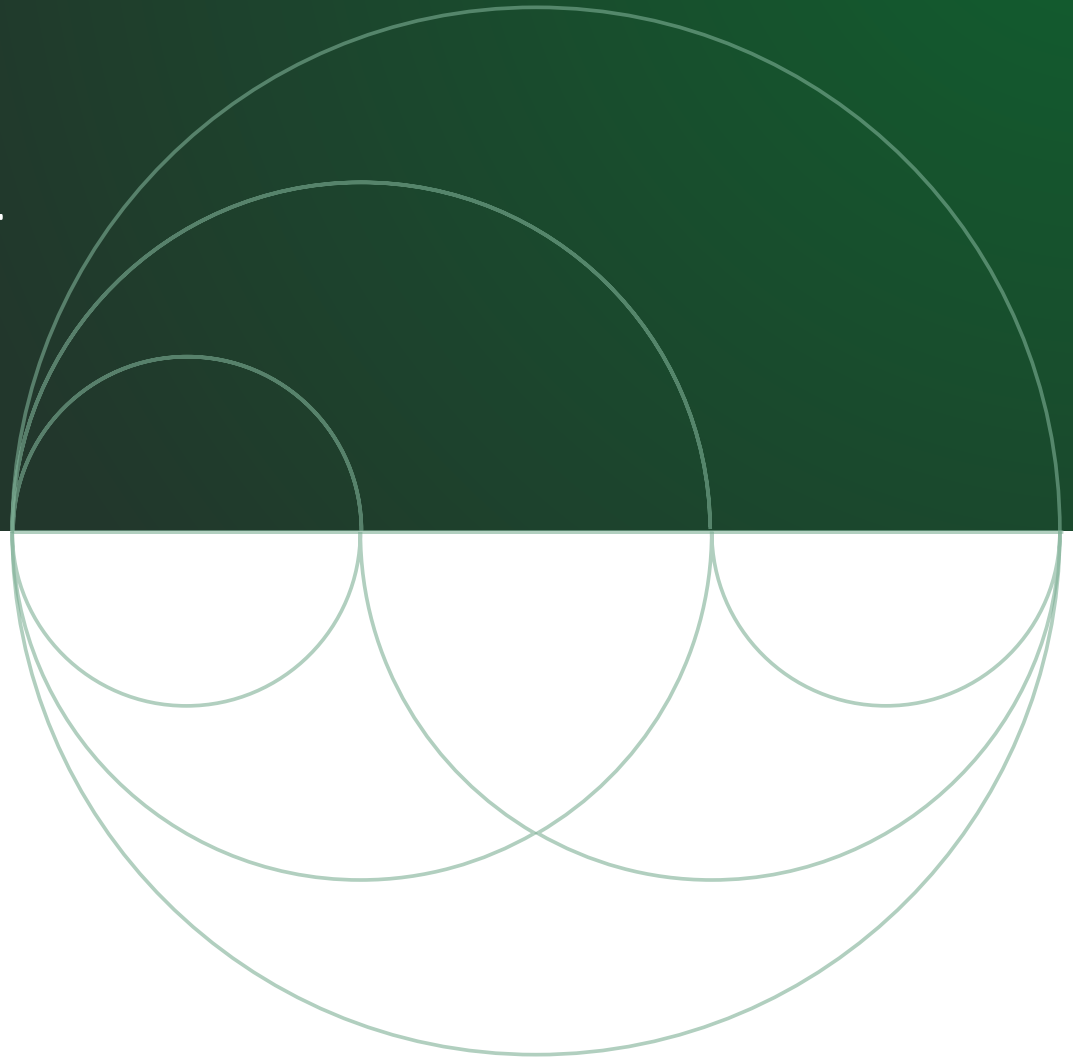
GDV Gesamtverband der Versicherer

Forum Versicherungsrecht

Datenschutz im Versicherungsunternehmen – Hindernis für die Digitalisierung?



