universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

„Die Versicherung fährt mit“

Pay as you drive-Tarife und der Datenschutz

verfasst von / submitted by

Kathrin Felkel

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2023 / Vienna 2023

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 942
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Informations- und Medienrecht
Betreut von / Supervisor:	Prof. Dr. Thomas Hoeren

„Die Versicherung fährt mit“
Pay as you drive-Tarife und der Datenschutz

Inhaltsverzeichnis

1) Einleitung

Im Jahr 2021 waren in Österreich 7.214.970 Kraftfahrzeuge zum öffentlichen Verkehr zugelassen, davon 5.133.836 Personenkraftwagen[1] (PKW). Seit dem Jahr 1929 schreibt das Österreichische Kraftfahrzeuggesetz (KFG) den Abschluss einer Haftpflichtversicherung für alle zum öffentlichen Verkehr zugelassenen Kraftfahrzeuge (Kfz) zwingend vor[2]. Mittlerweile sind seit Einführung dieser obligatorischen Kfz-Haftpflichtversicherung mehr als 90 Jahre vergangen und seit dem haben sich nicht nur die Kraftfahrzeuge selbst, sondern auch die angebotenen Kfz-Versicherungsmodelle laufend verändert. Die kontinuierliche Weiterentwicklung im Bereich der Fahrzeugtechnik hat dazu geführt, dass moderne Kraftfahrzeuge heute bereits standardmäßig über verschiedene integrierte und automatisierte Funktionen wie Navigationssysteme, Fahrassistenz oder Einparkhilfen verfügen[3]. Zudem sind Autohersteller seit dem 31.03.2018 dazu verpflichtet, Personenkraftwagen die in der Europäischen Union (EU) neu zum Verkehr zugelassen werden, mit dem sogenannten eCall auszustatten[4].

Viel mehr noch als die technischen Neuerungen im Kfz-Bereich, hat aber das Smartphone unseren Alltag nachhaltig verändert. Im Jahr 2022 besitzen bereits 87% aller Österreicher und Österreicherinnen ein Smartphone und davon können sich ganze 68% ein Leben ohne Smartphone überhaupt nicht mehr vorstellen[5].

Innovative Versicherungskonzepte wie "Pay as you drive"[6] sind nicht zuletzt diesen technischen Fortschritten geschuldet. In den folgenden Kapiteln dieser Master Thesis

[1]Versicherungsverband Österreich (VVO), Jahresbericht 2021, Datenteil; https://www.vvo.at/vvo/vvo.nsf/sysPages/x52885E94068B6B49C125883600331E8D/$file/VVO_Jahresbericht_2021_Datenteil_August.pdf (abgerufen am 17.10.2022).
[2]Vlg: Presseaussendung der Allianz Gruppe in Österreich vom 17.12.2009; https://www.ots.at/presseaussendung/OTS_20091217_OTS0020/kfz-haftpflichtversicherung-feiert-ihren-80-geburtstag (abgerufen am 17.10.2022).
[3]*Bönninger/Schüppel*, Vertrauen erhalten – Datenschutz und Datensicherheit bei modernen Fahrzeugen, ZVR 2015, 474.
[4]Verordnung (EU) 2015/758 des Europäischen Parlamentes und des Rates vom 29. April 2015 über Anforderungen für die Typengenehmigungen zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG.
[5]Smartphone Nutzung in Österreich; https://de.statista.com/themen/3654/smartphone-nutzung-in-oesterreich/#topicHeader__wrapper (abgerufen am 17.10.2022).
[6]Wörtlich übersetzt: „Zahle wie du fährst".

werden das Versicherungskonzept “Pay as you drive” und die damit verbundenen datenschutzrechtlichen Fragestellungen näher betrachtet.

2) Was sind Telematiktarife?

2.1 Definition

Die Verbraucherschutzminister der Länder in Deutschland haben den Begriff “Telematiktarife” wie folgt definiert: „*Versicherungsverträge, bei denen ein bestimmtes risikorelevantes Verhalten zumindest teilweise (digital) erfasst und bei entsprechendem Wohlverhalten belohnt wird*“[7]. Telematiktarife sind nicht nur in der Kfz-Versicherung (“Pay as you drive”) sondern auch in anderen Versicherungssparten denkbar, wie beispielsweise in der Krankenversicherung (“Pay as you live”) oder in der Haushalts- und Eigenheimversicherung, insbesondere wenn es sich bei dem versicherten Objekt um ein “smart home” handelt[8].

2.2 Technische Umsetzung

Aus der oben angeführten Begriffsbestimmung ergibt sich, dass es bei Telematiktarifen um die Erfassung von risikorelevantem Nutzerverhalten geht. “Pay as you drive”-Tarife (PAYD-Tarife) werden technisch durch das Mitführen einer sogenannten On-Board-Unit im versicherten Kfz umgesetzt. Als On-Board-Unit (OBU) kann das eigene Smartphone des Versicherungsnehmers/der Versicherungsnehmerin oder ein eigens im Kfz verbautes Gerät verwendet werden. In beiden Fällen fallen für den Versicherer Kosten für die Entwicklung der Software an (zB App für Smartphone), bei eigens verbauten OBU kommen noch Kosten für die Anschaffung bzw Entwicklung der Hardware und deren Einbau hinzu.

Als dritte Möglichkeit kann die bereits im Kfz vorhandene Hard- und Software als OBU verwendet werden (zB Navigationssystem, Fahrassistenz oder eCall). In der Literatur ist man bis 2018 davon ausgegangen, dass insbesondere die Einführung des verpflichtenden eCalls zu einem deutlich vermehrten Angebot an Telematiktarifen führen wird. Dies, weil erwartet wurde, dass durch den eCall die Hard- und Softwarekosten sinken und

[7] *Brand*, Zulässigkeit und Ausgestaltung von Telematiktarifen, VersR 2019, 725.
[8] *Zoppel*, Digitale Anreizmodelle in der privaten Krankenversicherung und ihre Grenzen, ALJ 2022, 3.

Telematiktarife für den Versicherer dadurch rentabler werden[9]. Beim eCall handelt es sich um ein automatisches Notrufsystem. Im Falle eines Unfalls oder bei manueller Auslösung durch den Lenker/die Lenkerin wird ein Notruf abgesetzt. Dabei werden an die Notrufzentrale eine Reihe von Daten übermittelt, welche sich für die Ausgestaltung eines Telematiktarifes eignen würden (zB GPS-Koordinationsdaten des Unfallortes, Unfallzeit, Anzahl der Passagiere und Information, ob diese angegurtet waren etc)[10]. Entgegen der Erwartungen hat die Einführung des eCalls, zumindest in Österreich, aber nicht zu einem Anstieg von Telematiktarifen geführt[11].

2.3 Beweggründe für das Anbieten bzw Abschließen von Telematiktarifen

„Daten sind das "Grundnahrungsmittel" der Versicherungstechnik."[12] Für den Versicherer bieten Telematiktarife den großen Vorteil, das versicherte Risiko genauer einschätzen und bewerten und dadurch eine risikoäquivalente Prämie berechnen zu können. Zwar wird auch bei klassischen Versicherungstarifen üblicherweise das individuelle Risiko in die Berechnung der Prämie miteinbezogen (zB PS des versicherten Kfz in der Kfz-Versicherung, Vorerkrankungen in der Krankenversicherung), zumeist liegt aber eine Informationsasymmetrie zulasten des Versicherers vor[13]. Der Versicherer ist nämlich darauf angewiesen, dass die Versicherungsnehmer*innen vorvertraglich alle bekannten Risiken wahrheitsgemäß und vollständig angeben. Andernfalls kann er relevante Risiken nicht in der Prämienkalkulation berücksichtigen. Informationsasymmetrien können durch Telematiktarife zu einem großen Teil aufgelöst werden. Dennoch ergab eine umfassende betriebswirtschaftliche Analyse, dass die zu erwartenden betriebswirtschaftlichen Ergebniseffekte von PAYD-Versicherungstarifen nicht unbedingt als positiv und rentabel einzuschätzen sind[14]. Das dürfte wohl auch der Grund dafür sein, dass selbst die Einführung des eCalls nicht zu einem vermehrten Angebot an PAYD-Tarifen geführt hat.

---

[9] *Brandl/Pfaffeneder*, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, Aufsatzteil, Jahrbuch Datenschutzrecht 2014, 193.
[10] *Bönninger/Schüppel*, Vertrauen erhalten – Datenschutz und Datensicherheit bei modernen Fahrzeugen, ZVR 2015, 474.
[11] Eine Internetrecherche hat ergeben, dass zum 05.04.2023 kein österreichischer Versicherer einen PAYD-Versicherungstarif anbietet.
[12] *Pscheidl*, Was erwartet die Versicherungswirtschaft? EU-Legislaturperiode 2014-2019, VR 2015, H1-2, 44.
[13] *Zoppel*, Digitale Anreizmodelle in der privaten Krankenversicherung und ihre Grenzen, ALJ 2022, 1-2.
[14] *Gerpott/Berg*, Pay-As-You-Drive Angebote von Erstversicherern für Privatkunden, Eine betriebswirtschaftliche Analyse, online publiziert am 7. Mai 2011 im Springer Verlag.

Für die Versicherungsnehmer*innen können Telematiktarife einerseits zu einer Prämienersparnis führen, da risikoarmes Verhalten belohnt wird. Andererseits können Telematiktarife einen Anreiz zur bewussten Änderung des Fahrstils (bzw. des Lebensstils bei "Pay as you life") setzen und damit zu einer Reduzierung von Risiken führen. Es kann zB der Anreiz gesetzt werden, langsamer oder weniger häufig zu fahren. Telematiktarife sollen angeblich auch dazu führen, konventionell nicht mehr versicherbare Risiken doch noch versicherbar zu machen. Als Beispiel werden in der Literatur Kfz-Versicherungstarife für junge, unerfahrene Fahrer*innen oder Krankenversicherungstarife für Menschen mit ernsthaften Vorerkrankungen genannt. Telematiktarife befriedigen in einer gewissen Weise auch das wachsende Bedürfnis nach „Selbstoptimierung"[15]. All diesen Vorteilen stehen jedoch gewisse Nachteile und Risiken, insbesondere datenschutzrechtlicher Natur, gegenüber.

2.4 Tarifmodelle und zivilrechtliche Vertragsgestaltung

Der Vollständigkeit halber erlaube ich mir an dieser Stelle einen Exkurs in das allgemeine Zivilrecht und stelle die Möglichkeiten und Grenzen der Vertragsgestaltung von PAYD-Tarifen überblicksartig dar. Aus vertragsrechtlicher Sicht sind verschiedene Modelle von Telematiktarifen denkbar:

A) Die vorvertraglich vereinbarte maximale Prämie kann – je nach Fahrverhalten – niedriger werden. Das bedeutet, dass risikoarmes Fahrverhalten belohnt wird. Zu einer Sanktionierung von risikoreichem Fahrverhalten und einem Anstieg der Prämie kommt es jedoch nicht.

B) Die vorvertraglich vereinbarte Prämienhöhe kann – je nach Fahrverhalten – sowohl höher als auch niedriger werden. Ein risikoarmer Fahrstil führt zu einer Reduktion der vereinbarten Prämie, während ein risikoreiches Fahrverhalten eine Prämienerhöhung nach sich zieht[16].

C) Es wird vorvertraglich keine Einigung über die Höhe der Prämie in absoluten Zahlen getroffen, sondern es werden lediglich die Parameter der Prämienberechnung (dh die prämienrelevanten Faktoren) festgelegt.

[15] *Zoppel*, Digitale Anreizmodelle in der privaten Krankenversicherung und ihre Grenzen, ALJ 2022, 3.
[16] *Brandl/Pfaffeneder*, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, Jahrbuch Datenschutzrecht 2014, 192.

Damit ein Vertrag wirksam zustande kommt, muss „*zumindest eine Vereinbarung der essentialia negotii erfolgen; werden Hauptpunkte nicht geregelt, kann der Vertrag nicht wirksam sein*“[17]. Unter den essentialia negotii versteht man den nötigen Mindestinhalt, den ein Vertrag aufweisen muss und über den die Vertragsparteien Einigkeit erzielen müssen, damit der Vertrag wirksam zustande kommt[18]. Der OGH hat klargestellt, dass beim Versicherungsvertrag, als essentialia negotii, zumindest über die Art der Versicherung, das versicherte Risiko und über die Prämie Einigkeit hergestellt werden muss[19]. Die Prämie muss bestimmt oder bestimmbar festgelegt sein. Gemäß § 1054 ABGB muss der Kaufpreis (hier die Prämie) „*in barem Gelde bestehen, und darf weder unbestimmt, noch gesetzwidrig sein“*. Zudem ergibt sich auch aus § 915 ABGB, dass Vertragsbestimmungen hinreichend bestimmt und verständlich sein müssen.

Bei allen beschriebenen Tarifmodellen (A-C) ist die letztendlich zu bezahlende Prämie - und somit eines der essentialia negotii - nicht ziffernmäßig bestimmt. Nach der hM genügt jedoch eine objektive Bestimmbarkeit des Preises (hier der Prämie)[20] [21]. Um die Prämienhöhe bestimmen zu können, sind die Parameter und Faktoren, die für die Berechnung der Prämie ausschlaggebend sind, nachvollziehbar zu beschreiben. Die Versicherungsnehmer*innen müssen wissen, wie sich ihr Fahrverhalten auf die Prämienhöhe auswirkt (zB pro x gefahrenem Kilometer x Euro an Prämie; pro Überschreitung der Mindestgeschwindigkeit um x km/h, x Euro an Prämie etc).

Jedes der oben beschriebenen Modelle hat dem Bestimmtheitserfordernis zu entsprechen. Auf den ersten Blick ist diese Anforderung bei den Modellen A) und B) einfacher umzusetzen als beim Modell C), da in beiden Fällen eine Basisprämie festgelegt wird und die Prämie nicht gänzlich variabel ist. Aber auch bei diesen Modellen müssen alle Parameter und Faktoren, die zu einer Veränderung der Basisprämie führen, nachvollziehbar und bestimmbar festgelegt werden. Die Versicherungsnehmer*innen müssen verstehen können, welches Verhalten sich in welchem Ausmaß auf die Prämie auswirkt. Das gilt auch für das Modell A), obwohl es sich dabei im Wesentlichen um ein Rabattmodell handelt, bei dem sich die festgelegte Prämie lediglich reduzieren kann[22].

[17] Vgl: Arb. 9349, 10.486; SZ 53/101; ZAS 1987/12 uva.
[18] OGH 17.01.1990, 9 ObA 365/89.
[19] OGH 19.03.2003, 7 Ob 31/03i.
[20] *Barth/Dokalik/Potyka*, ABGB (MTK)[27] § 1054 ABGB (Stand 1.7.2022, rdb.at).
[21] *Verschraegen* in *Kletečka/Schauer*, ABGB-ON[1.08] § 1054, RZ 25 (Stand 1.5.2020, rdb.at).
[22] *Zoppel*, Digitale Anreizmodelle in der privaten Krankenversicherung und ihre Grenzen, ALJ 2022, 4.

Handelt es sich bei dem Versicherungsnehmer/der Versicherungsnehmerin um einen Verbraucher/eine Verbraucherin, so sind außerdem die Bestimmungen des Konsumentenschutzgesetzes (KSchG) einzuhalten. Gemäß § 6 Abs 1 Z 5 KSchG sind „*für den Verbraucher (...) besonders solche Vertragsbestimmungen im Sinn des § 879 ABGB jedenfalls nicht verbindlich, nach denen dem Unternehmer auf sein Verlangen für seine Leistung ein höheres als das bei der Vertragsschließung bestimmte Entgelt zusteht, es sei denn, daß der Vertrag bei Vorliegen der vereinbarten Voraussetzungen für eine Entgeltänderung auch eine Entgeltsenkung vorsieht, daß die für die Entgeltänderung maßgebenden Umstände im Vertrag umschrieben und sachlich gerechtfertigt sind sowie daß ihr Eintritt nicht vom Willen des Unternehmers abhängt*".

§ 6 Abs 1 Z 5 KSchG ist auf das Modell A) nicht anwendbar, da dieses keine Erhöhung der Prämie vorsieht. Bei Modell B) kann es hingegen zu einer Erhöhung der Prämie kommen, weshalb es im Anwendungsbereich des § 6 Abs 5 Z 1 KSchG liegt. Nach dieser Bestimmung sind Prämienerhöhungen nur dann zulässig, wenn sie den in leg cit genannten Erfordernissen entsprechen. Das Model B) sieht bei Eintritt der vereinbarten Voraussetzungen nicht nur eine Erhöhung, sondern auch eine Reduktion der Prämie vor, dh die Prämienanpassung "geht in beide Richtungen". Der Eintritt der maßgebenden Umstände hängt nicht vom Willen der Versicherung ab. Im Gegenteil – bei PAYD-Tarifen können die Versicherungsnehmer*innen durch ihr Verhalten den Eintritt der maßgebenden Umstände herbeiführen. Außerdem sieht § 6 Abs 5 Z 1 KSchG vor, dass die maßgebenden Umstände im Vertrag umschrieben sein müssen. Das ergibt sich auch aus den allgemeinen zivilrechtlichen Grundsätzen (§§ 915, 1054 ABGB; siehe dazu oben). Im Anwendungsbereich des KSchG ist jedoch ein noch strengerer Maßstab an die Transparenz und Nachvollziehbarkeit anzulegen (Transparenzgebot, § 6 Abs 3 KSchG)[23].

Fazit: Unabhängig vom gewählten Modell, stellt die Beschreibung jener Faktoren, die sich auf die Höhe der Prämie auswirken, eine Herausforderung für den Versicherer dar. Es sind die prämienrelevanten Faktoren und somit komplexe kalkulatorische Grundlagen so darzustellen, dass die Versicherungsnehmer*innen diese nachvollziehen können[24].

[23] *Pletzer* in *Kletečka/Schauer*, ABGB-ON[1.03], § 869, RZ 25 (Stand 1.8.2019, rdb.at).
[24] Vgl: *Grubmann*, VersVG[9] § 1, E 7 (Stand 1.7.2022, rdb.at): *„Jedenfalls aber muss eine wirksame Rabattvereinbarung bestimmt iSd § 869 ABGB sein".*

Rein nutzenbasierte Modelle, die ausschließlich auf die Anzahl der gefahrenen Kilometer abstellen, sind vor diesem Hintergrund sicherlich am einfachsten umzusetzen.

3) Fahrzeug- und Telematikdaten

3.1 Datenarten

In modernen Fahrzeugen sind rund 80 technische Geräte verbaut[25] (*Anm: Stand 2014*) und täglich werden rund 600 Gigabyte an Daten generiert[26]. Die im Kfz verbauten Geräte (zB Sensoren) kommunizieren untereinander, aber auch mit der Außenwelt (zB mit anderen Fahrzeugen, mit Mautsystemen etc) – man spricht vom vernetzen Fahrzeug[27]. Es wird geschätzt, dass der Anteil an vernetzten Automobilen in der EU im Jahr 2035 bei 97% liegen wird[28].

Das vernetzte Fahrzeug ist eine Kombination aus Hard- und Software und es fallen zunächst Daten über das Fahrzeug selbst an (Fahrzeugdaten), wie zum Beispiel:

- die Fahrzeug-Identifizierungsnummer (VIN)
- MAC-Adresse der Netzwerkkarte für die Kommunikation mit dem WLAN
- RFID-Kennung (zB bei Autoschlüsseln mit Fernbedienungsfunktion)
- SIM-Karten-Nummer für die Übertragung von Daten
- Daten über die Gangschaltung
- Daten über die Beleuchtung (zB wie lange die Scheinwerfer eingeschalten waren)
- Daten über den Sicherheitsgurt (zB wie oft der Sitzgurt aufgrund einer Bremsung gestrafft wurde)

Neben den Fahrzeugdaten werden auch sogenannte Telematikdaten erfasst. Dabei handelt es sich um Daten, die während der Fahrt generiert werden. Zu ihnen zählen beispielsweise:

- Standortdaten
- Fahrtrichtung

[25] *Roßnagel*, Fahrzeugdaten – wer darf über sie entscheiden?, SVR 8/2014, 281.
[26] *Karsten/Wienroeder*, Der Entwurf des Data Act - Auswirkungen auf die Automobilindustrie, RAW 2/2022, 99.
[27] *Krauß/Waidner*, IT-Sicherheit und Datenschutz im vernetzten Fahrzeug, DuD 6/2015, 383.
[28] *Karsten/Wienroeder*, Der Entwurf des Data Act - Auswirkungen auf die Automobilindustrie, RAW 2/2022, 100.

