

IT-Sicherheitsrechtstag 2018

TeleTrust – Bundesverband IT-Sicherheit e.V.

Berlin, 25.10.2018

Die DSGVO in der Praxis

RA Karsten U. Bartels LL.M.

HK2 Rechtsanwälte

Vorstand TeleTrust



Karsten U. Bartels LL.M.*

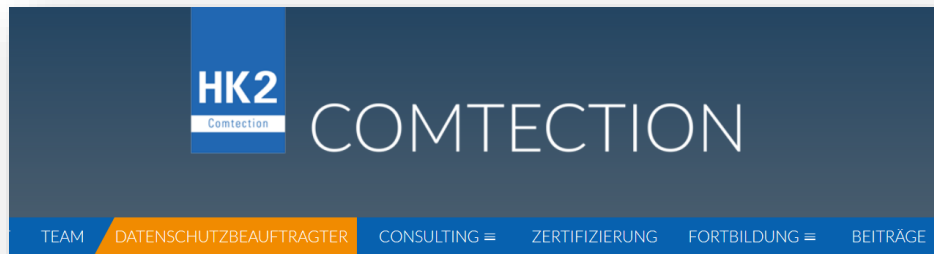
- Partner/ Rechtsanwalt, HK2 Rechtsanwälte
- Geschäftsführer HK2 Comtection GmbH
- Zert. Datenschutzbeauftragter (TÜV)
- Vorstand Bundesverband IT-Sicherheit e. V. (TeleTrust)
- Stellv. Vorsitzender Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e. V.

(*) Rechtsinformatik

Vorstellung HK2



- IT-Recht
 - IP-Recht
 - Arbeitsrecht
-
- Sitz: Berlin
 - Gegründet: 2002
 - www.hk2.eu



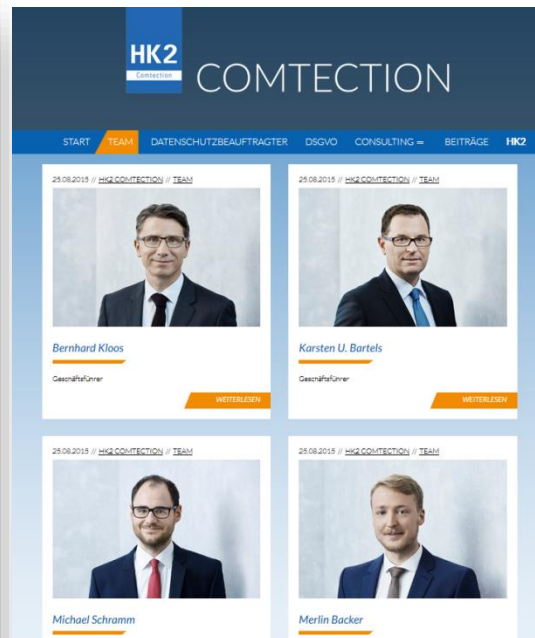
DATENSCHUTZBEAUFTRAGTER

Als externer Datenschutzbeauftragter nehmen wir dessen Pflichten und Rechte wahr, z.B. Überwachung der Verarbeitungsvorgänge, Prüfung der Vereinbarkeit mit den Datenschutzgesetzen, Vertretung vor den Aufsichtsbehörden.

Unsere Mitarbeiter verfügen über langjährige Erfahrung im Datenschutz. Das ermöglicht eine zielorientierte und effiziente Zusammenarbeit. Sämtliche HK2 Comtection-Mitarbeiter können nach § 4f BDSG persönlich ernannt werden.

Was spricht für uns:

- die nach dem Gesetz erforderliche Fachkunde und Zuverlässigkeit unserer Mitarbeiter ist selbstverständlich und kann Dritten gegenüber dokumentiert werden
- bedarfs- und aufwandsgerechte Vergütung
- bessere Erreichbarkeit, da z.B. Urlaub und Krankheit durch Vertreter aufgefangen werden können
- Beratung aus Dienstleistersicht
- keine Einschränkung von Kündigungsrechten wie bei internen Datenschutzbeauftragten, sondern Möglichkeit zur flexiblen Vertragsgestaltung
- keine Einschränkung von Weisungsrechten gegenüber internen Mitarbeitern
- der Aufwand für Ausstattung sowie Fort- und Weiterbildungskosten eines intern bestellten Datenschutzbeauftragten entfallen



www.comtection.de

Agenda

- Praxisbericht
- Technische und organisatorische Maßnahmen
- Dokumentation
- Auftragsverarbeitung und Joint Controllershship



Zum Einstieg einige Thesen ...

1.

Die DSGVO ist kein Projekt.

2.

Auslegungsspielräume der DSGVO sind historisch groß, aber degressiv.

3.

Der technische Datenschutz ist auf dem Niveau der IT-Sicherheitsgesetze reguliert.

4.

Die DSGVO kann nur in dauerhaften Teams aus Geschäftsleitung, IT und Recht umgesetzt werden.

5.



Wie wird umgesetzt?

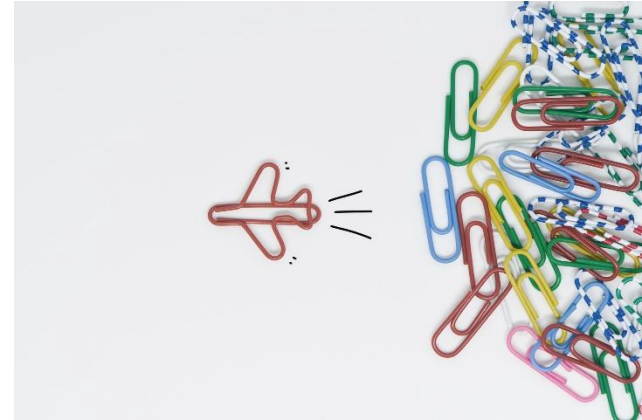
... in Teams



	GL	IT	Recht	Datenschutz
Kleinstunterne- hmen	Geschäfts- führer	IT- Dienstleister	Externer Rechtsanwalt	-
Kleiner Mittelstand	Geschäfts- führer	interne/ externe IT	Externer Rechtsanwalt	Datenschutz- beauftragter
Großer Mittelstand/ große Unternehmen	Zuständiger GF	CTO, CISO	Syndikus und externer Rechtsanwalt	Datenschutz- beauftragter/ Konzern-DSB

Woran orientieren?

... an den gesetzlichen Dokumenten!



