bAV in Zeiten der DSGVO – Datenschutzrechtliche Brennpunkte

Dr. Thomas Granetzny

Kölner Tage Betriebsrente – 24.01.2020

Freshfields Bruckhaus Deringer

Rechtslage seit dem 25.05.2018

Die Datenschutz-Grundverordnung (**DSGVO**)

- **Ein** Regelwerk für **alle** EU Mitgliedstaaten im Hinblick auf die Verarbeitung personenbezogener Daten
- Erhebliche Relevanz auch für die betriebliche Altersversorgung
- Unmittelbares Gesetzesrecht (Art. 288 AEUV)
- **BDSG n.F.** dient der Umsetzung der DSGVO und nutzt die darin vorgesehenen Öffnungsklauseln

Personenbezogene Daten

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung oder besonderen persönlichen Merkmalen identifiziert werden kann, Art. 4 Nr. 1 DSGVO.

Sensible personenbezogene Daten

- Rasse oder ethnische Herkunft
- Politische und religiöse Anschauungen
- Sexualleben
- **Physische oder psychische Gesundheit**
- Gewerkschaftszugehörigkeit
- Daten über Straftaten

Verarbeitung

Beschreibt jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, Art. 4 Nr. 2 DSGVO. Darunter fallen insbesondere:

- Erhebung
- Erfassung
- Organisation
- Speicherung
- Anpassung oder Veränderung
- Filterung
- Abfrage
- Verwendung
- Bereitstellung
- Ausrichtung
- Verknüpfung
- Einschränkung
- Löschung
- Vernichtung

Wer ist für die Datenverarbeitung verantwortlich?

Verantwortlicher
Entscheidet über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten

Vertragliche Vereinbarung zur Datenverarbeitung

Auftragsverarbeiter
Verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen

Pflichten des Verantwortlichen und des Auftragsverarbeiters unter der DSGVO

Verantwortlicher

- Wahrung der Grundsätze der Datenverarbeitung (Art. 5 und 6 DSGVO)
- Informationspflichten (Art. 13, 14 DSGVO)
- Pflichten infolge der Wahrnehmung von Rechten Betroffener (Art. 15 – 22 DSGVO)
- Weitreichende Dokumentationspflicht (Verarbeitungsverzeichnis)
- Risikoreiche Verarbeitung: Datenschutzfolgeabschätzung
- Data Breach: Meldepflicht
- Ggf. Bestellung eines Datenschutzbeauftragten
- Besondere Pflichten bei Übermittlung von Daten an EU/EWR-Drittländer (Art. 44-50)

Auftragsverarbeiter

Wird aufgrund eines Vertrages mit dem Verantwortlichen tätig, ist aber unmittelbar Adressat eigener Pflichten unter der DSGVO (Art. 27 ff. DSGVO).

- Verarbeitung nur auf Weisung des Verantwortlichen
- Unterstützung des Verantwortlichen bei der Wahrnehmung seiner Pflichten unter der DSGVO
- Weitreichende eigenständige Dokumentationspflicht (Verarbeitungsverzeichnis)
- Pflicht zur Vornahme technisch-organisatorischer Maßnahmen (TOM)
- Meldung von Sicherheitsverstößen an den Verantwortlichen
- Bestellung eines Datenschutzbeauftragten

Übermittlung innerhalb des Konzerns und Joint Control

Übermittlung innerhalb des Konzerns

- Datenübermittlung einer Tochtergesellschaft an die Mutter oder an eine andere Tochter bedarf stets eines eigenständigen Erlaubnistatbestandes → **kein Konzernprivileg unter der DSGVO**
- Datenübermittlungen innerhalb einer Konzerngruppe können jedoch oft über ein **berechtigtes Interesse** gerechtfertigt werden

Gemeinsame Verantwortlichkeit (sog. joint control nach Art. 26 DSGVO)

