DMC DATENSCHUTZ MANAGEMENT & CONSULTING

UpDate! Datenschutz by Esturias

Zusammenarbeit mit Dienstleistern und Auftragsverarbeitung

GRUNDSÄTZE DER AV, ABGRENZUNGSFRAGEN, VERTRAGSGESTALTUNG

DMC DATENSCHUTZ MANAGEMENT & CONSULTING

Thomas Müthlein

Seit 1990 im Datenschutz tätig: Geschäftsführer der GDD, Konzern-DSB, zertifizierter DSB (GDD), Datenschutzberater, Fach-Autor und Referent

Mitglied des Vorstandes der GDD mit den Schwerpunkten Datenschutzpraxis, Outsourcing, Internationaler Datentransfer und Recht bei Telekommunikations- und Multimediaeinsatz

Geschäftsführer der DMC Datenschutz Management & Consulting GmbH & Co. KG – Datenschutzberatung und -auditierung

Zertifizierter Datenschutzauditor (DSZ) zur Auditierung nach dem Datenschutzstandard für die Auftragsdatenverarbeitung DS-BvD-GDD-01

06.12.2018 © Th. Müthlein

Grundsätze der AV, Abgrenzungsfragen, Vertragsgestaltung

DMC DATENSCHUTZ MANAGEMENT & CONSULTING

Bayerisches Landesamt für Datenschutzaufsicht

BayLDA Aktuelles Online-Services Themen Veröffentlichungen Unsere Behörde Suche...

Themen > Datenschutzprüfungen

Datenschutzprüfungen

Datenschutzverletzungen bei (Unter-)Auftragverarbeitern Status: Anstehend

Start: offen Ende: offen

Kurzbeschreibung	Die DS-GVO hat die Meldeschwelle für sogenannte "Datenpannen" an das Risiko für die natürlichen Personen angepasst, das sich aus einer Verletzung der Sicherheit ergibt. Dies führte zu einer deutlichen Zunahme der Meldungen nach Art. 33/34 DS-GVO beim BayLDA. Auffallend bei den Meldungen ist bislang, dass die Ursache des Risikos fast ausschließlich beim Verantwortlichen in Bayern liegt. Da nach der DS-GVO allerdings auch Verletzungen der Sicherheit bei Dienstleistern (sogar bei weiterer Unterauftragvergabe) für die Verantwortlichen eine Meldeverpflichtung auslöst, stellt sich dem BayLDA die Frage, wieso es kaum Meldungen gibt, die von (internationalen) Dienstleistern ausgelöst werden. Die Prüfung soll diese Fragestellung erhellen und beschäftigt sich mit dem "Incident Response" bei den größeren und datengetriebenen Unternehmen.
Prüfgrundlage	Art. 33 DS-GVO Art. 34 DS-GVO Art. 28 DS-GVO
Zielgruppe	Größere und Datengetriebene Unternehmen mit (vermutlich) vielen Dienstleistern im internationalen Umfeld
Auswahlkriterien	Manuelle Auswahl von Unternehmen, bei denen von einer größeren Anzahl (internationaler) Auftragsverarbeitungen auszugehen ist.
Anzahl der geprüften Unternehmen	15
Vor-Ort-Kontrolle geplant bei	7

06.12.2018 © Th. Müthlein

DMC DATENSCHUTZ MANAGEMENT & CONSULTING

Inhalt

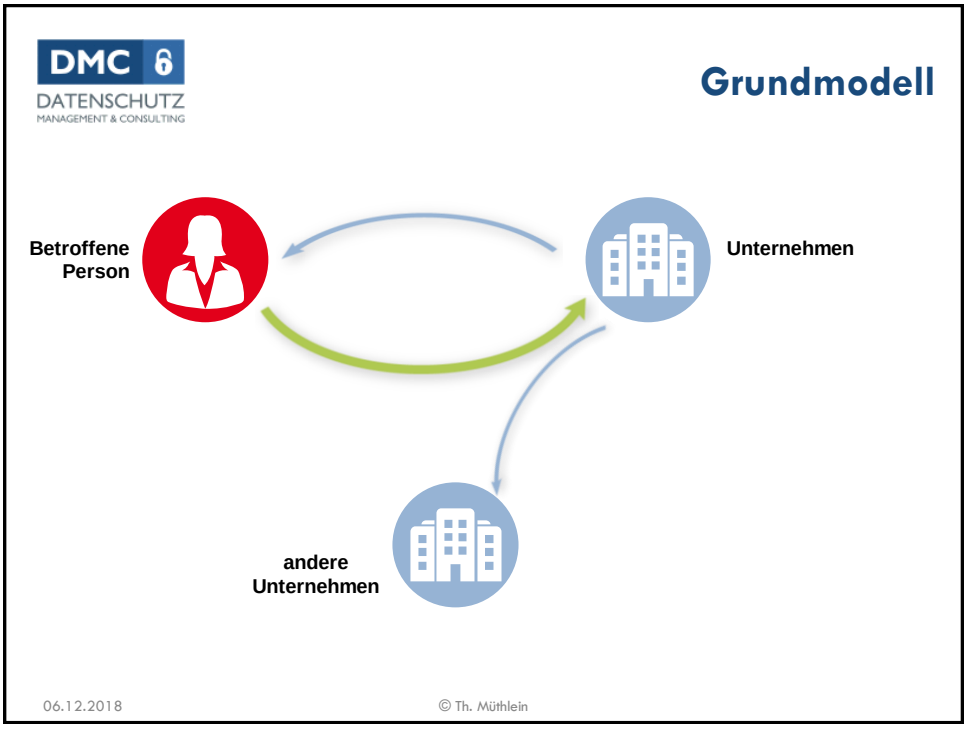
1 Grundsätzliches zur Auftragsverarbeitung

