Datenschutz auch für KMU?

Wie löst man Datenschutzanforderungen in kleineren Betrieben insbesondere bei geringen Ressourcen.

Herangehensweise aus Sicht eines externen Datenschutzbeauftragten.

Manfred Beth

Datenschutzrecht in der Praxis | 21.06.2017 | Saarbrücken

UIMC Dr. Vossbein GmbH & Co KG | Nützenberger Straße 119 | 42115 Wuppertal
Tel: 0202 / 265 74 - 0 | Fax: 0202 / 265 74 - 19 | E-Mail: consultants@uimc.de | Internet: www.UIMC.de

Manfred Beth

UIMC®

- Berater der UIMC Dr. Vossbein GmbH & Co KG, Wuppertal
- Geschäftsstellenleiter Saarbrücken
- GDD-Erfa-Kreis-Leiter Saarland/Pfalz
- 2004 eine Ausbildung zum Datenschutzbeauftragten nach dem Ulmer Modell
- 2005 Betriebswirtschaft an der Wirtschaftakademie in Blieskastel.
- Diplomarbeit: „Datenschutz und Datensicherheit bei fortschreitender Technik“:
- Mehrjähriger Tätigkeit als betrieblicher Datenschutzbeauftragter in einer Reha-Klinik.
- Seminarleiter bei Ausbildungsgängen zum Thema Datenschutz im Gesundheitswesen.

Unternehmensgruppe

UIMC®

UIMC®
Dr. Vossbein Betriebs-GmbH

UIMC®
Dr. Vossbein
GmbH & Co KG

UIMC austria

UIMCollege®

UIMCert®
GmbH

akkreditiert durch:

DAkkS
Deutsche
Akkreditierungsstelle
D-ZM-17294-01-01

Datenschutz-Gütesiegel Schleswig-Holstein
Beim ULD anerkannte sachverständige Prüfstelle für IT-Produkte (rechtlich / technisch)

Dienstleistungen der UIMC

Datenschutz

Von einzelnen Stellungnahmen und Tools bis zur Übernahme der externen Datenschutzbeauftragung

Informationssicherheit

Aufbau eines Informationssicherheits-Managementsystems bis zur Zertifizierungsreife

Organisations- / Strategie-Beratung

Beratungsleistungen in konzeptionellen und strategischen Fragestellungen

- Analyse / Auditierung
- Planung & Beratung
- Konzept-Erarbeitung
- Schulung & Sensibilisierung
- Umsetzung (mit Tools)

Agenda

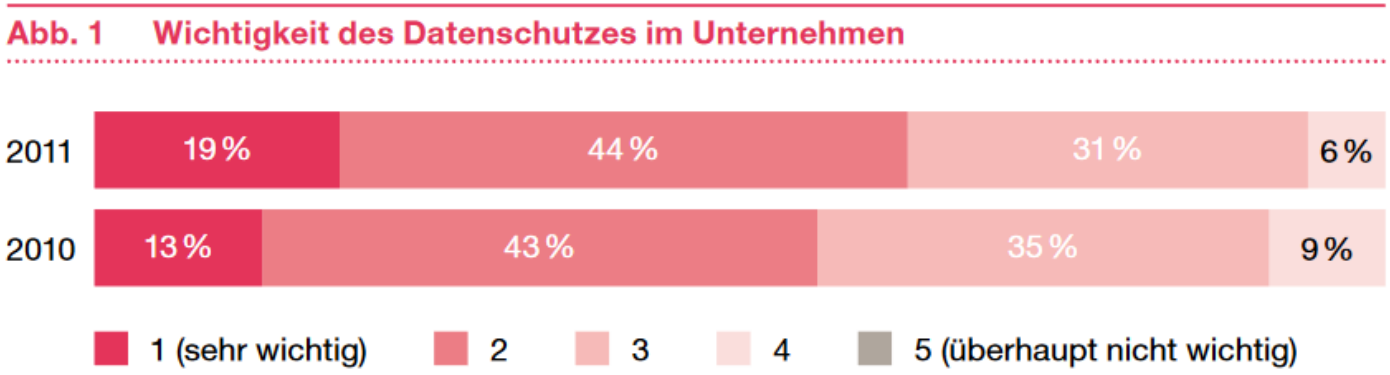
- Datenschutz?
- Datenschutzbeauftragter
  - Aufgaben
  - Umsetzung
  - Intern - Extern
- Change zur EU-DSGVO
  - Change Organisation
- Diskussion

Datenschutz?