- Geschwindigkeit
- Zeit und Dauer einer Fahrt[29]

Es ist technisch durchaus möglich, dass ein modernes Fahrzeug sogar biometrische Daten (zB Fingerabdruck als Schlüssel) oder Gesundheitsdaten (zB Herzschlag und Atmung des Fahrers/der Fahrerin über den Sicherheitsgut) erfassen kann[30].

Welche Daten im Zusammenhang mit einem PAYD-Versicherungstarif tatsächlich verarbeitet werden, hängt immer von der jeweiligen konkreten technischen Umsetzung und der vertraglichen Ausgestaltung ab. Greift der Versicherer auf Fahrzeug- und Telematikdaten zurück, die von einem vernetzten Fahrzeug erfasst werden, so stehen uU mehr oder andere Daten zur Verfügung, als wenn extra verbaute Geräte oder das eigene Smartphone der Versicherungsnehmer*innen als OBU verwendet werden.

3.2 Personenbezug von Fahrzeug- und Telematikdaten

Seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DSGVO)[31] die rechtliche Grundlage für den Datenschutz in Österreich. Die DSGVO ist unmittelbar anwendbar (Vollharmonisierung)[32] und wird durch das österreichische Datenschutzgesetz (DSG) ergänzt[33]. Artikel 1 des DSG steht im Verfassungsrang und normiert ein Grundrecht auf Datenschutz sowie auf Geheimhaltung personenbezogener Daten. Im versicherungsrechtlichen Bereich sieht § 321 VAG außerdem das sogenannte Versicherungsgeheimnis vor.

Die DSGVO findet Anwendung auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie auf die nicht-automatisierte Verarbeitung

[29] *Stingl*, Smart Cars und der Datenschutz“ Datenschleuder oder sinnvolle Datenverwendung?, Jahrbuch Datenschutzrecht 2016, *Jahnel* (Hrsg), 166.
[30] *Hansen*, Das Netz im Auto & das Auto im Netz, DuD 6/2015, 368.
[31] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.
[32] *Ehmann/Selmayr/Zerdick*, 2. Aufl 2018, DS-GVO Art 1 RN 3.
[33] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG).

personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen (Art 2 Abs 1 DSGVO)[34] [35].

Die DSGVO kommt nur dann zur Anwendung, wenn personenbezogene Daten verarbeitet werden. Nach der Definition von Art 4 DSGVO versteht man unter personenbezogenen Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen[36]. Als identifizierbar wird eine natürliche Person angesehen, „*die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann*."

Eine Person ist dann eindeutig identifiziert, wenn sie durch bestimmte Merkmale unverwechselbar als genau die eine betroffene Person gekennzeichnet ist. Insbesondere der Name einer Person ist dazu geeignet, eine Person von einer anderen zu unterscheiden. Bei Namensgleichheit sind weitere Merkmale zur eindeutigen Unterscheidbarkeit heranzuziehen (zB Name in Kombination mit dem Geburtsdatum)[37].

Ein Personenbezug besteht gemäß Art 4 Z 1 DSGVO aber auch dann, wenn die betroffene Person zwar nicht identifiziert, aber direkt oder indirekt identifizierbar ist. Direkte Identifizierbarkeit liegt vor, wenn sich aus den vorliegenden Daten genügend individualisierende Personenmerkmale ergeben, aus denen tatsächlich die jeweilige betroffene Person festgestellt werden kann. Indirekte Identifizierbarkeit liegt vor, wenn aus der Gesamtheit aller vorliegenden Merkmale, die für sich genommen schwach und wenig aussagekräftig sind, eine Person nach allgemeinem Ermessen wahrscheinlich bestimmt werden kann[38]. Für die Herstellung eines Personenbezuges ist es demgemäß

[34] *Bäcker* in BeckOK DatenschutzR, 43. Ed 1.11.2021, DS-GVO Art 2 RN 2.
[35] *Meyerdierks* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap 3, RZ 13 (Stand 1.4.2021, rdb.at).
[36] *Schröder*, Datenschutzrecht für die Praxis[4], 14.
[37] *Hödl* in *Knyrim,* DatKomm Art 4 DSGVO, RZ 11 (Stand 1.12.2018, rdb.at).
[38] *Bergauer*, Personenbezogene Daten, Begriff und Kategorien, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 52-53.

ausreichend, dass die betroffene Person mit hoher Wahrscheinlichkeit identifiziert werden kann, eine tatsächliche Feststellung der Identität ist aber nicht gefordert.

Die bei PAYD-Versicherungstarifen gesammelten Fahrzeug- und Telematikdaten beziehen sich nicht zwangsläufig auf eine bestimmte Person, sondern primär auf ein bestimmtes Fahrzeug. Nur wenn das versicherte Fahrzeug ausschließlich vom Versicherungsnehmer/von der Versicherungsnehmerin gefahren wird, liegt ein eindeutiger Personenbezug vor. Sobald das Fahrzeug aber von mehreren Personen benutzt wird - was gerade innerhalb einer Familie häufig der Fall ist - können die erfassten Daten nicht mehr eindeutig einer bestimmten identifizierten Person zugeordnet werden[39]. In der Literatur wird der Personenbezug von Fahrzeug- und Mobilitätsdaten dennoch übereinstimmend bejaht. Ein Kfz ist nämlich einem bestimmten Halter/einer bestimmten Halterin zugeordnet. Eine Kfz-Versicherung bezieht sich auf diesen Halter/diese Halterin und versichert sein/ihr Risiko. Wird ein Kfz üblicherweise vom Halter/von der Halterin benutzt, ist ein Personenbezug auch dann gegeben, wenn das Kfz noch von anderen Personen gefahren wird[40] [41] [42]. Zur Herstellung eines Personenbezugs ist es ausreichend, dass die gesammelten Daten mit dem Halter/der Halterin in Verbindung gebracht bzw grundsätzlich zugeordnet werden können[43]. Eine tatsächliche Zuordnung der Daten zu einem bestimmten Fahrer/einer bestimmten Fahrerin ist nicht gefordert[44]. Die Zuordnung des versicherten Kfz zum Halter/zur Halterin stellt den Personenbezug mit ausreichend hoher Wahrscheinlichkeit her (indirekte Identifizierbarkeit).

Darüber hinaus sprechen noch weitere Argumente dafür, Fahrzeug- und Telematikdaten als personenbezogene Daten zu behandeln. Viele der in einem vernetzten Fahrzeug verbauten Hardwarekomponenten, können einer eindeutigen Kennung zugeordnet werden. Kennungen wie die MAC-Adresse der Netzwerkkarte oder die Fahrzeug-Identifikationsnummer sind global einmalig vergebene Identifikatoren, die unveränderlich

[39] *Brandl/Pfaffeneder*, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, Jahrbuch Datenschutzrecht 2014, 194.
[40] *Stingl*, Smart Cars und der Datenschutz" Datenschleuder oder sinnvolle Datenverwendung?, Jahrbuch Datenschutzrecht 2016, 170, *Jahnel* (Hrsg).
[41] *Brandl/Pfaffeneder*, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, Jahrbuch Datenschutzrecht 2014, 195.
[42] *Schröder* nennt Angaben als Kfz-Halter als Positivbeispiel für das Vorliegen eines Personenbezuges. Siehe dazu: *Schröder,* Datenschutzrecht für die Praxis[4], 15.
[43] *Taeger/Gabel/Arning/Rothkegel*, 4. Aufl 2022, DS-GVO Art 4 RN 14.
[44] *Kunnert*, „Autonomes Fahren" aus datenschutzrechtlicher Sicht, Autonomes Fahren und Recht, in *Eisenberger, Lachmayer, Eisenberger* (Hrsg), 188-189.

sind. Sie können noch eindeutiger zugeordnet werden als eine IP-Adresse[45], die aber als personenbezogen gilt[46] [47].

Darüber hinaus kann ein Personenbezug auch durch die Kombination mehrerer Daten, die für sich genommen nicht personenbezogen wären, hergestellt werden. Das könnte zum Beispiel dann der Fall sein, wenn durch die Auswertung von Telematikdaten Rückschlüsse auf Wohn- und Dienstort gezogen werden können[48]. Die Nutzung von Standortdaten wird in der Literatur explizit als Möglichkeit zur Identifizierung genannt[49].

Fazit: Fahrzeug- und Telematikdaten sind personenbezogene Daten und unterliegen der DSGVO sowie dem DSG.

3.3 Fahrzeug- und Telematikdaten als besonders schutzwürdige Daten?

Die DSGVO trifft für die Verarbeitung besonderer Kategorien personenbezogener Daten gesonderte Regelungen. In Art 9 DSGVO werden jene personenbezogene Daten behandelt, die besonders schutzwürdig sind. In Art 10 behandelt die DSGVO die Verarbeitung von sogenannten strafrechtsbezogenen Daten. Die in diesen beiden Artikeln genannten Daten entsprechen jenen Daten, die vor dem In-Kraft-Treten der DSGVO als „sensibel" bezeichnet wurden[50].

In ErwGr 51 wird ausgeführt, dass die in Art 9 Abs 1 DSGVO genannten Daten besonders sensibel sind, mit ihrer Verarbeitung enorme Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen verbunden sein können und aus diesen Gründen ein besonderer Schutz geboten ist[51]. Gemäß Art 9 Abs 1 DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten daher grundsätzlich untersagt und nur unter einem der zehn Ausnahmetatbestände des Art 9 Abs 2 DSGVO gestattet[52].

---

[45]Anm: Findige User kennen jedoch Möglichkeiten, die MAC-Adresse zu verschleiern. Siehe dazu beispielsweise: https://www.ionos.at/digitalguide/server/knowhow/was-ist-mac-spoofing/ (abgerufen am 12.01.2023).
[46]EuGH 19.10.2016, C-582/14.
[47]*Weichert*, Datenschutz im Auto - Teil 1, Das Kfz als großes Smartphone auf Rädern, SVR 6/2014, 204.
[48]*Hansen*, Das Netz im Auto & das Auto im Netz, DuD 6/2015, 369.
[49]*Karg* in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 4 Nr 1 RN 57.
[50]*Bergauer*, Personenbezogene Daten, Begriff und Kategorien, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 56.
[51]*Kastelitz/Hötzendorfer/Tschohl* in *Knyrim,* DatKomm Art 9 DSGVO, RZ 3 (Stand 7.5.2020, rdb.at).
[52]*Arning;Rohwedder* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap 5, RZ 159 (Stand 1.4.2021, rdb.at).

Besonders schutzwürdig nach Art 9 Abs 1 DSGVO sind Daten über:

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse und weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- genetische Daten
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung

Sieht man sich den Wortlaut des Art 9 Abs 2 DSGVO genauer an, so erkennt man drei unterschiedliche Kategorien an sensiblen Daten:

1 Gesundheitsdaten, Daten zum Sexualleben sowie genetische Daten können als „an sich sensible Daten" bezeichnet werden und fallen schon dem Wortlaut nach immer unter das Schutzregime des Art 9 DSGVO.
2 Gehen aus einer Datenverarbeitung Informationen über die rassische und ethnische Herkunft, die politische Meinung, die religiöse oder weltanschauliche Überzeugung oder über eine Gewerkschaftszugehörigkeit hervor, liegen ebenfalls sensible Daten vor. In der Literatur wird von sogenannten „Hervorgehens-Daten" gesprochen.
3 Biometrische Daten sind dann als sensibel einzustufen, wenn sie zum Zwecke der eindeutigen Identifizierbarkeit einer natürlichen Person verarbeitet werden[53] [54].

Telematikdaten, einschließlich Standortdaten, sind keine „an sich sensiblen Daten". Aus ihrer Verarbeitung können aber sensible Daten hervorgehen („Hervorgehens-Daten"). Das muss aber nicht zwangsläufig so sein, weswegen man in diesem Zusammenhang auch von „potentiell sensiblen Daten"[55] spricht (passender vielleicht: „potentiell sensible Hervorgehens-Daten"). Wird zum Beispiel ein versichertes Fahrzeug in der Nähe einer Kirche, Parteizentrale oder Krankenanstalt abgestellt, könnten aus der Verarbeitung

[53] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 9 DSGVO, RZ 15 (Stand 1.12.2020, rdb.at).
[54] *Ehmann/Selmayr/Schiff,* 2. Aufl 2018, DS-GVO Art 9 RN 13, 27.
[55] *Goricnik/Grünanger* in *Grünanger/Goricnik*, Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] Kap 7, RZ 7.66 (Stand 1.11.2018, rdb.at).

dieser Standortdaten Informationen über die religiöse Überzeugung, die politische Meinung oder den Gesundheitszustand der Versicherungsnehmer*innen hervorgehen[56].

Nach der Literatur sollen Daten dann als sensibel gelten, wenn die besondere Schutzwürdigkeit der Information für einen durchschnittlichen, objektiven Dritten erkennbar ist. Es soll aber nicht jeder indirekte Hinweis und nicht jede erdenkliche theoretische Möglichkeit zur Herleitung von sensiblen Informationen zur Anwendbarkeit des Art 9 DSGVO führen[57] [58]. Daten sollen daher nur dann unter Art 9 DSGVO fallen, wenn sich aus ihnen mit „hinlänglicher Sicherheit" besonders schutzwürdige Informationen herleiten lassen. In der Literatur wird auch vertreten, dass Art 9 DSGVO in Zweifelsfällen gerade nicht anwendbar sein soll, um seinen Anwendungsbereich nicht unnötig „aufzublähen"[59].

Das erscheint mir zweckmäßig und konsistent mit der übrigen Auslegungspraxis. Aus dem ErwGr 51 ergibt sich beispielsweise, dass auch Bilddaten nicht generell als sensible Daten anzusehen sind. Das ist eine mE relativ restriktive Ansicht, denn immerhin könnte wohl jeder durchschnittliche Dritte anhand eines Bildes auf die rassische Herkunft der abgebildeten Person schließen. Auch die deutsche Datenschutzkonferenz hat in ihrem Kurzpapier Nr 17 zu den Besonderen Kategorien personenbezogener Daten festgehalten, dass sich zum Beispiel aus dem Geburtsort keine ausreichenden Hinweise auf die rassische Herkunft ergeben oder dass aus dem einmaligen Besuch einer sakralen Stätte noch nicht auf die Religion einer Person geschlossen werden kann[60]. Vor diesem Hintergrund können Standortdaten mE nicht per se als besonders schutzwürdige Daten im Sinne des Art 9 DSGVO eingestuft werden.

Bei PAYD-Versicherungstarifen werden - je nach Vertragskonstellation – kontinuierlich Telematikdaten (inklusive Standortdaten) erfasst und ausgewertet, so dass auch Bewegungsprofile erstellt werden könnten. Daraus lassen sich Rückschlüsse auf

[56] *Stingl*, Smart Cars und der Datenschutz" Datenschleuder oder sinnvolle Datenverwendung?, Jahrbuch Datenschutzrecht 2016, 170-171, *Jahnel* (Hrsg).
[57] *Bergauer*, Personenbezogene Daten, Begriff und Kategorien, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 60.
[58] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim,* DatKomm Art 9 DSGVO, RZ 19 (Stand 7.5.2020, rdb.at).
[59] *Gola/Heckmann/Schulz*, 3. Aufl 2022, DS-GVO Art 9 RN 13.
[60] Kurzpapier Nr 17 der dt Datenschutzkonferenz, Besondere Kategorien personenbezogener Daten, Stand: 27.03.2018, Seite 1, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_17.pdf (abgerufen am 07.02.2023).

regelmäßige Verhaltensweisen ziehen. Wie oben erwähnt, wird zwar der einmalige Besuch einer Kirche noch keinen Hinweis auf eine religiöse Überzeugung liefern, der regelmäßige Besuch hingegen schon. Auch der regelmäßige Besuch von Krankenhäusern und Gesundheitseinrichtungen kann Hinweise auf den Gesundheitszustand geben, insbesondere betreffend chronischer Erkrankungen (zB Besuch eines Dialysezentrums, einer onkologischen Tagesklinik)[61]. Grundsätzlich gilt: „*Je dichter ein Bewegungsprofil, desto individueller wird sein Charakter*“[62].

Ein gewisser Grad an „Unsicherheit“ bleibt jedoch selbst bei der Auswertung von dichten und umfassenden Bewegungsprofilen bestehen. Immerhin könnte ein Krankenhaus zB auch deswegen regelmäßig aufgesucht werden, weil die betroffene Person dort arbeitet oder Waren dorthin liefert.

Aus meiner Sicht kommt es bei der Beurteilung der Frage, ob Telematikdaten besonders schutzwürdige Daten im Sinne des Art 9 DSGVO sind, immer auf die individuelle Situation im Einzelfall an. Eine unbedingte Anwendung des Art 9 DSGVO auf alle PAYD-Versicherungstarife kommt mE nicht in Frage, auch dann nicht wenn eine besonders „intensive“ Datenverarbeitung stattfindet. Zum einen bleibt sogar bei der Auswertung von dichten Bewegungsprofilen eine gewisse Unschärfe bestehen und zum anderen werden aus den meisten Bewegungsprofilen wohl gar keine sensiblen Informationen hervorgehen, etwa weil die betroffene Person weder Kirchen noch Krankenhäuser regelmäßig besucht. Der Versicherer muss daher nicht davon ausgehen, dass sich aus den erhobenen Telematikdaten mit hinlänglicher Sicherheit sensible Inhalte ableiten lassen. Eine generelle Anwendung des hohen Schutzniveau des Art 9 DSGVO wäre mE daher überschießend[63].

Andererseits halte ich die von *Goricnik/Grünanger* vertretene Ansicht, den Art 9 DSGVO nur dann anzuwenden, wenn der Verantwortliche zweifelsfrei erkennt, dass tatsächlich sensible Daten verarbeitet werden[64], für zu wenig weitreichend. Denn bei evidenter

---

[61] *Goricnik/Grünanger* in *Grünanger/Goricnik*, Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle^2 Kap 7, RZ 7.66 (Stand 1.11.2018, rdb.at).

[62] *Kunnert*, „Autonomes Fahren“ aus datenschutzrechtlicher Sicht, Autonomes Fahren und Recht, in *Eisenberger, Lachmayer, Eisenberger* (Hrsg), 191.

[63] Vgl: *Gola/Heckmann/Schulz*, 3. Aufl 2022, DS-GVO Art 9 RN 13.

[64] *Goricnik/Grünanger* in *Grünanger/Goricnik,* Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle^2 Kap 7, RZ 7.70 (Stand 1.11.2018, rdb.at).

Verarbeitung von sensiblen Daten sind die Bestimmungen des Art 9 DSGVO selbstverständlich immer anzuwenden. Es wäre praxistauglich den Art 9 DSGVO immer dann anzuwenden, wenn der Versicherer, aus welchen Gründen auch immer, davon ausgehen muss, dass mit hoher Wahrscheinlichkeit sensible Daten verarbeitet werden.

Fazit: Telematikdaten (insbesondere Standortdaten) können – müssen aber nicht zwangsläufig – besonders schutzwürdige Daten im Sinne des Art 9 DSGVO sein. Für die Zwecke dieser Master Thesis wird davon ausgegangen, dass es sich dabei nicht um schutzwürdige Daten im Sinne des Art 9 DSGVO handelt.