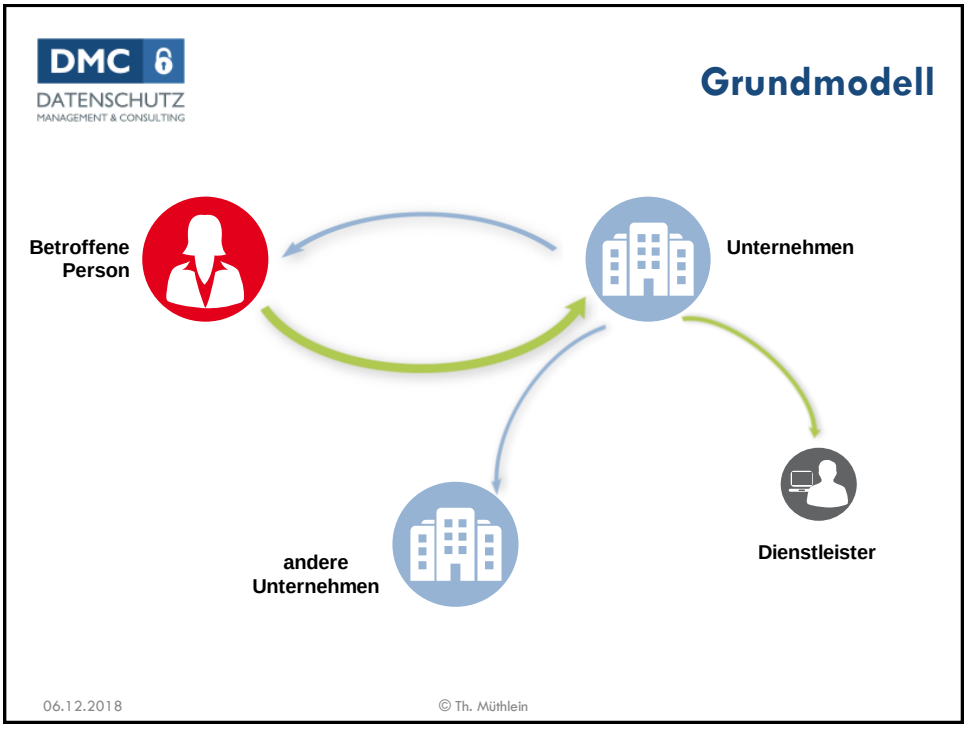
2 Abgrenzungsfragen (Übermittlung, „gemeinsame Verantwortung)

3 Vertragsgestaltung

06.12.2018 © Th. Müthlein

Grundsätze der AV, Abgrenzungsfragen, Vertragsgestaltung

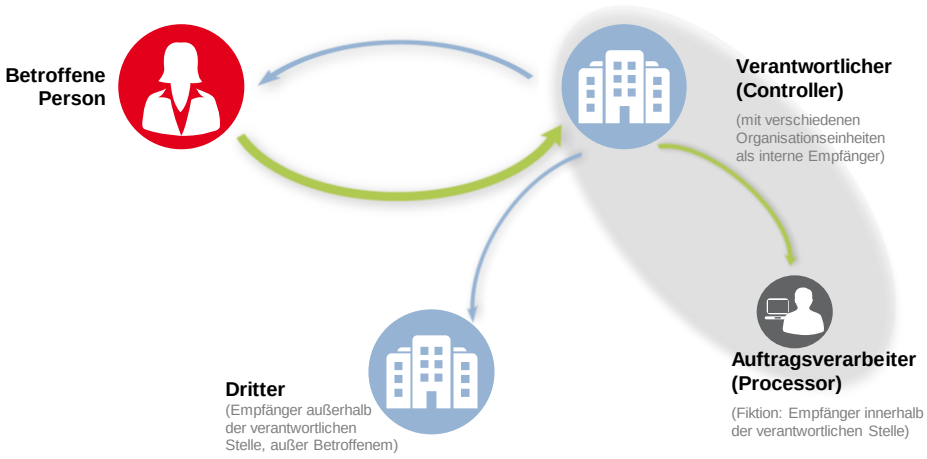




Grundsätze der AV, Abgrenzungsfragen, Vertragsgestaltung

DMC DATENSCHUTZ MANAGEMENT & CONSULTING

Grundmodell



06.12.2018 © Th. Müthlein

DMC DATENSCHUTZ MANAGEMENT & CONSULTING

Zentrale Regelung

Art. 28 DS-GVO

Abs. 1
Auswahl eines Auftragsverarbeiters

Abs. 2
Einsatz von Unterauftragnehmern

Abs. 3
- Vertragserfordernis und Inhalte
- Hinweispflicht bei rechtswidrigen Weisungen

Abs. 4
Ausgestaltung eines Unterauftrags

Abs. 5
Verhaltensregeln und Zertifizierung

Abs. 6
Nutzung von Standardverträgen

Abs. 7, 8
Standardverträge der Kommission / Aufsichtsbehörden

Abs. 9
Form des Vertrages

Abs. 10
Auftragsverarbeiter als Verantwortlicher

06.12.2018 © Th. Müthlein

Grundsätze der AV, Abgrenzungsfragen, Vertragsgestaltung

Grundsätzliches

Grundsatz

Abwicklung der Datenverarbeitung wird auf einen Dienstleister übertragen

Verantwortung

beim Auftraggeber verbleibt
- die inhaltliche Verantwortung für die Aufgabenerfüllung (Zwecke und Mittel)