„Datenschutz ist für den Erfolg unserer Geschäftstätigkeit schon heute von grundlegender Bedeutung. Ich bin mir sicher, dass die Bedeutung mit der weiteren Entwicklung der Online-Medien zukünftig erheblich zunehmen wird.“

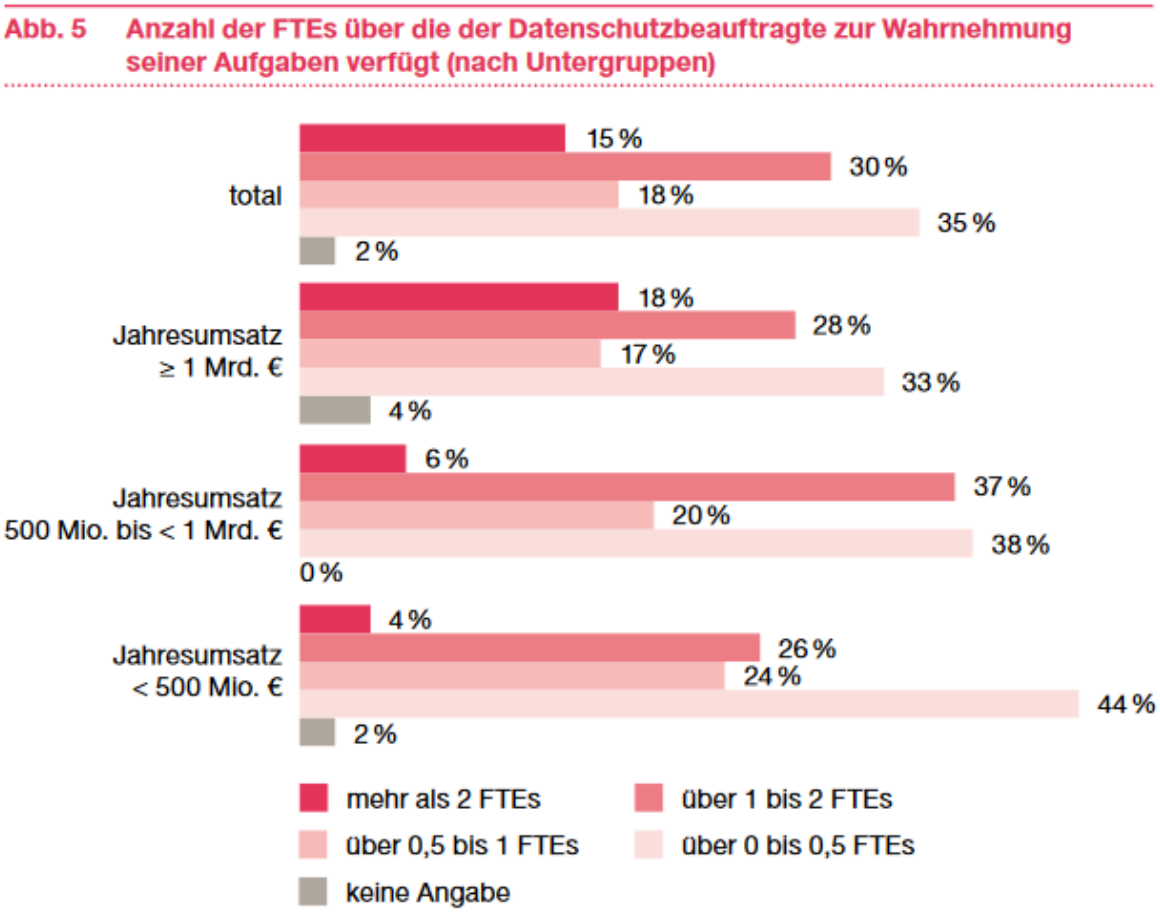
Dr. Claus-Dieter Ulmer, Konzernbeauftragter für den Datenschutz, Deutsche Telekom AG

