EVERS
Rechtsanwälte für Vertriebsrecht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Umsetzung der Datenschutz-Grundverordnung im Geschäftsbetrieb des bAV-Beraters

Referent: Jürgen Evers

Datum: 12.07.2018

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Datenschutz-Grundverordnung (DSGVO)

- Regelungen der DSGVO sind seit dem 25. Mai 2018 einzuhalten
- wesentliche Inhalte der DSGVO sind für das deutsche Recht nicht neu
- aber: es gibt auch Neuregelungen und Änderungen

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

Datenschutz als Compliance-Maßstab

CAMPUS INSTITUT

- Datenschutz ist den Compliance-Richtlinien eines Unternehmens zuzuordnen
- DSGVO erhöht Anforderungen an den Datenschutz und verschärft Folgen von Verstößen
- Neu: Betroffene haben bei Verstößen gegen das Datenschutzrecht Anspruch auf einen Ersatz für immaterielle Schäden – Schmerzensgeld – (Art. 82 I DSGVO)
- Bußgelder können bis zur Höhe von € 20,0 Mio. oder aber 4% des weltweiten Jahresumsatzes verhängt werden (Art. 83 DSGVO) – es gilt der höhere Wert!

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

Bedeutung der Umsetzung der DSGVO beim bAV-Berater

CAMPUS INSTITUT

- Datenverarbeitung beim bAV-Berater ist vielfach umfangreich und betrifft oft besondere Kategorien personenbezogener Daten (z.B. Gesundheitsdaten, Gewerkschaftszugehörigkeit)
- durch Einbeziehung unterschiedlicher Personengruppen – Arbeitgeber (AG), Versorgungsträger, Arbeitnehmer (AN), Betriebsrat, externe Berater – fallen Verstöße eher auf
- Bußgeldhöhe bei Verstößen kann Geschäftsbetrieb des bAV-Beraters gefährden
- Umsetzung der DSGVO ist für bAV-Berater existentiell

EVERS
Rechtsanwälte für Vertriebsrecht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Umsetzung in 11 Einzelschritten
Schritt 1: Der Datenschutzbeauftragte

Referent: Jürgen Evers

Datum: 12.07.2018

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

1. Der Datenschutzbeauftragte

- Prüfung, ob bAV-Berater einen Datenschutzbeauftragten (DSB) benennen und bekanntmachen muss
- DSB muss benannt werden, wenn bAV-Berater:
  - mindestens 10 Personen ständig mit automatisierter Verarbeitung personenbezogener Daten beschäftigt (§ 38 I1 BDSG)
  - oder wenn Kerntätigkeit „*in umfangreicher Verarbeitung besonderer Kategorien von Daten gemäß Art. 9*“ DSGVO besteht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

1. Der Datenschutzbeauftragte

- DSGVO Erwägungsgrund 91:

„Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn sie Patienten- oder Mandanten-Daten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder RA erfolgt. In diesen Fällen sollte eine Datenschutz- Folgenabschätzung nicht zwingend vorgeschrieben sein.“

  - dieser Erwägungsgrund kann u.E. auch für den Umfang der Verarbeitung besonderer Kategorien personenbezogener Daten herangezogen werden

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

1. Der Datenschutzbeauftragte

- Maßstab dafür, ob bAV-Berater wegen der Verarbeitung besonderer Kategorien personenbezogener Daten einen DSB benennen und bekanntmachen muss, ist der Umfang dieser Datenverarbeitung
- Einzelberater und auch kleine bis mittlere Beratungseinheiten unter 10 Mitarbeitern werden i.A. keinen Datenschutzbeauftragten benennen müssen
- In Zweifelsfällen empfiehlt sich Anfrage beim zuständigen Landesdatenschutzbeauftragten (LDSB) unter Darstellung des Umfangs der Verarbeitung besonderer Kategorien personenbezogener Daten

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

1. Der Datenschutzbeauftragte

- Art. 37 VII DSGVO: DSB muss zuständiger Aufsichtsbehörde bekannt gemacht = zuständigen LDSB genannt werden (für die Meldung haben die LDSB Onlinemeldeverfahren eingeführt)
- Art. 37 VII DSGVO: Kontaktdaten des DSB sind zu veröffentlichen (z.B. auf der vom bAV-Berater unterhaltenen Webseite)

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

1. Der Datenschutzbeauftragte

- wenn ein DSB benannt werden muss: besser „irgend jemanden“ benennen als niemanden – d.h.: ein ggf. auch nicht ausreichend qualifizierter DSB macht die Bemühung um den Datenschutz deutlicher als gar keiner

EVERS
Rechtsanwälte für Vertriebsrecht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Schritt 2: Überprüfung Website und E-Mails

Referent: Jürgen Evers

Datum: 12.07.2018

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

2. Überprüfung Website und E-Mails

- erhebt der bAV-Berater personenbezogene Daten über seine Website, muss er dort die Informationspflichten nach Artt. 13, 14 DSGVO erfüllen (siehe auch Schritt 3: „Erfüllung der Informationspflichten“)
- ist der bAV-Berater, z.B. in einer Kooperationsgemeinschaft, gemeinsam mit einem anderen Dienstleister Verantwortlicher, ist offenzulegen, wer von ihnen welche Verpflichtungen nach Artt. 13, 14 DSGVO erfüllt (Art. 26 DSGVO)