- Soweit bestimmte Verantwortliche **gemeinsam über Mittel und Zweck der Datenverarbeitung** bestimmen, müssen zwischen diesen Verträge abgeschlossen werden, die die jeweiligen Rechte und Pflichten in datenschutzrechtlicher Hinsicht abgrenzen („JCA")
- Nicht erforderlich: Vollständige gleichrangige Kontrolle über Datenverarbeitung (vgl. Facebook, Zeugen Jehovas)
- Sofern die beiden Verantwortlichen jeweils eigene Interessen verfolgen und somit keine tatsächliche/ rechtliche Einflussmöglichkeit auf den jeweils anderen Verantwortlichen existiert, ist eine gemeinsame Verantwortlichkeit nicht gegeben

Sanktionen bei Verstößen gegen die DSGVO

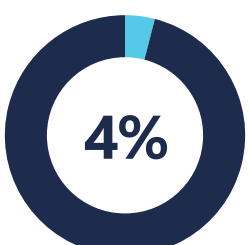
Je nachdem, welcher Betrag höher ist

Bis zu

€20m

oder

4%
des weltweit erzielten Jahresumsatzes



Konsequenzen außerhalb der DSGVO

Datenschutzrechtliche Verstöße können auch außerhalb der DSGVO zu Konsequenzen führen

Mögliche Strafbarkeit nach § 206 StGB bei unerlaubter Einsichtnahme in Telekommunikations-daten

Bußgelder bei Organisations-verschulden der Geschäftsleitung (§§ 30, 130 OwiG)

Haftung des Vorstandes ggü. der Gesellschaft (§ 93 II 1 AktG)

Datenschutz in der betrieblichen Altersversorgung

Datenschutzrechtliche Verantwortlichkeit und Handlungspflichten

Relevanz der DSGVO in der bAV

- **Im pensionsrechtlichen Kontext werden eine Vielzahl personenbezogener Daten verarbeitet. Hierzu gehören**
  - Geburtsdatum
  - Geschlecht
  - Anschrift
  - Familienstand
  - Eintrittsdatum
  - Gehaltsbestandteile, Umfang einer monatlichen Entgeltumwandlung
  - Ggf. Gesundheitsdaten und krankheitsbedingte Fehlzeiten (Art. 9 DSGVO)
  - Anträge auf bestimmte Leistungen (vorgezogene Altersrente, Invaliditätsversorgung).
- **Der datenschutzrechtliche Pflichtenkreis richtet sich einerseits nach den verarbeiteten Daten, andererseits aber auch nach dem Durchführungsweg.**
- **Entwicklung eines Löschkonzepts:** Das datenschutzrechtliche **Prinzip der Erforderlichkeit** verlangt klare und angemessenen Speicherfristen. Gerade im Bereich der bAV werden sich i.d.R. lange Aufbewahrungsfristen rechtfertigen lassen. Es darf jedoch nicht zu einer pauschalen und vorbeugenden Speicherung der Daten kommen.

Durchführungswege

unmittelbare Versorgungszusage

- Direktzusage

Leistungserbringung erfolgt unmittelbar durch AG

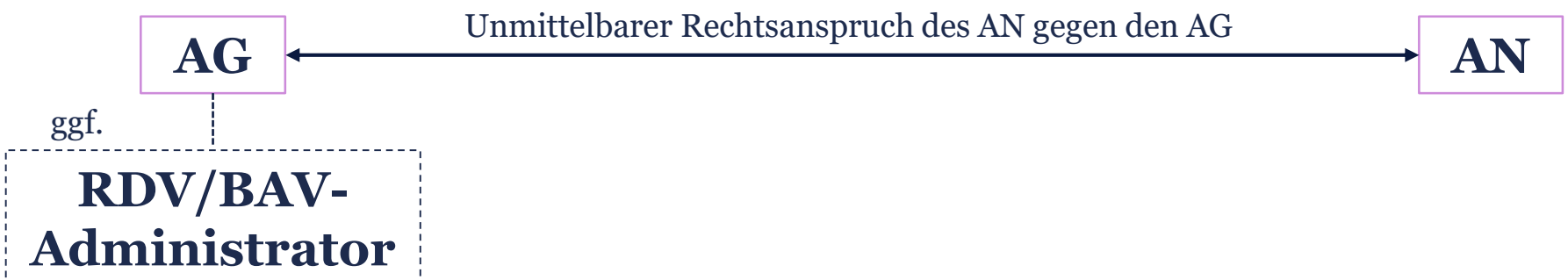
mittelbare Versorgungszusagen

- Direktversicherung (AG; VVaG)
- Pensionskasse (AG; VVaG)
- Unterstützungskasse (e. V.; GmbH; Stiftung)
- Pensionsfonds (AG; PFaG)