[und
- die Verantwortung für die Einhaltung des Datenschutzes]

Privilegierung

- Dienstleister gilt als (interner) Teil der verantwortlichen Stelle
- Datenaustausch erfolgt unter „erleichterten“ rechtlichen Voraussetzungen

Anforderungen

- Eingeschränkte Anwendbarkeit
- Sorgfältige Auswahl des Dienstleisters
- Schriftlicher Auftrag / Vertrag mit verpflichtenden Klauseln
- [Regelmäßige Kontrolle des Dienstleisters]

Voraussetzungen

Zulässigkeit der Verarbeitung

z. B. Art. 6 DS-GVO, § 26 BDSG

Zulässigkeit der Auslagerung

z. B. Art. 9 DS-GVO, § 203 StGB (s. a. Neuregelung)

Spezialgesetze

z. B. § 80 SGB X, TKG

Art. 28 DS-GVO

Dienstleistung

Art. 28 DS-GVO (weisungsgebunden)

DMC DATENSCHUTZ MANAGEMENT & CONSULTING

Inhalt

1 Grundsätzliches zur Auftragsverarbeitung

2 Abgrenzungsfragen (Übermittlung, „gemeinsame Verantwortung)

3 Vertragsgestaltung

06.12.2018 © Th. Müthlein

DMC DATENSCHUTZ MANAGEMENT & CONSULTING

Art. 4 - Begriffsbestimmungen

(7) "**Verantwortlicher**" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; …;

(8) "**Auftragsverarbeiter**" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im **Auftrag** des Verantwortlichen **verarbeitet;**

(10) „**Dritter**" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, **außer** der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten;

- Begriffsbestimmungen entsprechen weitgehend der RL 95/46/EG
- Auslegung durch Art. 29-Gruppe (WP 169: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter"

Grundsätze der AV, Abgrenzungsfragen, Vertragsgestaltung

Abgrenzung nach WP 169 – Wer ist Verantwortlicher?

Verantwortlicher

Alleinige oder gemeinsame Entscheidung über Zwecke und Mittel nach WP 169:

- Definition „Zweck“: „erwartetes Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet“
- Definition „Mittel“: „Art und Weise, wie ein Ergebnis oder Ziel erreicht wird“

Auftragsverarbeiter

- Die Entscheidung über den „Zweck“ der Verarbeitung ist dem „für die Verarbeitung Verantwortlichen“ vorbehalten.
- In Bezug auf technische oder organisatorische Fragen kann der für die Verarbeitung Verantwortliche die Entscheidung über die „Mittel“ der Verarbeitung delegieren.
- „… es [ist] durchaus möglich, dass ausschließlich der Auftragsverarbeiter über die technischen und organisatorischen Mittel entscheidet. …“

Abgrenzung Auftragsverarbeitung

Bayerisches Landesamt für Datenschutzaufsicht

FAQ zur DS-GVO

Stichworte	Auftragsverarbeitung, Abgrenzung
Norm	Art. 4 Nr. 8 und Art. 28 DS-GVO
Frage	Was ist Auftragsverarbeitung und was nicht?
Antwort	Auftragsverarbeitung im datenschutzrechtlichen Sinne liegt nur in Fällen vor, in denen eine Stelle von einer anderen Stelle **im Schwerpunkt mit der Verarbeitung** personenbezogener Daten beauftragt wird. Die Beauftragung mit **fachlichen Dienstleistungen anderer Art**, d. h., mit Dienstleistungen, bei denen nicht die Datenverarbeitung im Vordergrund steht bzw. bei denen die Datenverarbeitung nicht zumindest einen wichtigen (Kern-) Bestandteil ausmacht, stellt keine Auftragsverarbeitung im datenschutzrechtlichen Sinne dar.

LDA Bayern - https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf

06.12.2018 © Th. Müthlein

Hinweise zur Bestimmung über die Zwecke

Es ist die Frage zu klären, wann wird durch die Weitergabe auch die Befugnis über die (teilweise oder vollständige) Bestimmung der Zwecke durch den Übermittelnden aufgegeben. Dies wird sich insbesondere aus der (schuldrechtlichen) vertraglichen Situation und dem Auftreten gegenüber dem Betroffenen ergeben.

Indizien sind dabei z. B.

- dass es sich bei der Dienstleistung nicht um einen originären Prozess des Übermittelnden handelt
- der Grad der Verantwortung des Dienstleisters, insbesondere auch gegenüber dem Betroffenen, z. B. eigene Interessen des Dienstleisters
- Auftreten im eigenen Namen des Dienstleisters gegenüber dem Betroffenen
- Eigene Zwecke, die der Dienstleister mit den Daten verfolgt / verfolgen darf
- Grad der Bedeutung der Datenverarbeitung bei Auftragserteilung (ist die Datenverarbeitung „nur notwendiges Beiwerk“ des Auftrags? / Daten sind „Mittel zum Zweck“ für die Erbringung der Dienstleistung)

Beispiele*

Auftragsverarbeitung

- Werbeadressenverarbeitung in einem Lettershop,
- Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten,
- Outsourcing im Rahmen von Cloud-Computing, ohne dass ein inhaltlicher Datenzugriff des Cloud-Betreibers erforderlich ist,
- DV-technische Arbeiten z. B. für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren,
- Verarbeitung von Kundendaten durch ein Callcenter,
- Auslagerung der E-Mail-Verwaltung oder von sonstigen Datendiensten zu Webseiten (z. B. Betreuung von Kontaktformularen oder Nutzeranfragen),
- Datenträgerentsorgung durch Dienstleister,
- Prüfung oder Wartung (z. B. Fernwartung, externer Support) soweit bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Keine Auftragsverarbeitung

