

Handlungsempfehlung für eine Anpassung der DS-GVO zur erfolgreichen Digitalisierung

Positionspapier zur Anwendung der DS-GVO für einen rechtssicheren und praxistauglichen Datenschutz in kleinen und mittelständischen Unternehmen

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

September 2018

Handlungsempfehlungen

Sehr geehrte Leserinnen und Leser,

seit 128 Tagen ist die Europäische Datenschutzgrundverordnung, kurz DS-GVO, in allen EU-Mitgliedsstaaten verbindliches Recht. Die zweijährige Übergangsfrist ist schnell verstrichen und nicht ausreichend zur Information und Vorbereitung auf die Umstellung genutzt worden. Speziell kleine und mittelständische Unternehmen (KMU) sowie ehrenamtlich geführte Vereine und Institutionen fühlen sich von der DS-GVO überfordert. Eine Entwicklung, die wir mit Sorge beobachten.

Deutschland hat EU-weit die größte Expertise im Datenschutz und insbesondere im Einsatz betrieblicher Datenschutzbeauftragten. Diesen Wettbewerbsvorteil dürfen wir nicht verstreichen lassen. Mit der EU-DS-GVO sorgt eine einheitliche Regelung über nationale Grenzen hinweg für einen fairen Wettbewerb um die immer wichtiger werdende Ware „Daten“. Zunehmend beurteilen auch Kunden die Unternehmen nach Datenschutzkriterien. Datenschutz steht für Vertrauen und Qualität und wird zum Wettbewerbsvorteil. Datenschutzbeauftragte generieren somit einen echten und messbaren Mehrwert. Wir sind davon überzeugt, dass der betriebliche Datenschutzbeauftragte die kostengünstigste und effizienteste Möglichkeit für den Mittelstand darstellt, sich hier mit der erforderlichen Fachexpertise zu versorgen. Gleichzeitig ist er für viele Unternehmen der Ansprechpartner bei Fragen der Digitalisierung und der IT-Sicherheit und bietet den besten Schutz gegen auf Unwissenheit des Managements basierenden Fehlentscheidungen.

Der Berufsverband der Datenschutzbeauftragten möchte mit diesem Papier aufzeigen, wie aus der Sicht der Datenschutzpraktiker, der Umstieg im Kontext zunehmender Digitalisierung besser gelingen kann und daraus weitere Vorteile generiert werden können.

Wir haben dazu drei Handlungsempfehlungen identifiziert:

- (1) Anpassungen der gesetzlichen Regelungen für mehr Klarheit und weniger Bürokratie**
- (2) Verbesserung des Supports für KMU und Startups**
- (3) Verbesserung der Qualifikation in der Datenschutzberatung und Aufbau einer Infrastruktur zur Zertifizierung**

Wir haben diese Empfehlungen auf den folgenden Seiten in aller Kürze erläutert und stellen den direkten Nutzen für die deutsche Wirtschaft dar.

Ich wünsche Ihnen eine interessante und aufschlussreiche Lektüre.

Thomas Spaeing, BvD-Vorstandsvorsitzender

Handlungsempfehlungen

(1) Anpassungen der gesetzlichen Regelungen – für mehr Klarheit und weniger Bürokratie

Eine Anmerkung vorab: Wir wissen, dass einige dieser Vorschläge nicht allein durch den nationalen Gesetzgeber umgesetzt werden können, zumindest nicht im Einklang mit dem EU-Recht. Gleichwohl halten wir die Diskussion um diese Themen und Potenziale jetzt für richtig. Zudem hat Deutschland die größte Expertise im Bereich Datenschutz und kann mit nationalen Verbesserungen auch in Brüssel dringend erforderliche Akzente setzen.

1. Änderung der Meldepflicht bei Datenpannen

Die Regelungen aus Art. 33 DS-GVO (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde) stellen Unternehmen und auch Aufsichtsbehörden vor erhebliche Probleme und Aufwände. Die Unsicherheit über die Pflicht, das Verfahren und die Konsequenzen sind immens. Gerade im Mittelstand entscheiden sich die Verantwortlichen heute oft gegen die Meldung an die Aufsichtsbehörden. Damit gehen sie ein erhebliches Bußgeldrisiko ein. Allerdings landet in vielen Unternehmen ein Großteil der Meldungen auch zur Prüfung beim betrieblichen Datenschutzbeauftragten.