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

2. Überprüfung Website und E-Mails

- gemäß Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) vom 26. April 2018 gelten für sog. Tracking-Mechanismen seit dem 25. Mai 2018 nicht mehr die Bestimmungen §§ 12, 13 , 15 TMG, sondern ausschließlich die Regelungen der DSGVO!
  - d.h.: verwendet bAV-Berater auf seiner Website Cookies oder betreibt er Website-Tracking, ist dies nur zulässig, wenn er ein berechtigtes Interesse geltend machen kann, ein mit dem Betroffenen geschlossener Vertrag dies rechtfertigt oder der Betroffene eingewilligt hat
  - In der Praxis wird am häufigsten die Einwilligung genutzt

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

2. Überprüfung Website und E-Mails

- **Achtung:** die Einwilligung muss die Voraussetzungen Art. 7 DSGVO erfüllen (siehe auch Schritt 4: „Einwilligungserklärungen einholen oder anpassen“)
- zumindest wenn E-Mails besonders sensible Daten beinhalten, sind diese nach Art. 32 Ia DSGVO zu verschlüsseln (LDSB NRW)

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

2. Überprüfung Website und E-Mails

- Unklar ist, ob Betroffener auf Verschlüsselung verzichten kann:

  - das VG Berlin ging für das BDSG davon aus, dass Verzicht des Betroffenen auf die Verschlüsselung zulässig ist (VG Berlin, 24.05.2011 – 1 K 133/10 – Tz. 26)
  - die juristische Literatur und Datenschutzbeauftragte der Länder gehen tendenziell eher davon aus, dass der Betroffene auf die Pflicht zur Verschlüsselung nicht verzichten kann (Gerhards, (Grund-)Recht auf Verschlüsselung?, Diss. jur. 2010; LDSB Berlin, Jahresbericht 2013, S. 161, Verzicht auf Maßnahmen zur Datensicherheit gesetzlich nicht vorgesehen)

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

2. Überprüfung Website und E-Mails

- Problem:
  - lässt sich bAV-Berater Verzicht unterschreiben, wird dies außenwirksam und begründet ein Abmahnrisiko
  - lässt sich bAV-Berater Verzicht nicht unterschreiben, ist das Risiko eines Verstoßes höher
- Risikoabwägung: ist das Entdeckungsrisiko höher als das Verstoßrisiko, oder umgekehrt?

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

2. Überprüfung Website und E-Mails

- Erwägungsgrund 13:

„Organe und Einrichtungen der EU werden ebenso wie die Mitgliedstaaten und deren Aufsichtsbehörden dazu angehalten, bei der Anwendung der DSGVO die besonderen Bedürfnisse von Kleinstunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen.“

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

2. Überprüfung Website und E-Mails

- entspricht die Verschlüsselung dem technischen Standard für Kleinstunternehmen oder handelt es sich um ein größeres Unternehmen, ist von der Verschlüsselungspflicht auszugehen
- Empfehlung: E-Mailverschlüsselung oder bei Kleinstunternehmen Berufung auf Erwägungsgrund 13 und die Verhältnismäßigkeit
- bAV-Beratern, die z.B. Gesundheitsdaten verarbeiten, ist eher auch bei Kleinstunternehmen die Verschlüsselung zu empfehlen

EVERS
Rechtsanwälte für Vertriebsrecht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Schritt 3: Erfüllung der Informationspflichten

Referent: Jürgen Evers

Datum: 12.07.2018

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

3. Erfüllung der Informationspflichten

- werden Daten beim Betroffenen selbst erhoben, greifen Informationspflichten nach Art. 13 DSGVO
- werden Daten über den Betroffenen bei Dritten erhoben (z.B. in der Lohnbuchhaltung des AG über dessen AN), greifen die Informationspflichten nach Art. 14 DSGVO

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

3. Erfüllung der Informationspflichten

- **Achtung:** bAV-Berater ist, wenn er AN-Daten beim AG erhebt, kein Auftragsverarbeiter, da er die Daten zur Erfüllung eines eigenen Vertragszwecks – Beratung des AG – erhebt; für ihn gilt daher Art. 14 DSGVO im Verhältnis zu den AN
- entweder müssen die Daten der AN daher so pseudonymisiert werden, dass eine Identifizierung der AN nicht möglich ist, oder es müssen die Informationspflichten nach Art. 14 DSGVO vom bAV-Berater gegenüber dem AN erfüllt werden
- Folgende Informationen sind eingeführt worden:

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

3. Erfüllung der Informationspflichten

- wenn Datenverarbeitung auf berechtigtes Interesse des Verantwortlichen gestützt wird, um welches Interesse es sich handelt;
- Speicherdauer personenbezogener Daten oder Angabe der Kriterien, nach denen sich die Speicherdauer bemisst;
- Rechte des Betroffenen: Auskunft; Berichtigung; Löschung; Einschränkung der Verarbeitung; Widerspruchsrecht; Datenübertragbarkeit
- Widerruflichkeit einer erteilten Einwilligung und dass Widerruf nicht zurückwirkt
- Beschwerderecht bei einer Aufsichtsbehörde

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

3. Erfüllung der Informationspflichten

- Informationen sind auf Website des bAV-Beraters zur Verfügung zu stellen und bei erster Datenerhebung bei dem Betroffenen diesem zu überlassen;
- außerhalb der Website können online eingestellte Informationen in Papierform verwendet werden; Inhalte sind insoweit identisch;
- werden Daten bei Dritten erhoben, sind die Informationspflichten gegenüber dem Betroffenen, z.B. gegenüber dem AN, spätestens innerhalb eines Monats zu erteilen (Art. 14 IIIa DSGVO)

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

3. Erfüllung der Informationspflichten

- um Informationspflichten erfüllen zu können, muss bAV-Berater zunächst die einzelnen Vorgänge der Datenverarbeitung in seinem Unternehmen nach Kategorie von Betroffenen und Form der Datenverarbeitung analysieren und dokumentieren

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

3. Erfüllung der Informationspflichten

- im Bereich der bAV-Beratung kommen z.B. folgende Datenverarbeitungsvorgänge in Betracht (nicht abschließend):
  - Erhebung von Unternehmensdaten beim AG
  - Erhebung von AN-Daten beim AG
  - Erhebung von Kundendaten beim Privatkunden
  - Weitergabe von Unternehmens-, AN- oder Kundendaten an Pools/Verbünde/Back-Office-Dienstleister oder Versorgungsträger (jeweils getrennt betrachtet)

EVERS
Rechtsanwälte für Vertriebsrecht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Schritt 4: Einwilligungserklärungen einholen oder überarbeiten

Referent: Jürgen Evers

Datum: 12.07.2018

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

4. Einwilligungserklärung einholen / überarbeiten

- für bAV-Berater empfiehlt sich grundsätzlich, eine weitreichende Einwilligungserklärung des Betroffenen einzuholen (Verarbeitung von Gesundheitsdaten)
- Beschluss Düsseldorfer Kreis vom 13./14.09.2016 – Alteinwilligungen gelten fort, wenn diese nach der bisherigen Rechtslage wirksam gewesen sind und der Art nach der DSGVO entsprechen (!), ausgenommen:
  - es fehlt an der Freiwilligkeit der Einwilligung – was schon bei der Verwendung von AGB der Fall sein kann (!)
  - die Altersgrenze von 16 Jahren wurde für die Einwilligung nicht beachtet

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

4. Einwilligungserklärung einholen / überarbeiten

- Achtung bei Alteinwilligungen: Die Formulierung des Düsseldorfer Kreises ist durchaus missverständlich und unklar, welche Alteinwilligungen fortgelten können
- Formulierungen nach ist jede Alteinwilligung auf Vereinbarkeit mit DSGVO zu prüfen
- Empfehlung: Alteinwilligungen auch für Altfälle entsprechend der DSGVO neu einholen, z.B. zum nächsten turnusmäßigen Beratungstermin bei dem AG

EVERS
Rechtsanwälte für Vertriebsrecht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Schritt 5: IT-Sicherheit, Technisch-organisatorische Maßnahmen („TOM“)

Referent: Jürgen Evers

Datum: 12.07.2018

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

5. IT-Sicherheit und „TOM“

- bislang geregelt in Anlage zu § 9 I BDSG – „acht Gebote der Datensicherheit“
- z.T. werden diese „acht Gebote“ in Artt. 28, 32 DSGVO aufgegriffen, z.T. kommen neue Verpflichtungen hinzu, z.T. werden Verpflichtungen abgeschafft
- Wichtig: Die Maßnahmen des bAV-Beraters zur Datensicherheit und zu „TOMs“ sollten als Leitlinien dokumentiert werden, um sie auf Anfrage der zuständigen Aufsichtsbehörde vorlegen zu können (*„RiLi zur IT-Nutzung und -Sicherheit“*)

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

5. IT-Sicherheit und „TOM“

- übernommen wurden, mit anderen Begriffen, aus Anlage zu § 9 I BDSG in Art. 32 Ib DSGVO:
  - Zutrittskontrolle: Maßnahmen, die
    - Unbefugten Zutritt zu Datenverarbeitungsanlagen des Betroffenen verwehren
    - verhindern, dass Unbefugte Datenverarbeitungsanlagen des Betroffenen nutzen können
  - Zugriffskontrolle: Maßnahmen, die sicherstellen, dass nutzungsberechtigte Personen nur auf solche Daten zugreifen können, auf die sie zugreifen dürfen
  - Weitergabekontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten bei/während Speicherung, Übertragung oder Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