Datenschutz?



pwc.de/de/compliance/assets/pwc_studie_datenschutz_2011.pdf

Datenschutz?



pwc.de/de/compliance/assets/pwc_studie_datenschutz_2011.pdf

Datenschutz heute

UIMC®

Deutsche Firmen schludern beim Datenschutz

Heute in genau einem Jahr muss die Datenschutzgrundverordnung in ganz Europa angewendet werden. Dieses neue Gesetz bringt für Unternehmen viele Neuerungen und einige zusätzliche Pflichten mit sich. Allerdings sind die Firmen schlecht vorbereitet - deutsche Betriebe machen da keine Ausnahme.

Problem erkannt - Problem ignoriert, so könnte man die Ergebnisse einer repräsentativen Studie zusammenfassen, die der Software-Anbieter Varonis in Auftrag gegeben hatte. Dabei empfanden es 81 Prozent der deutschen Unternehmen als Herausforderung, die neuen Regelungen des europäischen Datenschutzgesetzes im eigenen Betrieb umzusetzen.

Gleichzeitig stehen die nötigen Maßnahmen bei 58 Prozent der Firmen nicht oben auf der Prioritätenliste, man versucht sich also wegzuducken. Und dieser Trend zeigt sich bei deutschen Unternehmen deutlicher als in anderen Ländern.

B5 Wirtschaft am 25.5.2017 in B5 aktuell

Datenschutzbeauftragter (DSB)

Art. 37 DS-GVO i.V. § 38 BDSG (– neu) und auch nach § 4f BDSG

Schriftliche Bestellung

10 Beschäftigte verarbeiten pb Daten

(dies ist bspw. schon dann erreicht, wenn diese Mitarbeiter einen E-Mail-Account haben).

Meldung an die Aufsichtsbehörde Art 37 (7) DS-GVO

Art. 37 DS-GVO

(5) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.

Erwägungsgrund 97

…Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die von dem Verantwortlichen … verarbeiteten personenbezogenen Daten richten.

DSB

- zur Erfüllung der Aufgaben erforderliche Fachkunde und Zuverlässigkeit.
- Die fachliche Eignung muss kontinuierlich durch Fortbildungen aufgebaut und aufrecht erhalten werden.
- Juristische Kenntnisse – nicht nur BDSG
- Unternehmenskenntnisse - Betriebsstruktur
- Betriebswirtschaftliche Kenntnisse – Orga, HR, QM usw.
- DV / IV Kenntnisse – Technik, Betriebssystem, Anwendersoftware

Umfassende Aufgaben I

- Aufbau einer Datenschutz-Organisation mit entsprechenden Prozessen und Richtlinien
- Information und Beratung der Geschäftsführung
- Prüfung der Rechtmäßigkeit der Datenverarbeitung
- Beratung der Mitarbeiter und Fachbereiche
- Überwachung der ordnungsgemäßen Anwendung der EDV
- Schulung und Sensibilisierung der Mitarbeiter
- Überwachung der Übersicht der verwendeten Verfahren (Verfahrensverzeichnis)

Umfassende Aufgaben II

- Prüfung/Auditierung der Dienstleister (Auftragsdatenverarbeitung)
- Hinwirken auf Einhaltung der technisch-organisatorischen Maßnahmen unter Berücksichtigung der Angemessenheit
- Durchführung einer Vorabkontrolle – Beratung bezüglich der Datenschutzfolgenabschätzung
- usw.

Wer kann das alles erfüllen?

Kompetenz und Ressourcen

Die Zuverlässigkeit des Datenschutzbeauftragten bereitet zumeist Probleme, da eine Interessenkollision in vielen Fällen gegeben ist.