Zur Entlastung der KMU schlägt der BvD vor, die Meldepflicht der einfachen Datenpanne (geschätzte 95 Prozent der Vorgänge) ausschließlich an den benannten Datenschutzbeauftragten zu richten. Dieser führt eine Übersicht der Vorgänge, begleitet und dokumentiert die Maßnahmen. Die Aufsichtsbehörde kann sich jederzeit beim Datenschutzbeauftragten über den Stand informieren. Ermittelt der Datenschutzbeauftragte ein hohes Risiko für die Betroffenen, wird dieser die Leitung des Verantwortlichen informieren. Die Leitung kann die vom Datenschutzbeauftragten vorbereitete, diesen Fällen vorbehaltene Meldung an die Aufsichtsbehörde und die Benachrichtigung an die Betroffenen in Gang setzen.

2. Datenschutz-Folgenabschätzung erfolgt durch den Datenschutzbeauftragten

Die Durchführung der Datenschutz-Folgeabschätzung ist für mittelständische Unternehmen aufgrund der Komplexität, des fehlenden Know-hows und mangelnder Erfahrung i.d.R. nicht möglich. In Unternehmen, die einen Datenschutzbeauftragten haben, wird momentan überwiegend auch die Datenschutz-Folgeabschätzung durch diesen erstellt, obwohl die DS-GVO dies so nicht vorsieht. Da bereits die Vorabkontrolle nach bis 25.05.2018 geltenden Recht Pflicht des Datenschutzbeauftragten war und durch diesen erstellt wurde, ist hier auch das erforderliche Know-how i. d. R. vorhanden.

Der BvD schlägt zur Entlastung der Unternehmen vor, die Datenschutz-Folgeabschätzung unter Einbindung der Fachbereiche durch den Datenschutzbeauftragten vorbereiten zu lassen. Dieser stellt das Ergebnis der Leitung vor und diese legt dann auf Basis dieser Vorschläge die weitere Vorgehensweise fest.

Handlungsempfehlungen

3. Verzeichnis der Verarbeitungstätigkeiten (KMU)

Die Betreuung und Führung der Verarbeitungsübersicht stellt kleine und mittelständische Unternehmen (KMU) vor erhebliche Probleme. I.d.R. ist dazu kein Know-how vorhanden. Die Ergebnisse sind nach Erfahrungen des BvD mangelhaft und stellen für die Unternehmen ein erhebliches Risiko im Rahmen der Rechenschaftspflicht dar. Unternehmen, die einen qualifizierten Datenschutzbeauftragten haben, werden dabei eng unterstützt, wie dies bereits im alten Bundesdatenschutzgesetz (BDSG a.F.) vorgesehen war.

Der BvD schlägt vor, dass zur Entlastung der Unternehmen der Datenschutzbeauftragte die Erstellung der Verarbeitungsübersicht zur Erstellung des Verzeichnisses bei KMU koordiniert und das Verzeichnis der Verarbeitungstätigkeiten führt. Das Unternehmen hat lediglich die Aufgabe, die Mitarbeiter der entsprechenden Fachbereiche zur Mitarbeit und Bereitstellung der Inhalte und Kontrolle der Vollständigkeit der Verarbeitungsübersicht zu verpflichten. Der Verantwortliche gibt die Übersicht frei.

4. Informationspflichten

Die Informationspflichten aus Art. 13 und 14 DS-GVO stellen die Unternehmen vor erhebliche Probleme. Teilweise wurden wichtige Unternehmensprozesse (zum Beispiel Kontaktpflege, Newsletter oder Kundeninformationen) aufgrund von Unklarheiten eingestellt.

Der BvD schlägt vor, die Informationspflichten im vorhandenen Umfang wahlweise auf einem der folgenden Kanäle zu ermöglichen:

- Aushang, Flyer, Merkblatt
- Schriftlich per Brief
- Schriftlich per E-Mail
- Textuell per Link und Internetseite

Das Unternehmen legt selbst fest, welchen Kanal es wählt. Dieser soll allerdings zum Geschäftsmodell passen. Das Unternehmen soll dies begründen können.

Zum Bürokratieabbau bedarf es einer rechtlichen Klarstellung, dass ein aktives Zutun durch eine Einwilligung oder Bestätigung durch den Betroffenen nicht erforderlich ist. Die Nachweispflicht durch den Verantwortlichen kann auch anderweitig erfolgen.