DSGVO To-Do's nach Dokumenten 1/2

Dokument	Details	DSGVO	h	sichtb.
Verzeichnis von Verarbeitungstätigkeiten	als Verantwortlicher	Art. 30 Abs. 1	+++	-
Verzeichnis von Verarbeitungstätigkeiten (AV)	als Auftragsverarbeiter	Art. 30 Abs. 2	(++)	-
Dokumentation der technischen und organisatorischen Maßnahmen	unternehmensbezogen (100%)	Artt. 32, 5 Abs. 2	+++	-
Dokumentation der technischen und organisatorischen Maßnahmen	leistungsbezogen	Artt. 32, 5 Abs. 2	++	+
Auftragsverarbeitungs-Vereinbarungen	AG, AN, neutral	Art. 28	++	+
Vereinbarung über gemeinsame Verantwortlichkeit	joint controllers	Art. 26	+++	+
Datenschutz-Folgenabschätzung	Verfahren und Durchführung	Art. 35	++	-
Erstellung von Einwilligungstexten		Art. 7	+	++
Datenschutzerklärung für Mitarbeiter, Kunden und Dienstleister, Website		Artt. 13, 14	++	+++

DSGVO To-Do's nach Dokumenten 2/2

Dokument	Details	DSGVO	h	sichtb.
Konzept Meldepflicht		Artt. 33, 34	+	-
Verfahren Betroffenenrechte: Auskunft, Berichtigung, Löschung, Einschränkung, Datenportabilität, Widerspruch		Artt. 15, 16, 17, 18, 20, 21	++	+++
Notfallplan/ Business Continuity Management (BCM)	TOM	Art. 32 Abs. 1 c)	++	-
Berechtigungskonzept	TOM		++	-
Löschkonzept (inkl. Aufbewahrungsfristen)	TOM		++	-
(Verpflichtungserklärung der Mitarbeiter auf Vertraulichkeit)		Art. 32 Abs. 4	+	+++
(Schulungsunterlagen)	i. V. m. Schulungspflicht des DSB	Art. 39 Abs. 1 a)	++	++

DSGVO To-Do's nach Dokumenten 1/2

Dokument	Details	DSGVO	h	sichtb.
Verzeichnis von Verarbeitungstätigkeiten	als Verantwortlicher	Art. 30 Abs. 1	+++	-
Verzeichnis von Verarbeitungstätigkeiten (AV)	als Auftragsverarbeiter	Art. 30 Abs. 2	(++)	-
 Dokumentation der technischen und organisatorischen Maßnahmen	unternehmensbezogen (100%)	Artt. 32, 5 Abs. 2	+++	-
 Dokumentation der technischen und organisatorischen Maßnahmen	leistungsbezogen	Artt. 32, 5 Abs. 2	++	+
 Auftragsverarbeitungs-Vereinbarungen	AG, AN, neutral	Art. 28	++	+
 Vereinbarung über gemeinsame Verantwortlichkeit	joint controllers	Art. 26	+++	+
Datenschutz-Folgenabschätzung	Verfahren und Durchführung	Art. 35	++	-
Erstellung von Einwilligungstexten		Art. 7	+	++
Datenschutzerklärung für Mitarbeiter, Kunden und Dienstleister, Website		Artt. 13, 14	++	+++

DSGVO To-Do's nach Dokumenten 1/2

Dokument	Details	DSGVO	h	sichtb.
Verzeichnis von Verarbeitungstätigkeiten	als Verantwortlicher	Art. 30 Abs. 1	+++	-
Verzeichnis von Verarbeitungstätigkeiten (AV)	als Auftragsverarbeiter	Art. 30 Abs. 2	(++)	-
 Dokumentation der technischen und organisatorischen Maßnahmen	unternehmensbezogen (100%)	Artt. 32, 5 Abs. 2	+++	-
 Dokumentation der technischen und organisatorischen Maßnahmen	leistungsbezogen	Artt. 32, 5 Abs. 2	++	+

Sicherheit der Verarbeitung

Art. 32 DSGVO

Gewährleistung eines dem Risiko angemessenen Schutzniveaus

↓

Geeignete technische und organisatorische Maßnahmen (TOM)

berücksichtigen

→ Eintrittswahrscheinlichkeit und Schwere des Risikos einer Rechtsverletzung des Betroffenen (*Schutzbedarfsanalyse*)

→ Art, Umfang, Menge, Zweck der Verarbeitung

→ Stand der Technik



Stand von Wissenschaft
und Forschung



Stand der Technik



Allgemein anerkannte
Regeln der Technik

Beim Stand der Technik handelt es sich um die im Waren- und Dienstleistungsverkehr verfügbaren Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten kann.

[Bartels/ Backer/ Schramm: Der „Stand der Technik“ im IT-Sicherheitsrecht - Wirkung des Verweisungsbegriffs und Lösungsansätze zur legislativen Verwendung, Tagungsband 15. Deutscher IT-Sicherheitskongress, S. 503]

Stand der Technik bezeichnet die am Markt verfügbare Bestleistung einer Maßnahme oder eines Maßnahmenbündels zur Erreichung eines gesetzlichen IT-Sicherheitszieles.

[Bartels/ Backer/ Schramm: Der „Stand der Technik“ im IT-Sicherheitsrecht - Wirkung des Verweisungsbegriffs und Lösungsansätze zur legislativen Verwendung, Tagungsband 15. Deutscher IT-Sicherheitskongress, S. 503]

Handreichung zum Stand der Technik

Bundesverband IT-Sicherheit e. V.

<https://www.teletrust.de/stand-der-technik/>

TeleTrust – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.



IT-Sicherheitsgesetz und Datenschutz-Grundverordnung:
Handreichung zum "Stand der Technik"
technischer und organisatorischer Maßnahmen

Revidierte und erweiterte Ausgabe
2018

Fragenkatalog zur Ermittlung des Stands der Technik

- Maßnahmenbeschreibung und IT-Sicherheitsziele
- verfügbare Dokumentationen
- Bezug auf Standards/ Normungen
- Empfehlungen von Fachverbänden/ Experten
- Regelmäßige Überprüfung der Maßnahme
- Grad der Fortschrittlichkeit
- Praxiserprobung
- Vergleichbare Maßnahmen



Untergesetzliche Normen, Zertifikate

- Rechtliche Bedeutung technischer Normen und Richtlinien
 - BSI IT-Grundschutz
 - ISO 27001 u. a.
- Zertifizierungen gem. Art. 42 ff. DSGVO

Sicherheit der Verarbeitung

Art. 32 DSGVO

Gewährleistung eines dem Risiko angemessenen Schutzniveaus

↓

Geeignete technische und organisatorische Maßnahmen (TOM)

berücksichtigen

→ Eintrittswahrscheinlichkeit und Schwere des Risikos einer Rechtsverletzung des Betroffenen (*Schutzbedarfsanalyse*)

→ Art, Umfang, Umstände, Zweck der Verarbeitung

→ Stand der Technik

Wirksamkeitsprüfung, ...