Geschäftsführer, Personalleiter, IT-Leiter und Vertriebs-/Marketingleiter und Betriebsräte

Lassen sich Interessen und Aufgaben mit den Tätigkeiten des Datenschutzbeauftragten vereinbaren und sich selbst kontrollieren?

Sie dürfen per Gesetz nicht bestellt werden.

Intern - Extern

- „Der Prophet im eigenen Land“ wird oftmals nicht erhört. Deshalb kann ein Externer in der Regel unvoreingenommener an Fragestellungen herangehen und notwendige Maßnahmen vorantreiben kann.
- Auch wenn die gesetzliche Basis in Form der datenschutzrelevanten Gesetze (bspw. BDSG) für alle Unternehmen generell gleich ist, so erfordert die Umsetzung eine jeweils passende Lösung. Gerade in kleinen und mittleren Unternehmen (KMU), deren Kerngeschäft nicht maßgeblich durch den Datenschutz beeinflusst wird, sind angemessene Lösungen notwendig.

Die „Low-Budget-Idee“

Im Outsourcing sind die Vor-Ort-Leistungen des beratenden Unternehmens die teuersten Leistungen. Es ist aus Effizienzgründen Ziel, diese Leistungen zu reduzieren.

Durch Nutzung

- moderner Kommunikationstechniken,
- standardisierter Organisationsmittel mit Best Practice
- computergestützter Verfahren und Tools (z. B. für die Analyse und Schulung)
- werden hoch individuelle und Vor-Ort-Leistungen reduziert und optimiert.

Vorgehensweise

Analyse der Ist-Situation
(unter KMU-Bedingungen)

Etablierung eines Konzepts
(u. a. Handbuch und Richtlinien)

Schulung und Sensibilisierung
(z. B. mittels eCollege)

Umsetzung
(u. a. mit Hilfe von Tools)

(jährliche) Revision
und laufende Betreuung

Analyse der Ist-Situation

Analyse-Tools für Anforderungen an Datenschutz und/oder Informationssicherheit

Schwachstellenanalyse zur Bewertung der Ist-Situation

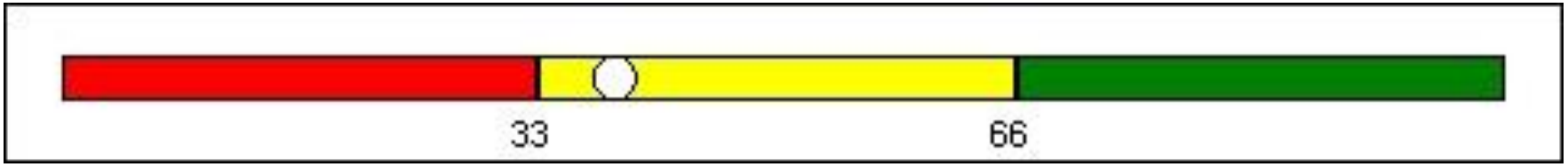
Prüfungsinhalte

- Gesetzlichen Anforderungen an den Datenschutz
- Zulässigkeitsfragestellungen, technische und organisatorische Maßnahmen etc.
- Informationssicherheit
- Sensibilisierung der Geschäftsführung und der Mitarbeiter

Status-Quo

Status-Quo-Bericht mit Positiv- und Negativbefunden

Kunden-Datenschutz



Es werden personenbezogene Daten sowohl von Privatkunden als auch von Geschäftspartnern verarbeitet, wie bspw. Informationen zu den Ansprechpartnern bei Lieferanten, Kunden o. ä.

Es wird nicht geprüft, ob die Datenerhebung dem Grundsatz der Datenvermeidung und Datensparsamkeit genügt.