Externe Inanspruchnahme von Aufgaben/Funktionen wie

- Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer)
- Inkassobüros mit Forderungsübertragung
- Bankinstituts für den Geldtransfer
- Postdienstes für den Brieftransport
- Mitarbeiterrekrutierung
- Vertragskundenbetreuung
- Finanzberatung
- Unternehmensberatung
- Sachverständigen- bzw. Gutachterbeauftragung an/ durch Dritte mit eigenverantwortlicher Wahrnehmung
- Bewachungsdienste
- Reinigungsdienstleistungen
- Handwerkereinsätze in Unternehmen für Reparaturen und Wartung

Weiterer Beispiele s. LDA Bayern https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf

** Quelle: nach DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO*

Wartung und Fernzugriffe

Kurzpapier Nr. 13
Auftragsverarbeitung,
Art. 28 DS-GVO

Stand: 16.01.2018

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

Wartung und Fernzugriffe

Ist Gegenstand des Vertrages … die **IT-Wartung oder Fernwartung** (z. B. Fehleranalysen, Support-Arbeiten in Systemen des Auftraggebers) und besteht in diesem Rahmen … die **Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten**, so handelt es sich … ebenfalls um eine Form oder Teiltätigkeit einer Auftragsverarbeitung … .

Anders ist dies bei einer **rein technischen Wartung** der Infrastruktur einer IT durch Dienstleister (z. B. Arbeiten an Stromzufuhr, Kühlung, Heizung), die nicht zu einer Qualifikation des Dienstleisters als Auftragsverarbeiter und einer Anwendung von Art. 28 DS-GVO führen.

06.12.2018 © Th. Müthlein

Keine Auftragsverarbeitung – Besonderheiten –

DMC 6 DATENSCHUTZ MANAGEMENT & CONSULTING

Berufsrechtliche Besonderheiten

Berufsrecht schließt Funktion als Auftragnehmer aus

Keine Auftragsverarbeitung, sondern die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen, für die bei der Verarbeitung (einschließlich Übermittlung) personenbezogener Daten eine Rechtsgrundlage gemäß Art. 6 DS-GVO gegeben sein muss, sind beispielsweise in der Regel die Einbeziehung eines Berufsgeheimnisträgers (**Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer**) …"

(DSK, Kurzpapier Nr. 13 - Auftragsverarbeitung, Art. 28 DS-GVO, S. 4)

Eine gewerbliche Tätigkeit ist ihnen grundsätzlich untersagt. Das widerspricht der Weisungsgebundenheit für eine Auftragsdatenverarbeitung …

(LDA Bayern TB 2011/12, S. 32 ff)

Geheimhaltungsvereinbarung

Bei der Aufgaben- oder Funktionsauslagerung an bereichsspezifisch streng reglementierte Dritte, wie z. B.

- der Auslagerung der Lohnabrechnung, Steuererklärung oder Finanzbuchhaltung an einen Steuerberater oder
- der betriebsärztlichen Betreuung an einen niedergelassenen Arzt,

sind aus unserer Sicht allgemeinere Regelungen zu den durchzuführenden Tätigkeiten, zur Zweckbindung von übermittelten Daten und zur Geheimhaltung ausreichend, weil die dort geltenden berufsrechtlichen Vorschriften (Steuerberatergesetz, Ärztliche Berufsordnung, § 203 Abs. 1 StGB, usw.) schon Grenzen ziehen und eigenverantwortliche Pflichten festlegen. Zudem besteht dort auch noch eine berufsrechtliche Kammeraufsicht, die für die Einhaltung der rechtlichen Pflichten ihrer Kammer-Mitglieder zuständig ist.

(so LDA BayernTB 2013/14, S. 41)

DMC 6 DATENSCHUTZ MANAGEMENT & CONSULTING

Steuerberater

Bayerisches Landesamt für Datenschutzaufsicht

FAQ zur DS-GVO

Frage	Muss mit Steuerberatern ein Vertrag zur Auftragsverarbeitung nach der DS-GVO geschlossen werden?
Stichworte	Steuerberater, Auftragsverarbeitung,
Norm	Art. 4 Nr. 8 DS-GVO, Art. 28 DS-GVO
Antwort	In dem bundesweit abgestimmten DSK-Kurzpapier Nr. 13 zur Auftragsverarbeitung nach der DSGVO steht u.a. folgendes: „Keine Auftragsverarbeitung, … , sind beispielsweise in der Regel die Einbeziehung eines … Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer) …" … Des Weiteren ist den Steuerberatern eine gewerbliche Tätigkeit außerhalb des Steuerberaterrechts grundsätzlich untersagt (§ 57 Abs. 4 Nr. 1 Steuerberatungsgesetz). Auch wenn Steuerberater nur die Lohnbuchhaltung für einen Mandanten durchführen, müssen sie dafür aufgrund des Steuerberaterrechts die eigene Verantwortung übernehmen und können sich nicht, wie allgemeine Dienstleister zur Lohnabrechnung, auf Weisungen von Mandanten berufen. Steuerberater arbeiten deshalb aus unserer Sicht regelmäßig eigenverantwortlich aufgrund eines Mandantenvertrags und dürfen von den Mandanten im Rahmen der Erforderlichkeit für ihre Tätigkeit im Sinne von Art. 6 Abs. 1 Satz 1 lit. f DS-GVO personenbezogene Kunden- und/oder Arbeitnehmerdaten verarbeiten.

