Erste Erfahrungen mit der Umsetzung der DSGVO in der Versicherungswirtschaft

Verein zur Förderung der Versicherungswissenschaft

am 6. Juni 2019 in Hamburg

Dr. Martina Vomhof

GDV
DIE DEUTSCHEN VERSICHERER

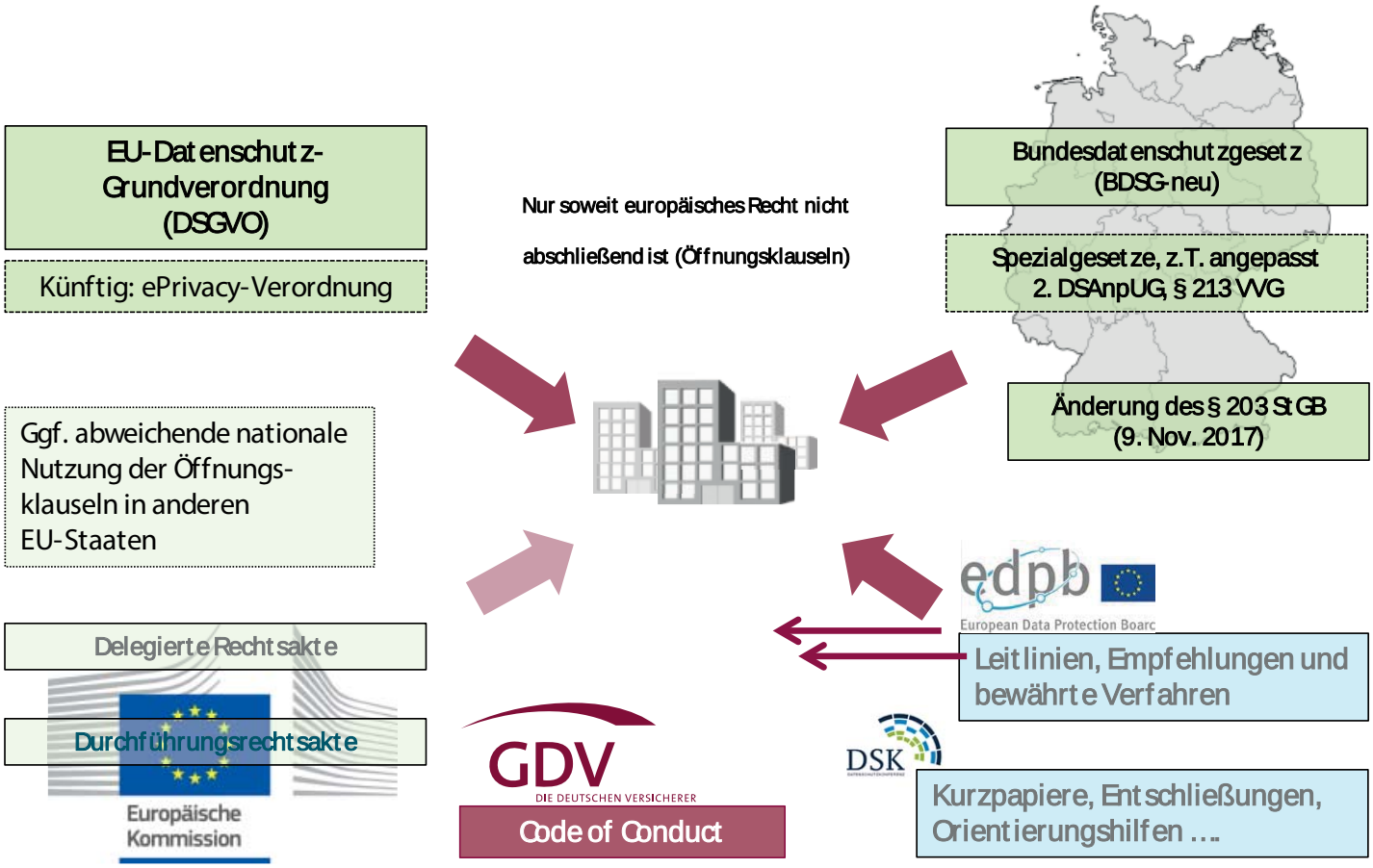
Übersicht

1. Der neue Rechtsrahmen
2. Branchenspezifische Regelungen
3. Zulässigkeit der Datenverarbeitung zu Versicherungszwecken
4. Ausblick