Leistungserbringung erfolgt mittelbar durch Dritten

Durchführungswege - Direktzusage

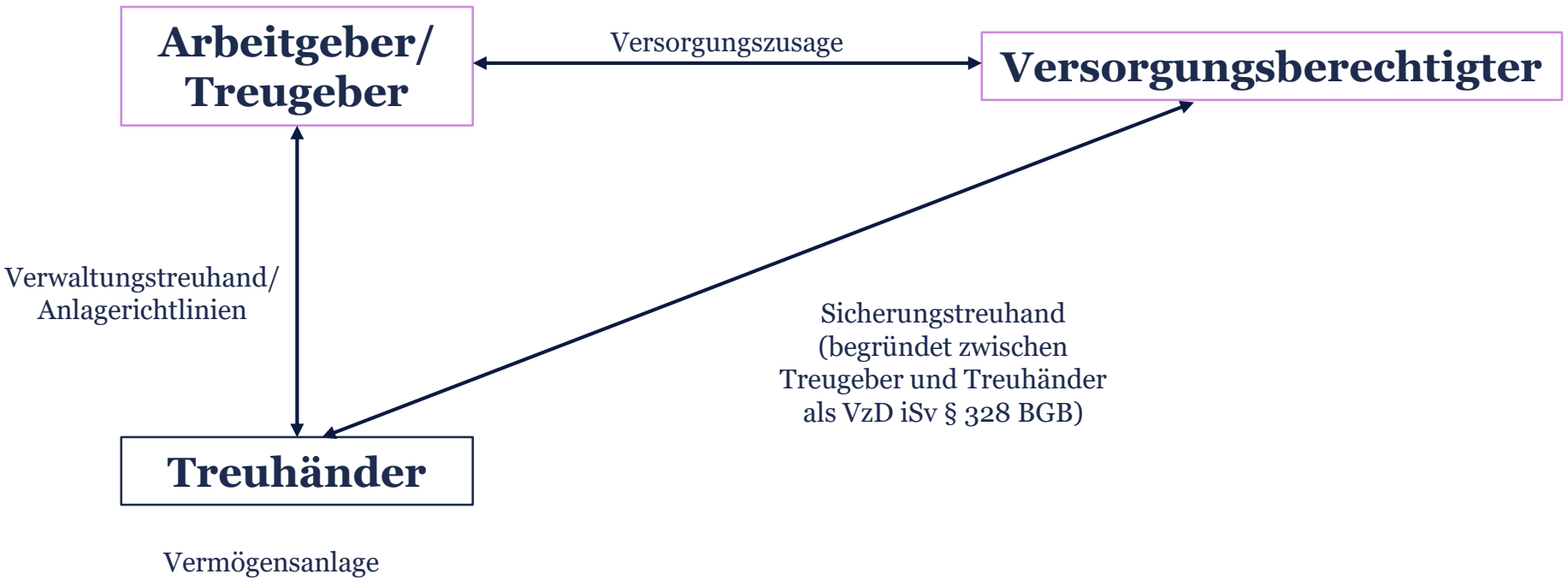
- Grundsätzlich bilaterales Rechtsverhältnis mit Verantwortlichkeit des Arbeitgebers
- Einbeziehung Dritter (Rückdeckungsversicherung, BAV-Administrator) ist aber denkbar
  - Datenübermittlung an Dritte controller to controller transfer oder controller to processor transfer?
  - Maßgeblich für die Bestimmung des datenschutzrechtlichen Pflichtenkreises ist hier die Ausgestaltung der jeweiligen Rechtsbeziehungen.