5. September 2023

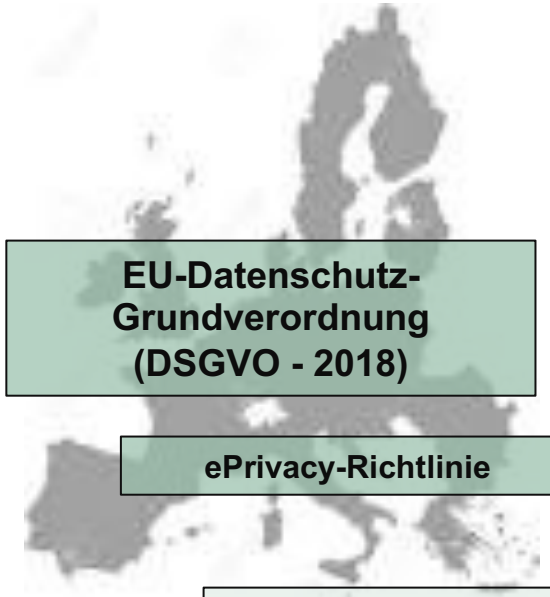
Dr. Martina Vomhof

Datenverarbeitung in der Versicherungsbranche

Die Verarbeitung personenbezogener Daten gehört zum Kerngeschäft der Versicherungsunternehmen.
Ein guter Datenschutz ist zwingende Voraussetzung für das Vertrauen der Kunden.

Datenschutzrechtsrahmen

Verhaltens-regeln für die Daten-verarbeitung



EU-Datenschutz-Grundverordnung (DSGVO - 2018)

ePrivacy-Richtlinie

Delegierte Rechtsakte

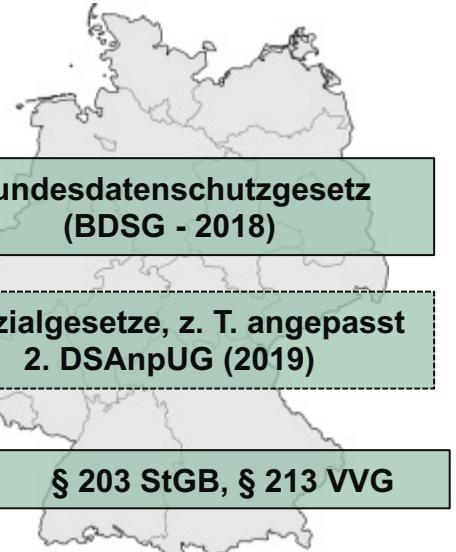
Durchführungsrechtsakte

Europäische Kommission

Ggf. abweichende nationale Nutzung der Öffnungs-klauseln in anderen EU-Staaten

Leitlinien, Empfehlungen

edpb European Data Protection Board



Bundesdatenschutzgesetz (BDSG - 2018)

Spezialgesetze, z. T. angepasst 2. DSAnpUG (2019)

§ 203 StGB, § 213 VVG

TTDSG (2021)

DSK

Kurzpapiere, Entschließungen, Orientierungshilfen ….

DSGVO ist „technologieneutral“

DSGVO
Erwägungsgrund 15

Satz 1: Um ein ernsthaftes Risiko einer Umgehung der Vorschriften zu vermeiden, sollte der **Schutz natürlicher Personen technologieneutral** sein und **nicht von den verwendeten Techniken abhängen.**

Satz 2:
Der Schutz natürlicher Personen sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung von personenbezogenen Daten, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Meinungen zur DSGVO 2023

„Der vielfach beschworene Goldstandard erdrückt uns wettbewerblich. Die Überprüfung der DSGVO nächstes Jahr muss deshalb zu einer echten Reform führen, wenn wir in einer datengetriebenen Welt überhaupt noch eine Rolle spielen wollen."

„Es geht nicht nur um Probleme bei grenzüberschreitenden Verfahren, sondern es geht um eine Modernisierung der DSGVO insgesamt in Bezug auf Entwicklungen wie Blockchain, Cloudlösungen, KI sowie Abbau der massiven Bürokratielast und der Ermöglichung von Datenverarbeitung ohne die Grundrechte des Einzelnen zu verletzen."

Axel Voss, MdEP (EVP)

https://www.cducsu.eu/artikel/voss-verbesserung-der-datenschutzgrundverordnung-ist-ueberfaellig

„Wenn wir so weitermachen, riskieren wir Wettbewerbsfähigkeit und Innovationskraft."