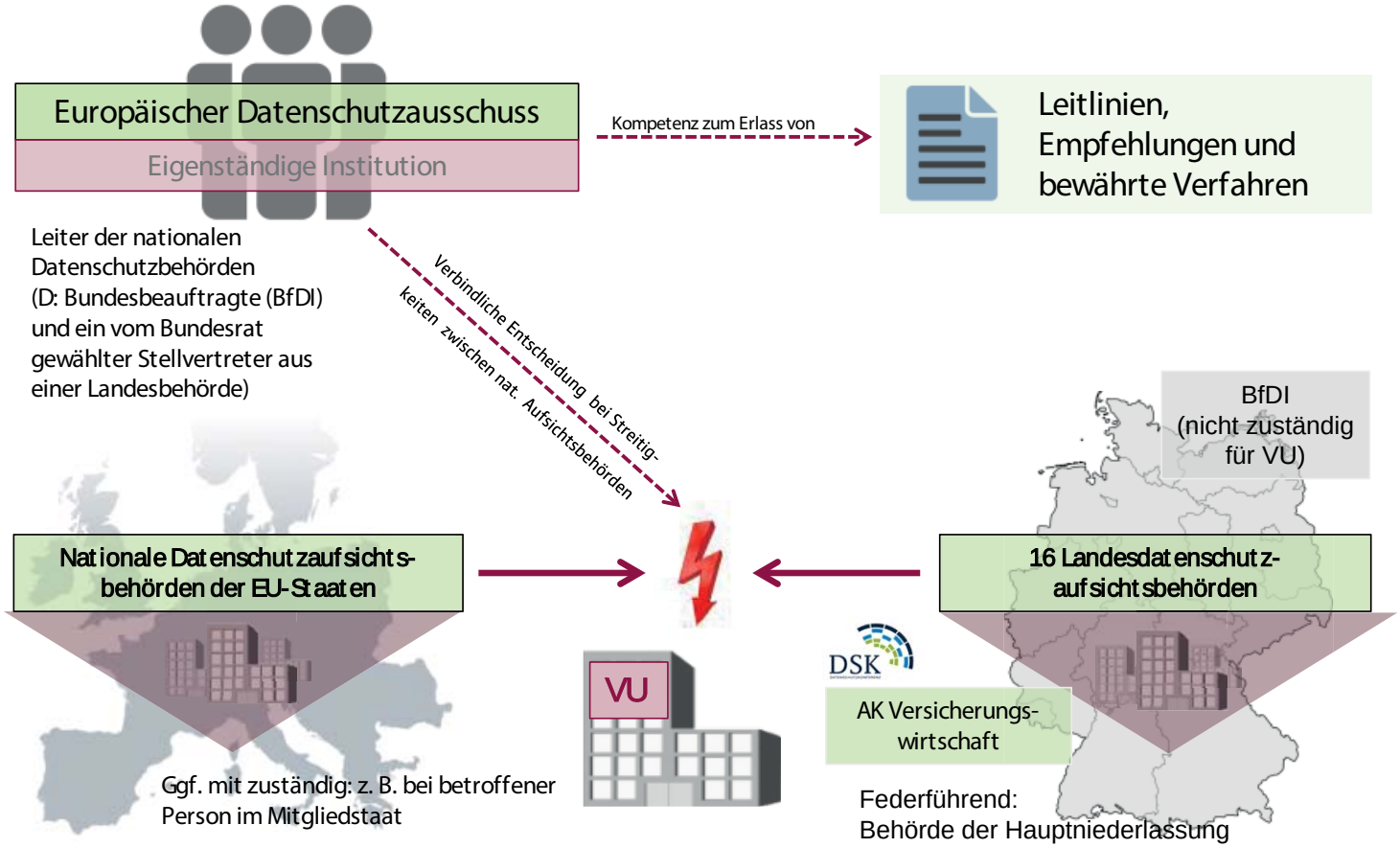
Übersicht

1. **Der neue Rechtsrahmen**
   - Rechtsgrundlagen Datenschutz
   - Aufsichtsstruktur
   - Umsetzung der DSGVO in den Versicherungsunternehmen
2. Branchenspezifische Regelungen
3. Zulässigkeit der Datenverarbeitung zu Versicherungszwecken
4. Ausblick