Durchführungswege - Direktversicherung

- Die Versicherung ist regelmäßig nicht von den Weisungen des Arbeitgebers abhängig.
- Die Versicherung erfüllt regelmäßig einen eigenständigen Vertrags- und Geschäftszweck.
- Sie hat in rechtlicher/ tatsächlicher Hinsicht selbst entscheidenden Einfluss auf die Datenverarbeitung und legt selbst die Mittel und Zwecke der Datenverarbeitung i.R.d. bAV fest (vgl. Art. 4 Nr. 7 DSGVO).
  - → I.d.R. eigene Verantwortlichkeit sowohl des Arbeitgebers als auch des Versicherers.
  - → Vergleichbare Bewertung für andere externe Versorgungsträger (Pensionskasse, Pensionsfonds, Unterstützungskasse)?

Sonderfall: Contractual Trust Arrangements (CTAs)



- Außerhalb des Sicherungsfalls: Vielfach Auftragsverarbeiter (wegen Weisungsgebundenheit)
- Im Sicherungsfall: Eigene Verantwortlichkeit

Denkbare Rechtfertigungsgrundlagen für Verarbeitungsvorgänge

- Einwilligung (Art. 6 Abs. 1 lit. a DSGVO, § 26 Abs. 2 BDSG), (jederzeit widerruflich)
- Datenverarbeitung zum Zwecke der Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO)
- Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO)
- Verarbeitung wegen eines berechtigten Interesses (Art. 6 Abs. 1 lit. f DSGVO)
- Betriebsvereinbarung oder andere Kollektivvereinbarungen (§ 26 Abs. 4 S. 1 BDSG)
- ➢ **Bei der Verarbeitung besonderer Kategorien personenbezogener Daten sind zusätzlich die Vorgaben von Art. 9 DSGVO zu beachten**

Informationspflichten und Betroffenenrechte

Informationspflichten, Art. 13, 14 DSGVO

- Verantwortlicher muss betroffene Personen umfassend über Datenverarbeitung informieren, wenn er personenbezogene Daten von diesen erhebt bzw. anderweitig erhält

Recht auf Auskunft, Art. 15 DSGVO

- Verantwortlicher muss auf Anfragen von betroffenen Personen Auskunft über Verarbeitungen von diesen betreffenden personenbezogenen Daten geben

Recht auf Berichtigung/Löschung/Einschränkung, Art. 16-18 DSGVO

- Verantwortlicher muss unrichtige Daten auf Anfrage berichtigen und ggf. löschen bzw. die Verarbeitung einschränken
- Aus der Natur der Sache folgt, dass Daten zur Erfüllung von Aufbewahrungspflichten und zur Durchführung der betrieblichen Altersversorgung auch noch nach der Beendigung des Arbeitsverhältnisses benötigt werden und daher nicht gelöscht werden müssen

Auskunftsrecht

Inhalt des Auskunftsrechts

Art. 15 Abs. 1 DSGVO

- Versorgungsberechtigte haben Recht auf Auskunft über
  - Verarbeitungszwecke
  - Datenkategorien
  - Empfänger oder Kategorien von Empfängern
  - Dauer der Datenspeicherung bzw. Kriterien zur Bemessung der Dauer
  - Betroffenenrechte und Beschwerderecht
  - Herkunft der Daten
  - Automatisierte Entscheidungsfindung und Profiling
  - Übermittlung in Drittländer sowie der Übermittlung zu Grunde liegende Schutzmaßnahmen

Auskunftsrecht

Anspruch auf Anfertigung von Kopien

Art. 15 Abs. 3 DSGVO

- Arbeitgeber stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung
- Stellt der Versorgungsberechtigte den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen

Art. 15 Abs. 4 DSGVO

- Das Recht auf Erhalt einer Kopie gemäß Absatz 3 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen

Auskunftsrecht

Kurze Frist: Arbeitgeber müssen organisatorisch vorbereitet sein

Art. 12 Abs. 3 DSGVO

- Auskunftsanspruch ist unverzüglich zu erfüllen, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags
- Verlängerung der Frist um weitere zwei Monate möglich, wenn erforderlich wegen
  - Komplexität des Antrags
  - Anzahl von Anträgen