4) Grundsätze der Verarbeitung personenbezogener Daten

Im Kapitel II der DSGVO finden sich die Voraussetzungen unter denen die Verarbeitung von personenbezogenen Daten zulässig ist. Die zentralen Bestimmungen werden in Art 5 DSGVO (Grundsätze) und Art 6 DSGVO (Rechtmäßigkeit) normiert. Die Verarbeitung personenbezogener Daten hat den Anforderungen beider Artikel zu entsprechen[65]: „*Die Verarbeitung personenbezogener Daten ist zulässig, wenn sie – unter Einhaltung der in Art 5 DSGVO genannten Verarbeitungsgrundsätze – auf Grund einer der in Art 6 DSGVO genannten Erlaubnistatbestände erfolgt*[66]“.

Bei den Grundsätzen des Art 5 DSGVO handelt es sich um programmatische und allgemein formulierte Prinzipien, die aber dennoch unmittelbar gelten und deren Nicht-Einhaltung sanktioniert werden kann[67] [68].

Die Regelungen des Kapitel II DSGVO finden sich im dritten Hauptstück des österreichischen DSG (§§ 36 ff) wieder.

[65]Vgl: *Ehmann/Selmayr/Heberlein*, 2. Aufl 2018, DS-GVO Art 5 RN 5.
[66]BVwG 30.10.2019, W258 2216873-1.
[67]*Hötzendorfer/Tschohl/Kastelitz* in *Knyrim,* DatKomm Art 5 DSGVO, RZ 1, 3 (Stand 7.5.2020, rdb.at).
[68]*Paal/Pauly/Frenzel,* 3. Aufl 2021, DS-GVO Art 5 RN 1.

4.1 Grundsätze der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art 5 Abs 1 lit a DSGVO)

Der Grundsatz der Rechtmäßigkeit ist Ausgangspunkt und Basis jeder Verarbeitung von personenbezogenen Daten[69] und ist als Verweis auf die in Art 6 DSGVO genannten Rechtmäßigkeitstatbestände zu verstehen. Jede Datenverarbeitung hat den dort genannten Anforderungen zu entsprechen[70] [71].

Personenbezogene Daten dürfen außerdem nur nach Treu und Glauben verarbeitet werden. Was man unter Treu und Glauben zu verstehen hat, definiert die DSGVO nicht und eröffnet damit einen weiten Spielraum für Interpretation und Rechtsfortbildung. In der englischsprachigen Fassung der DSGVO wird Treu und Glauben mit "fairly" und "fairness" übersetzt, weswegen man auch vom Gebot der fairen Datenverarbeitung sprechen kann[72]. Unter Fairness versteht man ein anständiges und gerechtes Verhalten[73]. Nach ständiger Rechtsprechung des OGH spielt der Grundsatz von Treu und Glauben im versicherungsrechtlichen Bereich eine besonders wichtige Rolle. „*Der Grundsatz von Treu und Glauben beherrscht das Versicherungsverhältnis im besonderen Maß*[74]". Aus den OGH-Entscheidungen ergibt sich keine allgemein gültige Definition, auf die bei der Auslegung von Art 5 DSGVO zurück gegriffen werden könnte. Die Urteile des OGH vermitteln aber den Eindruck, als ob der Grundsatz von Treu und Glauben im versicherungsrechtlichen Bereich als flexibler Auffangtatbestand eingesetzt wird und großzügig auszulegen ist[75].

Aus Art 5 Abs 1 lit a DSGVO ergibt sich außerdem der Grundsatz der Transparenz der Datenverarbeitung. Die betroffene Person muss nachvollziehen können, wie und zu welchen Zwecken ihre personenbezogenen Daten erhoben, verwendet, eingesehen und verarbeitet werden. Informationen betreffend die Verarbeitung personenbezogener Daten müssen vollständig, verständlich sowie in klarer und einfacher Sprache abgefasst sein. Nur wenn die betroffene Person ausreichend transparent informiert wurde, ist sie in der

[69] *Lachmayer* in *Knyrim*, DatKomm § 37 DSG, RZ 8 (Stand 7.5.2020, rdb.at).
[70] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 5 DSGVO RZ 8 (Stand 1.12.2020, rdb.at).
[71] BVwG 16.10.2019, W256 2222862-1.
[72] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 5 DSGVO RZ 10 (Stand 1.12.2020, rdb.at).
[73] Vgl: Duden | fair | Rechtschreibung, Bedeutung, Definition, Herkunft (abgerufen am 10.02.2023).
[74] RS0018055.
[75] „Treu und Glauben können nach hM auch ergänzende Leistungs- oder Verhaltenspflichten schaffen." Vgl: *Hoch*, EvBl-LS 2016/168, ÖJZ 22/2016, 1035-136; OGH 15.6.2016, 7 Ob 86/16x.

Lage, die ihr zustehenden Betroffenenrechte auch wahrzunehmen[76] [77] und eine wirksame Einwilligung im Sinne des Art 6 Abs 1 lit a DSGVO zu erteilen. Zu den zivilrechtlichen Anforderungen an Bestimmtheit und Transparenz siehe Punkt 2.4.

4.2 Zweckbindungsgrundsatz (Art 5 Abs 1 lit b DSGVO iVm Art 6 Abs 4 DSGVO)

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Der Zweckbindungsgrundsatz ist in Art 8 Abs 2 GRC ausdrücklich verankert und wird in Art 5 Abs 1 lit b DSGVO konkretisiert. Er zählt zu den wichtigsten datenschutzrechtlichen Grundsätzen, der in den unterschiedlichsten Bereichen des Datenschutzrechts seinen Niederschlag findet. Der Zweckbindungsgrundsatz ist beispielsweise bei der Prüfung der zulässigen Speicherdauer, bei der Gestaltung von Einwilligungserklärungen oder bei Datenschutzfolgeabschätzungen zu beachten[78].

Die Zwecke der Datenverarbeitung müssen schon vor der erstmaligen Erhebung[79] von personenbezogenen Daten festgelegt sein und jede weitere Verarbeitung muss mit diesen festgelegten Zwecken vereinbar sein[80]. Für PAYD-Tarife bedeutet das, dass die Versicherungsnehmer*innen spätestens vor Versicherungsbeginn darüber informiert werden müssen, zu welchen Zwecken die erhobenen Telematikdaten verarbeitet werden. In der Praxis sollten die Versicherungsnehmer*innen sinnvollerweise nicht erst mit der Polizzierung und dem Versicherungsbeginn über die Verarbeitungszwecke informiert werden, sondern bereits im vorvertraglichen Stadium, idealerweise im Zuge des Beratungsgespräches.

---

[76] *Roßnagel* in *Simitis/Hornung/Spiecker gen. Döhmann,* 1. Aufl 2019, Datenschutzrecht, DSGVO Art 5 RN 50.
[77] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 5 DSGVO, RZ 14, 15 (Stand 1.12.2020, rdb.at).
[78] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 5 DSGVO, RZ 18 (Stand 1.12.2020, rdb.at).
[79] *Ehmann/Selmayr/Heberlein*, 2. Aufl 2018, DS-GVO Art 5 RN 13.
[80] *Kastelitz,* Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 102.

Die Verarbeitungszwecke müssen ausreichend bestimmt sein. Wichtig ist, dass die betroffenen Personen ein vollständiges und für sie verständliches Bild über die Zwecke der Verarbeitung bekommen. Daher sind die Verarbeitungszwecke in einfacher und klarer Sprache, aber dennoch hinreichend detailliert zu beschreiben. Die Anforderungen an die Bestimmtheit sind relativ hoch und allgemeine Beschreibungen wie „Marketingzwecke" oder „zum Zweck der Produktoptimierung" sind nicht ausreichend[81]. Die Verarbeitungszwecke sind möglichst konkret anzugeben, vage und zu breite Formulierungen sind unzulässig[82].

Für PAYD-Tarife schlagen *Brandl/Pfaffeneder* vor, den Verarbeitungszweck mit „*Berechnung einer dem Fahrverhalten des Versicherungsnehmers entsprechenden Prämie in der Kfz-Haftpflichtversicherung*" zu definieren[83]. Meines Erachtens ist diese Zweckbeschreibung aus datenschutzrechtlicher Sicht ausreichend bestimmt und eindeutig. Aus zivilrechtlicher Sicht ist jedoch eine detailliertere Beschreibung der prämienrelevanten Faktoren und deren Auswirkung geboten. Den Versicherungsnehmer*innen ist mitzuteilen, dass beispielsweise eine Überschreitung der Höchstgeschwindigkeit oder abruptes Bremsen zu einer Mehrprämie von x Euro führt. Daraus ergibt sich implizit auch der Zweck der Erhebung der Fahrgeschwindigkeit bzw der Erhebung des Bremsverhalten. Trotz inhaltlicher Überschneidungen sollte der Versicherer aus Transparenzgründen darauf achten, die Informationen zur Prämiengestaltung von den datenschutzrechtlichen Informationen zu trennen. Sofern die Datenverarbeitung auf Basis einer Einwilligung der Versicherungsnehmer*innen nach Art 6 Abs 1 lit a DSGVO geschieht, scheidet eine Vermischung von zivil- und datenschutzrechtlichen Bestimmungen ohnehin schon aufgrund der Vorgaben des Art 7 DSGVO aus. Gemäß dieser Bestimmung müssen die Verarbeitungszwecke nämlich direkt in der Einwilligungserklärung genannt werden, welche wiederum von anderen Sachverhalten (zB Prämienhöhe) zu trennen ist[84] (siehe Punkt 5.1).

[81] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 5 DSGVO, RZ 25, 27 (Stand 1.12.2020, rdb.at).
[82] *Gola/Heckmann/Pötters*, 3. Aufl 2022, DS-GVO Art 5 RN 15.
[83] *Brandl/Pfaffeneder*, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, Aufsatzteil, Jahrbuch Datenschutzrecht 2014, 195.
[84] *Kastelitz* in *Knyrim,* DatKomm Art 7 DSGVO, RZ 21, 22, 24 (Stand 7.5.2020, rdb.at).

4.2.1 Kompatible Weiterverarbeitung

Während personenbezogene Daten ausschließlich für die festgelegten Zwecke erhoben werden dürfen, gelten für die Weiterverarbeitung von einmal erhobenen Daten flexiblere Regeln[85]. Eine Weiterverarbeitung zu Zwecken, die mit den ursprünglichen Zwecken vereinbar bzw kompatibel sind, ist erlaubt. Nach Art 5 Abs 1 lit a DSGVO ist eine Weiterverarbeitung von personenbezogenen Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke mit den ursprünglichen Zwecken vereinbar. Demnach dürfte der Versicherer die erhobenen Daten zB für die Erstellung von Unfallstatistiken verwenden.

Will der Versicherer die erhobenen Fahrzeug- und Telematikdaten zu anderen, als den in Art 5 Abs 1 lit a DSGVO ausdrücklich genannten Zwecken weiter verarbeiten, so hat er einen sogenannten „Kompatibilitätstest" durchzuführen. Mit diesem wird festgestellt, ob die Weiterverarbeitung kompatibel im Sinne des Art 5 Abs 1 lit b DSGVO ist[86] [87]. Art 6 Abs 4 DSGVO definiert folgende fünf Kriterien anhand derer die Kompatibilität zu prüfen ist:

a) Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden und den Zwecken der beabsichtigten Weiterverarbeitung;
b) Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen;
c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 DSGVO verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DSGVO verarbeitet werden;
d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen;
e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann[88].

[85] *Kastelitz,* Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 102.
[86] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 6 DSGVO, RZ 100 (Stand 1.12.2020, rdb.at).
[87] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 5 DSGVO, RZ 29 (Stand 1.12.2020, rdb.at).
[88] *Arning; Rohwedder* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle^2 Kap. 5, RZ 154 (Stand 1.4.2021, rdb.at).

Diese Kriterien geben den Rahmen für die Prüfung der Kompatibilität im konkreten Einzelfall vor. Jedes der fünf Kriterien ist zu berücksichtigen, wobei die Beurteilung aber im Rahmen eines beweglichen Systems erfolgt. Der Versicherer sollte die Durchführung der einzelnen Schritte des Kompatibilitätstestes sowie dessen Ergebnis dokumentieren[89] [90].

Zu lit a): Grundsätzlich gilt, dass je enger die Zwecke miteinander verbunden sind, desto eher wird eine kompatible Zweckänderung gerechtfertigt sein. Der Spielraum für den Versicherer ist daher umso größer, je weiter der ursprüngliche Verarbeitungszweck formuliert wurde[91] (soweit zulässig; siehe Punkt 4.2). In der Literatur wird die Meinung vertreten, dass erhobene Kundendaten in der Regel für Kundenbetreuung und für Marketing zu unternehmenseigenen Zwecken weiterverarbeitet werden dürfen[92]. Ein Versicherer dürfte seinen Versicherungsnehmer*innen demnach Werbematerial zur Bewerbung eigener Produkte zuschicken. Aus meiner Sicht dürfte der Versicherer außerdem eine Auswertung des Fahrverhalten durchführen und den besonders rasant fahrenden PAYD-Versicherungsnehmer*innen gezielt Werbung für ein Fahrsicherheitstraining oder Informationsmaterial über die Risiken von aggressivem Fahrverhalten zuschicken. Bei diesen Beispielen liegen der ursprüngliche Zweck und der Zweck der nachträglichen Weiterverarbeitung sowohl in sachlich-inhaltlicher Hinsicht (Reduzierung des Risikos und damit Reduzierung der risikobasierten Prämie) als auch in zeitlicher Hinsicht (während aufrechtem Versicherungsverhältnis) eng genug beieinander um von einer kompatible Weiterverarbeitung ausgehen zu können.

Beispiele für eine nicht kompatible Weiterverarbeitung von Telematikdaten wären eine Weiterverarbeitung für andere Versicherungszweige (zB zur Prüfung, ob ein Antrag auf Abschluss einer Unfallversicherung angenommen werden kann), für Prüfungen der Leistungspflicht des Versicherers im Schadensfall oder für personelle Angelegenheiten (zB Bewertung von Bewerber*innen oder Mitarbeiter*innen) In diesen Fällen liegen die Zwecke mE inhaltlich zu weit auseinander um noch miteinander vereinbar zu sein.

[89] *Fritz*, Jahrbuch Datenschutzrecht 2020, 156.
[90] *Gola/Heckmann/Schulz*, 3. Aufl 2022, DS-GVO Art 6 RN 136.
[91] *Fritz*, Jahrbuch Datenschutzrecht 2020, 157, 158.
[92] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 6 DSGVO, RZ 104 (Stand 1.12.2020, rdb.at).

Zu lit b): Beim Kompatibilitätstest ist das Verhältnis zwischen der betroffenen Person und dem Verantwortlichen zu berücksichtigen. Gemeint ist, ob ein Abhängigkeitsverhältnis[93] zwischen den Parteien oder eine Zwangslage besteht. Außerdem kommt es auch darauf an, ob die betroffen Person vernünftigerweise mit der konkreten Weiterverarbeitung der Daten rechnen musste[94] [95]. Bei PAYD-Versicherungsverträgen besteht in der Regel kein Abhängigkeitsverhältnis zwischen den Vertragsparteien. Es ist aber dennoch denkbar, dass sich Versicherungsnehmer*innen nach dem Eintritt eines Schadens in einer Art faktischen Zwangslage befinden. Sie sind auf die finanzielle Entschädigung angewiesen, haben zum Zeitpunkt des Schadenseintritts keine Möglichkeit mehr den Versicherer oder das Tarifmodell zu wechseln und sind im Falle einer gerichtlichen Auseinandersetzung meist in einer finanziell und ressourcenmäßig schwächeren Position als der Versicherer. Aus diesem Grund wäre eine Weiterverarbeitung von Telematikdaten zur Leistungsprüfung mE nicht kompatibel mit dem Zweck der Prämienberechnung. Auch die Weiterverarbeitung von Telematikdaten für Zwecke des Personalmanagements würde daran scheitern, dass zwischen Arbeitnehmer*innen und Arbeitgeber*innen gewisses Abhängigkeitsverhältnis besteht. Außerdem muss niemand damit rechnen, dass Daten aus einem Kfz-Versicherungsvertrag zur Bewertung der Geeignetheit als Arbeitskraft verwendet werden.

Zu lit c): Beim Kompatibilitätstest ist zu berücksichtigen, ob besonders schutzwürdige Daten gemäß Art 9 oder Art 10 DSGVO verarbeitet werden. Deren Weiterverarbeitung ist zwar nicht generell untersagt, aber je sensibler ein Datum ist, umso eher scheidet eine kompatible Weiterverarbeitung aus[96] [97].

Zu lit d): Der Kompatibilitätstest hat außerdem die Auswirkungen einer beabsichtigten Weiterverarbeitung auf die betroffene Person zu umfassen. Dabei sind alle denkbaren negativen und positiven Folgen zu berücksichtigen. Sind negative Folgen zu befürchten, so ist auch deren Eintrittswahrscheinlichkeit und Schwere zu bewerten[98]. Erhalten die Versicherungsnehmer*innen beispielsweise Werbematerial für ein

[93] *Roßnagel* in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 6 Abs 4 RN 46.
[94] *Fritz*, Jahrbuch Datenschutzrecht 2020, 161-162.
[95] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 6 DSGVO, RZ 100 (Stand 1.12.2020, rdb.at).
[96] *Fritz*, Jahrbuch Datenschutzrecht 2020, 164.
[97] *Gola/Heckmann/Schulz*, 3. Aufl 2022, DS-GVO Art 6 RN 139.
[98] *Fritz*, Jahrbuch Datenschutzrecht 2020, 167.

Fahrsicherheitstraining, so sind keine negative Auswirkungen auf die betroffenen Personen zu erwarten. Verarbeitet der Versicherer die Telematikdaten hingegen für die Prüfung seiner Leistungspflicht, kann das große finanzielle Auswirkungen auf die Versicherungsnehmer*innen haben. Eine Verwendung von Telematikdaten zur Bewertung von Mitarbeiter*innen oder Bewerber*innen, kann ebenfalls negative Folgen für die betroffenen Personen haben. Theoretisch wäre es denkbar, dass ein risikoreiches Fahrverhalten den Versicherer dazu veranlasst, an sich geeignete Bewerber*innen nicht einzustellen oder Mitarbeiter*innen zu kündigen. In beiden Fällen wäre die Auswirkung auf die betroffene Person als schwer einzustufen und eine Kompatibilität der Weiterverarbeitung mit dem ursprünglichen Verarbeitungszweck daher zu verneinen.

Zu lit e): Das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann, ist ebenfalls in den Kompatibilitätstest mit einzubeziehen. Das bedeutet aber nicht, dass in jedem Fall der Weiterverarbeitung eine Verschlüsselung oder eine Pseudonymisierung stattzufinden hat. Am Beispiel der Zusendung von Werbematerial für ein Fahrsicherheitstraining sieht man, dass eine Pseudonymisierung die Weiterverarbeitung verunmöglichen würde. In aller Regel kann man wohl davon ausgehen, dass die Voraussetzungen des lit e schon dann erfüllt sein werden, wenn der Versicherer ausreichende technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit getroffen hat[99].

Fazit: Abschließend kann festgehalten werden, dass der Zweckbindungsgrundsatz für die erstmalige Erhebung von Daten strikt einzuhalten ist, dem Versicherer aber hinsichtlich der Weiterverarbeitung durchaus verschiedene Möglichkeiten offen stehen. Die Praxisrelevanz des Art 6 Abs 4 DSGVO dürfte hoch sein und es ist zu erwarten, dass Versicherer die Grenzen der kompatiblen Weiterverarbeitung über die nächsten Jahre hinweg „austesten“ werden.