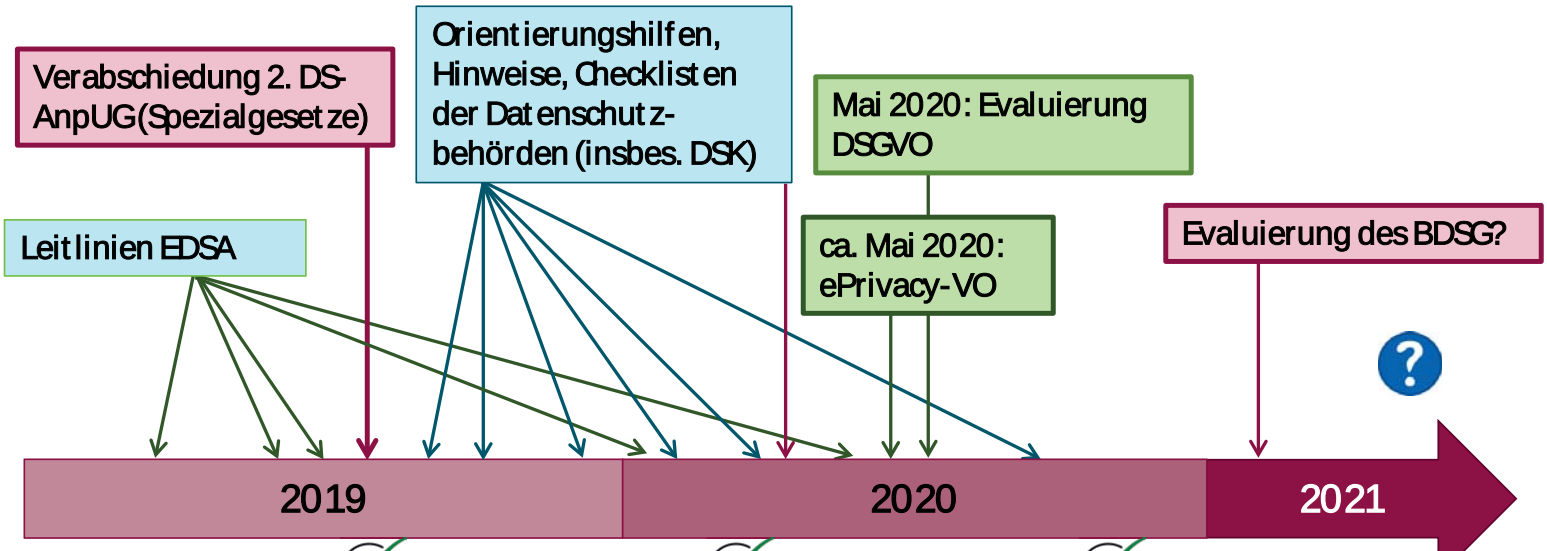
Rechtsgrundlagen Datenschutz



Aufsichtsstruktur



Umsetzung der DSGVO in den Versicherungsunternehmen



Unternehmen sind **mit** den für die Branche **wichtigen Rechtsänderungen vertraut** (u. a. durch Rundschreiben, Infoveranstaltungen, unverbindl. Orientierungshilfe, laufende Informationen des GDV)

Anpassungen sind **vorgenommen**; laufend **Kontrolle in Bezug auf neue Prozesse und neue rechtliche Bewertungen erfoderlich** (z. B. weitere Gesetze, Leitlinien EDSA, Checklisten Datenschutzbehörden).

Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die Deutsche Versicherungswirtschaft (**Code of Conduct**) wurden an das neue Recht angepasst. Fortgeltung für VU

Muster
- Informationspflichten
- Information HIS
- **Einwilligungen/ Schweigepflichtentbindungen** zur Abstimmung bei Datenschutzbehörden

Übersicht

1. Der neue Rechtsrahmen
2. Branchenspezifische Regelungen
   - Code of Conduct der Versicherungswirtschaft
   - Unverbindl. Muster einer Einwilligung/Schweigepflichtentbindung
3. Zulässigkeit der Datenverarbeitung zu Versicherungszwecken
4. Ausblick

Code of Conduct der Versicherungswirtschaft (1)

Code of Conduct als Hilfsmittel für die Umsetzung der DSGVO

- Der Code of Conduct wurde inhaltlich an die Anforderungen der DSGVO angepasst
- Seit 1. August 2018 ist er auf der Homepage des Verbandes veröffentlicht (https://www.gdv.de/de/ueber-uns/unsere-services/daten-schutz-ko-dex---code-of-conduct---15544).
- Die branchenspezifische Konkretisierung der DSGVO wurde mit den Datenschutzbehörden abgestimmt.
- Daher: Als Auslegungshilfe verwendbar, Verhalten im Einklang mit dem Code of Conduct dürfte nicht als Verstoß gegen die DSGVO betrachtet werden
- Verband hat Antrag auf Genehmigung des Code of Conduct nach Art. 40 Abs. 5 DSGVO bisher nicht gestellt
- Anforderungen der Leitlinie 1/2019 des Europäischen Datenschutzausschusses zu Codes of Conduct und Überwachungsstellen

Code of Conduct der Versicherungswirtschaft (2)