LDA Bayern - https://www.lda.bayern.de/media/FAQ_Steuerberater_keine_ADV.pdf

LDI NRW: Bei gemischten Tätigkeiten – eigenverantwortliche Steuerberatung sowie weisungsgebundene Dienstleistungen – ist zu differenzieren …

LDI NRW; https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Datenverarbeitung-in-der-Steuerberatung/Datenverarbeitung-in-der-Steuerberatung.html

06.12.2018 © Th. Müthlein

DMC 6 DATENSCHUTZ MANAGEMENT & CONSULTING

Berufsgeheimnisträger

DSK DATENSCHUTZKONFERENZ

Kurzpapier Nr. 13
Auftragsverarbeitung, Art. 28 DS-GVO

Stand: 16.01.2018

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

Fortbestehende Sonderregelung …

… Zu beachten ist, dass die Datenverarbeitung im Auftrag auch künftig keine Erlaubnis darstellt, Daten dem Auftragsverarbeiter zu offenbaren, die aufgrund gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, vertraulich zu behandeln sind (vgl. § 1 Abs. 2 S. 3 BDSG).

Mit dem „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ wurden jedoch verschiedene Gesetze zu Berufsgeheimnissen novelliert. So dürfen nunmehr u.a. die in § 203 Abs. 1 oder 2 StGB genannten Berufsgeheimnisträger z.B. externen Dienstleistern, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, Geheimnisse unter den Voraussetzungen des § 203 Abs. 3 und 4 StGB offenbaren. Im Gegenzug unterliegt der Auftragsverarbeiter nach § 203 Abs. 4 StGB nunmehr ebenfalls einer auch strafrechtlich sanktionierten Verschwiegenheitspflicht. …

s. a. Bitkom, Muster - Umsetzung des Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30. Oktober 2017 Vertraulichkeitsverpflichtung i.S. des Art. 28 Abs. 3 lit. b DS-GVO https://www.bitkom.org/noindex/Publikationen/2018/Leitfaeden/180803-IT-Einsatz-durch-Berufsgeheimnistraeger-Muster-zur-Umsetzung-der-Neuregelung-des-203-StGB/20180718-Muster-203StGB-final.pdf

06.12.2018 © Th. Müthlein

DMC 6 DATENSCHUTZ MANAGEMENT & CONSULTING

Besondere Geheimhaltungspflichten

Geheimhaltungspflicht schränkt Auftragsvergabe nach Art. 28 DS-GVO ein

Insbes. **Ärzte, Steuerberater, Wirtschaftsprüfer, Rechtsanwälte** unterliegen einer besonderen Geheimhaltungspflicht. Dabei wird die **unbefugte Offenbarung des Geheimnisses nach § 203 StGB** sanktioniert. Eine Beauftragung im Rahmen der Auftragsverarbeitung rechtfertigt die Offenbarung an einen Dienstleister nicht, so dass die Strafbarkeit des Auftraggebers erhalten bleibt.

Es sind die Voraussetzungen des § 203 Abs. 3 StGB (ggf. i.V.m. dem jeweiligen Berufsrecht) zu beachten:

> *3) … Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber **sonstigen Personen** offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.*

s. a. Bitkom, Muster - Umsetzung des Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30. Oktober 2017 Vertraulichkeitsverpflichtung i.S. des Art. 28 Abs. 3 lit. b DS-GVO https://www.bitkom.org/noindex/Publikationen/2018/Leitfaeden/180803-IT-Einsatz-durch-Berufsgeheimnistraeger-Muster-zur-Umsetzung-der-Neuregelung-des-203-StGB/20180718-Muster-203StGB-final.pdf

DMC DATENSCHUTZ MANAGEMENT & CONSULTING

Hosting von statischen Webseiten

Bayerisches Landesamt für Datenschutzaufsicht

FAQ zur DS-GVO

Frage	Ist das Hosting von rein statischen Websites (zur Selbstdarstellung) z.B. von Vereinen oder Kleinunternehmen, wenn keine personenbezogenen Daten über die Seitenaufrufe an den Verein oder das Kleinunternehmen fließen, Auftragsverarbeitung?
Stichworte	Hosting von statischen Webseiten
Norm	Art. 28 DS-GVO
Antwort	Das **Hosting von rein statischen Websites** (zur Selbstdarstellung) z.B. von Vereinen oder Kleinunternehmen, ist, wenn keine personenbezogenen Daten über die Seitenaufrufe an den Verein oder das Kleinunternehmen fließen und auch kein Nutzer-Tracking stattfindet, **keine Auftragsverarbeitung**. Die Tatsache, dass auch beim Hosting von statischen Webseiten zwangsläufig IP-Adressen, d.h. personenbezogene Daten, verarbeitet werden müssen, führt nicht zur Annahme einer Auftragsverarbeitung. Das wäre nicht sachgerecht. Die (kurzfristige) IP-Adressenspeicherung ist vielmehr noch der TK-Zugangsvermittlung des Website-Hosters nach dem TKG zuzurechnen und dient in erster Linie Sicherheitszwecken des Hosters.