4.3 Grundsatz der Datenminimierung (Art 5 Abs 1 lit c DSGVO)

Der Grundsatz der Datenminimierung zielt darauf ab, die Verarbeitung von personenbezogenen Daten auf ein Mindestmaß zu reduzieren und jede unnötige Datenverarbeitung zu vermeiden. Eine Datenverarbeitung darf nur in dem Ausmaß

[99] *Fritz*, Jahrbuch Datenschutzrecht 2020, 167.

stattfinden, als sie dem Zweck angemessen ist und soweit sie zur Erreichung dieses Zweckes notwendig und geeignet ist. Die Verarbeitung personenbezogener Daten ist auf das absolut notwendige Maß zu beschränken[100]. Aus ErwGr 39 ergibt sich, dass personenbezogene Daten überhaupt nur dann verarbeitet werden dürfen, wenn der Zweck der Verarbeitung zumutbarer Weise nicht auch durch andere Mittel erreicht werden kann („*Zweck-Mittel-Relation*")[101] [102]. Der Verantwortliche darf Daten außerdem nicht „auf Reserve" speichern, um sie zu einem späteren Zeitpunkt für einen bislang noch unbekannten Zweck zu verwenden[103].

Auch der PAYD-Versicherer darf nur jene Daten verarbeiten, die er zur Erreichung der festgelegten Zwecke benötigt. Werden Telematikdaten zB nur zum Zweck der Prämienberechnung verarbeitet und basiert die Prämienhöhe nur auf der Anzahl der gefahrenen Kilometer und der Fahrgeschwindigkeit, ist die Verarbeitung von Daten zum Bremsverhalten unzulässig.

Der Versicherer hat außerdem zu prüfen, ob der Zweck der Prämienberechnung auch durch gelindere Mittel als durch die Verarbeitung von personenbezogenen Daten erreicht werden kann[104]. Bei PAYD-Tarifen handelt es sich um Tarife, die auf dem individuellen Fahrverhalten einer Person basieren, so dass naturgemäß nicht auf die Verarbeitung von personenbezogenen Daten verzichtet werden kann. Hat der Versicherer aber mehrere Möglichkeiten um das gewünschte Ziel zu erreichen, so hat er jene Möglichkeit zu wählen, die für die betroffene Person am schonendsten ist. Die Anzahl der gefahrenen Kilometer muss beispielsweise nicht durch die Auswertung von GPS-Tracking-Daten ermittelt werden, wenn auch ein einfacher Kilometerzähler ausreicht.

4.4 Grundsatz der Richtigkeit (Art 5 Abs 1 lit d DSGVO)

Der Grundsatz der Richtigkeit besagt, dass personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein müssen[105] und dass der Verantwortliche

[100] *Haidinger* in *Knyrim*, Datenschutzrecht[4] Kap 5, RZ 5.17 (Stand 1.4.2020, rdb.at).
[101] *Roßnagel* in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 5 RN 116.
[102] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 5 DSGVO, RZ 32-35 (Stand 1.12.2020, rdb.at).
[103] *Brandl/Pfaffeneder*, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, Aufsatzteil, Jahrbuch Datenschutzrecht 2014, 196.
[104] *Hötzendorfer/Tschohl/Kastelitz* in *Knyrim,* DatKomm Art 5 DSGVO, RZ 36 (Stand 7.5.2020, rdb.at).
[105] *Ehmann/Selmayr/Heberlein*, 2. Aufl 2018, DS-GVO Art 5 RN 24.

alle angemessenen Maßnahmen zu treffen hat, damit unrichtige Daten unverzüglich gelöscht oder berichtigt werden. Richtig sind Daten dann, wenn sie der Realität entsprechen. Demnach können nur Angaben über Tatsachen richtig oder nicht richtig im Sinne des Art 5 Abs 1 lit d DSGVO sein, Werturteile hingegen nicht[106].

Der Verantwortliche muss sowohl bei der erstmaligen Erhebung der Daten sowie bei deren Weiterverarbeitung sicherstellen, dass die Daten richtig sind. Er hat organisatorische und technische Maßnahmen zu treffen, die dem Risiko, dem Verarbeitungszweck und der Art der Daten angemessen sind. Da die Unrichtigkeit von Daten im Regelfall von der betroffenen Person erkannt wird, ist der Grundsatz der Richtigkeit eng an die Betroffenenrechte der Art 15-21 DSGVO geknüpft. Der Verantwortliche ist aber auch dazu verpflichtet, unrichtige Daten pro-aktiv zu berichtigen oder zu löschen[107] [108].

4.5 Grundsatz der Speicherbegrenzung (Art 5 Abs 1 lit e DSGVO)

Nach dem Grundsatz der Speicherbegrenzung dürfen personenbezogene Daten nur so lange gespeichert werden, wie es zur Erreichung der Verarbeitungszwecke notwendig ist[109] [110]. Ist der Verarbeitungszweck erreicht, sind die Daten zu löschen bzw zu anonymisieren. Der Art 5 Abs 1 lit e DSGVO nennt keine konkreten Kriterien und Fristen, die der Verantwortliche einzuhalten hat. Wie lange personenbezogene Daten gespeichert werden dürfen, hängt vom jeweiligen Zweck der Verarbeitung ab und kann daher von Fall zu Fall variieren[111].

Bei PAYD-Tarifen liegt der Zweck der Verarbeitung primär in der Berechnung der Versicherungsprämie. Demnach wäre mit Bezahlung der Prämie der Verarbeitungszweck erreicht und die dahinterliegenden Daten wären zu löschen. Bei der Festlegung von Lösch- bzw Speicherfristen, sind jedoch die anwendbaren Verjährungsfristen zu beachten (siehe Punkt 6.6.1).

---

[106] *Hötzendorfer/Tschohl/Kastelitz* in *Knyrim,* DatKomm Art 5 DSGVO, RZ 44 (Stand 7.5.2020, rdb.at).
[107] *Hötzendorfer/Tschohl/Kastelitz* in *Knyrim,* DatKomm Art 5 DSGVO, RZ 46 (Stand 7.5.2020, rdb.at).
[108] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 5 DSGVO, RZ 43-44 (Stand 1.12.2020, rdb.at).
[109] *Moos* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle^2 Kap 4, RZ 21 (Stand 1.4.2021, rdb.at).
[110] *Roßnagel* in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 5 RN 154.
[111] JusGuide 2021/38/19745 (OGH).

Nach dem Grundsatz der Speicherbegrenzung hat der Versicherer die Versicherungsnehmer*innen bereits bei Erhebung der Daten über deren Speicherung und soweit möglich über die Speicherdauer zu informieren. Weiters muss der Versicherer die Speicherfristen in das Verzeichnis der Verarbeitungstätigkeiten aufnehmen[112]. Außerdem hat er technische und organisatorische Maßnahmen zu implementieren, die für die zeitgerechte Löschung (bzw Anonymisierung) von personenbezogenen Daten sorgen. In der Praxis erarbeitet der Versicherer am besten ein sogenanntes „Löschkonzept“[113].

4.6 Grundsatz der Integrität und Vertraulichkeit (Art 5 Abs 1 lit f DSGVO)

Gemäß Art 5 Abs 1 lit f DSGVO sind personenbezogene Daten so zu verarbeiten, dass sie vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Datenverlust, Zerstörung oder Schädigung geschützt sind. Der Verantwortliche hat für eine angemessene Sicherheit durch geeignete technische und organisatorische Maßnahmen Sorge zu tragen. Beim Grundsatz der Integrität und Vertraulichkeit geht es letztendlich um die Herstellung eines angemessenen Datensicherheitsniveaus[114].

4.7 Rechenschaftspflicht (Art 5 Abs 2 DSGVO)

„Der Verantwortliche ist für die Einhaltung der Grundsätze der DSGVO (Art 5 Abs 1) verantwortlich und unterliegt der Rechenschaftspflicht nach Art 5 Abs 2, wonach er deren Einhaltung nachweisen können muss.“[115]

Der Art 5 der DSGVO setzt sich aus zwei Bestandteilen zusammen. In Abs 1 werden die inhaltlichen Pflichten des Verantwortlichen – die datenschutzrechtlichen Grundsätze – festgelegt. Daran anschließend normiert der Abs 2 leg cit die Verpflichtung, die Einhaltung dieser datenschutzrechtlichen Grundsätze nachweisen zu können. Gemeinsam bilden der Abs 1 und Abs 2 des Art 5 DSGVO die sogenannte Rechenschaftspflicht des Verantwortlichen[116]. In der Praxis bedeutet die Rechenschaftspflicht vor allem

[112] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 5 DSGVO, RZ 47 (Stand 1.12.2020, rdb.at).
[113] *Moos* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap 4, RZ 21 (Stand 1.4.2021, rdb.at).
[114] *Kastelitz,* Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 104.
[115] DSB 23.07.2019, DSB-D123.822/0005-DSB/2019; DSB 14.01.2019, DSB-D123.224/0004-DSB/2018.
[116] *Hötzendorfer/Tschohl/Kastelitz* in *Knyrim,* DatKomm Art 5 DSGVO, RZ 57 (Stand 7.5.2020, rdb.at).

umfangreiche Dokumentations- und Nachweispflichten für die Verantwortlichen[117]. Gerade größere Unternehmen, wie Versicherungen, sollten ein umfassendes Datenschutzmanagement aufbauen und auf diese Weise sicherstellen, dass sämtliche datenschutzrechtliche Prozesse, Maßnahmen und sonstige datenschutzrelevante Tätigkeiten ausreichend dokumentiert werden[118] [119].

Auf den ersten Blick wirkt es so, als ob die Rechenschaftspflicht des Art 5 Abs 2 DSGVO zu einer allgemeinen Beweislastumkehr führen würde. Entsprechend dem risikobasierten Ansatz der DSGVO gilt aber auch für Rechenschaftspflicht der Verhältnismäßigkeitsgrundsatz[120]. So hat das Bundesverwaltungsgericht (BVwG) bereits festgestellt, dass der Art 5 Abs 2 DSGVO keine generelle Beweislastumkehr bewirkt und eine Verhältnismäßigkeitsabwägung zu erfolgen hat. In dem Fall, den das BVwG zu beurteilen hatte, war mangels konkretem Risiko kein allzu strenger Maßstab an die Rechenschaftspflicht anzusetzen. Weiters hat das BVwG festgestellt, dass Nachweise nur gegenüber der zuständigen Aufsichtsbehörde zu erbringen sind[121] und die Rechenschaftspflicht von der Beweislastverteilung in einem Zivilverfahren zu trennen ist[122]. Die deutsche Rechtsprechung setzt sich etwas differenzierter mit den Beweislastregeln auseinander, kommt aber letztendlich zum selben Ergebnis. Das OLG Stuttgart hat entschieden, dass der Verantwortliche im Zivilverfahren zwar den Nachweis der Rechtmäßigkeit der Datenverarbeitung erbringen muss, die Rechenschaftspflicht aber zu keiner Beweislastumkehr hinsichlich Schaden und Kausalität von Datenschutzverstößen führt[123] [124]. Siehe dazu auch Punkt 6.5 (Recht auf Berichtigung).

Für den Versicherer bedeutet die Rechenschaftspflicht zunächst einmal einen Mehraufwand hinsichtlich Dokumentation[125] und Datenschutzmanagement. Grundsätzlich gilt, dass sich der Umfang der Rechenschaftspflicht am jeweiligen Risiko zu orientieren hat und verhältnismäßig sein soll[126]. Bei einem PAYD-Tarif steigt das

[117] *Wybitul*, EU-Datenschutz-Grundverordnung im Unternehmen Kap III, RZ 77 (Stand 11.8.2016, rdb.at).
[118] *Ritzer* in *Ruhmannseder/Lehner/Beukelmann*, Compliance aktuell 15010, RZ 20 (Stand 1.5.2022, rdb.at).
[119] *Ehmann/Selmayr/Heberlein*, 2. Aufl 2018, DS-GVO Art 5 RN 31.
[120] *Hötzendorfer/Tschohl/Kastelitz* in *Knyrim,* DatKomm Art 5 DSGVO, RZ 59 (Stand 7.5.2020, rdb.at).
[121] BVwG 12.05.2022, W252 2237237-1.
[122] *Hötzendorfer/Tschohl/Kastelitz* in *Knyrim,* DatKomm Art 5 DSGVO, RZ 58 (Stand 7.5.2020, rdb.at).
[123] *Gola/Heckmann/Pötters*, 3. Aufl 2022, DS-GVO Art 5 RN 35.
[124] OLG Stuttgart Urteil vom 31.3.2021 – 9 U 34/21, ZD 2021, 375.
[125] *Gola/Heckmann/Pötters*, 3. Aufl 2022, DS-GVO Art 5 RN 35.
[126] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 5 DSGVO, RZ 54, 57 (Stand 1.12.2020, rdb.at).

datenschutzrechtliche Risiko an, wenn eine große Menge an Daten erhoben wird und sich die Datenlage zu einer betroffenen Person verdichtet oder wenn besonders schutzwürdige Daten verarbeitet werden. In diesen Fällen darf der Versicherer nicht davon ausgehen, dass kein allzu strenger Maßstab an die Rechenschaftspflicht anzulegen ist. Anders als in der oben beschriebenen Entscheidung des BVwG[127], wird bei PAYD-Tarifen mE nämlich regelmäßig ein konkretes datenschutzrechtliches Risiko bestehen, zumindest dann wenn Bewegungs- und Standortdaten erhoben werden.

5) Rechtmäßigkeit der Datenverarbeitung (Art 6 DSGVO)

Damit die Verarbeitung von personenbezogenen Daten zulässig ist, muss sie aber nicht nur den Grundsätzen des Art 5 DSGVO entsprechen, sondern auch die Bedingungen des Art 6 DSGVO erfüllen. Art 6 DSGVO funktioniert nach dem Verbotsprinzip. Das bedeutet, dass die Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist[128]. Nur dann, wenn einer der Erlaubnistatbestände des Art 6 DSGVO erfüllt ist, ist eine Datenverarbeitung zulässig. Art 6 DSGVO enthält eine taxative Aufzählung von Erlaubnistatbeständen (hier verkürzt wiedergegeben)[129]:

- lit a: Einwilligung
- lit b: Vorliegen eines Vertrages oder vorvertragliche Maßnahmen
- lit c: Rechtliche Verpflichtung des Verantwortlichen
- lit d: Schutz lebenswichtiger Interessen
- lit e: Öffentliches Interesse oder Ausübung öffentlicher Gewalt
- lit f: Berechtigte Interessen des Verantwortlichen oder eines Dritten

Für die Verarbeitung von Fahr- und Telematikdaten im Rahmen eines PAYD-Tarifes sind primär lit a, b und f relevant. Der Versicherer darf eine Datenverarbeitung auch auf mehre Erlaubnistatbestände stützen. Das ist in der Praxis insbesondere dann der Fall, wenn der Versicherer eine Einwilligung nur „sicherheitshalber“ einholt, die Datenverarbeitung aber schon aufgrund eines anderen Erlaubnistatbestandes zulässig ist[130].

[127] BVwG 12.05.2022, W252 2237237-1.
[128] *Schröder*, Datenschutzrecht für die Praxis[4], 17-18.
[129] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim,* DatKomm Art 6 DSGVO, RZ 2 (Stand 7.5.2020, rdb.at).
[130] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim,* DatKomm Art 6 DSGVO, RZ 15 (Stand 7.5.2020, rdb.at).

Damit nicht zu verwechseln sind Fälle, in denen dieselben Daten zu unterschiedlichen Zwecken verarbeitet werden und die Verarbeitung jeweils auf einen anderen Erlaubnistatbestand gestützt wird. In diesen Fällen wird nicht ein Verarbeitungsvorgang auf mehrere Erlaubnistatbestände gestützt, sondern es liegen unterschiedliche Verarbeitungsvorgänge vor[131]. Das trifft zum Beispiel dann zu, wenn der Versicherer die erhobenen Daten zur Fahrgeschwindigkeit einerseits für die Berechnung der Prämie verwendet und andererseits für die Zusendung von zielgerichtetem Werbematerial an besonders rasante Fahrer. Im ersten Fall kann sich der Versicherer darauf stützen, dass die Datenverarbeitung zur Vertragserfüllung notwendig ist. Im zweiten Fall kann er sich auf die Einwilligung der betroffenen Person stützen.

5.1 Einwilligung (Art 6 Abs 1 lit a iVm Art 7 DSGVO)

Die Einwilligung der betroffenen Person in die Verarbeitung ihrer personenbezogenen Daten ist ein besonders wichtiges Instrument des Datenschutzrechts und dient einerseits als Erlaubnistatbestand und ist andererseits Ausdruck des informationellen Selbstbestimmungsrechts[132]. Art 6 Abs 1 lit a DSGVO legt fest, dass sich die Einwilligung der betroffenen Person auf einen oder mehrere konkret bezeichnete Zwecke beziehen muss[133]. Ändern sich die Zwecke der Verarbeitung, so hat der Verantwortliche eine neue Einwilligung einzuholen, es sei denn die Datenverarbeitung kann auf einen anderen Erlaubnistatbestand des Art 6 DSGVO gestützt werden[134].

In Art 7 DSGVO werden die Bedingungen bzw Anforderungen für eine wirksame Einwilligung näher definiert. Diese können schlagwortartig wie folgt zusammengefasst werden:

- Nachweispflicht
- Transparenz
- Widerruf
- Freiwilligkeit & Koppelungsverbot

[131] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 6 DSGVO, RZ 7-8, 11 (Stand 1.12.2020, rdb.at).
[132] *Albrecht* in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Einführung zu Artikel 6, RN 4.
[133] *Gola/Heckmann/Schulz*, 3. Aufl 2022, DS-GVO Art 6 RN 21, 24.
[134] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 6 DSGVO, RZ 18, 21 (Stand 1.12.2020, rdb.at).

Will sich der Versicherer auf eine Einwilligung der betroffenen Person stützen, muss er nachweisen können, eine wirksame Einwilligung eingeholt zu haben[135]. Obwohl die DSGVO keine Formvorschriften vorsieht, ist es empfehlenswert eine Einwilligung stets in schriftlicher oder geschriebener Form einzuholen und zumindest für die Dauer der Verarbeitungstätigkeit aufzubewahren. Angesichts der Nachweispflicht des Art 7 Abs 1 DSGVO oder der Rechenschaftspflicht des Art 5 DSGVO wäre es fast schon fahrlässig, würde sich der Versicherer auf eine mündlich eingeholte Einwilligung verlassen[136] [137]. Meiner Einschätzung nach ist das Einholen schriftlicher Einverständniserkärungen aber ohnehin für jeden Versicherer eine Selbstverständlichkeit.

In Art 7 Abs 2 DSGVO wird festgelegt, dass das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache zu erfolgen hat. Die Einwilligungserklärung muss außerdem von anderen Sachverhalten klar zu unterscheiden sein. Durch eine deutliche Trennung der datenschutzrechtlichen Einwilligung von anderen Sachverhalten soll sichergestellt werden, dass das Ersuchen um Einwilligung nicht versteckt und den Versicherungsnehmer*innen „untergejubelt" wird. Eine Unterscheidbarkeit kann durch eine grafische Hervorhebung bzw durch eine entsprechende Platzierung der Einwilligungserklärung erreicht werden[138] [139]. Es ist nicht abschließend geklärt, ob Einwilligungserklärungen in die AGB eingebettet werden können[140]. Wichtig ist jedenfalls, dass die Versicherungsnehmer*innen ihre Einwilligung aktiv erteilen, dh selbst ein Kreuzchen setzen oder die Einwilligung mit gesonderter Unterschrift erklären. Nach ErwGr 32 stellen vor-angekreuzte Kästchen keine wirksame Einwilligungserklärung dar[141] [142]. Die Einwilligung ist für einen oder mehrere bestimmt bezeichnete und konkret beschriebene Verarbeitungszwecke zu erteilen. General- bzw Pauschaleinwilligungen sind nicht zulässig[143].