Änderungen in der 2. Auflage des Code of Conduct

- **Anpassung aller Bestimmungen an die Anforderungen der DSGVO**
- **Anpassung der Anforderungen in vorhandenen Verhaltensregeln**, z. B.
  - Risikobasierter Ansatz (Art. 32 DSGVO > Art. 4 CoC)
  - Statistik (Art. 89 DSGVO, § 27 BDSG > Art. 10 CoC)
  - Information (Art. 13, 14 DSGVO, §§ 29, 32, 33 BDSG > Art. 7 Abs. 3 u. Art. 8 Abs. 3 bis 6 CoC)
  - Auskunft u. a. Betroffenenrechte (Art. 16 ff. DSGVO, § 34 BDSG > Art. 23 bis 24d CoC)
  - Umgang mit Datenpannen (Art. 33 f. DSGVO > Art. 29 CoC)
- **Gänzlich neue Verhaltensregeln**, z. B. neu
  - Datenschutz-Folgenabschätzung (Art. 35 f. DSGVO > Art. 26a CoC)
  - Datenportabilität (Art. 20 DSGVO > Art. 23a CoC)
  - Gemeinsame Verantwortlichkeit (Art. 26 DSGVO > Art. 22a CoC)
  - Wissenschaftliche Forschung (Artikel 10 Abs. 7 CoC),
  - Schadenklassendatei (Artikel 16 Abs. 4 CoC)

?
- Keine Aussage zu „**Kopie**“ der Daten
- Auskunft an Betroffene selbst (Art. 23 IV)

?
- **Risiko:** insbes. wenn Identitätsdiebstahl, finanzieller Verlust od. Rufschädigung zu befürchten ist
- **Konzept** für Umgang mit Datenpannen (Art. 29 VII)

Code of Conduct der Versicherungswirtschaft (3)

Änderungen in der 2. Auflage des Code of Conduct

- **Erleichterungen für die Versicherungsunternehmen**, z. B.
  - Wegfall des Schriftformerfordernisses für die Einwilligung (Art. 5 Abs. 6 CoC)
  - Wegfall des Grundsatzes der Direkterhebung (Art. 7, 8 CoC)
  - Verarbeitung von Gesundheitsdaten auf gesetzlicher Grundlage (Art. 9 Abs. 2 DSGVO > Art. 6 Abs. 2 ff. CoC)
  - Datenverarbeitung bei Rückversicherern (Art. 17 CoC)
  - Datenübermittlung an Dienstleister von Maklern/Maklerpools (Art. 20 Abs. 4 CoC)
- In wenigen Fällen mangels Einigung mit den Datenschutzbehörden **nur Wiedergabe des Gesetzestextes**, insbes.
  - Scoring und Bonitätsabfragen (Art. 11, 12 CoC)
  - Werbung (Art. 18 CoC)
  - Verarbeitung von Gesundheitsdaten zur Gesundheitsvorsorge und -versorgung (§ 22 Abs. 1 Ziff. 1 lit. b BDSG > Art. 6 Abs. 4 CoC)

Umsetzung der DSGVO in den Unternehmen

Anpassung der unverbindlichen GDV-Muster einer Einwilligung/Schweigepflichtentbindung

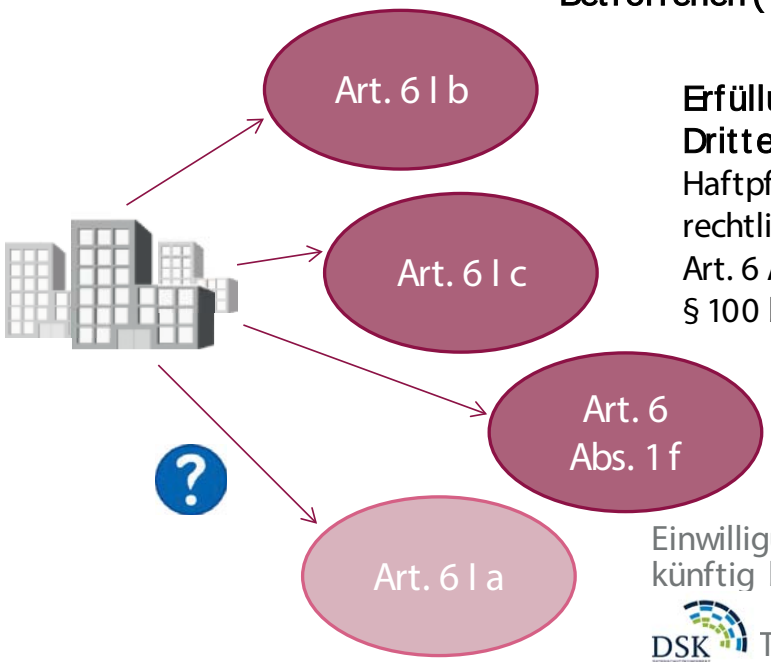
- Übergangslösung: Alte Muster der Einwilligung/Schweigepflichtentbindung können mit Hinweis auf das Widerrufsrecht weiterhin verwendet werden (GDV-Portal, RS-1299772 vom 19.01.2018)
- Projektgruppen der Kommission Datenschutz und der Sparten entwickeln in Workshops neue Muster für Leben/Kranken, Unfall und Haftpflicht
- Ziele:
  - Regelung für Gesundheitsdaten und genetische Daten im Rahmen des § 18 GenDG
  - Anpassung an die DSGVO und die Änderungen des § 203 StGB
  - Aufnahme weiterer praxisrelevanter Regelungen
    - Vollautomatisierte Entscheidungen
    - Gruppenversicherung
  - Verzicht auf Einwilligungen, wenn gesetzliche Grundlagen vorhanden sind
  - weite Auslegung des Art. 9 Abs. 2 lit. f) DSGVO und Art. 28 DSGVO muss mit den Aufsichtsbehörden beraten werden