„Die DS-GVO hat ihr Versprechen… nicht eingelöst. Stattdessen führt die von jeder nationalen und regionalen Aufsicht eigenständige Interpretation der Regeln zu Rechtsunsicherheit. Viele Unternehmen verzichten deshalb auf die Entwicklung neuer Technologien und Dienste – oder verlagern ihre Projekte ins Ausland…"

Achim Berg, Bitkom-Präsident

https://www.bitkom.org/Presse/Presseinformation/Fuenf-Jahre-DS-GVO

Digitalisierung in der Versicherungswirtschaft

Verarbeitungsprozess	„Alte Welt“	„Neue Welt“
Information und Vertragsanbahnung	über Vermittler oder telefonisch	auf verschiedenen Kanälen, häufig online, teils Nutzung von Chatbots
Produkte	Standardprodukte	auch neue, maßgeschneiderte Produkte, z. B. für kurzfristig stattfindende Ereignisse; Telematik-Tarife; Risikovermeidung
Risikoprüfung	manuelle Prüfung, Eischätzungsgrundsätze, Einschätzungsbücher von Rückversicherern	Online-Tools, Hinzuziehung externer Informationen (z. B. Wetterdaten, Maschinendaten)
Vertragsverwaltung, IT	gewachsene IT-Systeme, Großrechner	Cloud-Lösungen, dezentrale Speicherung, auch im Ausland, 24/7-Support
Bearbeitung Leistungsfälle	manuelle Prüfung, Gutachter vor Ort, Betrugsexperten	Schadenmeldung online, automatisierte Auswertung von Fotos, vollautomatisierte Prüfung und Auszahlung

Konfliktpunkte Digitalisierung und Datenschutz

- **Automatisierte Einzelfallentscheidungen** (Art. 22 DSGVO)
- Datenübermittlung in **Drittstaaten** (Art. 44 ff. DSGVO)
- **Zweckändernde Datenverarbeitung** (Art. 6 Abs. 4 DSGVO)

und viele andere, z. B.

- Elektronische Kommunikation, z. B. per E-Mail oder Messenger-Dienste (Art. 32 DSGVO)
- Zugriff auf Endgeräte (TTDSG)
- Erfüllung von Informationspflichten (Art. 13, 14 DSGVO)
- ….

Automatisierte Einzelfallentscheidung (1)

- Die DSGVO sieht für **digitale Verarbeitungsprozesse** grundsätzlich keine speziellen Regelungen vor.
- **Automatisierte Einzelfallentscheidungen** sind jedoch in Art. 22 DSGVO geregelt:

Art. 22 Abs. 1 DSGVO

„Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt."

Produktangebote, Chatbots

Risikoprüfung, Vertragsschluss

Leistungs-prüfung

Automatisierte Einzelfallentscheidungen (2)

Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden **Entscheidung** unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Keine vorbereitenden Maßnahmen

- Zeigen und Erläutern von Produkten ist grundsätzlich keine Entscheidung
- Schlussanträge EuGH-Generalanwalt, 16.03.2023, Az. C-634/21 (SCHUFA-Scoring), Ziff. 36 ff, insbes. 42: auch vorbereitende Maßnahmen, wenn Entscheidung vorbestimmt

Allgemeine Produktangebote,

Chat Bots

Automatisierte Einzelfallentscheidungen (3)

Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden **Entscheidung** unterworfen zu werden, die ihr gegenüber **rechtliche Wirkung** entfaltet **oder** sie **in ähnlicher Weise erheblich beeinträchtigt**.

Annahme Vertrag

Gewährung Leistung

Ablehnung Vertrag

Ablehnung Leistung

Nur schwerwiegende Auswirkungen

- Schlussanträge EuGH-Generalanwalt,16.03.2023, Az. C-634/21 (SCHUFA-Scoring), Ziff. 34 und Artikel-29-Gruppe, WP 251 Rev. 01, S. 23: „… wird anhand der Wortwahl klar, dass diese Bestimmung [Art. 22] **nur schwerwiegende Auswirkungen** abdeckt.“
- Teleologische Reduktion erscheint vertretbar

Automatisierte Einzelfallentscheidung (4)

Vollautomatisierte Einzelentscheidung ist nach Art. 22 Abs. 2 erlaubt, wenn

Art. 22 Abs. 2 lit. a DSGVO

…die Entscheidung für den Abschluss oder die Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist.

Blockade jedes Fortschritts durch Auslegung?

Unternehmerische Freiheit?

- Nur für Verträge zwischen betroffener Person und Versicherer (nicht Haftpflicht)
- Abschluss oder Erfüllung (nicht Beendigung)
- „**Erforderlich**“: sehr enge Auslegung durch die Datenschutzbehörden
- Artikel-29-Gruppe, WP 251, S. 25: „Sind für das Erreichen desselben Ziels andere wirksame und weniger eingreifende Mittel verfügbar, wäre diese Art der Verarbeitung nicht „erforderlich“.“
- Versicherungsvertrag in der Regel auch manuell möglich!