---

[135] *Klement* in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 7 RN 10.
[136] *Arning;Rohwedder* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle^2 Kap. 5, RZ 291, 292 (Stand 1.4.2021, rdb.at).
[137] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 7 DSGVO, RZ 4, 5, 7 (Stand 1.12.2020, rdb.at).
[138] *Stemmer* in BeckOK DatenschutzR, 43. Ed 1.5.2022, DS-GVO Art 7 RN 64, 69.
[139] *Kastelitz* in *Knyrim,* DatKomm Art 7 DSGVO, RZ 21, 22 (Stand 7.5.2020, rdb.at).
[140] *Kastelitz* in *Knyrim,* DatKomm Art 7 DSGVO, RZ 24 (Stand 7.5.2020, rdb.at).
[141] ErwGr 32 DSGVO.
[142] Siehe auch: EuGH 11.11.2020, C-61/19 Orange România SA. Vgl: https://verbraucherrecht.at/rechtmaessige-einwilligung-datenverarbeitung/5289 (abgerufen am 07.04.2023).
[143] *Arning;Rohwedder* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle^2 Kap 5, RZ 270 (Stand 1.4.2021, rdb.at).

Auch der PAYD-Versicherer muss auf eine strikte Trennung der Einwilligungserklärung von anderen Sachverhalten achten. Es darf auch dann nicht zu einer Vermischung mit zivilrechtlichen Bestimmungen kommen, wenn es inhaltliche Überschneidungen gibt (siehe Punkt 4.2).

Die betroffene Person hat das Recht, die Einwilligung jederzeit und ohne Angabe von Gründen zu widerrufen[144]. Ein Widerruf wirkt ex-nunc und die bis zum Widerruf vorgenommenen Datenverarbeitungen bleiben rechtmäßig[145] [146]. Die betroffene Person ist schon vor Abgabe der Einwilligungserklärung über ihre Widerrufsmöglichkeit aufzuklären[147]. Die Weigerung eine Einwilligung zu erklären oder der Widerruf einer Einwilligung dürfen zu keinen Nachteilen für die betroffene Person führen[148] – nur dann wurde die Einwilligung wirklich freiwillig erteilt. Wird die Erfüllung oder der Abschluss[149] eines Vertrages von der Einwilligung in die Verarbeitung personenbezogener Daten abhängig gemacht, obwohl das für die Vertragserfüllung nicht erforderlich ist, ist keine Freiwilligkeit gegeben (Koppelungsverbot)[150] [151].

Der Versicherer sollte sich gut überlegen, ob und welche Datenverarbeitungsvorgänge er auf eine Einwilligung stützen möchte. Bezieht sich bei PAYD-Tarifen die Einwilligungserklärung auf Daten, die zur Prämienberechnung unbedingt erforderlich sind, kann die Prämie nach einem Widerruf nicht mehr berechnet werden. Sofern rechtlich möglich, sollten Datenverarbeitungen die für die Prämienberechnung unbedingt notwendig sind, daher auf den Erlaubnistatbestand des Art 6 Abs 1 lit b DSGVO (Vertragserfüllung) gestützt werden.

Wie weiter oben im Punkt 5 beschrieben, kann der Versicherer eine Datenverarbeitung von Anfang an auf mehrere Rechtsgrundlagen stützen. In diesen Fällen sind die Versicherungsnehmer*innen darüber zu informieren, welcher Datenverarbeitungsvorgang auf welche Rechtsgrundlagen gestützt wird (Art 13 Abs 1 lit c DSGVO). *"Bei Vorliegen*

[144] *Pollirer*, Checkliste für die Einwilligungserklärungen der Art 7 und 8 DSGVO, Dako 2017/56 (91).
[145] *Ehmann/Selmayr/Heckmann/Paschke*, 2. Aufl 2018, DS-GVO Art 7 RN 92.
[146] *Kastelitz* in *Knyrim,* DatKomm Art 7 DSGVO, RZ 32 (Stand 7.5.2020, rdb.at).
[147] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 7 DSGVO, RZ 18, 19 (Stand 1.12.2020, rdb.at).
[148] Siehe dazu ErwGr 42 DSGVO.
[149] *Klement* in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 7 RN 56, 57.
[150] OGH 6 Ob 140/18h VbR 2018/127 (233).
[151] *Schröder,* Datenschutzrecht für die Praxis[4], 166.

mehrerer Zwecke und Rechtsgrundlagen für den gleichen Datensatz ist dieser mit einem entsprechenden Vermerk zu versehen"[152]. Wichtig ist, dass die Versicherungsnehmer*innen erkennen können, in welchen Fällen ein Widerruf möglich bzw nicht möglich ist[153].

Hat der Versicherer eine Datenverarbeitung nicht von Anfang an auf mehrere Rechtsgrundlagen gestützt, sondern nur auf eine Einwilligungserklärung, so kann er im Falle eines Widerrufs nicht nachträglich auf eine andere Rechtsgrundlage wechseln und so die Vertragserfüllung "retten". Vom EDSA wird die Ansicht vertreten, dass es missbräuchlich ist *"gegenüber der betroffenen Person eine Datenverarbeitung auf Einwilligung zu stützen und im Falle des Widerrufs der Einwilligung der Datenverarbeitung eine andere Rechtsgrundlage zugrunde zu legen"*[154] [155]. Diese Ansicht ist mE inhaltlich richtig, entspricht den Grundsätzen von Treu und Glauben sowie den allgemeinen versicherungsrechtlichen Grundsätzen des § 128 Abs 1 VAG[156].

5.2 Vertrag (Art 6 Abs 1 lit b DSGVO)

„Nach Art 6 Abs 1 lit b DSGVO ist die Verarbeitung personenbezogener Daten erlaubt, wenn dies für die Vertragserfüllung im weiten Sinn (somit auch von Nebenpflichten) erforderlich ist. Maßgeblich ist der aus dem Vertragsinhalt hervorgehende Vertragszweck und das, was zur Erfüllung der Vertragspflichten oder der Wahrnehmung von Rechten bzw für die Durchführung vorvertraglicher Maßnahmen geboten ist"[157].

Der Begriff der Erforderlichkeit ist eng auszulegen[158]. Die konkrete Datenverarbeitung muss für die Erfüllung eines bestimmten Vertrages erforderlich ist[159]. Der Vertragsinhalt

[152] DSB 05.02.2019, DSB-D123.495/0007-DSB/2018.
[153] *Braun/Hasenauer*, Die Rechtmäßigkeit der Verarbeitung gemäß Art 6 DSGVO (FN 1), Jahrbuch Datenschutzrecht 2018, 9 (18).
[154] *Braun/Hasenauer*, Die Rechtmäßigkeit der Verarbeitung gemäß Art 6 DSGVO (FN 1), Jahrbuch Datenschutzrecht 2018, 9 (18).
[155] *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP259 rev.01, 17/DE, 27 f, <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> (17.03.2023).
[156] § 128 (1) VAG: *Versicherungsunternehmen haben bei ihrer Versicherungsvertriebstätigkeit ihren Versicherungsnehmern und Anspruchsberechtigten gegenüber stets ehrlich, redlich und professionell in deren bestmöglichem Interesse zu handeln*.
[157] OGH 23.06.2021, 6 Ob 56/21k, RS0133707.
[158] *Kühling/Buchner/Buchner/Petri*, 3. Aufl 2020, DS-GVO, Art 6 RN 40a.
[159] *Braun/Hasenauer*, Die Rechtmäßigkeit der Verarbeitung gemäß Art 6 DSGVO (FN 1), Jahrbuch Datenschutzrecht 2018, 9 (23).

eines Versicherungsvertrages besteht im Wesentlichen in der Verpflichtung des Versicherers, den Versicherungsnehmer*innen bei Eintritt eines Versicherungsfalles den Schaden zu ersetzen. Im Gegenzug dafür leisten die Versicherungsnehmer*innen die vereinbarte Prämie (§ 1 VersVG). Bei PAYD-Tarifen ist die endgültige Höhe der Prämie vom individuellen Fahrverhalten der Versicherungsnehmer*innen abhängig. *Brandl/Pfaffender* gehen dennoch davon aus, dass die Verarbeitung von Fahr- und Telematikdaten für die Erfüllung eines PAYD-Vertrages nicht unbedingt erforderlich ist. Ihrer Ansicht nach benötigt der Versicherer die Daten zwar notwendigerweise zur Berechnung der Prämie, nicht aber zur Erfüllung des Versicherungsvertrages an sich. Daher kommt für *Brandl/Pfaffender* ausschließlich die Einwilligungserklärung der betroffenen Person als Rechtfertigungstatbestand für die Verarbeitung von Fahr- und Telematikdaten durch den PAYD-Versicherer in Frage. Sie schlagen daher auch vor, schon bei Vertragsabschluss festzulegen, wie die Prämie im Falle eines Widerrufs berechnet wird[160].

Der Ansicht von *Brandl/Pfaffender* kann ich mich nur bedingt anschließen. Wie in Punkt 2.4 beschrieben, sind verschiedene vertragsrechtliche Konstellationen bei der Ausgestaltung von PAYD-Tarifen denkbar. Es gibt einerseits Modelle, bei denen die vereinbarte Prämienhöhe niedriger oder höher werden kann (Modelle A und B). Es sind aber durchaus auch Modelle denkbar, bei denen keine Basisprämie festgelegt wird, sondern der Versicherer die laufenden Prämien ausschließlich aufgrund des Fahrverhaltens der Versicherungsnehmer*innen berechnet (Modell C).

Betreffend die Modelle A) und B) kann ich mich der Ansicht von *Brandl/Pfaffender* anschließen. Bei diesen Modellen ist die Verarbeitung von Fahr- und Telematikdaten nur für die Berechnung von Rabatten oder Zuschlägen zur Basisprämie notwendig. Offenbar gehen *Brandl/Pfaffender* davon aus, dass der Versicherungsvertrag auch ohne die Verarbeitung von Fahr- und Telematikdaten erfüllt werden kann[161]. Das wäre zum Beispiel dann denkbar, wenn die betroffene Person nach einem Widerruf die vereinbarte Basisprämie bezahlt und der Versicherer den Versicherungsschutz weiterhin wie vereinbart erbringt.

[160] *Brandl/Pfaffeneder*, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, Jahrbuch Datenschutzrecht 2014, 197-199.
[161] *Brandl/Pfaffeneder*, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, Jahrbuch Datenschutzrecht 2014, 199-200.

Anders verhält es sich mE aber bei Versicherungsverträgen mit gänzlich variabler Prämie (Modell C). Um die Prämienhöhe für einen solchen Versicherungsvertrag ermitteln zu können, muss der Versicherer zwangsläufig die Fahr- und Telematikdaten der betroffenen Person verarbeiten. Andernfalls kann er die Prämie nicht berechnen und vorschreiben und die Versicherungsnehmer*innen können ihrer vertraglichen Hauptleistungspflicht (Bezahlung der Prämie) nicht nachkommen. Auch *Schulz* geht davon aus, dass die Verarbeitung von *essentialia negotii* in der Regel erforderlich für die Durchführung eines Vertrages ist[162].

Der EDSA vertritt die Ansicht, dass es darauf ankommt, *"ob bestimmte Handlungen im Rahmen von normalen Vertragsbeziehungen vernünftigerweise vorhersehbar und notwendig sind"*[163]. Als Beispiel führt der EDSA die Verwendung von Adressdaten für die Zusendung von Mahnungen an[164]. Wenn die Zusendung von Mahnungen – also das „Eintreiben" ausständiger Prämie – als erforderlich angesehen wird, dann muss das Berechnen und Vorschreiben einer Prämie konsequenterweise ebenfalls als erforderlich gelten.

Der EDSA hat außerdem folgende „Prüffragen" formuliert, die zur Beurteilung der Anwendbarkeit des Art 6 Abs 1 lit b DSGVO herangezogen werden können:

(a) *Welche Art von Dienstleistung wird der betroffenen Person erbracht? Welches sind ihre charakteristischen Unterscheidungsmerkmale?*
(b) *Welches ist der genaue Grundgedanke des Vertrages (d.h. seine Zielsetzung und sein grundlegender Gegenstand)?*
(c) *Was sind die wesentlichen Elemente des Vertrags?*
(d) *Welches sind die gegenseitigen Perspektiven und Erwartungen der Vertragsparteien? Wie wird der Dienst der betroffenen Person gegenüber angepriesen oder beworben?*

[162] *Gola/Heckmann/Schulz,* 3. Aufl 2022, DS-GVO Art 6 RN 39.
[163] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 6 DSGVO, RZ 29 (Stand 1.12.2020, rdb.at).
[164] Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, V2.0, RZ 38.

(e) *Würde ein normaler Nutzer des Dienstes vernünftigerweise erwarten, dass in Anbetracht der Art des Dienstes die geplante Verarbeitung erfolgt, um den Vertrag zu erfüllen, dessen Partei er ist?*[165]

Die Berechnung einer risikobasierten Prämie ist das zentrale Element eines Telematiktarifes und charakterisiert und unterscheidet ihn von herkömmlichen Versicherungstarifen. Grundgedanke eines Telematiktarifes ist es, die Prämienhöhe vom individuellen Fahrverhalten abhängig zu machen[166]. Es ist anzunehmen, dass sich Versicherungsnehmer*innen eine Prämienreduktion erwarten und davon ausgehen, die Prämienhöhe mit ihrem Fahrverhalten (positiv) beeinflussen zu können. Versicherungsnehmer*innen können nicht nur vernünftigerweise vorhersehen, dass ihre Fahr- und Telematikdaten zur Berechnung der Prämie verarbeitet werden, vielmehr erwarten sie sich das.

Fazit: Aufgrund dieser Überlegungen ist die Verarbeitung von Fahr- und Telematikdaten zur Berechnung der Prämie bei solchen Tarifmodellen, bei denen sich die Prämienhöhe ausschließlich aus dem individuellen Fahrverhalten ergibt, meiner Ansicht nach unbedingt erforderlich. In diesen Fällen darf sich der Versicherer mE auf den Erlaubnistatbestand des Art 6 Abs 1 lit b DSGVO stützen.

5.3 Berechtigtes Interesse (Art 6 Abs 1 lit f DSGVO)

Eine Datenverarbeitung kann auch aufgrund eines berechtigten Interesse eines Verantwortlichen oder eines Dritten rechtmäßig sein. Voraussetzung dafür ist, dass die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen und dass die Datenverarbeitung zur Erreichung des berechtigten Interesses erforderlich ist[167]. Bei der Beurteilung, ob ein berechtigtes Interesse nach Art 6 Abs 1 lit f DSGVO besteht, ist eine Interessenabwägung vorzunehmen[168]. Dabei sind folgende Aspekte zu berücksichtigen:

---

[165] Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, V2.0, RZ 33.

[166] *Brand*, Zulässigkeit und Ausgestaltung von Telematiktarifen, VersR 2019, 725.

[167] *Arning;Rohwedder* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle^2 Kap. 5, RZ 69 (Stand 1.4.2021, rdb.at).

[168] *Gola/Heckmann/Schulz*, 3. Aufl 2022, DS-GVO Art 6 RN 59.

(a) Ist Verarbeitung der Daten zur Verwirklichung des berechtigen Interesses wirklich erforderlich?
(b) Konnte die betroffene Person vernünftigerweise damit rechnen, dass ihre Daten für diesen konkreten Zweck verarbeitet werden?
(c) Welche Auswirkungen hat die Datenverarbeitung auf die betroffene Person bzw welche Gefahren sind damit verbunden?
(d) Wie „gewichtig" ist das Interesse des Verantwortlichen?[169]

Im ErwGr 47 werden ua folgende Beispiele für das Bestehen eines berechtigten Interesses genannt: Betrugsbekämpfung, Direktwerbung, Übermittlung im Konzern für interne Verwaltungszwecke, Verteidigung von Rechtsansprüchen oder Anzeige strafrechtlich relevanter Sachverhalte[170].

Die Verwendung von Telematikdaten zum Zweck der Erstellung eines Bewegungs-, Nutzungs- oder Persönlichkeitsprofils kann hingegen nicht auf ein berechtigtes Interesse des Verantwortlichen gestützt werden, weil dies mit hohen Risiken für die betroffene Person verbunden ist[171].

Im Alltag eines PAYD-Versicherers dürften diese zwei Anwendungsfälle von besonderer Relevanz sein:

- Prüfung der Leistungspflicht des Versicherers im Falle eines Unfalls und
- Betrugsbekämpfung

Erkennt etwa ein PAYD-Versicherer anhand der erhobenen Telematikdaten, dass ein ihm gemeldeter Kfz-Schaden sich unmöglich so zugetragen haben kann, wie in der Unfallmeldung beschrieben und vermutet er Versicherungsbetrug, liegt mE ein berechtigtes Interesse des Versicherers an der Verwendung der Telematikdaten zur Betrugsbekämpfung vor. Erhärtet sich der Verdacht auf Betrug, so darf der Versicherer die Telematikdaten mE zur Erstattung einer Anzeige an die Strafverfolgungsbehörde nutzen. Streitet der/die Versicherungsnehmer*in den Versicherungsbetrug ab und klagt die Versicherungsleistung ein, so darf sich der Versicherer zur Verteidigung seiner

[169] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 6 DSGVO, RZ 76, 78 (Stand 1.12.2020, rdb.at).
[170] ErwGr 47 DSGVO.
[171] *Kühling/Buchner/Buchner/Petri*, 3. Aufl 2020, DS-GVO Art 6 RN 153.

Rechtsansprüche mE auch vor Gericht auf die erhobenen Telematikdaten stützen. Die Interessenabwägung geht in diesen Fällen zu Gunsten des Versicherers aus. Das Interesse des Versicherungsnehmers/der Versicherungsnehmerin, eine strafrechtlich relevante Tat folgenlos und unentdeckt zu begehen, überwiegt nicht das Interesse des Versicherers an der Bekämpfung von Betrug und der Vermeidung von ungerechtfertigten Auszahlungen. Ein Versicherer hat ein starkes und allgemein nachvollziehbares Interesse an der Bekämpfung von Versicherungsbetrug. Versicherungsnehmer*innen müssen vernünftigerweise damit rechnen, dass der Versicherer ihre Telematikdaten zum Zwecke der Betrugsbekämpfung verwendet. Die Interessen des Versicherers wiegen meiner Ansicht nach so schwer, dass trotz der gravierenden Auswirkungen auf die Versicherungsnehmer*innen (Strafverfahren), ein berechtigtes Interesse des Versicherers an der Verarbeitung der Telematikdaten zu den oben genannten Zwecken gegeben ist.

Anders verhält es sich mE bei der Verwendung von Telematikdaten zur Prüfung der Leistungspflicht des Versicherers im Schadensfall. In diesem Fall geht die Interessenabwägung mE nicht zu Gunsten des Versicheres aus. Versicherungsnehmer*innen müssen vernünftigerweise nicht damit rechnen, dass der Versicherer Telematikdaten im Falle eines Unfalls gegen sie verwendet. Das ist insbesondere dann der Fall, wenn ein PAYD-Tarif mit Prämienersparnis beworben und als vorteilhafter als herkömmliche Kfz-Tarife dargestellt wird. Eine Datenverarbeitung zur Leistungsprüfung hat mE schwere Auswirkungen auf Versicherungsnehmer*innen, die im Falle eines Unfalls oftmals auf die Versicherungsleistung angewiesen sind. Sie schließen genau aus diesem Grund einen Versicherungsvertrag ab. Die Interessen des Versicherers wiegen mE weniger schwer, als die Interessen der Versicherungsnehmer*innen. Eine Datenverarbeitung zum Zwecke der Leistungsprüfung müsste daher auf eine Einwilligungserklärung gestützt werden.

5.4 Sonstige Rechtfertigungstatbestände des Art 6 Abs 1 DSGVO

Art 6 Abs 1 DSGVO sieht folgende weitere Rechtfertigungstatbestände für die Verarbeitung personenbezogener Daten vor:

- lit c: die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

- lit d: die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- lit e: die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

Diese Rechtfertigungstatbestände sind meiner Einschätzung nach bei der Verarbeitung von Fahr- und Telematikdaten kaum von Praxisrelevanz. Es ist natürlich denkbar, dass der Versicherer Standortdaten an einen Rettungsdienst weitergibt, um der betroffenen Person nach einem Unfall Hilfe zukommen zu lassen. In diesem Fall würde der Versicherer die Daten rechtmäßig, weil zum Schutz der lebenswichtigen Interessen der betroffenen Person, verarbeiten. Derartige Anwendungsfälle dürften in der Praxis aber kaum vorkommen, da im Falle eines Verkehrsunfalls das vernetzte Fahrzeug über den eCall einen direkten Notruf an die zuständige Einsatzstelle absetzt.