Übersicht

1. Der neue Rechtsrahmen
2. Branchenspezifische Regelungen
3. **Zulässigkeit der Datenverarbeitung zu Versicherungszwecken**
   - Risiko- und Leistungsprüfung
   - Vollautomatisierte Entscheidungen
   - Einschaltung von Dienstleistern
   - Statistik
4. Ausblick

Risiko- und Leistungsprüfung (1)

Risiko-/Leistungsprüfung ist i. d. R. zum Abschluss bzw. zur Erfüllung **eines Vertrages mit dem Betroffenen (= VN)** erforderlich



Erfüllung von Ansprüchen Dritter, z. B. Geschädigter in Haftpflicht: Erfüllung einer rechtlichen Verpflichtung gem. Art. 6 Abs. 1 lit. c DSGVO i. V. m. § 100 bzw. § 115 VVG

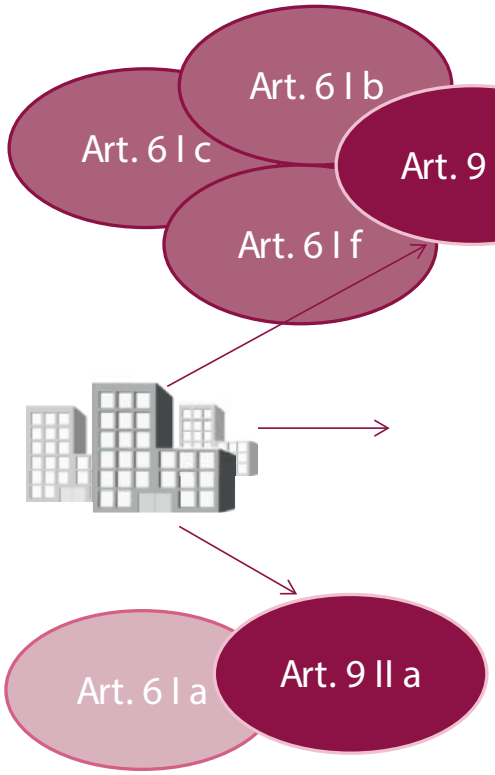
Berechtigte Interessen, z.B. Statistik, HIS Leitlinie 2/2019 EDSA: bei **Profilbildung** nicht Art. 6 Abs. 1 b

Einwilligung, wenn andere Normen nicht reichen – evtl. künftig bei vernetzten Geräten nach ePrivacy-VO

DSK Tracking für Werbezwecke auch nach DSGVO

Risiko- und Leistungsprüfung (2)

Rechtsgrundlagen für die Personenversicherung und die Regulierung von Personenschäden in der Haftpflichtversicherung



Datenverarbeitung zur **Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen** „erforderlich“

Art. 6 Abs. 2 S. 2 Code of Conduct: „Prüfung und Abwicklung der Ansprüche von Versicherten sowie von Geschädigten in der Haftpflichtversicherung“

Haftpflichtversicherung:
- Regulierung von Schäden Dritter
- Regressfälle

Personenversicherung:
- Leistungsprüfung

– Unterschiedliche Kommentarliteratur
– Unterschiedliche Umsetzung im EU-Ausland

Einwilligung wenn andere Normen nicht greifen, insbes. für die **Risikoprüfung** und **Datenabfrage bei Dritten** (§ 213 VVG)

➡ GDV-Muster für Leben/Kranken, Unfall und Haftpflicht

Risiko- und Leistungsprüfung (3)

Datenerhebung bei Ärzten, Krankenhäusern etc.