Handlungsbedarf

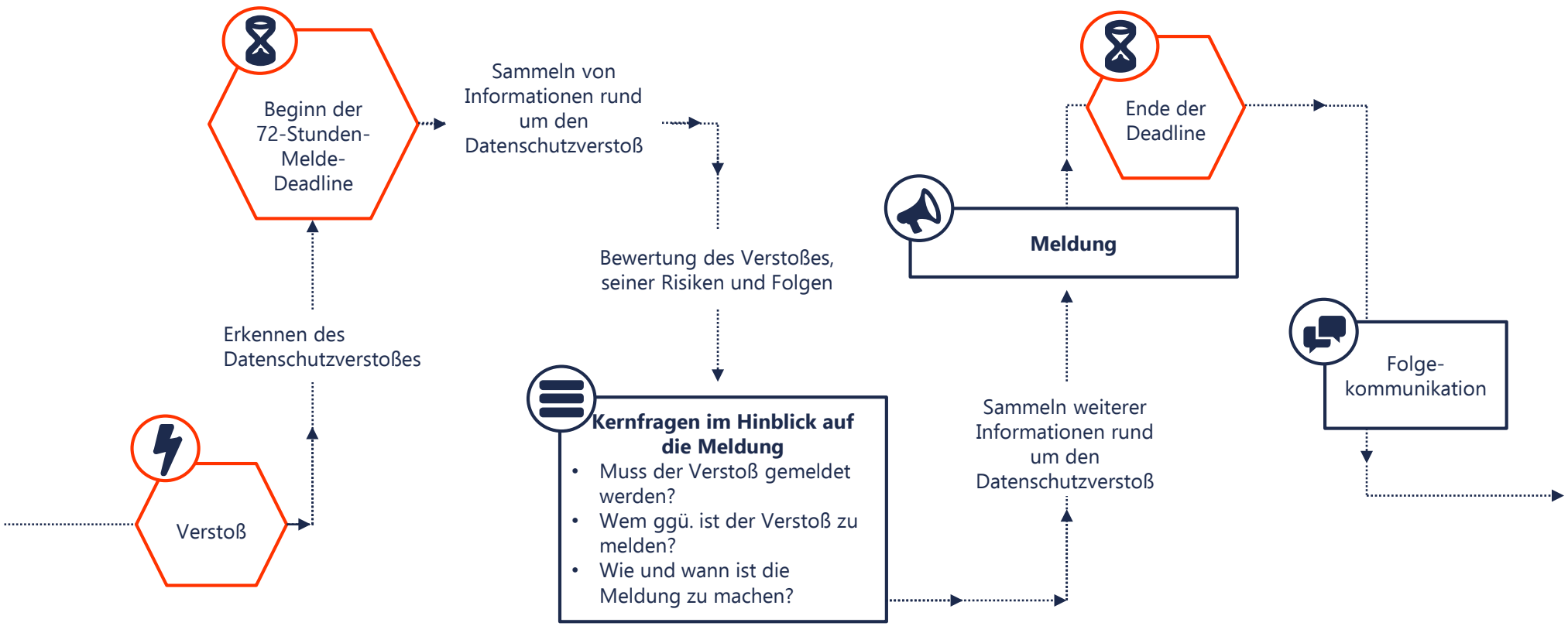
- Organisatorische Vorkehrungen treffen
- Anträge müssen sofort an die richtige Stelle weitergeleitet und sofort bearbeitet werden
- Arbeitgeber müssen Konzept haben, wie sie beispielsweise umgehen mit Daten in E-Mails, vertraulichen internen Bewertungen, Whistleblower-Meldungen
- Konzept entwickeln, ob und wann Versorgungsberechtigter um Konkretisierung der Anfrage gebeten werden kann (Erwägungsgrund 63 DSGVO)

Datenschutz in der betrieblichen Altersversorgung

Umgang mit Data Breaches

Die ersten 72 Stunden

Strategieplan



Ihr Kontakt

Thomas Granetzny
Principal Associate

Feldmühleplatz 1
40545 Düsseldorf

T: +49 211 4979-449

M: thomas.granetzny@freshfields.com

Vielen Dank!