Maßnahmenkatalog

UIMC®

ischenablage | Schriftart | Ausrichtung | Zahl | Formatvorlagen | Zellen | Bearbeiten

312 fx

	A	B	C	D	E	G	H	I	J	
1	Kapitel		Empfehlungen							Umsel
2	Nr.	Name	Maßnahmen / Anforderungen	Veran	DS/	Pric	Frist	Bemerkung [bei Erhebung]	Datum	Anmerkung
41	4.5.1	Anwendungsbereich des TKG	Es ist ein Verbot zur privaten Nutzung der Telekommunikationseinrichtungen (E-Mail, Internet, Telefon etc.) explizit zu erteilen und dies ist auch zu kontrollieren.	GF	DS	1		BV		
44	4.5.2	Gast-Netzwerke	Der Zugang zu diesem Gast-WLAN ist zu schützen.	EDV	DS	DSC			11.04.2017	
45	4.5.2	Gast-Netzwerke	Es sind weitere Maßnahmen zu ergreifen, die die Mitstörerhaftung durch Rechtsverstöße durch die Nutzer des Gast-WLANs reduzieren.	EDV	DS	DSC		Formblatt	11.04.2017	
47	4.5.3	Fernmeldegeheimnis	Die Geschäftsleitung hat eine Verpflichtungserklärung bezüglich des Fernmeldegeheimnisses aufsetzen zu lassen.	HR	DS	DSC			11.04.2017	
54	5.1.2	Angemessenheit und Risikobewertung	Es sind geeignete technische und organisatorische Sicherheitsmaßnahmen zur Datensicherheit zu treffen.	EDV	DS	DSC			11.04.2017	
56	5.1.3	Datenschutz durch Technik	Es ist durch interne Vorgaben verbindlich festzulegen, durch technische und organisatorische Maßnahmen die Grundsätze des Datenschutzes durch Technik (privacy by design) und durch datenschutzrechtliche Voreinstellungen (privacy by default) einzuhalten.	EDV	DS	2				
57	5.1.3	Datenschutz durch Technik	Personenbezogene Daten sind so schnell wie möglich zu pseudonymisieren.	EDV	DS	3				
59	5.1.4	Datenschutz-Folgeabschätzung	Es ist sicherzustellen, dass vor dem Beginn einer Datenverarbeitung geprüft wird, ob aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht.	EDV	DS	1				
	5.1.4	Datenschutz-Folgeabschätzung	Hierbei ist eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten	EDV	DS	1				

Change I

- Umstellung vom BDSG zur DS-GVO
- erhebliche Erweiterung der Anforderungen an die IT-Sicherheit mit umfassender Risikobetrachtung/-bewertung
- erheblich erweiterte Informations- und Auskunftspflichten zugunsten der Betroffenen
- neue Anforderungen an die Auftragsdatenverarbeitung
- erweiterter Pflichtenumfang des Auftragnehmers (insb. gesamtschuldnerische Haftung von Auftraggeber und Auftragnehmer bei Pflichtverletzungen)

Change II

- Gemeinsam für die Verarbeitung Verantwortliche als neue Form der Zusammenarbeit mit insbesondere formalen (vertraglichen) Anforderungen
- erheblich erweiterte Meldepflichten bei Datenpannen
- erheblich erweiterte Rechenschafts- und Dokumentationspflichten
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Vorsteinstellungen (data protection by design / data protection by default)
- Formalisierung hinsichtlich der Datenschutz-Folgenabschätzung (bisher Vorabkontrolle)

Change III

- Analyse
- Selbstauskunftsbogen und Checklisten, zur Prüfung der aktuellen Organisation und der vorliegenden Unterlagen auf EU-Konformität.
- Planung
- Auf Basis der Erkenntnisse der o. g. Analyse-Phase können Maßnahmen geplant werden.
- Maßnahmenplan und Muster-Konzepte

Change IV

- Umsetzung
- Datenschutzhandbuch und die Schulungsmedien an die neuen Anforderungen anpassen
- neue oder aktualisierte Muster und Vordrucke ein (beispielsweise zur Erfüllung der Informationspflichten oder Einwilligungserklärungen).
- Revision
- Maßnahmen nachhalten.