- Bei **Gesundheitsdaten** ist für Anfragen bei Ärzten und Krankenhäusern eine Einwilligung/Schweigepflichtentbindung erforderlich (§ 213 VVG, § 203 StGB)
- GDV-Muster sieht Wahl zwischen allgemeiner Einwilligung und Einwilligung im Einzelfall vor (§ 213 VVG)
- Einwilligung erfasst **auch nachträgliche Überprüfung** der Angaben des Versicherungsnehmers **bei Antragstellung** (Art. 15 Abs. 1 Code of Conduct)
- Ständige **Rechtsprechung des BGH** (BGH, Urt. v. 22.2.2017, IV ZR 289/14; BGH, Urt. v. 05.05.2017, IV ZR 121/15)
  - Angaben bei Antragstellung auch im Leistungsfall **ohne Anhaltspunkte** überprüfbar
  - **Beurteilungsspielraum** bei der Auswahl der zu prüfenden Tatsachen
  - Bei fehlenden Anhaltspunkten für den Prüfungsgegenstand Anwendung des vom BVerfG eingeführten **Dialogverfahrens** (BVerfG, Beschl. v. 17.07.2013, 1 BVR 3167/08; siehe auch BGH, a.a.O.)
  - Nach Ablauf der Fristen des § 21 Abs. 3 VVG (5 Jahre nach Vertragsschluss, zur Prüfung von Vorsatz und Arglist 10 Jahre) kein Grund mehr zur Datenerhebung

    ➡ daher von GDV-Einwilligung/Schweigepflichtentbindung nicht umfasst

Vollautomatisierte Entscheidungen (1)

Vollautomatisierte Risikobeurteilung und Schadenbearbeitung

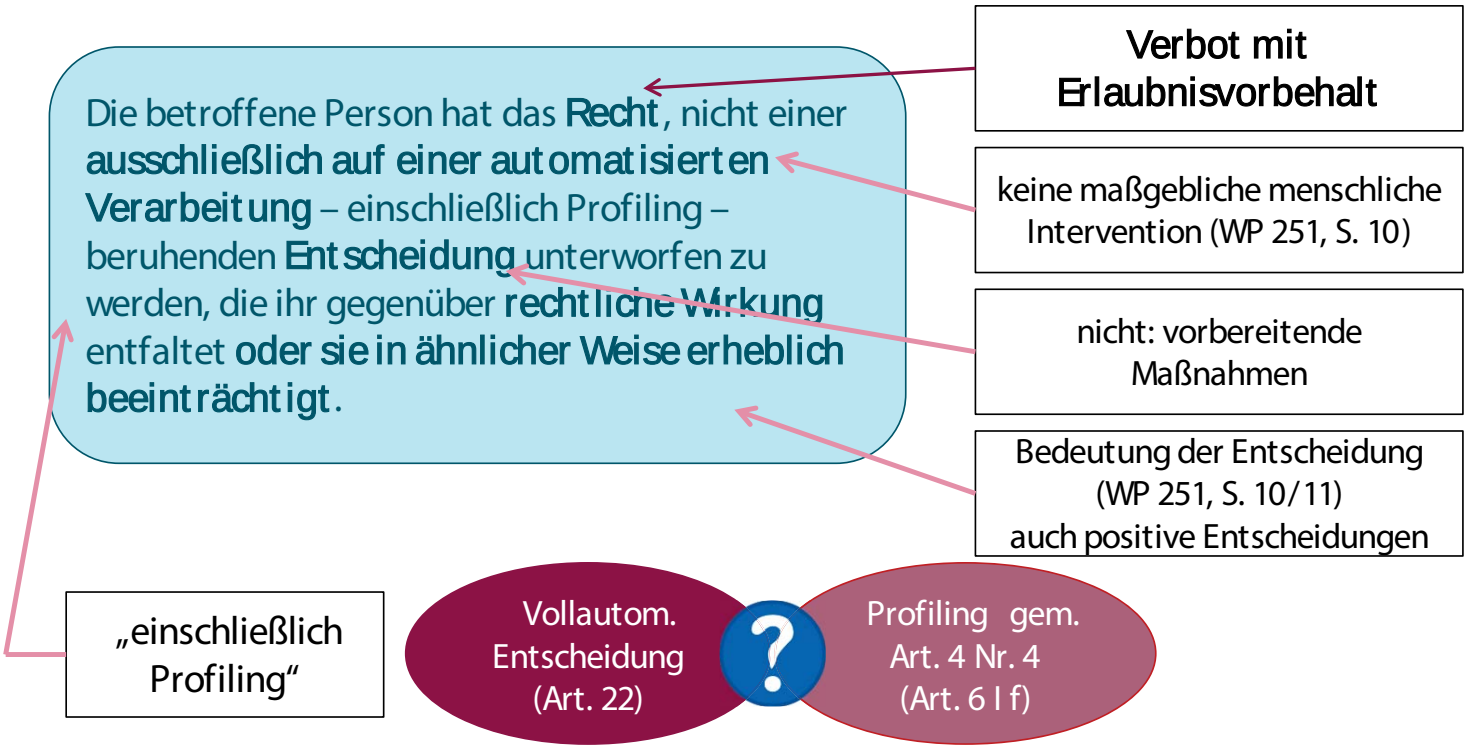
Die Risikoprüfung und Schadenbearbeitung wird zunehmend automatisiert!