5. IT-Sicherheit und „TOM“

- übernommen wurde ausdrücklich aus Anlage zu § 9 I BDSG in Art. 32 Ia DSGVO:
  - Verschlüsselungspflicht: Maßnahmen zur Verschlüsselung von Daten, soweit dem Datenschutz angemessen
- übernommen wurde ausdrücklich aus Anlage zu § 9 I BDSG in Art. 32 Ib, c DSGVO:
  - Verfügbarkeitskontrolle: Maßnahmen zum Schutz der Daten vor zufälliger Zerstörung oder Verlust (Datensicherung) sowie zur Wiederherstellung von Daten

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

5. IT-Sicherheit und „TOM“

- neu hinzugekommen ist in Art. 32 Ia DSGVO:
  - Pseudonymisierung: Maßnahmen, die gewährleisten, dass Daten nur unter Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden können
- neu hinzugekommen ist in Art. 32 Id DSGVO:
  - regelmäßige Überprüfung, Bewertung und Evaluierung der TOM: Maßnahmen, die gewährleisten, dass die TOM dauerhaft die Datensicherheit sicherstellen

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

5. IT-Sicherheit und „TOM“

- nur noch Auftragsverarbeiter trifft Pflicht nach Anlage 1 zu § 9 I BDSG gemäß Art. 28 DSGVO:
  - Auftragskontrolle: Maßnahmen, die sicherstellen, dass Daten, die im Wege der Auftragsverarbeitung überlassen werden, nur entsprechend der Weisungen des Verantwortlichen verarbeitet werden

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

5. IT-Sicherheit und „TOM“

- nicht übernommen wurde die folgende Pflicht nach Anlage 1 zu § 9 I BDSG:
  - Eingabekontrolle: Maßnahmen, mit denen sich nachträglich feststellen lässt, ob und von wem Daten in Datenverarbeitungssysteme eingegeben wurden oder dort verändert oder entfernt worden sind
  - **Achtung:** Maßnahmen zur Eingabekontrolle können aber als allgemeine Kontrollaufgabe, speziell zur Zugriffs- und Weitergabekontrolle notwendig sein
  - **Achtung:** bezogen auf die Verarbeitung von Daten zur Eingabekontrolle bedarf es eigenständiger Erlaubnisnorm (Abwägung Beschäftigtendatenschutz mit Art. 6 If DSGVO – berechtigte Interessen des Verantwortlichen)

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

5. IT-Sicherheit und „TOM“

- nicht übernommen wurde die folgende Pflicht nach Anlage 1 zu § 9 BDSG:
  - Trennungsgebot: Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können
  - **Achtung:** Trennungsgebot kann als Zugriffskontrolle unselbständig zu berücksichtigen sein

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

5. IT-Sicherheit und „TOM“

- Checklisten für Maßnahmen zur Datensicherheit:
  - https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
  - http://www.gppag.de/downloads/201507_isapluskatalog.pdf
  - „PrivazyPlan“ der SecureData, Kapitel 5.1

  Anhand dieser Checklisten kann eigene *„RiLi zur IT- und Datensicherheit des bAV-Beraters“* erstellt werden

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

5. IT-Sicherheit und „TOM“

- auf eigene *RiLi zur IT- und Datensicherheit* sollte bAV-Berater jeden Beschäftigten verpflichten, soweit dieser personenbezogene Daten verarbeitet oder bei der Verarbeitung mitwirkt
- *RiLi zur IT- und Datensicherheit* sollte auch eine regelmäßige Schulung der Beschäftigten als Maßnahme der regelmäßigen Überprüfung, Bewertung und Evaluierung vorsehen

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

5. IT-Sicherheit und „TOM“

- Art. 32 II DSGVO verpflichtet zu „angemessenem“ Schutzniveau, nicht zu perfektem, optimalen oder bestmöglichen
- Schutzniveau muss nach Art. 32 II DSGVO angemessen im Verhältnis zu bestehenden Risiken (insbesondere der Vernichtung, des Verlusts, der Veränderung oder unbefugten Offenlegung, des unbefugten Zugangs von personenbezogenen Daten) sein

EVERS
Rechtsanwälte für Vertriebsrecht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Schritt 6: Allgemeine Datenschutzprinzipien

Referent: Jürgen Evers

Datum: 12.07.2018

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

6. Allgemeine Datenschutzprinzipien

- Richtigkeit der personenbezogenen Daten (Art. 5 Id DSGVO, Erwägungsgrund 39):
  - personenbezogene Daten müssen jederzeit richtig sein, d.h. den Tatsachen entsprechen und vollständig sein
  - sind die Daten dies nicht, müssen sie korrigiert, d.h. berichtigt bzw. vervollständigt werden
  - baV-Berater muss Maßnahmen vorsehen und dokumentieren, die gewährleisten, dass Daten „unverzüglich“ korrigiert werden
  - „unverzüglich“ bedeutet rechtlich ohne schuldhaftes Zögern und meint einen Zeitrahmen von bis zu drei Tagen nach Kenntniserlangung