→ Implementierungskosten, ...

Berücksichtigen des Standes der Technik Art. 32 Abs. 1 DSGVO

- 
1. Wissen
 2. Fachliche Bewertung
 3. Schlussfolgerung

Angemessenheits- kriterien: technisch

- 
- A decorative background image on the left side of the slide, consisting of a dense, vertical stream of binary code (0s and 1s) in a light gray font, creating a digital rain effect.
- Interoperabilität der betreffenden Systeme
 - Abhängigkeit von Dritten
 - Einsatz nach SdT führt an anderer Stelle zum Absenken der IT-Sicherheit
 - Beurteilung von Maßnahmen-Bündeln/ -Paketen zulässig

Angemessenheits- kriterien: wirtschaftlich

- Quote des IT-Sicherheits-Budgets
- Letzte Investitionen
- Verhältnis zwischen Investition und Sicherheitszugewinn

Angemessenheits- kriterien: rechtlich

- aufsichtsrechtliche Vorgaben und Entscheidungen
- vertragliche Abhängigkeiten?

Sicherheit der Verarbeitung

Art. 32 DSGVO



Dokumentation

Art. 32 DSGVO



Dokumentation der TOM

Maßnahmen	Beschreibung

Dokumentation der TOM

Maßnahmen	Beschreibung	Stand der Technik		Schutz- bedarf	Wirksam- keits- prüfung
		objektiv-technisch	subjektive Auswahl		

Dokumentation der TOM

Maßnahmen	Beschreibung	Stand der Technik		Schutz- bedarf	Wirksam- keits- prüfung	Wieder- vorlage	...
		objektiv-technisch	subjektive Auswahl				

Gliederung TOM-Dokumentation

BDSG (Anlage zu § 9)	Sicherheit der Datenverarbeitung, § 64 BDSG-neu	Art. 32 DSGVO
Zugangskontrolle, Zutrittskontrolle	Zugangskontrolle (Nr. 1)	Vertraulichkeit, Integrität
Zugriffskontrolle	Datenträgerkontrolle (Nr. 2), Benutzerkontrolle (Nr. 4), Zugriffskontrolle (i.e.S.) (Nr. 5), Speicherkontrolle (Nr. 3)	
Weitergabekontrolle	Übertragungskontrolle (Nr. 6) Transportkontrolle (Nr. 8)	
Eingabekontrolle	Eingabekontrolle (Nr. 7)	
	Datenintegrität (Nr. 11)	
Auftragskontrolle	Auftragskontrolle (Nr. 12)	
	Wiederherstellbarkeit (Nr. 9)	Wiederherstellbarkeit
	Zuverlässigkeit (Nr. 10)	Belastbarkeit
Verfügbarkeitskontrolle	Verfügbarkeitskontrolle (Nr. 13)	Verfügbarkeit
Trennungsgebot	Trennbarkeit (Nr. 14)	Zweckbindung, Art. 5 Abs.1 b)

Gliederung TOM-Dokumentation

BDSG (Anlage zu § 9)	Sicherheit der Datenverarbeitung, § 64 BDSG-neu	Art. 32 DSGVO
Zugangskontrolle, Zutrittskontrolle	Zugangskontrolle (Nr. 1)	Vertraulichkeit, Integrität
Zugriffskontrolle	Datenträgerkontrolle (Nr. 2), Benutzerkontrolle (Nr. 4), Zugriffskontrolle (i.e.S.) (Nr. 5), Speicherkontrolle (Nr. 3)	
Weitergabekontrolle	Übertragungskontrolle (Nr. 6) Transportkontrolle (Nr. 8)	
Eingabekontrolle	Eingabekontrolle (Nr. 7)	
	Datenintegrität (Nr. 11) 	
Auftragskontrolle	Auftragskontrolle (Nr. 12)	
	Wiederherstellbarkeit (Nr. 9) 	Wiederherstellbarkeit
	Zuverlässigkeit (Nr. 10) 	Belastbarkeit
Verfügbarkeitskontrolle	Verfügbarkeitskontrolle (Nr. 13)	Verfügbarkeit
Trennungsgebot	Trennbarkeit (Nr. 14)	Zweckbindung, Art. 5 Abs.1 b)

Data protection by design and by default Art. 25 DSGVO

- geeignete technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik
- Adressat ist der Verantwortliche
- entspricht teilw. Datenvermeidung und Datensparsamkeit
- Abs. 1 - by Design
Umsetzung der Datenminimierung ist durch technische und organisatorische Mittel sicherzustellen
- Abs. 2 - by Default
Datenverarbeitungsprozesse müssen so voreingestellt sein, dass nur die erforderlichen Daten erhoben werden

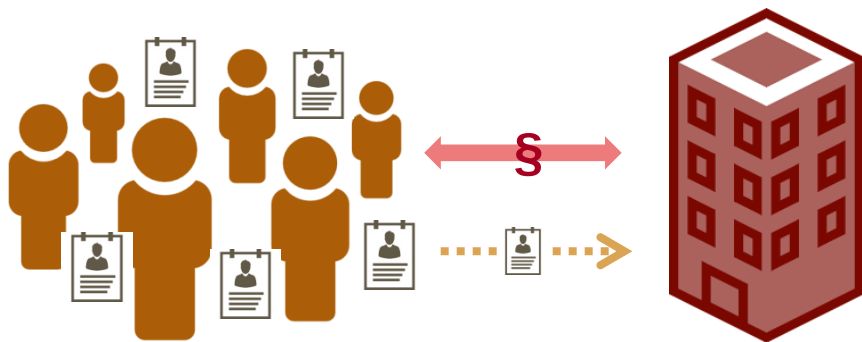


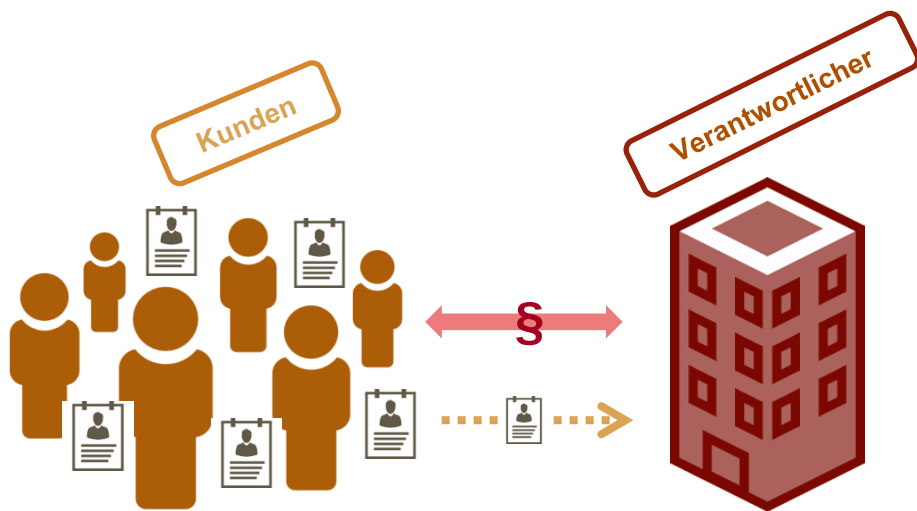
seit September 2018:

TeleTrusT-Arbeitskreis
security by design

DSGVO To-Do's nach Dokumenten 1/2

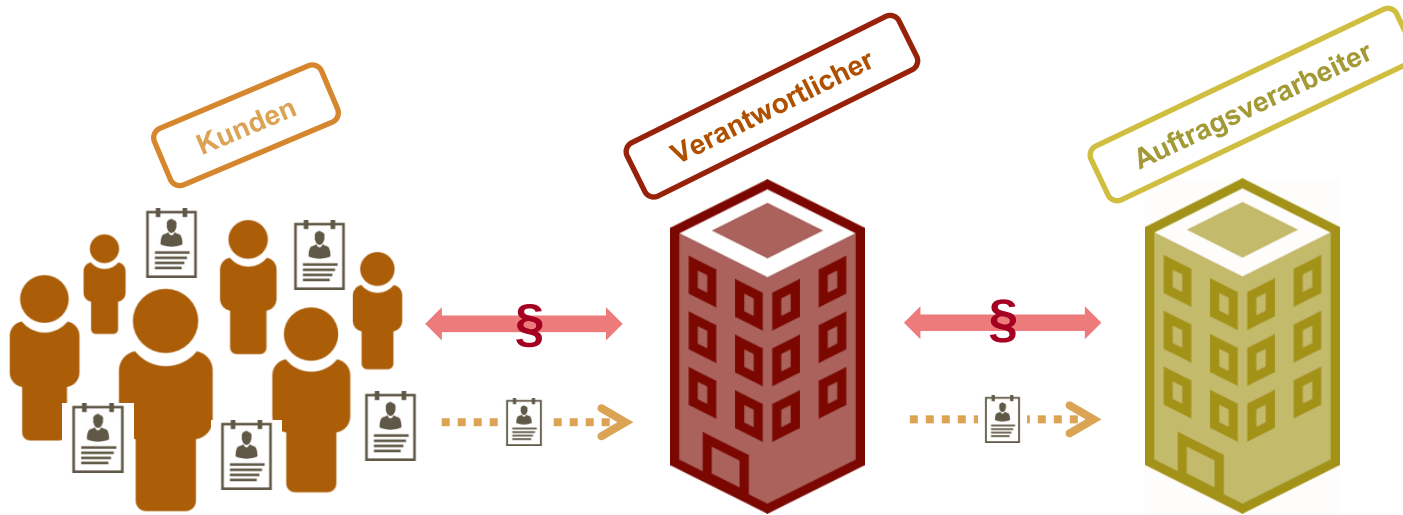
Dokument	Details	DSGVO	h	sichtb.
Verzeichnis von Verarbeitungstätigkeiten	als Verantwortlicher	Art. 30 Abs. 1	+++	-
Verzeichnis von Verarbeitungstätigkeiten (AV)	als Auftragsverarbeiter	Art. 30 Abs. 2	(++)	-
Dokumentation der technischen und organisatorischen Maßnahmen	unternehmensbezogen (100%)	Artt. 32, 5 Abs. 2	+++	-
Dokumentation der technischen und organisatorischen Maßnahmen	leistungsbezogen	Artt. 32, 5 Abs. 2	++	+
Auftragsverarbeitungs-Vereinbarung	AG, AN, neutral	Art. 28	++	+





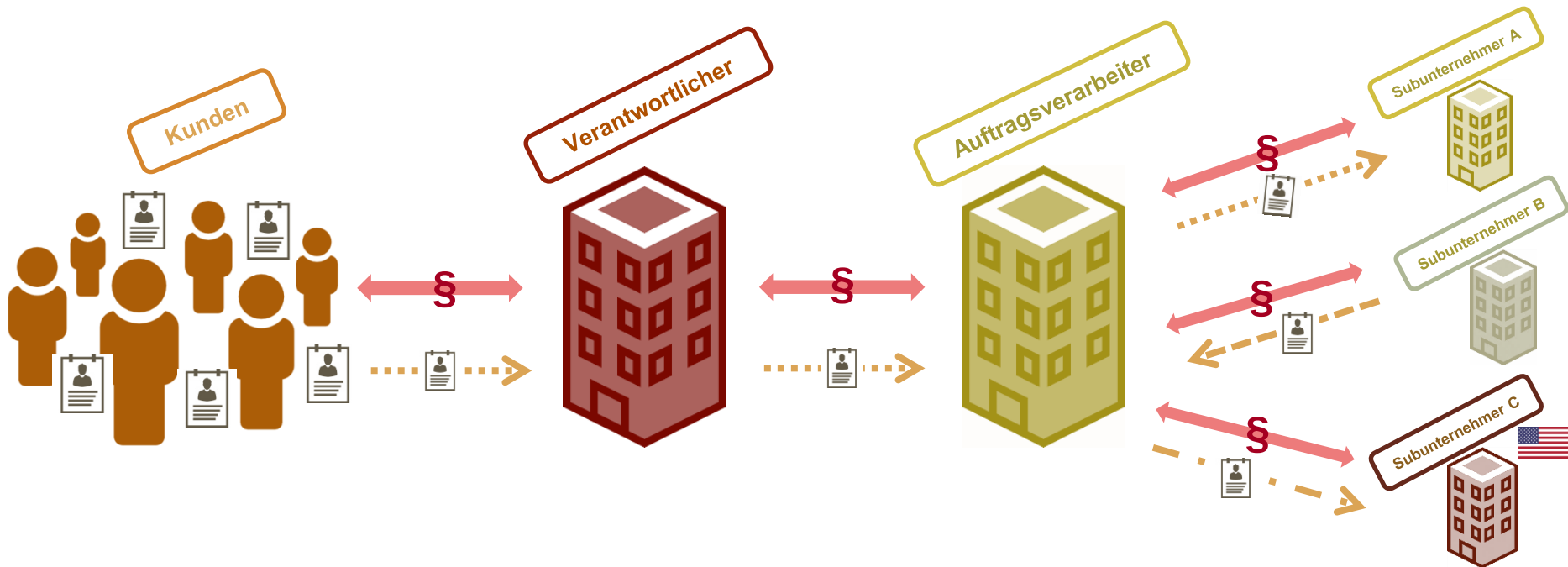
Auftragsverarbeitung

Art. 28 DSGVO



Auftragsverarbeitung mit Unterauftragnehmern

Art. 28 DSGVO



TOM in der Auftragsverarbeitung

§ 9 Satz 1 BDSG i. V. m. Anlage zum BDSG

The image shows a portion of the BDSG Annex form, specifically sections 3, 4, 5, 6, and 7. A large red circle with a diagonal slash is superimposed over the form, indicating that the form is not to be used or is prohibited.