Vorteile für Kunden und Versicherungswirtschaft

- Besserer Service für die Kunden: papierlose und schnelle Schadenregulierung
- Kosteneinsparungen für die Versicherungsunternehmen
- Gleiche Sachverhalte gleich behandeln
- Einfache Einbeziehung von mehr Informationen
- Einsatz von Blockchain-Technologie
- Einsatz von KI

Vollautomatisierte Entscheidungen (2)

Anwendungsbereich des Art. 22 DSGVO, Art. 13 CoC



Vollautomatisierte Entscheidungen (3)

Zulässigkeit vollautomatisierter Entscheidungen

Ausnahmen zusätzlich zu allgemeiner Erlaubnisgrundlage

- Art. 22 Abs. 2 lit. c DSGVO, Art. 13 Abs. 4 CoC: ausdrückliche **Einwilligung**
- Art. 22 Abs. 2 lit. a DSGVO, Art. 13 Abs. 2 CoC: wenn Entscheidung **für den Abschluss oder die Erfüllung eines Vertrages erforderlich** ist
  - nur Vertrag zwischen Versicherungsunternehmen und Betroffenem
  - Muss die Entscheidung erforderlich sein oder die automatisierte Form (vgl. Art.-29-Gruppe, WP 251)
  - Art. 13 Abs. 2 Ziff. 2 CoC: Erforderlichkeit ist gegeben bei „Entscheidungen gegenüber Versicherungsnehmern über Leistungsfälle im Rahmen des Versicherungsverhältnisses“

  - Anwendbar auch auf **Profilbildung**, wenn diese nicht unter Art. 6 Abs. 1 b DSGVO fallen soll (so Leitlinie 2/2019 EDSA)?

- Art. 22 Abs. 2 lit. b DSGVO i. V. m. § 37 Abs. 1 Nr. 1 BDSG, Art. 13 Abs. 3 Satz 1 CoC: im Rahmen der Leistungserbringung nach einem Versicherungsvertrag und **Begehren stattgegeben** (Vertrag und Haftpflicht)

Vollautomatisierte Entscheidungen (4)

Vollautomatisierte Entscheidungen und Profiling

- **Enge Ausnahmen vom Verbot vollautomatisierter Entscheidungen für Gesundheitsdaten**
  - Art. 22 Abs. 4 i. V. m. Art. 9 Abs. 2 a DSGVO ausdrückliche **Einwilligung**
  - Art. 22 Abs. 4, Art. 9 Abs. 2 g DSGVO, § 37 Abs. 1 Nr. 1, Abs. 2 BDSG: im Rahmen der Leistungserbringung nach einem Versicherungsvertrag, **Begehren stattgegeben** und angemessene Schutzmaßnahmen nach § 22 Abs. 2 Satz 2 BDSG

Einschaltung von Dienstleistern (1)

Rechtsgrundlagen für die Einschaltung von Dienstleistern

Art. 6 I b

Art. 6 I f

Art. 28

Art. 26

Dienstleistung kann zur **Durchführung eines Vertrages** „erforderlich" sein (Art. 22 I CoC)

Berechtigtes Interesse, auch im **Konzern** für „interne Verwaltungszwecke (ErwGr. 48), Art. 22 Abs. 2 ff. CoC

Rechtsanwälte
Art. 22 IX CoC

- Rechtsgrundlage
  (vgl. Art. 4 Nr. 10, Art. 28 III)
- Weisungsgebundenheit (Zwecke/Mittel)?

Keine Rechtsgrundlage; wohl nur zusätzliche Anforderungen? Art. 22a CoC, EuGH-Rspr.

Einschaltung von Dienstleistern (2)

Übermittlung von Gesundheitsdaten

Dienstleistung zur **Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen** „erforderlich“

Art. 6 I b

Art. 9 II f

Art. 6 I f

Art. 28

Art. 6 I a

Art. 9 II a

- Rechtsgrundlage (vgl. Art. 4 Nr. 10, Art. 28 III)
- Weisungsgebundenheit (Zwecke/Mittel)?