Die Verarbeitung von Telematikdaten zur Wahrnehmung einer öffentlichen Aufgabe ist wohl auch nicht von praktischer Bedeutung. Gemäß § 40a KFG werden Versicherungen im Rahmen ihrer Tätigkeit als Zulassungsstellen zwar hoheitlich tätig ("Beleihung") und sind bei der Wahrnehmung ihrer behördlichen Aufgaben[172] zur Verarbeitung von bestimmten personenbezogenen Daten befugt. Für eine Verarbeitung von Telematikdaten sehe ich im Rahmen der behördlichen Tätigkeit des Versicherers jedoch keine Notwendigkeit.

Eine Datenverarbeitung ist auch dann rechtmäßig, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Gemeint sind hier konkrete rechtliche Verpflichtungen zur Verarbeitung bestimmter Daten[173]. Versicherungen sind regelmäßig Adressaten von solchen rechtlichen Verpflichtungen, zB bestehen Meldepflichten zur Prävention von Geldwäsche[174]. Eine rechtliche Pflicht des Versicherers betreffend die Verarbeitung von Fahrzeug- und Telematikdaten, wie sie bei PAYD-Tarifen erhoben werden, besteht aber nicht.

[172] *Grubmann,* KHVG[5] § 40a KFG 1967, E 3 (Stand 1.2.2021, rdb.at).
[173] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim,* DatKomm Art 6 DSGVO, RZ 39 (Stand 7.5.20, rdb.at).
[174] § 16 FM-GwG.

6) Rechte der betroffenen Person

6.1 Transparente Information, Kommunikation, Modalitäten für die Ausübung der Rechte der betroffenen Person (Art 12 DSGVO)

Das dritte Kapitel der DSGVO beschäftigt sich mit den Rechten der betroffenen Person. Bevor in den einzelnen Artikeln die jeweiligen Betroffenenrechte konkretisiert werden, stellt der Art 12 DSGVO allgemeine Bestimmungen auf, die bei der Kommunikation mit betroffenen Person sowie bei der Bearbeitung von deren Anfragen und Anträgen zu beachten sind. Gemäß Art 12 DSGVO müssen Informationen und Mitteilungen nach Art 13-22 und 34 DSGVO in „*präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erteilt werden*“[175]. De facto ziehen sich diese Anforderungen quer durch das ganze Datenschutzrecht und sind nicht nur auf das dritte Kapitel der DSGVO beschränkt. Die betroffene Person muss verstehen und durchschauen können, welche „*sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden*[176]“. Der Verantwortliche soll in Informationen und Mitteilungen an die betroffene Person daher Alltagssprache benutzen, Fachbegriffe erklären, Schachtelsätze vermeiden, Untergliederungen vornehmen und auf Verweise verzichten[177] [178].

Der Verantwortliche steht bei der Kommunikation mit betroffenen Personen vor der Herausforderung einerseits alle notwendigen Informationen vollständig, präzise und verständlich zu darzulegen und andererseits einen “information-overkill“ zu vermeiden[179]. Nach Ansicht der Artikel-29-Datenschutzgruppe kann dieses Problem mit der sogenannten Mehrebenen-Datenschutzerklärung (“layered privacy statement“) gelöst werden. Das bedeutet, dass umfangreiche Dokumente mit Hilfe von Verlinkungen und Wegweisern so gestaltet werden, dass sich die betroffenen Personen schnell orientieren können und gezielt nur die für sie relevanten Textstellen lesen müssen[180]. Es entspricht durchaus der Realität, dass sich betroffene Personen mit datenschutzrechtlichen

[175] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 12 DSGVO, RZ 2 (Stand 1.12.2020, rdb.at).
[176] ErwGr 39 DSGVO.
[177] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 12 DSGVO, RZ 3-5 (Stand 1.12.2020, rdb.at).
[178] *Paal/Pauly/Paal/Hennemann*, 3. Aufl 2021, DS-GVO Art 12 RN 33.
[179] *Schilchegger*, Zur Erfüllung datenschutzrechtlicher Informationspflichten, ÖBA 2018, 319 (319).
[180] *Illibauer* in *Knyrim,* DatKomm Art 12 DSGVO, RZ 37 (Stand 1.12.2021, rdb.at).

Informationen und Mitteilungen nicht im Detail beschäftigen wollen. Eine Mehrebenen-Datenschutzerklärung befriedigt das Bedürfnis nach kurzer und knapper Information, die sich auf das Wesentliche beschränkt. Dennoch wirkt der Vorschlag der Artikel-29-Datenschutzgruppe auf mich befremdlich. Er zeigt mE, dass sogar das Beratungs- und Expertengremium der Europäischen Union davon ausgeht, dass die Informations- und Mitteilungspflichten der DSGVO an der Realität und an den Bedürfnissen der betroffenen Personen vorbeigehen.

Art 12 DSGVO sieht außerdem vor, dass Informationen und Mitteilungen an die betroffenen Personen grundsätzlich in schriftlicher oder elektronischer Form zu übermitteln sind. Sofern es die betroffene Person verlangt, sind Informationen mündlich zu erteilen. Im Fall der mündlichen Informationserteilung hat die betroffene Person ihre Identität in anderer Form (dh nicht mündlich) nachzuweisen. Bei mündlicher Informationserteilungen muss der Verantwortliche sicherstellen, dass er seiner Nachweis-, Dokumentations- und Rechenschaftspflicht nachkommen kann. Es sollte daher zumindest ein interner Vermerk erstellt und abgelegt werden[181]. Idealerweise wird der betroffenen Person eine Kopie dieses Vermerks zur Verfügung gestellt.

Übt die betroffene Person eines ihrer Rechte nach den Art 15-22 DSGVO aus, so hat sie der Verantwortliche über die Bearbeitung der jeweiligen Maßnahme unverzüglich, längstens aber innerhalb eines Monats nach Eingang des Antrags, zu informieren. Nur in Ausnahmefällen und unter bestimmten Voraussetzungen kann diese Frist auf zwei Monate ausgedehnt werden[182] [183]. Diese Fristen gelten auch dann, wenn der Verantwortliche die begehrte Maßnahme nicht durchführt, beispielsweise weil der verlangten Löschung eine Aufbewahrungspflicht entgegensteht[184] [185].

Die Information und Mitteilungen nach den Art 13-22 und 34 DSGVO sind unentgeltlich zur Verfügung zu stellen. Wenn die betroffene Person aber offenkundig unbegründet oder

[181] *Illibauer*, Informationsrecht und Modalitäten für die Ausübung der Betroffenenrechte, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 116, 117.
[182] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 12 DSGVO, RZ 16, 17 (Stand 1.12.2020, rdb.at).
[183] *Gola/Heckmann/Franck*, 3. Aufl 2022, DS-GVO Art 12 RN 26.
[184] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 12 DSGVO, RZ 15 (Stand 1.12.2020, rdb.at).
[185] *Quaas* in BeckOK DatenschutzR, 43. Ed 1.2.2023, DS-GVO Art 12 RN 40.

übermäßig viele Anträge stellt, kann der Verantwortliche ein angemessenes Entgelt verlangen oder sich weigern den Antrag umzusetzen[186].

6.2 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art 13 DSGVO)

Die Regeln des Art 13 DSGVO beziehen sich nur auf Daten, die bei der betroffenen Person erhoben wurden. Andernfalls ist Art 14 DSGVO anwendbar[187]. Die Abgrenzung zwischen dem Anwendungsbereich von Art 13 und Art 14 DSGVO ist nicht immer leicht und wohl auch der Mühe nicht wert, da sich die beiden Artikel inhaltlich ohnehin weitgehend decken[188]. Daten sind dann bei der betroffenen Person erhoben worden, wenn diese die Daten bewusst herausgegeben hat bzw wenn der Verantwortliche in irgendeiner Art und Weise Kontakt mit der betroffenen Person aufgenommen und infolgedessen Daten erhoben hat. Es kommt darauf an, ob die Daten durch „*ein aktives Verhalten, eine Entscheidung oder (unbewusste)*“ Mitarbeit/Mitwirkung der betroffenen Person erhoben wurden[189] [190].

Die vom PAYD-Versicherer erhobenen Fahrzeug- und Telematikdaten werden direkt bei der betroffenen Person erhoben und zwar unabhängig davon, ob die Daten über schon im Fahrzeug vorhandene Technik oder über eine eigens verbaute OBU erhoben werden. In jedem dieser Fälle setzen die Versicherungsnehmer*innen ein aktives Verhalten bzw treffen zumindest die Entscheidung zum Abschluss eines PAYD-Tarifes und damit zur Erhebung der Fahrzeug- und Telematikdaten. Die Daten werden nicht zur Überraschung der Versicherungsnehmer*innen und nicht ohne deren Wissen erhoben. Den Versicherer treffen im Hinblick auf Fahrzeug- und Telematikdaten somit die Informationspflichten des Art 13 DSGVO.

Gemäß Art 13 DSGVO ist die betroffene Person über die konkreten Verarbeitungszwecke und die jeweilige Rechtsgrundlage zu informieren[191]. Für den Fall, dass sich der Verantwortliche auf ein berechtigtes Interesse beruft, hat er der betroffenen Person

[186] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 12 DSGVO, RZ 23 (Stand 1.12.2020, rdb.at).
[187] *Illibauer* in *Knyrim,* DatKomm Art 13 DSGVO, RZ 20 (Stand 1.12.2021, rdb.at).
[188] *Pollirer*, Checkliste Erfüllung der Informationspflichten gem Art 13 und 14 DSGVO, Dako 2018/48 (87).
[189] *Illibauer* in *Knyrim,* DatKomm Art 13 DSGVO, RZ 21 (Stand 1.12.2021, rdb.at).
[190] *Sydow/Marsch,* DS-GVO/BDSG/*Ingold,* 3. Aufl 2022, DS GVO Art 13 RN 8.
[191] *Pollirer*, Checkliste Erfüllung der Informationspflichten gem Art 13 und 14 DSGVO, Dako 2018/48 (87).

mitzuteilen, welche Interessen er mit der Datenverarbeitung verfolgt. In der österreichischen Literatur wird die Ansicht vertreten, dass der betroffenen Person die Überlegungen, die im Zuge der Interessenabwägung angestellt wurden, nicht mitzuteilen sind. Die Artikel-29-Datenschutzgruppe vertritt jedoch eine andere Ansicht und es ist daher nicht klar, wie detailliert die Information hinsichtlich des berechtigten Interesses zu sein hat[192].

Werden personenbezogene Daten an Dritte übermittelt, so sind der betroffenen Person die Empfänger bzw die Kategorien der Empfänger bekannt zu geben. Dabei sind grundsätzlich die konkreten Empfänger zu nennen und nur wenn diese noch nicht namentlich bekannt sind oder deren Nennung einen unverhältnismäßig hohen Aufwand darstellen würde, reicht es aus nur die Kategorien von Empfängern anzuführen[193]. Darunter versteht man zB Branchenbezeichnungen wie Rechtsanwälte, Banken, Inkassounternehmen etc[194]. Sofern eine Übermittlung von Daten in ein Drittland beabsichtigt wird, ist die betroffene Person darüber zu informieren sowie über die Sicherstellung des angemessenen Schutzniveaus aufzuklären[195]. Darüber hinaus sind der betroffenen Person der Name und die Kontaktdaten des Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten zu nennen[196].

Nach Art 13 Abs 2 DSGVO ist die betroffene Person außerdem über folgendes zu informieren:

lit a: Speicherdauer;
lit b: Bestehen der Betroffenenrechte nach Art 15-18, 20-21 DSGVO;
lit c: Möglichkeit des Widerrufs einer Einwilligungserklärung;
lit d: Beschwerderecht bei der Aufsichtsbehörde;
lit e: Informationen, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist und welche Folgen die Nichtbereitstellung für die betroffene Person hätte;
lit f: Hinweis, ob eine automatisierte Einzellfallentscheidung einschließlich Profiling besteht und Informationen zur verwendeten Logik, Tragweite und Auswirkungen.

[192] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 13 DSGVO, RZ 26 (Stand 1.12.2020, rdb.at).
[193] DSB 22.08.2019, DSB-D130.206/0006-DSB/2019.
[194] *Illibauer* in *Knyrim,* DatKomm Art 13 DSGVO, RZ 35 (Stand 1.12.2021, rdb.at).
[195] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 13 DSGVO, RZ 28 (Stand 1.12.2020, rdb.at).
[196] *Schmidt-Wudy* in BeckOK DatenschutzR, 43. Ed 1.2.2023, DS-GVO Art 13 RN 42.

Gemäß Art 13 Abs 3 DSGVO hat der Verantwortliche für den Fall, dass er beabsichtigt Daten für einen anderen als den ursprünglichen Zweck weiterzuverarbeiten, die betroffene Person darüber zu informieren. Die Information hat vor Beginn der Weiterverarbeitung (im "Absichtsstadium") zu erfolgen und hat alle maßgeblichen Informationen zu enthalten[197].

6.3 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Artikel 14 DSGVO)

Für Daten, die nicht direkt bei der betroffenen Person erhoben wurden, gilt Art 14 DSGVO. Eine indirekte Erhebung von Daten liegt beispielsweise dann vor, wenn der Verantwortliche die Daten aus öffentlichen Quellen erlangt oder von Adresshändlern kauft. Die Informationspflichten des Art 13 und Art 14 DSGVO sind weitgehend identisch. Im Falle der indirekten Datenerhebung ist der betroffenen Person mitzuteilen, aus welcher Quelle die personenbezogenen Daten stammen. Das gilt auch dann, wenn die Daten aus öffentlich zugänglichen Quellen stammen. In diesem Fall muss die öffentliche Quelle konkret genannt werden (zB Telefonbuch, Instagram-Profil der betroffenen Person etc)[198]. Auf Fahrzeug- und Telematikaten, die im Rahmen von PAYD-Tarifen erhoben werden, ist Art 13 DSGVO anwendbar, so dass auf Art 14 DSGVO nicht näher eingegangen wird.

6.4 Auskunftsrecht der betroffenen Person (Artikel 15 DSGVO)

Die betroffene Person hat ein Recht darauf, eine Auskunft über die sie betreffenden personenbezogenen Daten zu erhalten. Die Auskunft hat folgende Inhalte zu umfassen:

lit a: Verarbeitungszwecke;

lit b: Kategorien personenbezogener Daten, die verarbeitet werden;

lit c: Empfänger oder Kategorien von Empfängern;

lit d: Speicherdauer bzw Kriterien für deren Festlegung;

lit e: Bestehen des Rechts auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung;

---

[197] *Arning* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap. 6, RZ 76, 78 (Stand 1.4.2021, rdb.at).

[198] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 14 DSGVO, RZ 1, 33, 34 (Stand 1.12.2020, rdb.at).

lit f: Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

lit g: alle Informationen zur Herkunft der Daten im Fall indirekter Datenerhebung;

lit h: Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und Informationen über die involvierte Logik, Tragweite und Auswirkungen auf die betroffene Person (siehe Punkt 6.9.1).

In einem ersten Schritt ist der betroffenen Person mitzuteilen, ob überhaupt sie betreffende personenbezogene Daten verarbeitet werden. Ist das nicht der Fall, ist eine Negativauskunft zu erteilen[199]. Werden personenbezogene Daten verarbeitet, ist die betroffene Person über den konkreten Inhalt der verarbeiteten Daten zu informieren[200]. Die erteilte Auskunft muss so konkret sein, dass die betroffene Person die Rechtmäßigkeit der Verarbeitung überprüfen und gegebenenfalls weitere Rechte, wie das Recht auf Berichtigung oder Löschung ausüben kann[201] [202].

Daraus lässt sich für PAYD-Tarife ableiten, dass eine Auskunft nach Art 15 DSGVO die konkret verarbeiteten Telematikdaten – und somit auch die Standort- und Bewegungsdaten – enthalten muss. Dieser Ansicht steht aber eine aktuelle, nicht rechtskräftige Entscheidung des Bundesverwaltungsgerichtes (BVwG) vom März 2023 entgegen (W274 2248601-1)[203]. Laut dieser Entscheidung darf ein Mobilfunkbetreiber die Auskunft über Standortdaten verweigern, wenn der Kunde/die Kundin nicht beweisen kann, dass sein/ihr Mobiltelefon ausschließlich von ihm/ihr selbst und nicht auch von einer dritten Person genutzt wurde. Das BVwG führt aus, dass sich der Anspruch auf Auskunft immer nur auf die jeweils eigenen personenbezogenen Daten einer betroffenen Person bezieht, nicht aber auf Daten anderer Personen. Das Auskunftsrecht darf die Freiheiten anderer Personen nicht verletzen und es muss sichergestellt sein, dass die betroffene Person nur über solche Standortdaten eine Auskunft erhält, die sie selbst betreffen. Da im konkreten Fall der Kunde aber nicht beweisen konnte, dass sein Mobiltelefon ausschließlich von ihm benutzt wurde, steht im kein Recht auf Auskunft über die Standortdaten nach Art 15 DSGVO zu. Das BVwG räumt ein, dass eine Verweigerung der Auskunft für die tatsächlichen Nutzer*innen eines Mobiltelefons

[199] *Dix* in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 15 RN 13.
[200] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 15 DSGVO, RZ 18 (Stand 1.12.2020, rdb.at).
[201] *Fritz*, Das Auskunftsrecht nach Art 15 DSGVO in der Entscheidungspraxis und Rechtsprechung, Jahrbuch Datenschutzrecht 2021, 65 (84).
[202] DSB 26.07.2019, DSB-D123.921/0005-DSB/2019.
[203] BVwG 03.03.2023, W274 2248601-1. Zum Zeitpunkt 11.05.2023 nicht rechtskräftig.

unbefriedigend sein kann, aber dass aufgrund eines möglichen Auseinanderfallens der Person des Vertragspartners/der Vertragspartnerin und des tatsächlichen Benutzers/der Benützerin nunmal mit datenschutzrechtlichen Problemstellungen zu rechnen ist[204]. Die Entscheidung ist nicht rechtskräftig, die betroffene Person hat bereits angekündigt eine Berufung an den Österreichischen Verwaltungsgerichtshof (VwGH) einbringen zu werden[205].

Meiner Ansicht nach ist diese Entscheidung widersprüchlich und inkonsistent. Nach Ansicht des BVwG sind Standortdaten zwar besonders schützenswerte personenbezogene Daten, können aber nicht einer bestimmten Person zugeordnet werden. Zur Frage, ob Standortdaten mangels Zuordenbarkeit zu einer betroffenen Person dann überhaupt noch personenbezogene Daten sind, hält das BVwG fest, „*dass allein der Umstand, dass ein Verantwortlicher die betroffene Person nicht identifizieren kann, das Vorliegen personenbezogener Daten iSd Art. 4 Z 1 DSGVO und somit die grundsätzliche Anwendbarkeit der DSGVO an sich und somit des Art. 15 (Auskunftspflicht) nicht ausschließt*". Demnach sind nach Ansicht des BVwG Standortdaten personenbezogene Daten und Art 15 DSGVO ist grundsätzlich anwendbar[206].