5. Erleichterungen für Vereine

Die Pflichten aus der DS-GVO stellen gemeinnützige Vereine vor oft unlösbare Probleme und erhebliche Kosten. Die aktuellen Fehlberatungen in diesem Bereich führen zu höheren Risiken, als die Verarbeitungen der Vereine selbst.

Handlungsempfehlungen

Der BvD schlägt vor, dass Vereine, die gemeinnützig und ehrenamtlich arbeiten und keine Verarbeitungen mit einem hohen Risiko für die Betroffenen durchführen, von folgenden Pflichten befreit werden:

- Erfüllung der Informationspflichten nach Art. 13/14
 - Führung der Verarbeitungsübersicht nach Art. 30
 - Meldepflicht gegenüber der Aufsichtsbehörde bei Datenpannen nach Art. 33
 - Mitteilungspflichten nach Art. 19
 - Datenübertragbarkeit nach Art. 20
- und ergänzend geregelt wird, dass erst im Wiederholungsfall ein Bußgeld gem. Art. 83 DS-GVO gegen diese Verarbeiter verhängt werden kann.

-
Allerdings sollen diese Stellen einen Ansprechpartner für den Datenschutz namentlich (z. B. Vorstandsmitglied) benennen, der die Mitgliedsversammlung regelmäßig zum Datenschutz im Verein informiert.

6. Auftragsverarbeitungen klarstellen

Der Abschluss von Verträgen über eine Auftragsverarbeitung ist heute in einer unüberschaubaren Fülle von Fällen gefordert, weil sich immer neue Experten in der Auslegung des Art. 28 DS-GVO verwirklichen. Die Unternehmen sind mit dieser Situation überfordert. Die Datenschutzbeauftragten unterstützen bereits heute mit pragmatischen Vorgaben, scheitern aber oft an spitzfindigen Auslegungen, ohne dass diese für die Betroffenen einen Nutzen enthalten.

Der BvD schlägt vor, dass der Gesetzgeber eindeutig festlegt, dass die Beauftragung eines Dienstleisters nur dann als eine Auftragsverarbeitung gilt, wenn der Kern der Dienstleistung die Verarbeitung personenbezogener Daten des Auftraggebers beinhaltet und diese z. B. nicht nur durch die Vertragserfüllung nicht ausgeschlossen werden können. Ebenso könnte durch den verbindlichen Auftrag zur Anwendung des Art. 28 Abs. 8 DS-GVO ein rechtssicheres Vertragstemplate für die Privatwirtschaft sowie Vereine und Institutionen geschaffen und bereitgestellt werden, dass den Aufwand für die Gestaltung und Prüfung von Verträgen über eine Auftragsverarbeitung erheblich reduzieren könnte.

7. Datenportabilität und Mitteilungspflicht

Die Regelungen der DS-GVO zur Datenportabilität nach Art. 20 sowie die besonderen Mitteilungspflichten nach Art. 19 sind für KMU, die nicht in der Digitalwirtschaft tätig sind, nicht sinnvoll. Die Gewährleistung dieser Pflichten stellt einen erheblichen Aufwand dar, dem kein sinnvoller Nutzen für den Betroffenen gegenübersteht.

Der BvD schlägt vor, dass die Regelung nach Art. 19 und 20 für KMU, die nicht in der Digitalwirtschaft tätig sind, entfällt. Die Betroffenenrechte sind unserer Ansicht nach durch die Rechte aus den Art. 15 (Auskunft), 16 (Berichtigung), 17 (Löschen/Vergessen) und 18 (Einschränken der Verarbeitung) ausreichend gewährleistet.

Handlungsempfehlungen

Fazit: Mit diesen Anpassungen des Datenschutzrechts würden Mittelstand, Vereine und Institutionen erheblich entlastet. Der bürokratische Aufwand ließe sich erheblich senken und die Datenschutzbeauftragten könnten bei diesen Verarbeitern noch effizienter unterstützen.

Die in diesem Zusammenhang vielfach diskutierte Änderung der Benennungspflicht würde an diesen Punkten überhaupt nichts verbessern. Vielmehr würde den Unternehmen der wichtigste Partner bei der unbürokratischen Umsetzung der komplexen rechtlichen Vorgaben genommen, die Aufgaben würden der Geschäftsleitung selbst zufallen. Kaum vorstellbar, dass ein Geschäftsführer dafür seine Hauptaufgaben zurückstellen könnte.