3. Zugriffskontrolle
Es ist zu gewährleisten, dass die Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf ihrer Zugriffsberechtigung beruhenden Daten zugreifen können.

4. Zugangsbeschränkung
☒ Benutzerrechte
☐ Authentifizierung
☐ Identifizierung
☐ Passwort
☐ Benutzername
☐ Zugangsverriegelung
☐ Einsatzzweck
☐ Sicherheit

5. Zugriffskontrolle
Es ist zu gewährleisten, dass Daten von externen Stellen nicht zugänglich sind.

6. Auftragskontrolle
Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nicht entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

7. Verfügbarkeitskontrolle
Daten sind gegen zufällige Zerstörung oder Verlust zu schützen, Maßnahmen zur Datensicherung (Backup-Verfahren, unterbrechungsfreie Stromversorgung, Firewall).

Art. 28 Abs. 3 c) i. V. m. Art. 32 DSGVO

Maßnahmen	Beschreibung (detailliert)

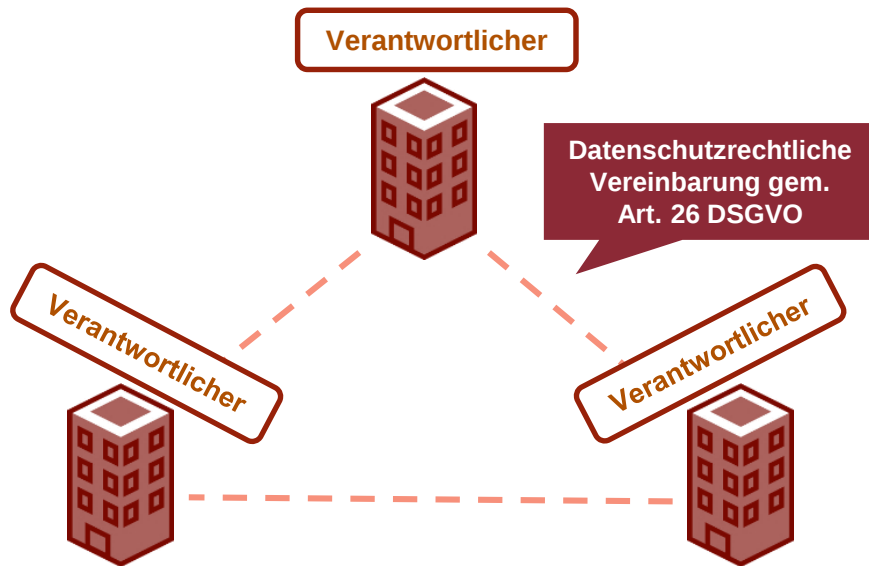
Maßnahmen	Beschreibung	Geeignetheit nach Art. 32 DSGVO

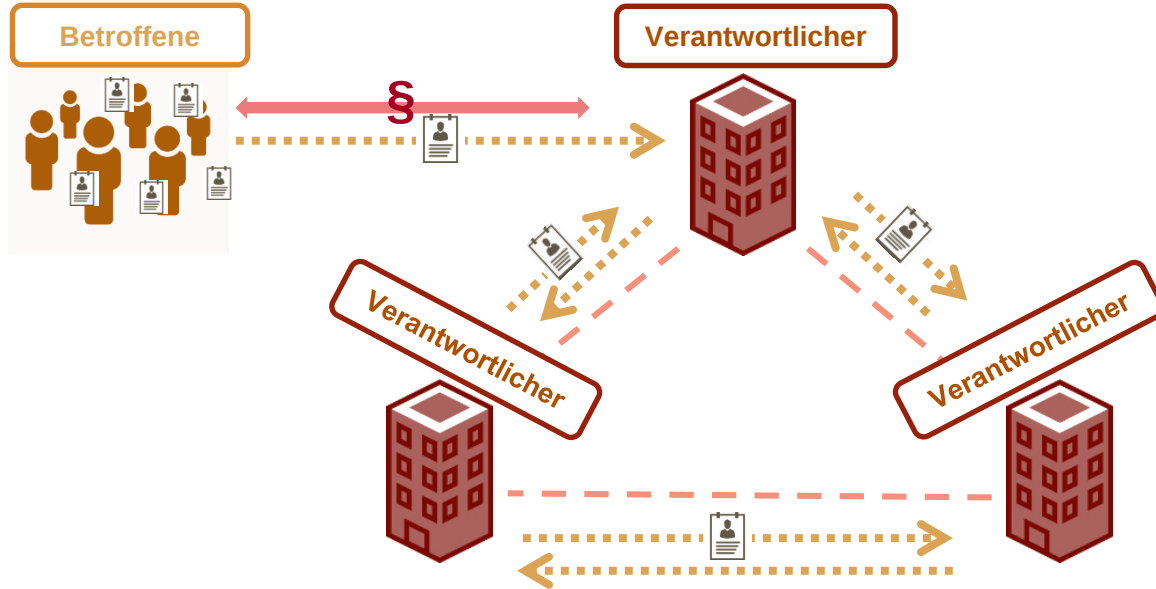
Maßnahmen	Beschreibung	Stand der Technik		Schutzbedarf	Wirksamkeitsprüfung
		objektiv-technisch	subjektive Auswahl		