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

6. Allgemeine Datenschutzprinzipien

- auch die allgemeinen Datenschutzprinzipien sind z.T. bereits von der bisherigen Rechtslage bekannt bzw. werden z.T. neu eingeführt
- Liste der allgemeinen Datenschutzprinzipien gemäß Art. 5 I DSGVO
- der bAV-Berater muss gegenüber den Aufsichtsbehörden Rechenschaft darüber ablegen können, dass und wie er die Umsetzung der allgemeinen Datenschutzprinzipien in seinem Betrieb sichergestellt hat
- die Rechenschaftspflicht umfasst Pflicht zur Dokumentation („Unternehmens-RiLi zum Datenschutz“)

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

6. Allgemeine Datenschutzprinzipien

- Prinzip der Rechtmäßigkeit (Art. 5 Ia DSGVO):
  - ergibt sich aus der Erlaubnis zur Datenverarbeitung („Verbot mit Erlaubnisvorbehalt“)
  - als eigenständiges Datenschutzprinzip hat Rechtmäßigkeit keine praktische Bedeutung
  - in Dokumentation sollte das Prinzip gleichwohl dargestellt werden

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

6. Allgemeine Datenschutzprinzipien

- Prinzip der Datenverarbeitung nach Treu und Glauben (Art. 5 Ia DSGVO):
  - unbestimmter Rechtsbegriff, der definiert wird als: „das Verhalten eines redlich und anständig Handelnden“
  - im Vergleich mit den Sprachregelungen anderer EU-Staaten bedeutet „Treu und Glauben“ hier: „fair“ – faire Verarbeitung von Daten (ebenfalls unbestimmt)
  - für die Dokumentation sollte auf beide unbestimmte Rechtsbegriffe: „Datenverarbeitung nach Treu und Glauben“ und „fairer Umgang mit personenbezogenen Daten“ abgestellt werden

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

6. Allgemeine Datenschutzprinzipien

- Prinzip der Transparenz (Art. 5 Ia DSGVO):
  - bezieht sich auf die Informationspflichten gegenüber Betroffenen, aber auch auf Auskunftsrechte des Betroffenen gegenüber Verantwortlichem
  - zu dokumentieren wäre, dass und wie bAV-Berater Informationspflichten einerseits und Auskunftsrechte Betroffener andererseits berücksichtigt

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

6. Allgemeine Datenschutzprinzipien

- Datenverarbeitung nur für festgelegte, eindeutige und legitime Zwecke (Art. 5 Ib DSGVO):
  - Verantwortlicher muss Zwecke der Datenverarbeitung für jede Datenverarbeitung definieren
  - Zweck der Datenverarbeitung muss eindeutig bestimmt sein
  - Zweck der Datenverarbeitung muss bei Erhebung der Daten feststehen; deshalb Zweckbestimmung nicht zu eng fassen!
  - jeder Zweck der Datenverarbeitung muss rechtmäßig sein

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

6. Allgemeine Datenschutzprinzipien

- Datenverarbeitung nur für festgelegte, eindeutige und legitime Zwecke (Art. 5 Ib DSGVO, Erwägungsgrund 39):
  - Achtung: auch wenn Zweck der Verarbeitung weit gefasst wird, ist immer darauf zu achten, dass Erlaubnistatbestand nach Art. 6 DSGVO erfüllt sein muss
  - daraus kann folgen, dass Rechtmäßigkeit des Zwecks nur sichergestellt werden kann, wenn er gerade nicht weit gefasst wird

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

6. Allgemeine Datenschutzprinzipien

- Datenminimierung (Art. 5 Ic DSGVO, Erwägungsgrund 39):
  - personenbezogene Daten dürfen nur verarbeitet werden, wenn der Zweck, der mit Datenverarbeitung verfolgt wird, nicht auch auf andere Weise erreicht werden kann
  - wenn Datenverarbeitung als solche erforderlich ist, dürfen auch nur die Daten verarbeitet werden, die zur Zweckerreichung erforderlich sind
  - in Dokumentation sind Löschfristen für Daten vorzusehen
  - ebenso muss bAV-Berater regelmäßige Prüfung der Notwendigkeit von Datenverarbeitung und -speicherung sowie möglicher Löschung einplanen

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

6. Allgemeine Datenschutzprinzipien

- Erwägungsgrund 39:

„Um sicherzustellen, dass personenbezogene Daten nicht länger als nötig gespeichert werden, sollte Verantwortlicher Fristen für Löschung oder regelmäßige Überprüfung vorsehen.“

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

6. Allgemeine Datenschutzprinzipien

- Speicherbegrenzung (Art. 5 Ie DSGVO):
  - Verantwortlicher muss festlegen, wie lange er personenbezogene Daten speichert
  - Speicherung darf nur so lange erfolgen, *„wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“*
  - für Bemessung der Speicherdauer kann auf Zwecke, für die die Daten verarbeitet werden, abgestellt werden

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

6. Allgemeine Datenschutzprinzipien

- Speicherbegrenzung (Art. 5 Ie DSGVO), Beispiel:

  „Die Speicherung Ihrer Daten erfolgt so lange, wie das mit Ihnen bestehende Vertragsverhältnis dies erfordert, damit wir die uns obliegenden Aufgaben erfüllen können, Ihnen bedarfsgerechte Verträge zu vermitteln und Sie vertragsbegleitend zu betreuen und zu beraten. Auch nach Beendigung unseres Auftrages halten wir Ihre Daten gespeichert, soweit wir diese benötigen, um Ihnen oder Dritten gegenüber erforderlichenfalls Rechenschaft über den uns erteilten Auftrag und dessen Ausführung ablegen zu können oder um eigene Rechte oder Ansprüche wahrzunehmen oder geltend zu machen.“

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

6. Allgemeine Datenschutzprinzipien

- Integrität und Vertraulichkeit (Art. 5 If DSGVO, Erwägungsgrund 39):
  - Verarbeitung personenbezogener Daten nur dann, wenn deren „angemessene“ Sicherheit gewährleistet ist
  - Daten sind zu schützen vor unbefugter oder unrechtmäßiger Verarbeitung; unbeabsichtigten Verlust, unbeabsichtigter Zerstörung sowie unbeabsichtigter Schädigung
  - Unbefugte dürfen keinen Zugang zu den Daten haben und dürfen auch Geräte, auf denen die Daten verarbeitet werden, nicht benutzen
  - das Prinzip greift damit TOM in Bezug auf Zutrittskontrolle u.a. auf
  - in der Dokumentation kann zur Wahrung von Integrität und Vertraulichkeit auf TOMs verwiesen werden

EVERS
Rechtsanwälte für Vertriebsrecht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Schritt 7: Verfahrensverzeichnis

Referent: Jürgen Evers

Datum: 12.07.2018

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

7. Verfahrensverzeichnis

- ein Verfahrensverzeichnis muss nach Art. 30 V DSGVO geführt werden, wenn:
  - Verantwortlicher mindestens 250 Mitarbeiter beschäftigt
  - vom Verantwortlichen vorgenommene Datenverarbeitung Risiken für Rechte oder Freiheiten des Betroffenen birgt
  - Datenverarbeitung nicht nur gelegentlich erfolgt
  - Datenverarbeitung die Verarbeitung besonderer Kategorien personenbezogener Daten mit umfasst

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

7. Verfahrensverzeichnis

- bAV-Berater sind daher im Regelfall zur Führung eines Verfahrensverzeichnisses verpflichtet, weil:
  - Verarbeitung personenbezogener Daten zählt zu Grundfunktionen
  - Gesundheitsdaten werden im Personengeschäft vielfach verarbeitet

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

7. Verfahrensverzeichnis

- Verfahrensverzeichnis muss folgenden Inhalt aufweisen (Liste Art. 30 I2 DSGVO):
  - Namen und Kontaktdaten des Verantwortlichen, dessen Vertreters (z.B. Geschäftsführer) und auch eines etwaigen Datenschutzbeauftragten
  - Zwecke der Datenverarbeitung – auch hier: entsprechend dem Datenschutzprinzip der Zweckbestimmung möglichst weit gefasst
  - Beschreibung der Kategorien betroffener Personen
  - Beschreibung der Kategorien personenbezogener Daten, die verarbeitet werden, ggf. nach dem jeweiligen Zweck kategorisiert
  - Kategorien von Empfängern (z.B. Auftragsverarbeiter, Versorgungsträger, VU, FA)
  - falls relevant, Übermittlung von Daten in ein Drittland
  - wenn möglich, Angabe der Löschfristen
  - wenn möglich, allgemeine Beschreibung der TOM

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

7. Verfahrensverzeichnis

- verantwortlich für das Verfahrensverzeichnis ist mit der DSGVO der Verantwortliche, bzw. dessen Vertreter, nicht mehr der DSB (Art. 30 I1 DSGVO)
- auch Auftragsverarbeiter müssen Verfahrensverzeichnis führen, wenn auf sie keine Ausnahme zutrifft
- bisher (§§ 4g II2, 4e S. 1 Nr. 1 bis 8 BDSG) war das Verfahrensverzeichnis allgemein zugänglich zu machen (externes Verfahrensverzeichnis); diese Pflicht entfällt mit der DSGVO

EVERS
Rechtsanwälte für Vertriebsrecht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Schritt 8: Folgenabschätzung

Referent: Jürgen Evers

Datum: 12.07.2018

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

8. Folgenabschätzung

- bAV-Berater sind im Regelfall dann nicht zu einer Durchführung der Folgenabschätzung verpflichtet, wenn es sich bei Ihnen um Einzelberater handelt oder um Betriebseinheiten bis zu einer mittleren Größe (Erwägungsgrund 91):

> *„Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder RA erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.“*

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

8. Folgenabschätzung

- der Vergleich mit einem einzelnen Arzt bzw. sonstigen Angehörigen eines Gesundheitsberufs macht deutlich, dass der bAV-Berater Gesundheitsdaten mindestens in einem Umfang verarbeiten muss, der den bei einem Arzt übersteigt, um zu einer Folgenabschätzung verpflichtet zu sein; das ist typischerweise nicht der Fall