Zudem halte ich die Anforderungen an die Beweispflicht der betroffenen Person für überzogen. Laut BVwG muss der Auskunftswerber/die Auskunftswerberin einen objektiven Nachweis darüber bringen, dass sein/ihr Mobiltelefon ausschließlich und zu jeder Zeit von ihm/ihr benutzt wurde. Für das BVwG war nicht relevant, dass das Mobiltelefon des Auskunftswerbers sowohl durch einen PIN-Code als auch durch Fingerprint geschützt war und der Auskunftswerber eidesstattlich versichert hat, sein Mobiltelefon nicht weitergegeben zu haben[207]. Es ist daher völlig unklar, wie der vom BVwG geforderte Beweis erbracht werden könnte. In der Realität wird den betroffenen Personen die Beweisführung so gut wie nie gelingen und das Auskunftsrecht betreffend Standortdaten wird somit regelmäßig ins Leere laufen.

[204]BVwG 03.03.2023, W274 2248601-1. Zum Zeitpunkt 11.05.2023 nicht rechtskräftig.
[205]Vgl: „Handy nicht persönlich genug für DSGVO-Schutz?!"; https://noyb.eu/de/handy-nicht-persoenlich-genug-fuer-dsgvo-schutz (abgerufen am 05.04.2023).
[206]BVwG 03.03.2023, W274 2248601-1. Zum Zeitpunkt 11.05.23 nicht rechtskräftig.
[207]Vgl: „Handy nicht persönlich genug für DSGVO-Schutz?!"; https://noyb.eu/de/handy-nicht-persoenlich-genug-fuer-dsgvo-schutz (abgerufen am 05.04.2023).

Für PAYD-Tarife bedeutet die Entscheidung des BVwG, dass Versicherungsnehmer*innen nur dann Auskunft über Standortdaten erhalten, wenn sie objektiv nachweisen können, das versicherte Fahrzeug ausschließlich selbst gefahren zu haben. Wenn die Beweisführung schon bei einem Mobiltelefon, das üblicherweise nur von einer bestimmten Person verwendet wird, derart schwierig ist, dann trifft das auf Fahrzeuge umso mehr zu. Fahrzeuge werden häufig von mehreren Personen genutzt und es ist faktisch unmöglich, den vom BVwG geforderten objektiven Nachweis für die alleinige Nutzung zu erbringen. Das wird wohl dazu führen, dass Versicherungsnehmer*innen eines PAYD-Tarifes so gut wie nie eine Auskunft über die verarbeiteten Standortdaten erhalten werden. In Folge dessen wird ihnen die Möglichkeit genommen, die Richtigkeit der erhobenen Standortdaten zu überprüfen und gegebenenfalls eine Berichtigung oder Löschung zu beantragen. Sofern die Standortdaten einen Einfluss auf die Höhe der Versicherungsprämie haben, kann die Auskunftsverweigerung direkte finanzielle Folgen für die betroffene Person haben.

Es ist richtig, dass das Auskunftsrecht die Rechte und Freiheiten anderer Personen nicht verletzen darf. Der Art 15 Abs 4 DSGVO verlangt aber nicht, dass schon die bloß abstrakte Möglichkeit einer Verletzung der Rechte und Freiheiten Dritter zu einer Beschränkung des Auskunftsrechtes führt[208]. Auch wenn Fahrzeuge häufig von mehreren Personen benutzt werden, kann es nicht im Sinne der DSGVO sein die Beauskunftung von Standortdaten derart rigoros einzuschränken. Vielmehr müsste nach Lösungen gesucht werden, um eine Auskunftserteilung an unberechtigte Personen zu verhindern. In der Literatur wird etwa vorgeschlagen, dass der Verantwortliche auf die Glaubhaftmachung der ausschließlichen Nutzung bestehen sollte. In der Praxis könnte zum Beispiel bei gemeinsam genutzten Fahrzeugen verlangt werden, dass ein gemeinsames Auskunftsbegehren gestellt wird[209]. Zudem stellt ErwGr 63 klar, dass Art 15 Abs 4 DSGVO nicht die Möglichkeit eröffnet, jegliche Auskunft zu verweigern. Die Auskunftserteilung könnte daher auch von einer Grundrechtsabwägung abhängig gemacht werden[210].

[208] *Blocher*, Dein Handy, aber nicht deine Daten?, ZIIR 2022, 7.
[209] *Blocher*, Dein Handy, aber nicht deine Daten?, ZIIR 2022, 8.
[210] *Paal/Pauly/Paal*, 3. Aufl 2021, DS-GVO Art 15 RN 41.

Während die Entscheidung des BVwG zu einer Schlechterstellung betroffener Personen führt[211], bedeutet sie für den Versicherer auf den ersten Blick eine Erleichterung bei der Bearbeitung von Auskunftsbegehren. Auf den zweiten Blick erkennt man aber, dass die Entscheidung auch für den Versicherer zu gewissen Risiken führt. Sie steht vor allem automatisierten Lösungen entgegen. Im ErwGr 63 wird etwa vorgeschlagen, der betroffenen Person über ein sicheres System (passwortgeschütztes Benutzerkonto) einen direkten Zugang zu ihren personenbezogenen Daten zu geben[212]. Dadurch kann sich die betroffenen Person laufend einen Überblick über den Inhalt der verarbeiteten personenbezogenen Daten verschaffen[213]. Angesichts der Entscheidung des BVwG wäre das aber gar nicht zulässig, da möglicherweise personenbezogene Daten Dritter eingesehen werden könnten. Siehe dazu auch Punkt 6.8 (Recht auf Datenübertragbarkeit).

6.5 Recht auf Berichtigung (Artikel 16 DSGVO)

Nach Art 16 DSGVO hat die betroffene Person das Recht, die Berichtigung von sie betreffenden unrichtigen personenbezogenen Daten oder die Vervollständigung unvollständiger personenbezogener Daten zu verlangen. Unrichtig sind Daten dann, wenn sie objektiv unrichtig sind und nicht der Realität entsprechen[214] [215]. Das kann in manchen Fällen leicht zu beurteilen sein, etwa dann wenn ein falsches Geburtsdatum oder eine unrichtige Angabe zum Familienstand verarbeitet wird. Bei Telematikdaten ist es hingegen schwierig festzustellen, ob diese tatsächlich der Realität entsprechen. Ist die betroffene Person etwa der Meinung, dass bei der Erhebung der Fahrgeschwindigkeit ein Fehler passiert ist (was durchaus vorkommen kann[216]) und die Höchstgeschwindigkeit entgegen der Aufzeichnung des Versicherers nicht überschritten wurde, wird ihr der entsprechende Nachweis nur schwer gelingen.

Für die Dauer der Überprüfung der Richtigkeit, kann die betroffene Person die Einschränkung der Verarbeitung verlangen (Art 18 DSGVO)[217].

---

[211] Vgl: „Handy nicht persönlich genug für DSGVO-Schutz?!“; https://noyb.eu/de/handy-nicht-persoenlich-genug-fuer-dsgvo-schutz (abgerufen am 05.04.2023).
[212] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 15 DSGVO, RZ 18 (Stand 1.12.2020, rdb.at).
[213] *Paal/Pauly/Paal*, 3. Aufl 2021, DS-GVO Art 15 RN 14, 15.
[214] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 16 DSGVO, RZ 4 (Stand 1.12.2020, rdb.at).
[215] *Haidinger* in *Knyrim,* DatKomm Art 17 DSGVO, RZ 22 (Stand 1.12.2021, rdb.at).
[216] *Schwichtenberg*, „Pay as you drive“ – neue und altbekannte Probleme, DuD 6/2015, 378.
[217] *Haidinger* in *Knyrim,* DatKomm Art 18 DSGVO, RZ 1 (Stand 1.12.2021, rdb.at).

Die DSGVO trifft keine Regelung zur Beweislastverteilung und in der Literatur gibt es die unterschiedlichsten Ansichten dazu, wer die Richtigkeit bzw Unrichtigkeit der Daten zu beweisen hat. In der Praxis wird meistens die betroffene Person den ersten Schritt setzen und die Richtigkeit der sie betreffenden personenbezogenen Daten bestreiten. Es ist unklar, ob die betroffene Person die Unrichtigkeit substantiiert bestreiten muss oder nicht. Es besteht lediglich darüber Einigkeit, dass die betroffene Person zumindest die Daten bezeichnen muss, die sie für unrichtig hält[218]. In einem zweiten Schritt setzt sich der Verantwortliche mit den Behauptungen der betroffenen Person auseinander und prüft die Richtigkeit der Daten. Falls notwendig, nimmt er die erforderlichen Korrekturen vor.

Problematisch wird es dann, wenn die Überprüfung weder die Richtigkeit noch die Unrichtigkeit der Daten ergibt ("non-liquet")[219]. In der Literatur wird teilweise vertreten, dass der Verantwortliche wegen des Grundsatzes der Datenrichtigkeit und aufgrund seiner Rechenschaftspflicht die Beweislast trägt. Diese Ansicht würde in der Praxis dazu führen, dass der Verantwortliche die strittigen Daten immer dann im Sinne der betroffenen Person ändern oder löschen müsste, wenn er deren Richtigkeit nicht beweisen kann[220]. Dieser Vorschlag führt faktisch zu einer Beweislastumkehr und ist mE nicht uneingeschränkt praxistauglich. Für PAYD-Tarife würde das zum Beispiel bedeuten, dass die betroffene Person nur die Unrichtigkeit bestimmter Telematikdaten behaupten müsste um die Höhe der Prämie zu beeinflussen. Das ist nicht sachgerecht und steht auch nicht im Einklang mit einer Entscheidung des BVwG vom Mai 2022[221], wonach die Rechenschaftspflicht nicht zu einer allgemeinen Beweislastumkehr führt und im Sinne der Verhältnismäßigkeit auszulegen ist (Punkt 4.7). Letztendlich ist es aber nicht geklärt, wie mit non-liquet-Situationen umgegangen werden soll, was sowohl für den Verantwortlichen wie auch für die betroffene Person unbefriedigend ist.

6.6 Recht auf Löschung (Artikel 17 DSGVO)

Die betroffene Person hat das Recht die unverzügliche Löschung personenbezogener Daten zu verlangen, wenn einer der Löschungsgründe des Art 17 Abs 1 DSGVO vorliegt

[218] *Arning* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap 6, RZ 352 - 353 (Stand 1.4.2021, rdb.at).
[219] *Arning* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap 6, RZ 354 - 355a (Stand 1.4.2021, rdb.at).
[220] *Haidinger* in *Knyrim,* DatKomm Art 17 DSGVO, RZ 22 (Stand 1.12.2021, rdb.at).
[221] BVwG 12.05.2022, W252 2237237-1.

und nicht eine der Ausnahmen des Abs 3 leg cit anwendbar ist. Nach Art 17 DSGVO trifft den Verantwortlichen außerdem die Pflicht personenbezogene Daten pro-aktiv zu löschen, sofern alle Voraussetzungen dafür vorliegen[222].

Die Löschung kann auch durch Entfernen des Personenbezuges durchgeführt werden. In diesem Fall muss sichergestellt sein, dass weder Dritte noch der Verantwortliche ohne unverhältnismäßigen Aufwand den Personenbezug wiederherstellen können („Anonymisierung")[223] [224]. Es ist nicht ausreichend nur den gezielten Zugriff auf die personenbezogenen Daten zu unterbinden[225].

Art 17 Abs 1 DSGVO sieht folgende Gründe für eine Löschung vor:

lit a: Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig.

lit b: Die betroffene Person widerruft ihre Einwilligung und die Verarbeitung kann nicht auf eine andere Rechtsgrundlage gestützt werden.

lit c: Die betroffene Person legt einen Widerspruch gegen die Verarbeitung ein.

lit d: Die Verarbeitung der personenbezogenen Daten war unrechtmäßig.

lit e: Die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung notwendig.

lit f: Die Einwilligung wurde durch ein Kind in Bezug auf Dienste der Informationsgesellschaft erteilt.

Die wichtigsten Löschgrunde resultieren entweder aus datenschutzrechtlichen Grundsätzen (zB Zweckbindungsgrundsatz) oder aus dem Wegfall von Erlaubnistatbeständen (zB Widerruf der Einwilligung). Daher wird auf die einzelnen Löschgründe an dieser Stelle nicht näher eingegangen, sondern auf die entsprechenden Kapitel dieser Master Thesis verwiesen.

Dem Recht auf Löschung stehen die folgenden Ausnahmetatbestände des Art 17 Abs 3 DSGVO entgegen:

lit a: Ausübung des Rechts auf freie Meinungsäußerung und Information.

---

[222] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 17 DSGVO, RZ 9, 10 (Stand 1.12.2020, rdb.at).
[223] DSB 05.12.2018, DSB-D123.270/0009-DSB/2018.
[224] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 17 DSGVO, RZ 13 (Stand 1.12.2020, rdb.at).
[225] OGH 15.04.2010, 6 Ob 41/10p.

lit b: Erfüllung einer rechtlichen Verpflichtung oder Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt.

lit c: Öffentliches Interesse im Bereich der öffentlichen Gesundheit.

lit d: Im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke.

lit e: Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Für PAYD-Tarife ist vor allem lit e leg cit von Relevanz, so dass hier nur auf diese Bestimmung näher eingegangen wird.

6.6.1 Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen - Verjährungsfristen

Ist die Datenverarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich, besteht gemäß Art 17 Abs 3 lit e DSGVO keine Pflicht zur Löschung. In der Praxis stellen sich zahlreiche Fragen zur Reichweite dieses Ausnahmetatbestandes. Es besteht Einigkeit darüber, dass im Falle eines schon anhängigen Rechtsstreits kein Anspruch auf Löschung besteht, sofern die personenbezogenen Daten für die Verfahrensführung erforderlich sind. Aber auch in diesen Fällen gilt, dass die Datenverarbeitung auf das notwendige Maß zu beschränken ist und dass die Daten nach rechtskräftigem Abschluss des Verfahrens zu löschen sind[226].

Nun ist es aber so, dass innerhalb offener Verjährungsfristen grundsätzlich jederzeit ein Rechtsstreit anhängig gemacht werden kann und nicht vorhersehbar ist, in welchem Ausmaß die Aufbewahrung von personenbezogenen Daten zur Geltendmachung von oder zur Verteidigung gegen Rechtsansprüche notwendig sein wird. Der VfGH hat entschieden, dass die bloß abstrakte Möglichkeit einer rechtlichen Auseinandersetzung nicht ausreichend ist um das Recht auf Löschung zu beschränken[227]. *Jahnel* hingegen vertritt die Ansicht, dass dieses VfGH Erkenntnis nicht verallgemeinerungsfähig ist, da im konkreten Fall besonders schutzwürdige Daten zum Sexualleben der betroffenen Person verarbeitet wurden und der VfGH die Löschpflicht unter anderem mit Art 8 EMRK begründet hat. Wird die Aussage des VfGH aus dem Zusammenhang gerissen und

[226] *Haidinger/Löffler*, BVwG 15.12.2021, W176 2247780-1, Dako 3/2022, 65.
[227] VfGH 12. 12. 2017, GZ E3249/2016.

auf Sachverhalte angewendet, in denen es nicht um die Verarbeitung besonders schutzwürdiger Daten geht oder in denen Rechtsstreitigkeiten üblicherweise erst längere Zeit nach Vertragserfüllung auftreten, geht das laut *Jahnel* an den Bedürfnissen der Praxis vorbei[228]. Das dürfte die DSB ähnlich sehen. Sie hat entschieden, dass Bewerberdaten vor Ablauf der sechsmonatigen Frist des § 29 Abs 1 GlBG nicht gelöscht werden müssen[229] [230]. Wenn man diese Ansicht verallgemeinert, so steht der betroffenen Person vor Ablauf der allgemeinen Verjährungsfrist kein Recht auf Löschung von personenbezogenen Daten zu.

Gemäß § 12 Abs 1 VersVG verjähren Ansprüche aus einem Versicherungsvertrag grundsätzlich nach drei Jahren. Steht der Anspruch nicht dem Versicherungsnehmer/der Versicherungsnehmerin zu, sondern einem Dritten, beginnt die Verjährungsfrist erst zu laufen, sobald dem Dritten sein Recht bekannt geworden ist. Ist diesem sein Recht nicht bekannt geworden, verjährt sein Anspruch nach zehn Jahren.

Unter den Voraussetzungen des § 12 Abs 3 VersVG kann die dreijährige Verjährungsfrist verkürzt werden. Gemäß § 12 Abs 3 VersVG ist der Versicherer dann leistungsfrei, wenn die Versicherungsnehmer*innen ihren Anspruch auf Leistung nicht innerhalb eines Jahres gerichtlich geltend machen. Voraussetzung dafür ist, dass der Versicherer einen gegen ihn erhobenen Anspruch schriftlich ablehnt und die Ablehnung mit einer gesetzlichen oder vertraglichen Bestimmung begründet. Außerdem hat er die Versicherungsnehmer*innen audrücklich über die Rechtsfolge einer nicht fristgerechten gerichtlichen Geltendmachung aufzuklären[231].

Die Verjährungsregeln des § 12 VersVG gelten aber nur für Ansprüche aus dem Versicherungsvertrag[232]. Werden andere Rechtsansprüche geltend gemacht, etwa aus dem Bereicherungsrecht, kommen die allgemeinen Regeln des ABGB (§§ 1478 ff ABGB) zur Anwendung. Das ABGB sieht als Standardfall eine „lange“ Verjährungsfrist von dreißig

[228] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 17 DSGVO, RZ 51, 52 (Stand 1.12.2020, rdb.at).
[229] DSB 27.8.2018, DSB-D123.085/0003-DSB/2018.
[230] In Deutschland sieht das Allgemeine Gleichbehandlungsgesetz (AGG) eine zweimonatige Anfechtungsfrist vor. Siehe dazu: *Schröder*, Datenschutzrecht für die Praxis[4], 48-50.
[231] *Grubmann*, VersVG[9] § 12, E 135, E 142 (Stand 1.7.2022, rdb.at).
[232] *Grubmann*, VersVG[9] § 12, E 207 (Stand 1.7.2022, rdb.at).

Jahren vor. Kommt keine Sonderregelung zur Anwendung, nach der eine kürzere Verjährungsfrist gilt (zB § 12 VersVG), so beträgt die Verjährungsfrist dreißig Jahre[233].
Der Versicherer hat ausgehend von § 12 VersVG und von §§ 1478 ff ABGB Löschfristen festzulegen. Wie komplex das sein kann, soll hier am Beispiel der PAYD-Versicherung dargestellt werden:

Grundsätzlich kommen für einen PAYD-Tarif keine anderen Löschfristen als für konventionelle Kfz-Versicherungstarife zur Anwendung, was bedeutet das auch für sie der § 12 VersVG einschlägig ist. Die allgemeine Verjährungsfrist beträgt drei Jahre, kann aber auch länger (max 10 Jahre) oder kürzer (ein Jahr) sein. Die zehnjährige Frist kommt nur dann zur Anwendung, wenn die Versicherungsleistung einem Dritten zusteht. Das ist primär bei Lebens- oder Unfallversicherungsverträgen der Fall, bei denen die bezugs- bzw erbberechtigten Personen nichts von ihrem Recht wissen. Für Kfz-Versicherungsverträge ist eine solche Konstellation nicht denkbar. Das heißt, dass sich die Löschfrist für PAYD-Tarife nicht an der langen Verjährungsfrist von zehn Jahren orientieren kann.

Die kurze Verjährungsfrist von einem Jahr hängt wiederum von der Einhaltung der Bedingungen des § 12 Abs 3 VersVG ab. Der Versicherer muss die Ablehnung des Leistungsanspruches schriftlich erklären, hinreichend begründen und ausdrücklich auf die Rechtsfolgen einer Fristversäumnis hinweisen[234]. In der Praxis werden diese Bedingungen nicht immer eingehalten bzw entscheidet sich ein Versicherer möglicherweise bewusst dazu, sich nicht auf die kurze Verjährungsfrist stützen zu wollen. Das ist etwa dann denkbar, wenn aus Gründen der Standardisierung oder Automatisierung davon abgesehen wird, Ablehnungsschreiben mit einer ausführlichen Begründung zu versehen. Darüber hinaus können Rechtsstreitigkeiten die unterschiedlichsten Ursachen haben und müssen ihren Ursprung nicht immer in einer Leistungsablehnung durch den Versicherer haben. Demnach sollte sich die Löschfrist für PAYD-Tarife nicht an der kurzen Verjährungsfrist von einem Jahr orientieren, sondern sollte der allgemeinen Verjährungsfrist von drei Jahren entsprechen. Nachdem die Löschfrist mit drei Jahren bestimmt wurde, hat der

[233] *Perner/Spitzer/Kodek*, Bürgerliches Recht[2], 198.
[234] *Grubmann*, VersVG[9] § 12, E 135, E 142 (Stand 1.7.2022, rdb.at).