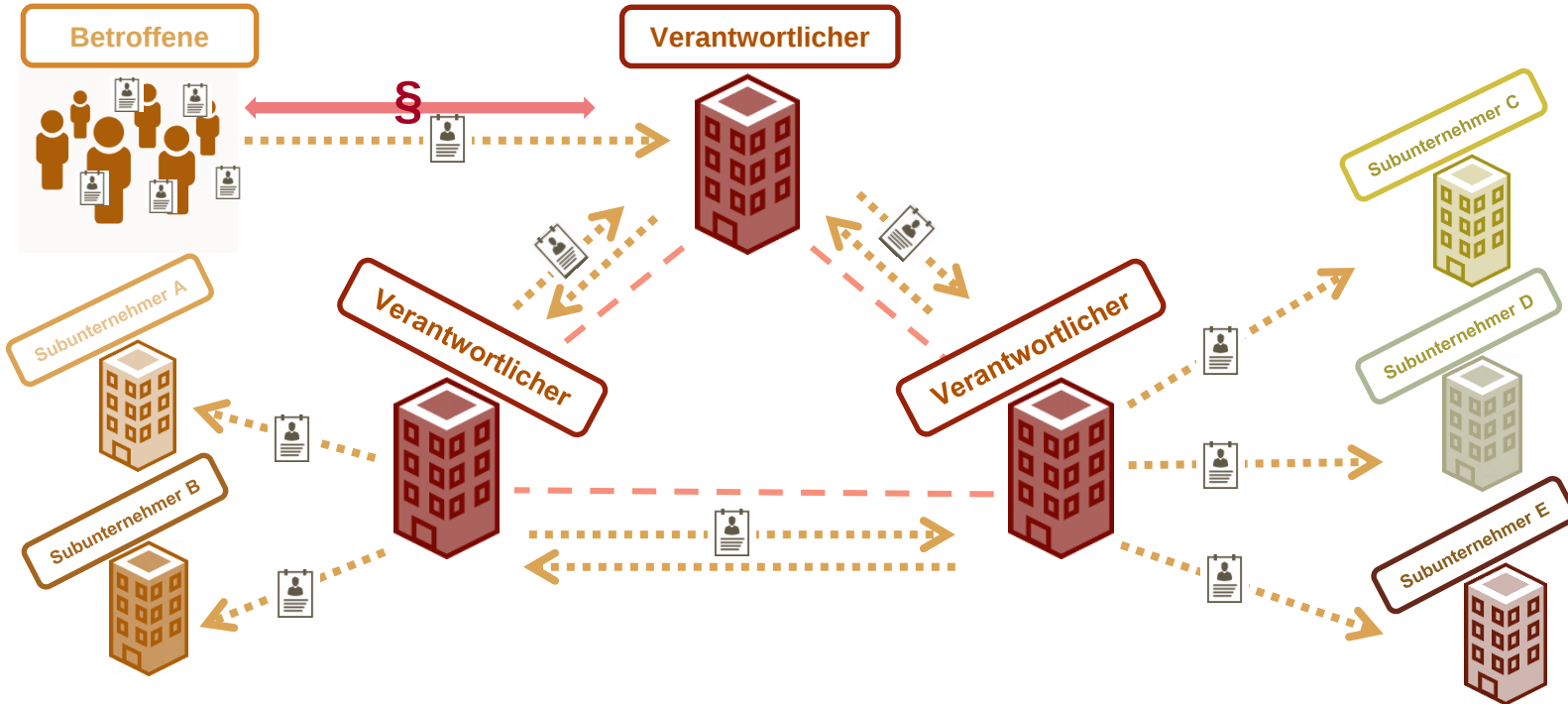
DSGVO To-Do's nach Dokumenten 1/2

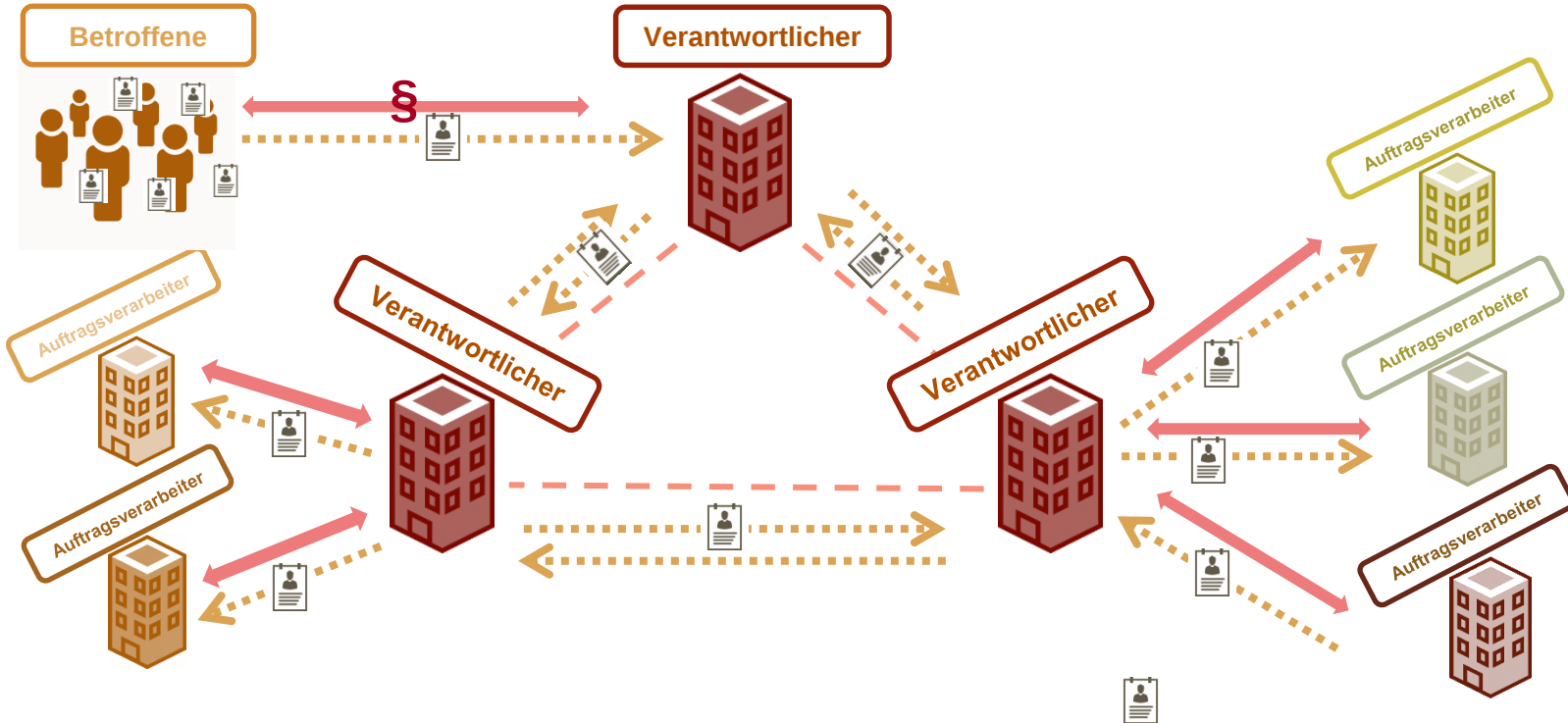
Dokument	Details	DSGVO	h	sichtb.
Verzeichnis von Verarbeitungstätigkeiten	als Verantwortlicher	Art. 30 Abs. 1	+++	-
Verzeichnis von Verarbeitungstätigkeiten (AV)	als Auftragsverarbeiter	Art. 30 Abs. 2	(++)	-
Dokumentation der technischen und organisatorischen Maßnahmen	unternehmensbezogen (100%)	Artt. 32, 5 Abs. 2	+++	-
Dokumentation der technischen und organisatorischen Maßnahmen	leistungsbezogen	Artt. 32, 5 Abs. 2	++	+
Auftragsverarbeitungs-Vereinbarungen	AG, AN, neutral	Art. 28	++	+
Vereinbarung über gemeinsame Verantwortlichkeit	joint controllers	Art. 26	+++	+