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

8. Folgenabschätzung

- Inhalt der Folgenabschätzung (Art. 35 VII DSGVO):
  - Beschreibung Datenverarbeitungsvorgänge und verbundener Zwecke
  - Verfolgt Verantwortlicher mit Datenverarbeitung berechtigtes Interesse (Art. 6 If DSGVO), muss dieses beschrieben werden (z.B. Direktwerbung)
  - Bewertung Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitungsvorgänge in Bezug auf den Zweck
  - Bewertung Risiken für Rechte und Freiheiten für Betroffene
  - Maßnahmen zur Bewältigung, Vermeidung oder Begrenzung der Risiken

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

8. Folgenabschätzung

- im Wesentlichen handelt es sich bei der Folgenabschätzung damit um ein vorweggenommenes Verfahrensverzeichnis mit Risikobewertung
- Betroffene müssen u.U. in die Folgenabschätzung einbezogen werden (Art. 35 IX DSGVO):

  „Verantwortlicher holt ggf. den Standpunkt des Betroffenen oder seines Vertreters zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.“

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

8. Folgenabschätzung

- auch wenn bAV-Berater nicht verpflichtet sein sollte, Folgenabschätzung durchzuführen, empfiehlt sich, neue Datenverarbeitungsvorgänge anhand der Folgenabschätzung zu prüfen, bevor sie ins Werk gesetzt werden

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

8. Folgenabschätzung

- ergibt Folgenabschätzung, dass Datenverarbeitungsvorgang:
  - zulässig ist, kann er durchgeführt werden
  - unzulässig ist, darf er nicht durchgeführt werden
  - möglicherweise unzulässig ist, weil Verarbeitung hohes Risiko zur Folge hätte, das nicht durch angemessene Maßnahmen beschränkt werden kann, konsultiert Verantwortlicher vor der Datenverarbeitung die zuständige Aufsichtsbehörde (Art. 36 I DSGVO)

EVERS
Rechtsanwälte für Vertriebsrecht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Schritt 9: Anweisung und Verpflichtung von Beschäftigten

Referent: Jürgen Evers

Datum: 12.07.2018

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

9. Anweisung und Verpflichtung von Beschäftigten

- der bAV-Berater muss natürliche Personen, die ihm unterstellt sind und die Zugang zu personenbezogenen Daten haben, auf die sie treffende Pflichten in Bezug auf Datenverarbeitung und Datenschutz hinweisen und auf die Einhaltung verpflichten (Art. 32 IV DSGVO)
- hierfür genügt es üblicherweise, wenn bAV-Berater Beschäftigte auf folgende Richtliniendokumente verpflichtet:
  - „RiLi zur IT-Nutzung und -Sicherheit“ (Dokumentation gemäß Schritt 5)
  - „Unternehmens-RiLi zum Datenschutz“ (Dokumentation gemäß Schritt 6)

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

9. Anweisung und Verpflichtung von Beschäftigten

- Leitlinien der Aufsichtsbehörden:

https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Internationales/Datenschutz-Grundverordnung/Kurzpapiere_der_DSK_als_Auslegungshilfen_zur_DSGVO/DSK_KP Nr_19_Verpflichtung_Beschaeftigte.pdf

https://www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

9. Anweisung und Verpflichtung von Beschäftigten

- **Achtung:** angemessene Information und Verpflichtung von Beschäftigten wirkt sich auf Haftung des bAV-Beraters aus:
  - wurden Beschäftigte angemessen unterrichtet und angewiesen und verstößt einer gegen Bestimmungen zum Datenschutz, entscheidet er selbst i.S.d. Art. 4 Nr. 7 DSGVO über die Datenverarbeitung, ist damit Verantwortlicher und schuldet ein Bußgeld, das verhängt wird, voraussichtlich selbst (!), wenn er vorsätzlich oder u.U. grob fahrlässig gehandelt hat
  - hat der Verantwortliche die Unterrichtung und Anweisung dagegen unterlassen oder nicht hinreichend verständlich formuliert, bleibt Haftung bei ihm

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

9. Anweisung und Verpflichtung von Beschäftigten

- Anweisung und Unterrichtung der Beschäftigten sollte bAV-Berater in regelmäßigen Abständen oder bei Änderungen wiederholen; s.o. Schritt 5:

„regelmäßige Überprüfung, Bewertung und Evaluierung der TOM: Maßnahmen, die gewährleisten, dass die TOM dauerhaft die Datensicherheit sicherstellen“

„die interne RiLi sollte auch eine regelmäßige Schulung der Beschäftigten als Maßnahme der regelmäßigen Überprüfung, Bewertung und Evaluierung vorsehen“

EVERS
Rechtsanwälte für Vertriebsrecht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Schritt 10: Datenübertragbarkeit sicherstellen

Referent: Jürgen Evers

Datum: 12.07.2018

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

10. Datenübertragbarkeit sicherstellen

- insbesondere im Bereich der bAV-Beratung werden überdurchschnittlich häufiger als in anderen Branchen:
  - andere Dienstleister in Beratung einbezogen, denen der Betroffene die ihn betreffenden Daten zur Verfügung stellen will
  - Berater gewechselt