Change Selbstauskunft

	Etablierung			UIMChange (Ziel: 25.05.2018)							Revision					
	Erstellung des Dokuments	Verantwortlicher	Frist	Nicht relevant (bitte begründen)	Sichtung der Dokumente	Anpassung an neue EU-Anforderungen	Verbindliche Verabschiedung	Kommunikation an Mitarbeiter	Erstellung des Revisionskonzepts	Verantwortlicher	Frist	Dokumentation der Umsetzung	Prüfung der Umsetzung	Prüfung der Wirksamkeit (ggf. Anpassung)	Verantwortlicher	Frist	Bemerkungen
ien / Konzepte / Prozessanweisungen	erledigte Aufgaben sind mit "ok" zu kennzeichnen																
nschutzkonzept/-handbuch	ja	-	erledigt	-						DSB					GF		siehe Anhang - Datenschutzhandbuch -, Für jeden einsehbar in unserem D.wiki
flichtung der Mitarbeiter auf das Datengeheimnis	ja	-	erledigt	-						DSB					HR		Verhaltenskodex und Arbeitsverträge
dlinien/Arbeitsanweisungen zur Nutzung der IT und der Daten	ja	-	Prüfung	-						DSB					HR		Durch neue Arbeitsverträge abgedeckt - muss das auch in die alten Verträge?
ulung der Mitarbeiter	ja	-	Prüfung	-						DSB					HR		Im Moment für der Betriebsrat die Selbstschulung Datenschutz durch - dann kommt nach und r
illigungen in die Datenverarbeitung durch den Betroffenen	ja	-	Prüfung	-						DSB					AL		Durch Arbeitsverträge abgedeckt, evtl. auch durch BV
ebsvereinbarungen	ja	-	erledigt	-						DSB					HR		Eine BV vorhanden - siehe Anhang
mationen der Betroffenen über Datenverarbeitung	ja	-	Prüfung	-						DSB					AL		Durch Arbeitsverträge abgedeckt, Jedox? BV noch in Arbeit
sifizierung von Informationen / Klassifizierungsschema	ja	-	erledigt	-						DSB					GF		siehe Anhang
etzung der Rechte der Betroffenen und Transparenz der Datenverarbeitung	nein	DSB		-						DSB					GF		Teilweise
ung der Datenverarbeitung	nein	DSB		-						DSB					DSB		ISO-Audit?
ung des internationalen Datentransfers (außerhalb der EU/EWR)	nein	DSB		-						DSB					DSB		Prüfung (ohne Regelung) intern - Google
ehrensübersicht	nein	GF		-						DSB					AL		
tionssicherheit	erledigte Aufgaben sind mit "ok" zu kennzeichnen																
icherheitskonzept/-handbuch	nein	EDV		-						DSB					EDV		Vorlage vorhanden
ware-Abwehr																	
Malware-Konzept (Viren, Trojaner etc.)	nein	EDV		-						DSB					EDV		gelebte Praxis
Patch- und Update-Management	nein	EDV		-						DSB					EDV		
kup-Konzept (Datensicherung, Wiederherstellungsverfahren etc.)	ja	-	erledigt	-						DSB					EDV		
all-Konzept/Notfallhandbuch (Business Continuity / Business Recovery)	nein	EDV		-						DSB					EDV		evtl. teilweise in Backup-Konzept vorhanden
ttskonzept (Bauliche Sicherungen, Zutrittskontrolle, Besucherregelungen etc.)	nein	FM		-						DSB					EDV		Zutrittskontrolle vorhanden
angskontrolle																	
Berechtigungskonzept	nein	EDV		-						DSB					EDV		In Accenon dokumentiert, sonst nicht