Einwilligung, wenn andere Normen nicht greifen

Einschaltung von Dienstleistern (3)

Weitergabe von nach § 203 StGB geschützten Privatgeheimnissen

- Strafbarkeit der unbefugten Offenbarung von Privatgeheimnissen in der Lebens-, Kranken- und Unfallversicherung (§ 203 Abs. 1 Ziff. 7 StGB)
- Auch bloßes Bestehen eines Vertrages (BGH Urt. v. 10.02.2010, Az.: VIII ZR 53/09)
- Bei Weitergabe an **Gutachter und**
- **Dienstleister** greift § 203 Abs. 3 Satz 2 StGB

„Geheimnisse dürfen an „**sonstige Personen**" offenbart werden, die an der beruflichen Tätigkeit des Geheimnisträgers „**mitwirken**", soweit dies **für die Inanspruchnahme des Dienstes erforderlich** ist (§ 203 Abs. 3 Satz 2 StGB)

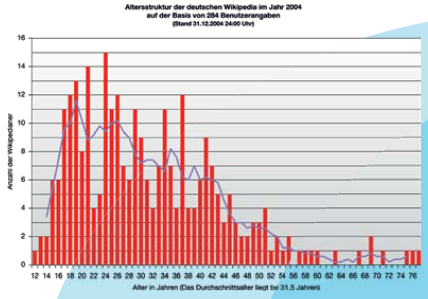
→ Keine Schweigepflichtentbindung mehr in GDV-Muster vorgesehen

Verschwiegenheitsverpflichtung nötig, soweit nicht selbst Berufsgeheimnisträger

Zur Sicherheit: Muster für Sonderfälle in den Fußnoten

Statistik

Art. 10 Code of Conduct



Art. 6 I f): berechtigte Interessen

Bei Gesundheitsdaten: Art. 9 II j) i.V.m. § 27 I BDSG: wenn erforderlich und erheblich überwiegendes Interesse des VU

Art. 89 u. § 27 Abs. 3 BDSG: Datenminimierung, z. B. Pseudonymisierung falls möglich; frühzeitige Anonymisierung

Zweckänderung Art. 6 IV, 5 I b)

Statistik ist im Ergebnis immer anonymisiert

Profilbildung in Bezug auf konkrete Personen ist keine Statistik!

Zweckänderung möglichst vermeiden

GDV-Statistik wurde den Anforderungen angepasst

Übersicht

1. Der neue Rechtsrahmen
2. Branchenspezifische Regelungen
3. Zulässigkeit der Datenverarbeitung zu Versicherungszwecken
4. Ausblick

Ausblick

Datenschutz 2019

Leitlinien des Europäischen Datenschutzausschusses

- Überarbeitung Leitlinien 1/2019 (Code of Conduct/Kontrollstellen) und der Leitlinien 2/2019 (Art. 6 DSGVO bei Online-Dienstleistungen)
- Weitere Leitlinien zur Interpretation der DSGVO

– Fortsetzung der Beratungen zur **ePrivacy-Verordnung**

– Arbeiten zur **Evaluierung der DSGVO** laufen bereits an

- Erleichterungen bei alltäglichen Datenverarbeitungen, Testdaten, zur Anonymisierung von Daten notwendige vorherige Datenverarbeitung
- Verantwortlichkeit der Hersteller von vernetzten Geräten und Software
- Transparenz, Nachvollziehbarkeit und Überprüfbarkeit beim Einsatz von künstlicher Intelligenz, Scoringverfahren und automatisierten Entscheidungen

– **Verabschiedung 2. DSAnpUG**

– Vorbereitung der **Evaluierung des BDSG**

– **Digitalisierung** spielt eine erhebliche Rolle auf europäischer und nationaler Ebene
Zentrale Themen sind Algorithmen und KI, Telematiktarife

Danke für Ihre Aufmerksamkeit.
Ihre Fragen?

Dr. Martina Vomhof
Leiterin Datenschutz/Grundsatzfragen
m.vomhof@ gdv.de

Wilhelmstraße 43 / 43G
10117 Berlin
Tel.: 030-2020 5000
Fax: 030-2020 6000
E-Mail: berlin@gdv.de

51, rue Montoyer
B-1000 Brüssel
Tel.: 0032-2-282 47 30
Fax: 0049-30-2020 6140
E-Mail: bruessel@gdv.de

www.gdv.de
www.DieVERSICHERER.de
facebook.com/DieVERSICHERER.de
Twitter: @gdv_de
www.youtube.com/user/GDVBerlin