Automatisierte Einzelfallentscheidung (5)

Vollautomatisierte Einzelentscheidung ist nach Art. 22 Abs. 2 erlaubt, wenn

Art. 22 Abs. 2 lit. b) DSGVO i.V.m. § 37 BDSG

…die Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht und

… dem Begehren der betroffenen Person stattgegeben wurde

… Anwendung verbindlicher Regelungen für Heilbehandlungen und Schutzmaßnahmen getroffen

Rechtssicherheit für

- positive Entscheidungen im Leistungsfall, auch Haftpflicht
- Krankenversicherung, insbes. Prüfung von GOÄ-Positionen, auch negative Entscheidungen

- Abs. 2: auch für Gesundheitsdaten

Automatisierte Einzelfallentscheidung (6)

Vollautomatisierte Einzelentscheidung ist nach Art. 22 Abs. 2 erlaubt, wenn

Art. 22 Abs. 2 lit. c DSGVO

…die Entscheidung mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Für Massengeschäft nicht tauglich

Informationelle Selbstbestimmung?

- wichtig vor allem bei vollautomatisierten Entscheidungen mit Gesundheitsdaten (Art. 22 Abs. 4, Art. 9 Abs. 2 lit. a DSGVO)
- ausdrückliche (keine konkludente) Einwilligung
- Bezug auf die „vollautomatisierte Entscheidung“
- Anforderungen des Art. 7 DSGVO an Einwilligungen gelten
- AK Versicherungswirtschaft der Datenschutzbehörden: Einwilligung ist nur freiwillig, wenn eine menschliche Entscheidung als Alternative angeboten wird.

Automatisierte Einzelfallentscheidung (7)

Begleitende Sicherungsmaßnahmen nach Art. 22 Abs. 3 DSGVO

In jedem Fall: angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren

Bei Ausnahmen nach Art. 22 Abs. 1 lit. a) und c) DSGVO und ähnlich nach § 37 BDSG mindestens Recht auf:

- menschliches Eingreifen in den Entscheidungsprozess
- Darlegung des eigenen Standpunkts
- Anfechtung der Entscheidung

Automatisierte Einzelfallentscheidung (8)

Zwischenergebnis

Eine ausdrückliche **Beschränkung des Anwendungsbereichs des Art. 22 Abs. 1 DSGVO** auf Entscheidungen mit schwerwiegenden Auswirkungen durch den EuGH wäre hilfreich (vgl. Schlussanträge Generalanwalt).

Die **Ausnahmen des Art. 22 Abs. 2 lit. a) und c) sollten** von den Datenschutzbehörden **nicht über den Wortlaut hinaus eingeschränkt werden**.

Eine **grundsätzliche Erlaubnis vollautomatisierter Entscheidungen in der Versicherungswirtschaft** im BDSG (oder der DSGVO) die zukunftsfähige Lösung. Sie ermöglicht im Massengeschäft schnelle Entscheidungen im Interesse der Kunden, denen es **unbenommen bleibt, „auf zweiter Ebene“ eine Überprüfung** zu verlangen.

Datenübermittlung in Drittstaaten (1)

- EuGH, Urteil vom 16. Juli 2020 (C 311/18 – „Schrems II“):
  - Privacy-Shield unwirksam
  - Kein angemessenes Datenschutzniveau in USA (staatliche Überwachungsmaßnahmen, kein ausreichender Rechtsschutz).
  - Bei jeder Datenübermittlung in Drittstaaten muss tatsächlich ein Schutzniveau für die personenbezogenen Daten sichergestellt sein, das dem in der Europäischen Union entspricht.