(2) Verbesserung des Supports für KMU und Startups

Unterstützung von Startups und KMU

Unternehmen, die am Beginn ihrer Tätigkeit stehen, müssen die Anforderungen der DSGVO erfüllen. Diese davon auszunehmen, führt zu einer Reihe von Risiken und ggf. sogar zur Unzulässigkeit der Verarbeitung. Diese Unternehmen sollten durch gezielte Förderprogramme unterstützt werden, damit die Erstberatung zur Datenschutz-Compliance nicht aus Kostengründen ausbleibt. Andernfalls können hier Modelle und Produkte entstehen, die auf dem Markt nicht bestehen können, weil sie den Datenschutzstandards nicht entsprechen. Dieses Risiko wird sich zunehmen auch bei der Kapitalbeschaffung der Startup-Branche bemerkbar machen. Kein Investor wird in solch unsichere Produkte investieren, die zudem erhebliches Risiko für die betroffenen Personen beinhalten.

Bereitstellung von qualifizierten Informationen

Aufgrund der umfassenden Falsch- und Fehlinformationen durch Presse und unqualifizierte Beratung besteht ein erheblicher Bedarf an praxisnahen Arbeitsmitteln und Materialien. Damit diese für Vereine und KMU bereitgestellt werden können, empfehlen wir, die Stiftung Datenschutz so aufzustellen, dass diese hier unterstützen kann. Die Datenschutzverbände BvD und GDD können dabei unterstützen. Durch die Arbeitskreise in den Verbänden wird bereits heute viel Material erstellt, das Wirtschaft, Behörden und Vereinen zur Verfügung gestellt wird. Diese Arbeit lässt sich noch ausweiten und in eine Zusammenarbeit mit der Stiftung einbringen.

Handlungsempfehlungen

(3) Verbesserung der Qualifikation in der Datenschutzberatung und Aufbau einer Infrastruktur zur Zertifizierung

Der Mittelstand braucht mehr qualifizierte Unterstützung

Unternehmen und Organisationen müssen bei der Umsetzung der DS-GVO bessere Unterstützung erhalten. Sie brauchen pragmatische, anwenderfreundliche Lösungen, die bürokratischen Aufwand beim Datenschutz reduzieren oder vermeiden und gleichzeitig unternehmensinterne Prozesse im Datenschutz effizient gestalten. Die Qualität des Datenschutzbeauftragten rückt hier in das Zentrum des unternehmerischen Interesses.

Die Bereitstellung qualifizierter Datenschutzbeauftragter in ausreichender Zahl ist leider nicht rechtzeitig gelungen. In der Folge ist ein Markt für „Heilsbringer und Schwarzmalerei“ entstanden, die zu weiterer Verunsicherung beigetragen haben. Der Markt im Bereich der Datenschutzbildung sieht nicht besser aus. Es sind Ausbilder unterwegs, die selbst gerade einen ersten Blick in die DS-GVO geworfen haben.

Bündnis für die Qualität in der Datenschutzausbildung

Der BvD schlägt vor, eine Zertifizierung für Datenschutzbeauftragte einzuführen, die eine qualifizierte Ausbildung, Erfahrungen und Kenntnisse in den Bereichen Datenschutzrecht, Informationstechnik und Betriebswirtschaft voraussetzt (siehe Berufsbild des Datenschutzbeauftragten – www.bvdnet.de).

Der Berufsverband hat hier bereits Vorarbeit geleistet und eine Selbstverpflichtung geschaffen. Die Datenschutzverbände (BvD und GDD) können hier, ggf. in enger Zusammenarbeit mit weiteren Organisationen, ein Zertifizierungsverfahren aufsetzen, um die Qualifikation zu verbessern und zu standardisieren.

Im Rahmen dieser Qualifizierung würden die Anforderungen an die Ausbildung von Datenschutzbeauftragten je nach Tätigkeitsbereich unterschiedlich hoch sein. Interne (Teilzeit-) Datenschutzbeauftragte eines Unternehmens müssen nicht in gleicher Weise ausgebildet werden, wie externe Datenschutzbeauftragte, die in verschiedenen Branchen und Unternehmensgrößen tätig sind.