- der bAV-Berater muss sich daher darauf einstellen, Daten des Betroffenen vergleichsweise schnell nach Art. 20 DSGVO zu übertragen

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

10. Datenübertragbarkeit sicherstellen

- Recht des Betroffenen, die ihn betreffenden personenbezogenen Daten in folgender Form zu erhalten (Art. 32 I DSGVO):

  - strukturiert
  - gängiges Format
  - maschinenlesbares Format

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

10. Datenübertragbarkeit sicherstellen

- Recht des Betroffenen, dass bAV-Berater die ihn betreffenden personenbezogenen Daten in derselben Form an einen anderen Verantwortlichen direkt übermittelt, sofern dies technisch machbar ist (Art. 32 II DSGVO)
- das Recht des Betroffenen besteht nur, wenn:
  - bAV-Berater die Daten direkt von dem Betroffenen erhalten hat – d.h. z.B. nicht, wenn ihm der AG die Beschäftigtendaten bereitgestellt hat (hier kann dann aber u.U. ein Anspruch des Betroffenen auf Löschung bestehen)
  - Verarbeitung auf Einwilligung oder auf Vertrag beruht – d.h. z.B. nicht, wenn bAV-Berater Daten aufgrund berechtigten Interesses erhoben hat

EVERS
Rechtsanwälte für Vertriebsrecht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Schritt 11: Verhalten bei DS-Verletzungen festlegen

Referent: Jürgen Evers

Datum: 12.07.2018

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

11. Verhalten bei DS-Verletzungen festlegen

- bAV-Berater ist verpflichtet, Datenschutzverletzungen zu dokumentieren (Art. 33 V DSGVO):

  „Verantwortlicher dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung stehenden Fakten, deren Auswirkungen und ergriffene Abhilfemaßnahmen. Dokumentation muss Aufsichtsbehörde Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.“

- Aufsichtsbehörde kann vom bAV-Berater verlangen, Zugang zur Dokumentation der Datenschutzverletzungen zu erhalten, bzw. diese zur Verfügung gestellt zu bekommen (Art. 58 Ia, Ie DSGVO)

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

11. Verhalten bei DS-Verletzungen festlegen

- Datenschutzverletzung liegt vor und ist zu dokumentieren, wenn sie folgende Voraussetzungen erfüllt (Art. 4 Nr. 12 DSGVO):

> *„Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;“*

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

11. Verhalten bei DS-Verletzungen festlegen

- eine Datenschutzverletzung kann schon vorliegen, wenn bAV-Berater Daten des Betroffenen unzulässig erhoben oder sonst verarbeitet hat (z.B., weil ihm vom Arbeitgeber „zu viele Daten“ übermittelt worden sind)
- zu dokumentieren sind (mindestens):
  - alle im Zusammenhang mit Verletzung stehenden Fakten (weitreichende Formulierung der Dokumentationspflicht)
  - Auswirkungen der Verletzung (z.B. Weitergabe an Dritte)
  - Maßnahmen zur Abhilfe (z.B. vorübergehende Sperrung und Information an Dritte, an die die Daten übermittelt worden sind)

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

11. Verhalten bei DS-Verletzungen festlegen

- Meldepflichten des bAV-Beraters:
  - unverzügliche Benachrichtigung des Betroffenen über Verstoß, d.h. innerhalb von maximal drei Tagen (Art. 32 II DSGVO)
  - Ebenfalls innerhalb von maximal drei Tagen – 72 Stunden – Meldung an Aufsichtsbehörde (Art. 33 I DSGVO, mit dem Inhalt gemäß Art. 33 III DSGVO)

EVERS
Rechtsanwälte für Vertriebsrecht

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Fazit

Referent: Jürgen Evers

Datum: 12.07.2018

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

CAMPUS INSTITUT

Fazit

Bei strukturiertem Vorgehen ist Umsetzung von DSGVO für bAV-Berater kein Hexenwerk:

- Klärung Erfordernis DSB
- Website anpassen, für E-Mail-Verschlüsselung sorgen
- Informationspflichten erfüllen
- Einwilligungserklärungen renovieren
- Datenschutzprinzipien beachten
- IT-Sicherheit und TOM dokumentieren
- Verfahrensverzeichnis anlegen
- Erfordernis einer Folgenabschätzung klären
- Beschäftigte einbeziehen
- Datenübertragbarkeit gewährleisten
- Verhaltensplan für DS-Verletzungen

0421 696 77 0
kanzlei@evers-vertriebsrecht.de

Bremen:

Schwachhauser Heerstraße 25
28211 Bremen

München:

Prinzregentenplatz 14
81675 München

Jürgen Evers, Inh.
Britta Oberst
Sascha Alexander Stallbaum
Reinhold Friele
Dr. Friedemann Utz
Evelin Freundt

Kontakt PR (Yener Coombs):
Y.Coombs@evers-vertriebsrecht.de