Hinweise und Stammdaten | Selbstauskunft | Dienstleister | Maßnahmenkatalog

EREIT 70 %

Change Organisation I

	KMU	Nicht-KMU	Maßnahmen-Gruppe	Maßnahmen	notwendiger Input	Frist	Netto-Arbeitstage (bis Frist)	Planungskollision	kritischer Meilenstein	Netto-Arbeitstage (bis krit. Meilenst	Bearbeit	
4												
5	x	x	Selbstauskunftsbogen	Klärung: Selbstauskunftsbogen oder Datenschutz-Checkup	Datum letzter DSC:	13.05.2013						Selb
6	x		Selbstauskunftsbogen	Versand		05.02.2017	-93	31.03.2017	-54		ok	
7	x		Selbstauskunftsbogen	Nachfass beim Kunden und Rücksendung (Deadline)		16.04.2017	-43	30.06.2017	13		ok	
8	x		Selbstauskunftsbogen	Auswertung		06.03.2017	-73	28.07.2017	33		ok	
9	x		Selbstauskunftsbogen	Versand des Maßnahmenkatalogs		20.03.2017	-63	28.07.2017	33		ok	
10	x		Selbstauskunftsbogen	Besprechung (während Revisionsbesuch)		13.04.2017	-45	31.12.2017	143		ok	
17	x	x	Handbuch	Überarbeitung	DSC-Bericht	22.07.2017	28	30.10.2017	99			
20	x	x	Handbuch	Verabschiedung durch Geschäftsführung		14.10.2017	88	28.02.2018	186	DSAP / GF		
21	x	x	Handbuch	Veröffentlichung / Kommunikation an Mitarbeiter			###	25.05.2018	248	DSAP / HR		
22	x	x	Richtlinien/Anweisungen	Anforderung der Unterlagen			###	30.05.2017	-12			
23	x	x	Richtlinien/Anweisungen	Prüfung Änderungsbedarf			###	30.09.2017	78			
24	x	x	Richtlinien/Anweisungen	Überarbeitung	DSC-Bericht	22.07.2017	28	30.10.2017	99			
30	x	x	Begleitende Dokumente	Überarbeitung der Einwilligungen			###	31.12.2017	143			
32	x	x	Begleitende Dokumente	Überarbeitung der Datenschutzerklärung (Informationspflicht)			###	31.12.2017	143			
34	x	x	Begleitende Dokumente	Überarbeitung der Verfahrensübersicht			###	30.04.2018	229			
36	x	x	Begleitende Dokumente	Überarbeitung der ADV-Verträge			###	31.12.2017	143			

... Kunden | Status | Status_krit | 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Change Organisation II

Anforderung der Unterlagen
Prüfung Änderungsbedarf
Überarbeitung
Abstimmung mit Fachbereichen
Abstimmung mit Betriebsrat
Verabschiedung durch Geschäftsführung
Veröffentlichung / Kommunikation an Mitarbeiter
Anforderung der Einwilligungen
Überarbeitung der Einwilligungen
Anforderung der Datenschutzerklärung (Informationspflicht)
Überarbeitung der Datenschutzerklärung (Informationspflicht)
Anforderung der Verfahrensübersicht
Überarbeitung der Verfahrensübersicht
Anforderung der ADV-Verträge
Überarbeitung der ADV-Verträge
Abstimmung mit Fachbereichen und ggf. Betriebsrat
Verabschiedung durch Geschäftsführung
Veröffentlichung / Kommunikation an Mitarbeiter
Etablierung eines Revisions-/Auditskonzepts
Etablierung von Meldewegen
Abstimmung mit Fachbereichen und ggf. Betriebsrat
Verabschiedung durch Geschäftsführung
Veröffentlichung / Kommunikation an Mitarbeiter

Diskussion - Fragen

Haben Sie noch Fragen?

UIMC Dr. Vossbein GmbH & Co. KG
Nützenberger Straße 119
42115 Wuppertal
Telefon: (0202) 265 74 - 0
Telefax: (0202) 265 74 - 19
E-Mail: consultants@uimc.de
Internet: www.UIMC.de

UIMCert GmbH
Moltkestraße 19
42115 Wuppertal
Telefon: (0202) 3 09 87 39
Telefax: (0202) 3 09 87 49
E-Mail: certification@uimcert.de
Internet: www.UIMCert.de

akkreditiert durch:

Datenschutz-Gütesiegel Schleswig-Holstein
Beim ULD anerkannte sachverständige Prüfstelle für IT-Produkte (rechtlich / technisch)

DAkkS
Deutsche Akkreditierungsstelle
D-ZM-17294-01-01