Ein in dieser Weise zertifizierter Datenschutzbeauftragter muss im Bereich Datenschutz beraten können, ohne dass daraus eine Verletzung des § 5 Rechtsdienstleistungsgesetz entsteht. Diese Regelung wird seitens der Rechtsanwaltskammern immer wieder gegen Datenschutzberater, die überwiegend erfahrene Praktiker, aber keine niedergelassenen Rechtsanwälte sind, in Stellung gebracht. Ein Bestand der Regelung würde dazu führen, dass die Datenschutzberatung für die Unternehmen nur noch durch einen zugelassenen Rechtsanwalt erfolgen darf, obwohl der Rechtsanwalt i.d.R. keine besonderen Kenntnisse im Bereich Datenschutz, Informationssicherheit, Organisation- und Branchen-Know-how besitzt.

Mit klaren Standards bei der Ausbildung und Qualifikation von Datenschutzbeauftragten fällt es den Unternehmen leichter, die richtigen Datenschutzbeauftragten zu finden.

Handlungsempfehlungen

Schließlich würden dann die Fähigkeiten und Schwerpunkte im Qualifikationsnachweis ausgewiesen. Damit verbessert sich auch die Preistransparenz.

Aufbau einer Infrastruktur zur Zertifizierung im Bereich Datenschutz nach DS-GVO

Die DS-GVO stellt ein System aus Transparenz, Vertrauen und Kontrolle dar, das künftig durch nationale Organisationen auch zertifizierbar sein sollte. Unternehmen sollten ihre Anstrengungen im Bereich Datenschutz durch die Zertifizierung nach außen darstellen können.

Diese Vorgehensweise ist in vielen Bereichen etabliert und wurde früher bereits auch im Datenschutz genutzt (Zertifizierung nach BSI – British Standard Institute). Die gewaltigen Investitionen der Wirtschaft, beispielsweise im Bereich des Qualitäts- oder Umweltmanagements, können durch eine Zertifizierung des jeweiligen Managementsystems als Wettbewerbsvorteil dargestellt werden. Der europäische Gesetzgeber ist mit dieser Struktur den Forderungen aus der Wirtschaft nachgekommen. Nun müssen dringend die Rahmenbedingungen dafür geschaffen werden, dass auch im Bereich Datenschutz eine anerkannte Zertifizierung möglich wird. Zuständig dafür sollen die Datenschutzaufsichtsbehörden sein. Angesichts der fehlenden Erfahrungen und Kapazitäten in diesem Bereich wird die Umsetzung allerdings noch viele Jahre auf sich warten lassen.

Der Vorteil des Datenschutz-Gütesiegels droht verloren zu gehen

So lange kann die deutsche Wirtschaft nicht warten. Wenn erst andere Länder diesen Stand erreicht haben, werden dort die Datenschutz- und Datensicherheitsstandards zur Digitalisierung gesetzt und die deutsche Wirtschaft hat das Nachsehen.

Bundesregierung gefordert

Der große Vorteil der DS-GVO ist vollkommen aus dem Blick geraten. Der deutsche Gesetzgeber, bzw. die Bundesregierung muss diese Aktivitäten mit Nachdruck fördern, damit der Wettbewerbsvorteil im Datenschutz durch die deutschen Unternehmen auch generiert werden kann. Es besteht sonst die Gefahr, dass uns andere Staaten innerhalb oder außerhalb der EU zuvorkommen und den Standard bei dem Gütesiegel setzen, welches für eine erfolgreiche Digitalisierung zukünftig von erheblicher Bedeutung ist.

Fazit: Zunehmend beurteilen Kunden Unternehmen, denen sie ihre Daten anvertrauen sollen, nach deren sichtbaren Maßnahmen zum Datenschutz. Hier muss Deutschland den Standard setzen – in Europa und darüber hinaus, wie bereits bei der Qualität „Made in Germany“.