Joint Controllers Art. 26 DSGVO









Art. 4 Ziff. 7 DSGVO

Maßgeblich:
Die datenschutzrechtliche
Verantwortlichkeit



Gemeinsam verantwortlich

Beispiele

- Gemeinsamer Aufbau und Nutzen einer Datenbank
 - Adressdaten
 - Unternehmens- oder Behördenportale
- Konzernweite nutzbare Anwendungen
- Gemeinsame Nutzung von IT-Ressourcen
- Industrie 4.0-Anwendungen
- Gemeinsame Studien
- Personalvermittlung bei Bewerber-Pool
- Nutzung von Social Media!

EuGH Urteil vom 05.06.2018

C-210/16

- Betrifft Nutzung von Facebook Fanpage
- Urteil ergang zum alten Recht
- Betreiber von Fanpages müssen lt. Entschließung der Aufsichtsbehörden
 - transparent darüber informieren, wie die Daten verarbeitet werden
 - bei Tracking grundsätzlich eine Einwilligung der User einholen und
 - mit Facebook eine Vereinbarung über die gemeinsame Verarbeitung treffen und deren wesentliche Inhalte den Betroffenen zur Verfügung stellen.
- FB stellt nun „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ zur Verfügung

„Vorlage zur Vorabentscheidung – Richtlinie 95/46/EG – Personenbezogene Daten – Personen bei der Verarbeitung dieser Daten – Anordnung zur Deaktivierung einer Facebook-Seite (Fanpage), die es ermöglicht, bestimmte Daten bezüglich der Besucher dieser Seite zu erheben und zu verarbeiten – Art. 2 Buchst. d – Für die Verarbeitung personenbezogener Daten Verantwortlicher – Art. 4 – Anwendbares nationales Recht – Art. 28 – Nationale Kontrollstellen – Einwirkungsbefugnisse dieser Stellen“

In der Rechtssache C-210/16

betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Bundesverwaltungsgericht (Deutschland) mit Entscheidung vom 25. Februar 2016, beim Gerichtshof eingegangen am 14. April 2016, in dem Verfahren

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

gegen

Wirtschaftsakademie Schleswig-Holstein GmbH,

Beteiligte:

Facebook Ireland Ltd,

Vertreter des Bundesinteresses beim Bundesverwaltungsgericht,

erlässt

DER GERICHTSHOF (Große Kammer)

unter Mitwirkung des Präsidenten K. Lenaerts, des Vizepräsidenten A. Tizzano (Berichterstatter), der Kammerpräsidenten M. Ilesić, L. Bay Larsen, T. von Danwitz, A. Rosas, J. Malenovský und E. Levits, der Richter E. Juhász, A. Borg Barthet und F. Biltgen, der Richterin K. Jürimäe sowie der Richter C. Lycourgos, M. Vilaras und E. Regan,

Generalanwalt: Y. Bot,

Kanzler: C. Strömholm, Verwaltungsrätin,

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 27. Juni 2017,

unter Berücksichtigung der Erklärungen

- des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, vertreten durch Rechtsanwälte U. Karpenstein und M. Kottmann,
- der Wirtschaftsakademie Schleswig-Holstein GmbH, vertreten durch Rechtsanwalt C. Wolff,

Gemeinsam Verantwortlich

Art. 26 DSGVO

- Zwei oder mehr Verantwortliche
- **Gemeinsame Festlegung der Zwecke und der Mittel der Datenverarbeitung**
- Gemeinsame Kontrolle erforderlich
- Keine „Gleichmäßigkeit“ notwendig
- Vereinbarung über die gemeinsame Verantwortlichkeit
- Optionale „Anlaufstelle“

Gemeinsame Mittel

- Technische und organisatorische Maßnahmen
- Es gelten zudem Artt. 5 Abs. 1 f); 24 Abs. 1 und 32 DSGVO
 - Berücksichtigung des Stands der Technik
 - Dokumentation
 - Kontrolle/ Audits
 - Zertifizierungen
 - Kostentragungsregelungen (str.)



Joint-Controllers-Vereinbarungen (JC-V)

Art. 26 DSGVO

Vereinbarung über die
gemeinsame Verarbeitung von Daten mit Personenbezug nach Art. 26 DSGVO
(JC-Vereinbarung)

Zwischen

[Verantwortlicher, Adresse],

- nachfolgend „Verantwortlicher 1“ -

und

[Verantwortlicher, Adresse],

- nachfolgend „Verantwortlicher 2“ -

und

[Verantwortlicher, Adresse],

- nachfolgend „Verantwortlicher 3“ -

wird Folgendes vereinbart:

Anlagen TOM aller Verantwortlicher

Maßnahmen	Beschreibung	Stand der Technik		Schutz- bedarf	Wirksam- keits-
		objektiv-	subjektive		
Maßnahmen	Beschreibung	Stand der Technik		Schutz- bedarf	Wirksam- keits-
		objektiv-	subjektive	bedarf	keits-
Maßnahmen	Beschreibung	Stand der Technik		Schutz- bedarf	Wirksam- keits- prüfung
		objektiv- technisch	subjektive Auswahl		

Inhalt eines JC-Vertrages



Inhalt eines JC-Vertrages

Art. 26 DSGVO

- ✓ Verantwortliche benennen
- ✓ Festlegung der Mittel und Zwecke der Verarbeitung
- ✓ Aufteilung der datenschutzrechtlichen Pflichten, u.a.
 - ✓ Information nach Artt. 13, 14
 - ✓ Auskunft
 - ✓ Berichtigung
 - ✓ Löschung
 - ✓ Datenportabilität
 - ✓ Widerspruch
- ✓ Optional: Anlaufstelle für die betroffenen Personen

Weitere Anforderungen an JC-Vertrag

Art. 26 DSGVO

- ✓ Transparente Form
- ✓ „tatsächliche Funktionen und Beziehungen“ darstellen
- ✓ Veröffentlichungspflicht der wesentlichen Teile des Vertrages.