06.12.2018 © Th. Müthlein

DMC DATENSCHUTZ MANAGEMENT & CONSULTING

Ärzte

Bayerisches Landesamt für Datenschutzaufsicht

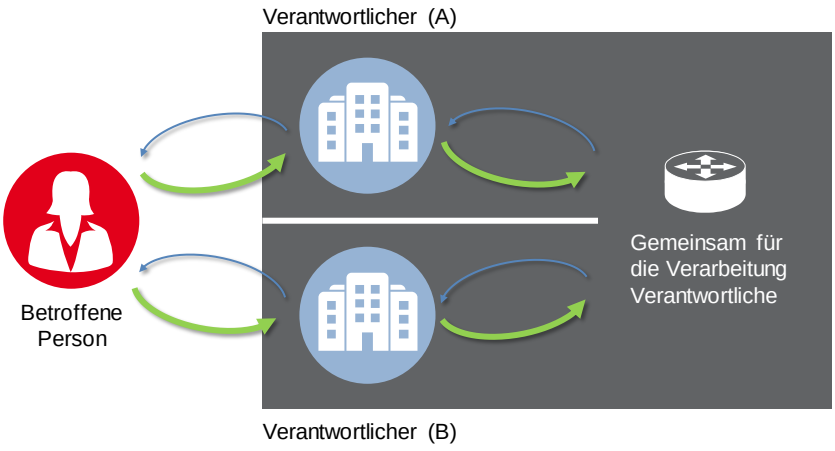
FAQ zur DS-GVO

Frage	Ist in einer Arztpraxis für folgende Fälle ein Vertrag zur Auftragsverarbeitung oder eine Einwilligung erforderlich: • Abrechnung über die KVB • Datenübermittlung an den MDK • Labor • private Abrechnungsstelle
Stichworte	Abrechnung über private Abrechnungsstelle, KVB, MDK, Labor
Norm	Art. 28 DS-GVO
Antwort	<u>KVB / MDK:</u> … Hierfür bedarf es keiner Einwilligung. … … keine Auftragsverarbeitung … <u>Labor:</u> … keine Auftragsverarbeitung … Ob eine Einwilligung erforderlich ist … , hängt davon ab, ob das Labor von einem Berufsgeheimnisträger i.S.v. Art. 9 Abs. 3 DS-GVO geführt wird. <u>Private Abrechnungsstelle:</u> … Wird nur eine Rechnung erstellt, …. Auftragsverarbeitung … Zu klären wäre …, ob … eine Schweigepflichtentbindung benötigt wird. … Forderungsübertragung … wird der Rahmen der Auftragsverarbeitung verlassen, … die Arztpraxis benötigt … eine Einwilligung.

06.12.2018 © Th. Müthlein

Abgrenzung zur „gemeinsamen Verantwortung“

Gemeinsam für die Verarbeitung Verantwortliche



© 2018 DATAKONTEXT GmbH – aus: *Gola/Jaspers/Müthlein/Schwartmann – DS-GVO/BDSG im Überblick*

DMC DATENSCHUTZ MANAGEMENT & CONSULTING

Art. 26 - Gemeinsam für die Verarbeitung Verantwortliche

(1) Legen zwei oder mehr Verantwortliche **gemeinsam die Zwecke der und die Mittel** zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

06.12.2018 © Th. Müthlein

DMC DATENSCHUTZ MANAGEMENT & CONSULTING

Abgrenzung EuGH

Fanpages
U. v. 5.6.2018 - C-210/16

CVRIA

- **Gegenstand ist nicht die Feststellung einer gemeinsamen Verantwortung sondern die Begründung der Verantwortung des Fanpagebetreiber. Hierfür wird der Umweg über eine gemeinsame Verantwortung genommen:**
  - **eine „Beteiligung" an der Entscheidung über die Zwecke und Mittel der Verarbeitung reicht für eine (gemeinsame) Verantwortung aus**
  - (gemeinsame) Verantwortung setzt nicht gleichen Zugang zu den Daten / das gleiche Ausmaß der Verarbeitung voraus – keine „gleichwertige" Verantwortung erforderlich
  - eine gemeinsame Verantwortung dient vornehmlich dem Schutz des Betroffenen
  - sie stellt keinen Erlaubnistatbestand dar
  - Aale Verantwortlichen müssen die Regelungen – vollumfänglich – selbst einhalten

Zeugen Jehovas
U. v. 10.07.2018 - C-25/17

- Die Religionsgemeinschaft und ihre als Verkündiger tätigen Mitgliedern sind **gemeinsam Verantwortliche** da die Verkündigungstätigkeit von dieser Gemeinschaft **organisiert und koordiniert wird**
- **Nicht erforderlich** sind
  - **Ein Zugriff der Gemeinschaft** auf diese Daten oder
  - nachweislich **schriftliche Anleitungen oder Anweisungen** zur Datenverarbeitung

06.12.2018 © Th. Müthlein

Grundsätze der AV, Abgrenzungsfragen, Vertragsgestaltung

Abgrenzung DSK

DSK DATENSCHUTZKONFERENZ

Kurzpapier Nr. 13
Auftragsverarbeitung, Art. 28 DS-GVO

Stand: 16.01.2018

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

Keine Auftragsverarbeitung liegt ferner vor, wenn **gemeinsame Verantwortlichkeit nach Art. 26 DSGVO** gegeben ist, d.h. wenn mehrere Verantwortliche gemeinsam über die Verarbeitungszwecke und -mittel entscheiden. Hierunter können je nach Gestaltung eine Reihe von Verarbeitungen fallen, die bisweilen unter BDSG-alt als sog. Funktionsübertragung eingestuft wurden, etwa

- klinische Arzneimittelstudien, wenn mehrere Mitwirkende (z. B. Sponsor, Studienzentren/Ärzte) jeweils in Teilbereichen Entscheidungen über die Verarbeitung treffen,
- gemeinsame Verwaltung bestimmter Datenkategorien (z.B. „Stammdaten“) für bestimmte gleichlaufende Geschäftszwecke mehrerer Konzernunternehmen.