Nutzung von Clouddiensten bedingt Datenverarbeitung in Drittstaaten

Service rund um die Uhr häufig aus Drittstaaten

Datenübermittlung in Drittstaaten (2)

- Begrenzte Lösung für die USA durch neuen Datenschutzrechtsrahmen (Data Privacy Framework) und neuen Angemessenheitsbeschluss der EU-Kommission vom 10. Juli 2023
  - Datenzugriff der Geheimdienste nur soweit notwendig und erforderlich
  - Rechtsschutzsystem (Beschwerdestelle, Data Protection Review Court)
  - Selbstzertifizierung der teilnehmenden US-amerikanischen Unternehmen
- Für alle anderen Länder ohne Angemessenheitsbeschluss gilt weiterhin das Schrems-II-Urteil.
- EU-Kommission hat Standardvertragsklauseln überarbeitet
- Erforderlich ist Transfer-Impact-Assessment (TIA) und – bei nicht angemessenem Schutzniveau – das Treffen von Maßnahmen zum Schutz der Rechte und Freiheiten betroffener Personen (z. B. Verschlüsselung)

Datenübermittlung in Drittstaaten (3)

- Datenschutzbehörden wenden den in der DSGVO verankerten risikobasierten Ansatz im Rahmen von Drittstaatentransfers nicht an.
- Überhöhte Anforderungen an Binding Corporate Rules (vgl. Empfehlungen 1/2022 des EDSA zu BCRs für Verantwortliche – Art. 47 GDPR)
- Sehr enge Auslegung der Ausnahmen des Art. 49 DSGVO
  - Ausdrückliche Einwilligung nur im Einzelfall nach entsprechender Unterrichtung über die Risiken der Datenübermittlung (Art. 49 Abs. 1 lit. a)
  - Beschränkung der Übermittlungen zur Erfüllung eines mit der betroffenen Person oder in deren Interesse geschlossenen Vertrages (Art. 49 Abs. 1 lit. b bzw. c) auf „gelegentliche“ Fälle

Datenübermittlungen in Drittstaaten (4)

Zwischenergebnis

Eine Anerkennung des **risikobasierten Ansatzes** für Drittstaatenübermittlungen durch die Datenschutzbehörden, den EuGH und notfalls den EU-Gesetzgeber wäre hilfreich.

Die Datenschutzbehörden sollten BCRs nicht beschränken und die **Ausnahmen des Art. 49 DSGVO nicht über den Wortlaut hinaus einschränken**.

Politische Lösungen (Angemessenheitsbeschlüsse für weitere Staaten) wären hilfreich.

Nutzung von Echtdaten für Entwicklung und Tests von Produkten und Systemen (1)

- Berechtigtes Interesse (Art. 6 Abs. 1 lit. f) DSGVO)
- Ggf. Zweckänderung nach Art. 6 Abs. 4 DSGVO
  - Verbindung zwischen den Zwecken
  - keine negativen Folgen der Weiterverarbeitung (nur Test)
  - Garantien, z. B. Pseudonymisierung, Verschlüsselung

Bevor mit synthetischen Daten entwickelte neue Anwendungen in den Verkehr gebracht werden, muss eine Überprüfung mit Echtdaten möglich sein.

Nutzung von Echtdaten für Entwicklung und Tests von Produkten und Systemen (2)

Sonderfall: Gesundheitsdaten

- Bei **besonderen Kategorien** personenbezogener Daten, insbes. Gesundheitsdaten, reicht berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO) nicht aus.
- Art. 9 Abs. 2 DSGVO enthält keine geeignete Rechtsgrundlage
- Art. 6 Abs. 4 DSGVO
  - Grundsätzlich auch für besondere Kategorien personenbezogener Daten anwendbar (vgl. Art. 6 Abs. 4 lit. c) DSGVO)
  - aber streitig, ob eigenständige Rechtsgrundlage (vgl. ErwGr. 50 S. 2)

Nutzung von Echtdaten für Entwicklung und Tests von Produkten und Systemen (3)

Für Hochrisiko-KI spezielle Rechtsgrundlage in **Art. 10 Abs. 5 KI-VO**:

Soweit dies für die Beobachtung, Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen unbedingt erforderlich ist, dürfen die Anbieter solcher Systeme besondere Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 der Verordnung (EU) 2016/679, Artikel 10 der Richtlinie (EU) 2016/680 und Artikel 10 Absatz 1 der Verordnung (EU) 2018/1725 verarbeiten, wobei sie angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen müssen, wozu auch technische Beschränkungen einer Weiterverwendung und modernste Sicherheits- und Datenschutz-maßnahmen wie Pseudonymisierung oder Verschlüsselung gehören, wenn der verfolgte Zweck durch eine Anonymisierung erheblich beeinträchtigt würde.

Nutzung von Echtdaten für Entwicklung und Tests von Produkten und Systemen (4)

Zwischenergebnis

Die Datenschutzbehörden sollten Art. 6 Abs. 4 DSGVO weit auslegen, um auch Tests neuer Anwendungen und Systeme mit (pseudonymisierten) Gesundheitsdaten zu ermöglichen.