Informationspflichten

- gegenüber Betroffenen
 - Art. 26 Abs. 2 DSGVO:
Das wesentliche der JC-Vereinbarung
 - Artt. 13, 14 DSGVO
- gemeinsame Verantwortliche untereinander
 - Artt. 13, 14 DSGVO

„Das wesentliche der Vereinbarung“ nach Art. 26 DSGVO

- Was ist wesentlich? Wesentlich für den Betroffenen, die IT-Sicherheit, objektiv-rechtlich ...?
- Zumindest: Bestimmungen über Gewährleistung der Transparenz
- Nicht im Zweifel die JC-Verträge vollständig veröffentlichen!

www.it-sicherheit-und-recht.de

IT-SICHERHEIT UND RECHT
Ihre Experten für IT Security, Compliance und Change Management

BLOG DSGVO IT-SICHERHEITSGESETZ VORTRÄGE PUBLIKATIONEN ANWÄLTE

DSGVO Quick Check

Technischen Datenschutz nach neuem Recht rechtskonform umsetzen ~ wir prüfen Ihren aktuellen Status!

IT COMPLIANCE

DSGVO, BDSG und IT-Sicherheitsgesetz ~ wir sorgen für Compliance!

RISIKO- & CHANGE MANAGEMENT

Für Geschäftsführer: Umfassende Beratung zum IT-Sicherheits- und Datenschutzrecht

ALLES NEU: EU UND IT-SICHERHEIT, IT-SICHERHEITSMASSNAHMEN

Save the date: IT-Sicherheitsrechtstag 2018

EU UND IT-SICHERHEIT, GESETZE UND VERORDNUNGEN

DSFA – Angst essen Seele auf?

HK2 – Der Rote Faden

Karsten U. Bartels LL.M.

Count-up: 150 Tage DSGVO
Updates, Tipps und To Do's rund um die Datenschutz-Grundverordnung

Das Recht auf Abwägung im Einzelfall

Das vom EuGH entwickelte „Recht auf Vergessenwerden“ und das Recht auf Löschung von Art. 17 DSGVO sind nicht gleichzusetzen. Darauf wird jetzt noch einmal das OLG Frankfurt hin, als es über einen datenschutzrechtlichen Lösungsanspruch gegen Google entschieden. Dies wird mit unterschiedlichen Abwägungskriterien begründet.

Ob eine Löschung durch die datenverarbeitende Stelle vorzunehmen ist, ist im Rahmen von Art. 17 DSGVO im Wege einer Abwägung im Einzelfall festzustellen. Dabei sind die Interessen des Betroffenen, mit den Interessen der Öffentlichkeit abzuwägen.

Das „Recht auf Vergessenwerden“ hingegen fordert eine Abwägung dahingehend, ob die Speicherung bzw. öffentliche Zugänglichmachung rechtmäßig war oder sich die ursprünglichen Zwecke und Gründe mittlerweile erledigt haben, also vor allem wenn der Sachverhalt an Aktualität verloren hat. Dabei sollen jedoch grundsätzlich die Rechte des Betroffenen überwiegen.

Unabhängig davon, welches Recht in der Praxis geltend gemacht wird, sollte zunächst eine **einzelfallabhängig** Feststellung erfolgen, ob eine Löschung tatsächlich verpflichtend ist.

Abmahnfähigkeit von DSGVO-Verstößen? Ja! Nein! – Vielleicht!

Größere DSGVO-Abmahnwellen sind bisher ausgeblieben, wohl auch weil bisher unstrittig war, ob bestimmte DSGVO-Verstöße überhaupt durch Mitbewerber abgemahnt werden können. Für fehlerhafte Datenschutzerklärungen war dies zwar bislang anerkannt. Anders als der vorerzählte zugrunde liegende § 13 TKG stellt die DSGVO nun aber eine umfassende Regelung mit eigenen Sanktionsmöglichkeiten dar, die insoweit von zahlreichen Experten als abschließend angesehen wird. Dazu wäre ein Vorgehen den Aufsichtsbehörden vorbehalten. Nach und nach landet die Frage nun auch vor den Gerichten, ohne dass hierdurch allerdings die Lage entscheidend erhellbar würde. Den Anfang machte das LG Würzburg, das die **Abmahnfähigkeit** mit Verweis auf die Rechtsprechung zu § 13 TKG bejahte, jedoch ohne sich inhaltlich mit der zentralen Problematik der abschließenden Regelung auseinanderzusetzen. Kurz darauf sah das LG Bochum die Frage genau entgegengesetzt und bezog zudem eindeutig Stellung: Neben der DSGVO ist kein Platz für das Wettbewerbsrecht und darauf gestützte Abmahnungen. In der Streitfrage steht es somit 1:1, allerdings nach klarem Abschieß des LG Würzburg.

Merlin Backes, LL.M. (Glasgow)

Michael Schramm Schramm,

www.hk2.eu/newsletter

Material

- Bartels/ Backer, Die Berücksichtigung des Stands der Technik in der DSGVO, DuD 4-2018, 214.
- Bartels/ Backer/ Schramm, Der „Stand der Technik“ im IT-Sicherheitsrecht, Tagungsband zum 15. Deutschen IT-Sicherheitskongress 2017, Bundesamt für Sicherheit in der Informationstechnik, 503.
- Bartels/ Schramm: Neue Anforderungen zum technischen Datenschutz nach der Datenschutz-Grundverordnung, BvD-News, 2017(1), 22-23.
- Bartels, Folgen des IT-Sicherheitsgesetzes für Telemedienanbieter – Umsetzung und Beauftragung von IT-Sicherheitsmaßnahmen nach Telemediengesetz, iX Heise, VI/ 2016.
- Bartels/ Backer, ITSiG-konforme Telemedien – Technische und organisatorische Vorkehrungen nach § 13 Abs. 7 Telemediengesetz, DuD, 40(1), 22.
- Bartels, Das IT-Sicherheitsgesetz – Folgen für Haftung und Vertragsgestaltung, ihk.wirtschaft, 12-2015, 14.
- Bartels, Das neue IT-Sicherheitsgesetz (ITSiG) – Umsetzung im Unternehmen, <kes> 2015, Heft 5, 30.
- Bartels: Bezugspunkte des IT-Sicherheitsgesetzes – Weichenstellungen einer nationalen Gesetzesinitiative, itbr, 4/2015, 92.

Haben Sie Fragen?



HK2
Rechtsanwälte

HK2
Rechtsanwälte

Rechtsanwalt

Karsten U. Bartels LL.M.

Hausvogteiplatz 11 A
10117 Berlin

Telefon +49 (0)30 27 89 00-0
Telefax +49 (0)30 27 89 00-10
E-Mail bartels@hk2.eu

www.hk2.eu

www.hk2.eu

www.comtection.de