Handlungsempfehlungen

Hintergrund:

Die DS-GVO will Bürgern in Zeiten von Facebook, WhatsApp und Co. einen besseren Schutz ihrer persönlichen Daten garantieren und war als EU-weit geltendes Datenschutzrecht längst überfällig. Denn personenbezogene Daten sind in unserer zunehmend digitalisierten Welt eine echte Handelsware. Die EU-weite Grundverordnung zielt auf die rapide wachsenden Datenmengen in Unternehmen, bei denen Daten das Kerngeschäft ausmachen. Aber auch Unternehmen mit konventionellen Geschäftsmodellen müssen die Vorgaben beachten. Somit gilt die DS-GVO für internationale Konzerne wie Automobilhersteller oder TV-Geräte-Produzenten genauso wie für den Versicherungsvertreter oder den kleinen Weinhändler. Die DS-GVO steht vor allen nationalen Datenschutzgesetzen und wird durch diese ergänzt. Allerdings sind nicht alle Betroffenenrechte und Vorschriften der DS-GVO für deutsche Unternehmen wirklich neu. Denn in ihrer Grundidee entspricht die DS-GVO in weiten Teilen dem bis dato gültigen deutschen Datenschutzrecht.

Ziele der DS-GVO laut der Bundesregierung:

Berlin, April 2017. Mit der Anpassung des Bundesdatenschutzgesetzes an die Datenschutz-Grundverordnung wird ein großer Schritt zur Angleichung der Datenschutzregelungen in Europa und damit zu einem harmonisierten digitalen Binnenmarkt gemacht. Deutschland hatte bereits in 2017 die erforderlichen Gesetzesänderungen vorgenommen. Damit wurde frühzeitig Rechtsklarheit geschaffen und allen Betroffenen Zeit gegeben, sich auf die neue Rechtslage vorzubereiten. Dazu Auszüge aus der Rede von Bundesinnenminister Dr. Thomas de Maizière:

„Der Datenschutz schützt die Freiheit und die Persönlichkeitsrechte von Menschen. Das ist der Auftrag des Datenschutzrechts, und darum geht es. {...} Wir wollen und werden auch angesichts neuer technischer Entwicklungen das hohe Niveau des Datenschutzes aufrechterhalten und gleichzeitig die modernen technischen Möglichkeiten nutzen – und das in ganz Europa mit demselben Recht. Das war das Anliegen der europäischen Datenschutz-Grundverordnung, und das ist auch das Ziel des vorliegenden Gesetzes. {...}

Ab Mai 2018 werden in Deutschland und allen europäischen Mitgliedstaaten einheitliche Datenschutzregeln und Datenschutzstandards gelten. Das ist eine datenschutzrechtliche Zäsur in Europa, und genau das war auch beabsichtigt. Unternehmen mit niedrigen Datenschutzstandards können sich in Zukunft nicht mehr gezielt in solchen Mitgliedstaaten ansiedeln, die niedrige Standards akzeptieren oder eine unzureichende Datenschutzaufsicht haben. Davon profitieren die Menschen, die Nutzer, die Anwender, die Forscher, und davon profitieren auch die Unternehmen in unserem Land. Es gibt Rechtssicherheit für alle. {...} Das ist ein großer Fortschritt.“

Handlungsempfehlungen

Über den BvD:

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. mit rund 1.400 Mitgliedern fördert und vertritt die Interessen der Datenschutzbeauftragten in Betrieben und Behörden. Der Verband bietet seinen Mitgliedern kompetente Unterstützung bei der täglichen Berufsausübung inklusive umfangreicher Weiterbildungsprogramme. Bei der Weiterentwicklung von Datenschutz und Digitalisierungsprojekten steht der BvD in einem permanenten Austausch mit Politik, Wirtschaft, Wissenschaft und Aufsichtsbehörden. Der BvD ist u. a. Träger der ehrenamtlichen Initiative „Datenschutz geht zur Schule“ und führt – in einer Kooperation mit dem Lehrstuhl Informations- und Technikmanagement der Ruhr-Universität Bochum – das Online-Lexikon Datenschutz-Wiki der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Der BvD in Zahlen:

- Gegründet 1989
- 1.600 Mitglieder insgesamt (Stand September 2018)
- 722 Firmenmitglieder
- 169 registrierte externe Datenschutzbeauftragte
- 332 Selbstverpflichtungen auf unser berufliches Leitbild
- 10 Regionalgruppen bundesweit
- 9 Arbeitskreise

Impressum

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
Budapester Straße 31
10787 Berlin
Telefon (0 30) 26 36 77 60
Telefax (0 30) 26 36 77 63
WWW: www.bvdnet.de
E-Mail: BvD-GS@bvdnet.de

Stand: 28.09.2018