Eine gesetzliche Erlaubnis auch über Art. 10 Abs. 5 KI-VO hinaus wäre sinnvoll.

Europäische Datenstrategie als Lösung?

- **Data Governance Act:** Prozesse und Strukturen für gemeinsame Datennutzung
- **Data Act:** Übertragung von Daten aus vernetzten Geräten (u. a.), Bedingungen für Datenteilen allgemein
- **Financial Data Access Regulation (FiDA-VO):** Übertragung von Finanzdaten
- **Europäischer Gesundheitsdatenraum (EHDS-VO):** Primär- und Sekundärnutzung elektronisch verfügbarer Gesundheitsdaten

- Es geht zumeist darum, die Daten (teilweise auf Wunsch des Kunden) für diesen oder Dritte zugänglich zu machen.
- Ergänzung zum Recht auf Datenportabilität nach Art. 20 DSGVO
- Versicherungsunternehmen können „Datenlieferant“ oder Empfänger sein.
- Wenn personenbezogene Daten betroffen sind, gilt meist die DSGVO (vgl. z. B. Art. 4 Abs. 5 u. 5 Abs. 6 sowie ErwGr. 7, 24, 30, 31 Data Act; ErwGr. 10, 48 FiDA-VO; ErwGr. 4 EHDS-VO, Ausnahme: Sekundärnutzung im EHDS)
- Teilweise engere Zweckbindung (Art. 6 Data Act, Art. 7 FiDA, Art. 34, 35 EHDS)

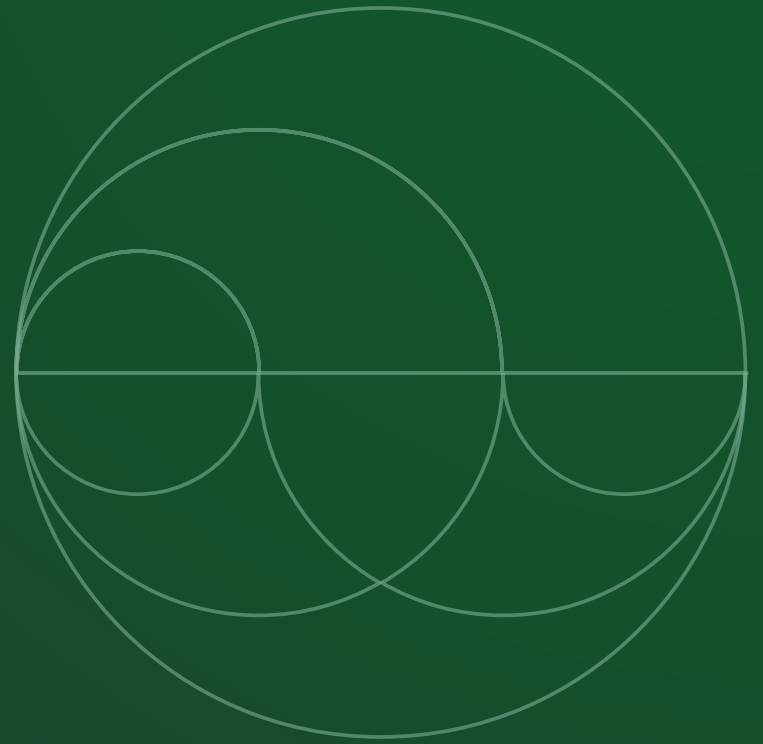
FAZIT

- Das geltende Datenschutzrecht, insbesondere die DSGVO, steht der Digitalisierung der Versicherungsbranche nicht zwingend im Weg.
- Nötig ist aber eine „digitalisierungsfreundliche Auslegung“ der Rechtsnormen durch die Datenschutzbehörden.
- Gesetzliche Klarstellungen wären hilfreich.
- Die im Rahmen der EU-Datenstrategie geplanten Regelungen zielen darauf ab, mehr Daten verfügbar zu machen, lockern aber die datenschutzrechtlichen Bestimmungen kaum.

Wilhelmstraße 43 / 43G
10117 Berlin
T: 030-2020 5000
F: 030-2020 6000
E: berlin@gdv.de

Rue du Champ de Mars 23
B - 1050 Brüssel
T: 0032-2-2 82 47 30
F: 0049-30-2020 6140
E: bruessel@gdv.de

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



GDV