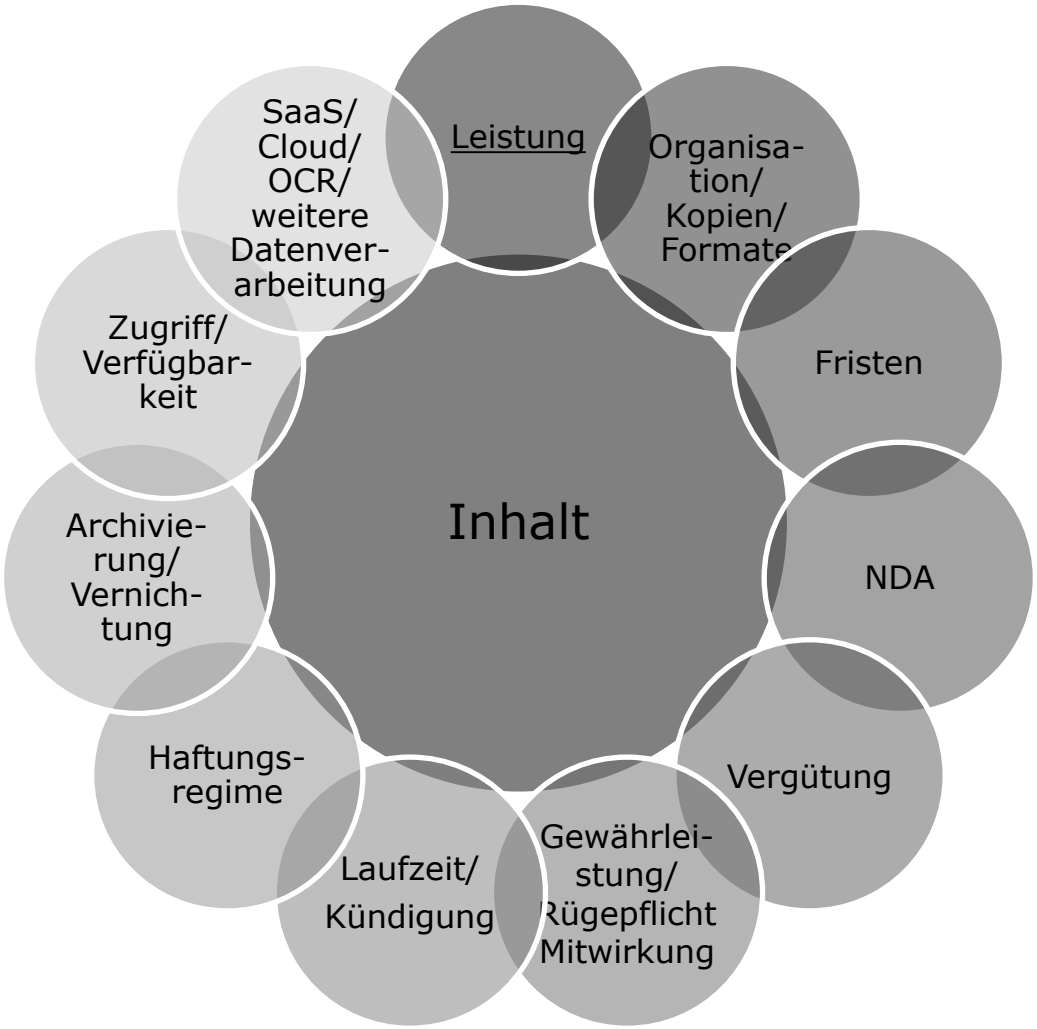
HK2
Rechtsanwälte

Problem.

Schutzbedarfsanalyse nur
durch Verantwortlichen selbst
am konkreten Dokument bzw. Anwendungsfall


LEISTUNG
ADV
TOM
ZERT.

2 Leistungsvertrag



Pflichtregelung

Einbeziehung der TR als Leistungsparameter

- „Der Auftragnehmer verpflichtet sich, die Leistung gemäß den Anforderungen der BSI TR 03138 in der jeweils aktuellen Fassung zu erbringen.“
- „Alle zwingenden (MUSS) und nachdrücklichen (SOLL) Empfehlungen der BSI TR 03138 sind gemäß des festgelegten Schutzmoduls umzusetzen. Abweichungen sind nur nach schriftlicher Zustimmung durch den Auftragnehmer zulässig. Der Auftragnehmer hat ausdrücklich schriftlich darauf hinzuweisen, dass eine Abweichung von der BSI TR 03138 erfolgt.“
- Evtl. Zusicherung einer Zertifizierung (1.8 TR)

Vorgaben der TR zum Outsourcing

4.2.2., A.O.5 - TR RESISCAN

- Im Anforderungskatalog vorgesehene Maßnahmen sind entsprechend umzusetzen, zudem:

Muss	**Soll**
Organisatorische und technische Schnittstellen	Analyse der zusätzlichen Risiken
Verpflichtung zur Einhaltung der Sicherheitsmaßnahmen	Unangemeldete Stichprobenprüfungen
	Baustein Outsourcing des IT-Grundschutz-Handbuches

Problem: Soll-Bestimmung = nachdrückliche Empfehlung, Abweichungen nur in wohlbegründeten Ausnahmefällen

Pflichtregelung

Festlegung des Schutzmoduls

- Projektphasen: Erhebung-Analyse-Beratung
- Schutzbedarfsanalyse der zu verarbeitenden Dokumente (3.2, 4.2.1 TR)
- „Die Leistung wird nach dem Basismodul gemäß den Anforderungen der BSI TR 03138 erbracht.“
- Option zur Aufwertung der gesamten Leistung oder einzelner Dokumente (CRM)

- Problem: Schutzbedarf kennt die Prozessordnung nicht, Schadensverlauf nur schwer kalkulierbar

Pflichtregelung

Einbeziehung der Verfahrensdokumentation

- „Die Verfahrensdokumentation ist als Anlage Bestandteil des Vertrages und entspricht den Vorgaben der BSI TR 03138.“
- Festlegung der organisatorischen und technischen Schnittstellen: Übertragungswege, Datenablageorte, beteiligte Akteure, Rückfallverfahren etc.

Baustein Outsourcing IT-Grundschutzhandbuch (BSI-B 1.11) und Festlegung/ Verpflichtung auf Sicherheitsmaßnahmen

- Analyse des Sicherheitsrisikos
- Sicherheitskonzept AG
- Sicherheitskonzept AN
- Sicherheitsmaßnahmen = Leistungsbestimmung

HK2
Rechtsanwälte

Ihre Punkte?

HK2
Rechtsanwälte

Karsten U. Bartels LL.M.

- Rechtsanwalt
- Zertifizierter Datenschutzbeauftragter (TÜV)
- DEKRA Schulungsanbieter
- Auditor der datenschutz cert GmbH
  - Datenschutz-Gütesiegel *ips* - internet privacy standards
  - Zertifikat zur Auftragsdatenverarbeitung
  - Zertifikat für Datenschutz-Management *priventum*
- Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich)
- Mitglied Geschäftsführender Ausschuss Arge Informationstechnologie im Deutschen Anwaltverein e.V.
- Leiter AG Recht, Bundesverband IT-Sicherheit e.V. – TeleTrusT
- Schlichter IT-Recht der IHK Berlin Schlichtungsstelle

Hausvogteiplatz 11 A
10623 Berlin
T +49 (0)30 27 89 00 - 0
F +49 (0)30 27 89 00 - 10
www.hk2.eu

about.me/KarstenUBartels