06.12.2018 © Th. Müthlein

Grundsätzliches

Grundsatz

Gemeinsame Abwicklung der Datenverarbeitung

Verantwortung

Verbleibt bei jedem beteiligten Verantwortlichen für

- die Zulässigkeit der ihm zur Verfügung stehenden Daten
- Alle Verpflichtungen als Verantwortlicher, insbes. hinsichtlich Rechte der Betroffenen, DS-Organisation, Haftung
- Gesamtschuldnerische Haftung mit den anderen „gemeinsam Verantwortlichen“

Keine Privilegierung

- Keine Rechtsgrundlage
- Datenaustausch erfolgt unter den „normalen“ rechtlichen Voraussetzungen

Anforderungen

- Vereinbarung über die tatsächlichen Funktionen und Beziehungen der Parteien gegenüber den Betroffenen
- Transparent / in wesentlichen Teilen den Betroffenen zur Verfügung zu stellen

DMC DATENSCHUTZ MANAGEMENT & CONSULTING

Vereinbarung

Ziel

Wahrung der Rechte der Betroffenen

Form

- Vereinbarung (≠ Vertrag)
- Grds. formfrei, aber:
  - „Transparent“
  - in wesentlichen Teilen den Betroffenen zur Verfügung zu stellen

Inhalte

- Darstellung der tatsächlichen Funktionen und Beziehungen der Parteien gegenüber den Betroffenen, insbesondere:
  - wer von ihnen welche Verpflichtung der DS-GVO erfüllt
  - Wie ist die Wahrnehmung der Rechte der betroffenen Person sichergestellt
  - wer kommt welchen Informationspflichten gemäß den Artikeln 13 und 14 nach
  - Ggf. Angabe einer „Anlaufstelle“ Betroffene

DMC DATENSCHUTZ MANAGEMENT & CONSULTING

Inhalt

1 Grundsätzliches zur Auftragsverarbeitung

2 Abgrenzungsfragen (Übermittlung, „gemeinsame Verantwortung)

3 Vertragsgestaltung

06.12.2018 © Th. Müthlein

DMC 6 DATENSCHUTZ MANAGEMENT & CONSULTING

Vertragsphase - Vertragsmuster

Artikel 28: Auftragsverarbeiter

(6) Unbeschadet eines **individuellen Vertrags** zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels **ganz oder teilweise** auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten **Standardvertragsklauseln** beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

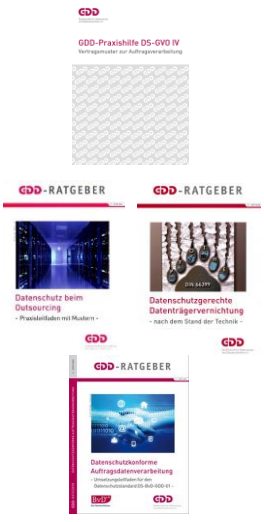
(7) Die **Kommission** kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 **Standardvertragsklauseln** zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine **Aufsichtsbehörde** kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 **Standardvertragsklauseln** zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

06.12.2018 © Th. Müthlein

DMC 6 DATENSCHUTZ MANAGEMENT & CONSULTING

Muster für ADV-Vereinbarungen



GDD-Praxishilfe DS-GVO IV – Mustervertrag zur Auftragsverarbeitung
(deutsch und englisch)
[https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_4.pdf]

GDD-Praxishilfe DS-GVO XII – Praxishinweise für Auftragsverarbeiter nach Art. 28 DS-GVO
[https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_12.pdf]

GDD-Ratgeber – Datenschutz beim Outsourcing - Praxisleitfaden mit Mustern

Verbandsübergreifendes Muster eines Auftragsdatenverarbeitungsvertrags im Gesundheitswesen
[https://www.gesundheitsdatenschutz.org/doku.php/adv-mustervertrag-2015]
Hinweise zur Anpassung des Musters an die DS-GVO
[https://www.gesundheitsdatenschutz.org/lib/exe/fetch.php/03_eu_ds-gvo_und_ADV.pdf]

GDD-Ratgeber - Datenschutzgerechte Datenträgervernichtung
- 7.2 Anlage: Vertrag zur Auftragsdatenverarbeitung S. 80
- 7.3 Anlage: Checkliste Auswahl eines Auftragnehmers gemäß § 11 BDSG S. 87

Weiteres zur ADV:

- GDD-Ratgeber – Datenschutzkonforme Auftragsdatenverarbeitung - Umsetzungsleitfaden zum Datenschutzstandard DS-BvD-GDD-01
- Datenschutz-Prüfung von Rechenzentren

06.12.2018 © Th. Müthlein

Grundsätze der AV, Abgrenzungsfragen, Vertragsgestaltung

DMC 6 DATENSCHUTZ MANAGEMENT & CONSULTING

Muster für ADV-Vereinbarungen

Bitkom:

- Mustervertragsanlage - Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) (DE/ENG)
  [https://www.bitkom.org/Bitkom/Publikationen/Mustervertragsanlage.html]
- Leitfaden - Begleitende Hinweise zu der Anlage Auftragsverarbeitung
  [https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-LF-Auftragsverarbeitung-online.pdf]

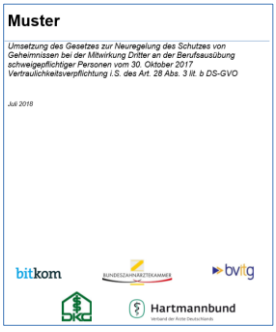
Aufsichtsbehörden:

- DSK: Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO
  [https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf]
- LDA Bayern: Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO (von weiteren Aufsichtsbehörden übernommen)
  [https://www.lda.bayern.de/media/muster_adv.pdf]
- ULD: Mustervereinbarung für einen Vertrag zur Auftragsverarbeitung
  [https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-3-ADV.pdf]
- CNIL (Fr): GUIDE FOR PROCESSORS - SEPTEMBER 2017 EDITION (ENG/FR)
  [https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil_en.pdf]

06.12.2018 © Th. Müthlein

DMC 6 DATENSCHUTZ MANAGEMENT & CONSULTING

Berufsgeheimnisträger



Bitkom e.V. / BZÄK / bvitg e.V. / DKG e.V. / Hartmannbund – Verband der Ärzte Deutschlands e.V.:

- Muster - Umsetzung des Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30. Oktober 2017 Vertraulichkeitsverpflichtung i.S. des Art. 28 Abs. 3 lit. b DS-GVO

  [https://www.bitkom.org/noindex/Publikationen/2018/Leitfaeden/180803-IT-Einsatz-durch-Berufsgeheimnistraeger-Muster-zur-Umsetzung-der-Neuregelung-des-203-StGB/20180718-Muster-203StGB-final.pdf]

06.12.2018 © Th. Müthlein

Grundsätze der AV, Abgrenzungsfragen, Vertragsgestaltung

DMC 6 DATENSCHUTZ MANAGEMENT & CONSULTING

Schriftform

Bayerisches Landesamt für Datenschutzaufsicht

FAQ zur DS-GVO

Frage	Welche Formerfordernisse bestehen für den Abschluss eines Auftragsverarbeitungsvertrages nach Art. 28 Abs. 9 DS-GVO?
Stichworte	Auftragsverarbeitung, Formerfordernis, Schrift- oder Textform
Norm	Art. 28 Abs. 9 DS-GVO
Antwort	Nach Art. 28 Abs. 9 DS-GVO ist der Vertrag zur Auftragsverarbeitung schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. Was mit dem elektronischen Format genau gemeint ist und auf welchen Wegen solche Verträge geschlossen werden können, wird derzeit unterschiedlich diskutiert. Jedenfalls ist es dabei aber Sache der Vertragspartner, den elektronischen **Vertragsabschluss** (per **übereinstimmender Willenserklärungen**) für eigene Zwecke und für Kontrollzwecke der Datenschutzaufsichtsbehörden sowie anderer Aufsichtsinstanzen (bei den Kreditinstituten: BaFin, Prüfungsverband, Bundesbank etc.) hinreichend und **beweiskräftig zu dokumentieren**, z. B. durch unterschriebene und eingescannte Texte mit Protokollierung des dazu geführten E-Mail-Verkehrs, durch eine Verfahrensweise nach § 126a BGB mit einer qualifizierten elektronische Signatur usw. Eine **qualifizierte elektronische Signatur ist also nicht zwingend**, sondern nur eine der denkbaren elektronischen Möglichkeiten, so zumindest die herrschende Auffassung in Deutschland.

LDA Bay. -https://www.lda.bayern.de/media/FAQ_ADV_Formerfordernis.pdf

06.12.2018 © Th. Mühlein

DMC 6 DATENSCHUTZ MANAGEMENT & CONSULTING

Schriftform - EU-Kommission

European Parliament

Parliamentary questions

27 August 2018

Answer given by Ms Jourová on behalf of the European Commission

Question reference: E-003163/2018

Übersetzung durch den Referenten - http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2018-003163&language=EN

... Die DS-GVO sieht ferner vor, dass dieser Vertrag oder Rechtsakt schriftlich, auch in elektronischer Form, erfolgen muss[3].

… **Die Regeln für den Abschluss von Verträgen** oder anderen Rechtsakten, auch in elektronischer Form, sind jedoch nicht in der DS-GVO, sondern in anderen EU- und/oder **nationalen Rechtsvorschriften festgelegt**.

Die E-Commerce-Richtlinie (Richtlinie 2000/31/EG) sieht die Beseitigung rechtlicher Hindernisse für die Nutzung elektronischer Verträge vor. Sie harmonisiert nicht die Form, in der elektronische Verträge abgeschlossen werden können. **Im Prinzip sind automatisierte Vertragsprozesse rechtmäßig**.

Es ist nicht notwendig, Verträgen eine elektronische Signatur beizufügen, damit sie Rechtswirkungen haben. **E-Signaturen sind eines von mehreren Mitteln, um ihren Abschluss und ihre Bedingungen zu beweisen.** …

(3) Artikel 28 Absatz 9 DS-GVO.

Festschreibung von TOM in Verträgen

Kurzpapier Nr. 13
Auftragsverarbeitung,
Art. 28 DS-GVO

Stand: 16.01.2018

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

Vertrag mit dem Auftragsverarbeiter

… Unter anderem muss der Vertrag außerdem vorsehen, dass der Auftragsverarbeiter die gemäß Art. 32 DS-GVO erforderlichen Maßnahmen ergreift. Da der Verantwortliche für die Rechtmäßigkeit der Verarbeitung insgesamt verantwortlich ist und bleibt (s. Art. 24 DS-GVO), ist weiterhin **anzuraten**, die **mindestens** erforderlichen technischen und organisatorischen Maßnahmen darzustellen.

06.12.2018 © Th. Müthlein

Vielen Dank für die Aufmerksamkeit!

Fragen?

DISKUSSION.

Und was können wir für Sie tun?

DMC Datenschutz Management & Consulting GmbH & Co. KG

Zur Mühle 2-4, D-50226 Köln-Frechen

Telefon +49.2234.964944-0
Fax +49.2234.964944-19

E-Mail info@dmc-datenschutz.de
Internet www.dmc-datenschutz.de