Versicherer in einem zweiten Schritt den Zeitpunkt zu bestimmen, an dem die Frist zu laufen beginnt[235].

Der Beginn der Verjährungsfrist richtet sich nach den allgemeinen zivilrechtlichen Regeln des § 1478 ABGB und beginnt mit dem Zeitpunkt zu laufen zu dem das Recht erstmals hätte ausgeübt werden können[236]. Bei Rechtsstreitigkeiten in Zusammenhang mit der Prämie beginnt die Verjährungsfrist jeweils mit jeder einzelnen Prämienvorschreibung zu laufen[237]. Geht es um Rechtsstreitigkeiten in Zusammenhang mit einer Leistung wegen eines Verkehrsunfalls oder eines sonstigen Schadens am Fahrzeug, beginnt die Verjährungsfrist mit dem Zeitpunkt des Unfalls bzw des Schadeneintritts zu laufen.

Telematikdaten, die ausschließlich zum Zweck der Prämienberechnung verarbeitet werden, sind demnach innerhalb von drei Jahren ab Vorschreibung derjenigen Prämie zu löschen, zu deren Berechnung sie verwendet wurden. Andere Daten, die nicht nur für die Berechnung der Prämie benötigt werden, wie etwa Adressdaten, sind zumindest für die Vertragsdauer zu speichern. Darüber hinaus ist es meines Erachtens gerechtfertigt, diese Daten auch für die Dauer der allgemeinen Verjährungsfrist, also für einen Zeitraum von drei Jahren ab Vertragsbeendigung, zu speichern.

Es ist grundsätzlich denkbar, dass auf Ansprüche in Zusammenhang mit PAYD-Verträgen die allgemeine dreißigjährige Verjährungsfrist des ABGB anzuwenden ist, etwa bei bereicherungsrechtlichen Rückabwicklungen. Diese rein theoretische Möglichkeit ist aus meiner Sicht aber nicht konkret genug, um eine Datenspeicherung über einen Zeitraum von dreißig Jahren zu rechtfertigen. Meines Erachtens würde hier die oben angeführte Rechtsprechung des VfGH greifen, wonach die bloß abstrakte Möglichkeit einer rechtlichen Auseinandersetzung nicht ausreichend ist[238]. Anders würde es sich mE verhalten, wenn sich die Wahrscheinlichkeit rechtlicher Auseinandersetzungen[239] zB durch neue Judikatur manifestiert. Sobald zum Beispiel aufgrund des EuGH Urteils vom 19.12.2013 (Rs C-209/12, *Endress)* erkennbar war, dass

[235] *Pollirer*, Checkliste Löschkonzept, Dako 2017/23 (42).
[236] *Grubmann*, VersVG[9] § 12, E 43 (Stand 1.7.2022, rdb.at).
[237] *Grubmann*, VersVG[9] § 12, E 19 (Stand 1.7.2022, rdb.at).
[238] VfGH 12. 12. 2017, GZ E3249/2016.
[239] *Ehmann/Selmayr/Kamann/Braun*, 2. Aufl 2018, DS-GVO Art 17 RN 64.

eine Vielzahl von Lebensversicherungsverträgen bereicherungsrechtlich abzuwickeln sind, war meines Erachtens eine ausreichend konkrete Erforderlichkeit im Sinne des Art 17 Abs 3 lit e DSGVO gegeben, um eine Speicherung der Daten aus Lebensversicherungsverträgen für einen Zeitraum von dreißig Jahren zu rechtfertigen.
Für den Versicherer ist das Festlegen der Löschfristen aber nur einer von vielen Aspekten, die er im Zusammenhang mit dem Recht auf Löschung zu berücksichtigen hat. Versicherungen haben entsprechende technische und organisatorische Vorkehrungen zu treffen um den Anforderungen des Art 17 DSGVO gerecht zu werden. Sie sollten ein umfassendes Löschkonzept erarbeiten, in dem ua Löschfristen festgelegt, Verantwortlichkeiten definiert, operative Prozesse beschrieben und die Bearbeitung von Löschanträgen geregelt wird[240].

6.7 Recht auf Einschränkung der Verarbeitung (Art 18 DSGVO)

Liegt einer der in Art 18 Abs 1 DSGVO genannten Gründe vor, hat die betroffene Person das Recht eine Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen[241].

Nach Art 4 Z 3 DSGVO ist unter Einschränkung der Verarbeitung "*die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken*" zu verstehen. Gemeint ist damit, dass die Verarbeitung der personenbezogenen Daten auf bestimmte, zulässige Verarbeitungsvorgänge zu reduzieren ist, beispielsweise auf das Speichern[242]. Das Recht auf Einschränkung ist zwar als eigenständiges Betroffenenrecht ausgestaltet, es besteht tatsächlich jedoch als Begleitanspruch zu anderen Betroffenenrechten, wie eben dem Recht auf Berichtigung oder Löschung[243]. Behauptet die betroffene Person beispielsweise die Unrichtigkeit der sie betreffenden personenbezogenen Daten und verlangt deren Richtigstellung, so kann für die Dauer der Überprüfung die Verarbeitung eingeschränkt werden[244].

[240] *Warter*, Rechtliche Vorgaben für ein Löschkonzept, Dako 2018/26 (29, 42).
[241] *Wybitul*, EU-Datenschutz-Grundverordnung im Unternehmen Kap VI, RZ 362 (Stand 11.8.2016, rdb.at).
[242] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 18 DSGVO, RZ 2 (Stand 1.12.2020, rdb.at).
[243] *Haidinger* in *Knyrim,* DatKomm Art 18 DSGVO, RZ 1 (Stand 1.12.2021, rdb.at).
[244] *Arning* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap 6, RZ 462 (Stand 1.4.2021, rdb.at).

Übt die betroffene Person das Recht auf Einschränkung aus, dann dürfen ihre personenbezogenen Daten weiterhin gespeichert werden. Eine über die Speicherung hinausgehende Verarbeitung ist aber nur dann zulässig, wenn die betroffene Person dem zustimmt, wenn die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Verantwortlichen erforderlich ist, zum Schutz der Rechte anderer natürlicher oder juristischer Personen oder wenn ein wichtiges öffentliches Interesse an der Verarbeitung besteht[245]. Bestreiten PAYD-Versicherungsnehmer*innen die Richtigkeit der verarbeiteten Telematikdaten und verlangt eine Einschränkung der Verarbeitung, dürfen die Telematikdaten für die Dauer der Überprüfung nur noch gespeichert, nicht aber zur Berechnung der Prämie oder für andere Zwecke verwendet werden.

6.8 Recht auf Datenübertragbarkeit (Art 20 DSGVO)

Nach Art 20 DSGVO hat die betroffene Person ein Recht auf Datenübertragbarkeit. Die betroffene Person kann verlangen, dass die sie betreffenden personenbezogenen Daten, die sie bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format übertragen werden. Sie kann auch verlangen, dass der Verantwortliche die Daten direkt an einen anderen Verantwortlichen überträgt[246]. Ziel dieser Regelung ist es, die datenschutzrechtliche Selbstbestimmtheit der betroffenen Person zu stärken. Mit dem Recht auf Datenübertragbarkeit werden aber auch wettbewerbsrechtliche Zielsetzungen verfolgt. Die betroffene Person soll möglichst einfach von einem Diensteanbieter zu einem anderen wechseln können[247].

Das Recht auf Datenübertragbarkeit ist an folgende Voraussetzungen geknüpft (Art 20 Abs 1 DSGVO):

- Die betroffene Person hat die Daten selbst bereitgestellt.
- Es handelt sich um Daten, die die betroffene Person betreffen.
- Die Verarbeitung der Daten basiert auf Einwilligung oder Vertrag.
- Der Verantwortliche verwendet automatisierte Verfahren zur Verarbeitung der Daten.

[245] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 18 DSGVO, RZ 17 (Stand 1.12.2020, rdb.at).
[246] *Fellner*, Betroffenenrechte nach der DSGVO, VbR 2018/47 (88).
[247] *Hübelbauer*, DSGVO: Das Recht auf Datenübertragbarkeit (Teil XIII), Dako 2017/64 (106).

Eine zentrale Fragestellung im Zusammenhang mit Art 20 DSGVO ist, was unter „Bereitstellung durch die betroffene Person“ zu verstehen ist. Nach Ansicht der Art 29-Datenschutzgruppe ist der Begriff weit auszulegen. Daten, die die betroffene Person aktiv und wissentlich dem Verantwortlichen übermittelt hat, sind jedenfalls davon umfasst. Das ist zum Beispiel dann der Fall, wenn die betroffene Person ihre Adress- oder Geburtsdaten bekannt gibt oder Fotos und Videos auf Social-Media-Plattformen hochlädt[248]. Der Begriff des Bereitstellens geht aber weiter und umfasst auch Daten, die durch die Nutzung eines Dienstes des Verantwortlichen entstanden sind. Es ist nicht erforderlich, dass die betroffene Person die personenbezogenen Daten aktiv übermittelt. Es reicht aus wenn die Daten aus einem Verhalten, das die betroffene Person wissentlich setzt, generiert werden. Nach dieser Auslegung gelten Telematikdaten, die durch die Nutzung von vernetzten Fahrzeugen entstehen oder durch eine OBU erfasst werden, als von der betroffenen Person bereitgestellt[249] [250].

Geht man davon aus, dass Telematikdaten im Rahmen eines PAYD-Tarifes vom Versicherer automatisiert verarbeitet werden und dass die Verarbeitung aufgrund eines Vertrages oder einer Einwilligung erfolgt, so ist Art 20 DSGVO anwendbar. Das heißt, dass Versicherungsnehmer*innen eines PAYD-Tarifes grundsätzlich eine Übertragung der sie betreffenden Telematikdaten an sie selbst oder an einen anderen Versicherer verlangen können.

Der Versicherer hat den betroffenen Personen bzw dem neuen Versicherer die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln. Die DSGVO ist technologieneutral formuliert und legt daher nicht fest, welche Formate für eine Übermittlung in Betracht kommen. Der verantwortliche Versicherer ist aber nicht dazu verpflichtet, ein bestimmtes IT-System zu verwenden oder bestimmte Lizenzen anzuschaffen. In der Literatur werden CSV- oder XML-Formate als gängige und geeignete Dateiformate für eine Datenübertragung genannt, während PDF-Formate nicht als geeignet gelten[251] [252]. In der Realität bringt eine Übertragung von Daten als CSV- oder XML-Datei aber keine wesentlichen Vorteile. Die betroffene Person erhält letztendlich

[248] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 20 DSGVO, RZ 13 (Stand 1.12.2020, rdb.at).
[249] *Haidinger* in *Knyrim,* DatKomm Art 20 DSGVO, RZ 20 (Stand 1.12.2022, rdb.at).
[250] *Dix* in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht Art 20, RN 8.
[251] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 20 DSGVO, RZ 23 (Stand 1.12.2020, rdb.at).
[252] *Hübelbauer*, DSGVO: Das Recht auf Datenübertragbarkeit (Teil XIII), Dako 2017/64 (107).

nichts anderes, als sie im Zuge eines Auskunftsbegehrens erhalten würde - nur in einem anderen Format. Und für den neuen Versicherer wird ein Import von Telematikdaten aus einer CSV- oder XML-Datei in sein eigenes IT-System einen großen Aufwand bedeuten. In der Literatur wird geschätzt, dass ein Import aus einer CSV- oder XML-Datei in ein fremdes IT-System mindestens denselben Aufwand verursacht, wie ein manuelles Abtippen[253]. Vermutlich sind das die Gründe für die geringe praktische Relevanz des Art 20 DSGVO[254].

Möglicherweise ist die fehlende Praxisrelevanz aber auch auf die bestehenden rechtlichen Unsicherheiten zurückzuführen. Wie in Punkt 6.4 beschrieben, ist vor Kurzem eine Entscheidung des BVwG ergangen, wonach ein Mobilfunkbetreiber eine Auskunft über Standortdaten verweigern durfte, weil der Kunde nicht nachweisen konnte, dass sein Mobiltelefon ausschließlich von ihm selbst verwendet wurde[255] [256]. Was für das Recht auf Auskunft gilt, muss mE konsequenterweise auch für das Recht auf Datenübertragbarkeit gelten. Solange die PAYD-Versicherungsnehmer*innen keinen objektiven Nachweis darüber erbringen können, dass sämtliche Mobilitätsdaten ausschließlich durch ihr Fahrverhalten erzeugt wurden, können sie sich mE nicht auf Art 20 DSGVO berufen.

Der Gesetzgeber hatte beim Recht auf Datenübertragbarkeit primär den Wechsel von einem sozialen Medium zu einem anderen im Hinterkopf[257]. Allerdings enthalten gerade Fotos oder Videos, die auf solche Plattformen hochgeladen werden, oftmals Daten anderer Personen („Freunde“). Die Art 29-Datenschutzgruppe schlägt diesbezüglich vor, der betroffenen Person die Möglichkeit zu geben, die Daten anderer Personen auszusondern oder deren Einwilligung zur Übertragung der Daten einzuholen[258] [259]. Wie das in der Praxis funktionieren soll, ist unklar[260]. Angesichts der Entscheidung des BVwG vom März 2023[261], wäre es außerdem gar nicht zulässig den Vorschlag der Art 29-Datenschutzgruppe umzusetzen. Damit die betroffene Person die Daten anderer Personen

[253] *Deusch/Eggendorfer*, Durchsetzung und Vollstreckung der Datenübertragbarkeit, KuR 2020, 105 (107).
[254] *Haidinger* in *Knyrim,* DatKomm Art 20 DSGVO, RZ 3 (Stand 1.12.2022, rdb.at).
[255] Vgl: „Handy nicht persönlich genug für DSGVO-Schutz?!“; https://noyb.eu/de/handy-nicht-persoenlich-genug-fuer-dsgvo-schutz (abgerufen am 05.04.2023).
[256] BVwG 03.03.2023, W274 2248601-1. Zum Zeitpunkt 11.05.2023 nicht rechtskräftig.
[257] *Haidinger*, Die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (134).
[258] *Artikel-29-Datenschutzgruppe,* Leitlinien zum Recht auf Datenübertragbarkeit (WP 242 rev.01) 12-13.
[259] *Dix* in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 20, RN 7.
[260] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 20 DSGVO, RZ 20 (Stand 1.12.2020, rdb.at).
[261] BVwG 03.03.2023, W274 2248601-1. Zum Zeitpunkt 11.05.2023 nicht rechtskräftig.

aussondern kann, müsste sie in einem ersten Schritt nämlich Auskunft über alle Daten erhalten, einschließlich der Daten Dritter.

PAYD-Versicherer sollten evaluieren, welches Risiko mit einer Übertragung von Telematikdaten einhergeht. Solange die offenen Fragen im Zusammenhang mit der Beauskunftung von Telematikdaten nicht höchstgerichtlich geklärt sind, ist es mE für jeden Versicherer ratsam, die Beauskunftung und damit auch die Übertragung von Telematikdaten zu verweigern (zumindest bis zum In-Kraft-Treten des Data Acts, siehe Punkt 6.8.1). Für Versicherungsnehmer*innen von PAYD-Tarifen bedeutet das jedoch, dass die Ausübung des Rechts auf Datenübertragbarkeit betreffend Telematikdaten mit aller Wahrscheinlichkeit ins Leere laufen wird.

6.8.1 Exkurs: Auswirkungen des EU Data Act auf das Recht auf Datenübertragbarkeit

Am 23.02.2023 veröffentlichte die EU-Kommission einen Entwurf für den neuen Data Act, der den Austausch von Daten und damit deren wirtschaftliches Potential fördern soll. Mit dem Data Act soll außerdem die Marktmacht der großen "Player" durchbrochen und der Wettbewerb angekurbelt werden[262]. Der Data Act ist derzeit[263] noch nicht in Geltung, der Gesetzgebungsprozess ist im Gange und in einem nächsten Schritt stehen die Trilog-Verhandlungen an[264]. Doch schon jetzt zeichnet sich ab, dass der Data Act einige juristische Herausforderungen mit sich bringen wird.

Im Zentrum des Data Act stehen Daten, die durch die Nutzung technischer Geräte wie zum Beispiel PKW, Windräder oder Rasenmähroboter entstehen. Diese maschinengenerierten Daten haben einen großen wirtschaftlichen Wert, der derzeit nicht voll ausgeschöpft wird. Mit dem Data Act soll einerseits die wirtschaftliche Nutzung dieser Daten gefördert und andererseits den Nutzer*innen dieser technischen Geräte ein

[262] *Heinzke*, Data Act: Auf dem Weg zur europäischen Datenwirtschaft, BB 2023, 201, 203.
[263] Stand 2. Mai 2023.
[264] *Müller*, Data, data everywhere: Richtungsweisende Neuigkeiten zum Data Act; https://www.haufe.de/recht/weitere-rechtsgebiete/wirtschaftsrecht/eu-data-act_210_590968.html (abgerufen am 21.04.2023).

umfassender Zugang zu jenen Daten eingeräumt werden[265] [266], „*zu deren Erzeugung sie beigetragen haben*“[267].

Vom Anwendungsbereich des Data Acts sind personenbezogene und nicht-personenbezogene Daten umfasst. Die Bestimmungen der DSGVO werden vom Data Act nicht berührt oder abgeändert. Durch den Data Act soll es insbesondere zu keiner Einschränkung des Schutzniveaus der DSGVO kommen[268].

Das Recht auf Bereitstellung von Daten nach dem Data Act unterscheidet sich in folgenden Punkten vom Recht auf Datenportabilität nach der DSGVO:

- Der Act Data umfasst personenbezogene und nicht-personenbezogene Daten.
- Nutzer*innen im Sinne des Data Act können sowohl natürliche wie auch juristische Personen sein.
- Nach dem Data Act sind den Nutzer*innen jene Daten zur Verfügung zu stellen, zu deren Erzeugung sie beigetragen haben. Zur Begründung des Anspruchs reicht es aus, dass die Daten bei der Nutzung eines vernetzen Geräts oder der Inanspruchnahme einer Leistung erzeugt wurden. Anders als nach Art 20 DSGVO müssen die Daten nicht von den Nutzer*innen bereitgestellt worden sein.
- Der Data Act sieht vor, dass die Daten den Nutzer*innen oder einem Dritten in Echtzeit und kontinuierlich zur Verfügung zu stellen sind[269].

Sofern ein technisches Gerät (zB ein PKW) personenbezogene Daten erzeugt, kann ein Anspruch auf Datenbereitstellung sowohl auf den Data Act, als auch auf die DSGVO gestützt werden. Dennoch muss der Dateninhaber (der Verantwortliche) die generierten Daten als personenbezogen oder nicht-personenbezogen klassifizieren. Dieser Klassifizierung kommt sogar große Bedeutung zu, denn wenn der Nutzer/die Nutzerin eines Gerätes und die betroffene Person nicht ident sind, bringt die parallele Anwendbarkeit von Data Act und DSGVO den Dateninhaber in eine Zwickmühle[270] [271]. In dieser Situation „*steht der Dateninhaber vor einem Dilemma: Er verstößt gegen den Data*

[265] *Ensthaler/Üge*, Wem gehören die durch die Nutzung von Maschinen generierten Daten?, BB 2022, 2051.
[266] *Specht-Riemenschneider,* Der Entwurf des Data Act, MMR 2022, 809.
[267] *Hoeren*, Der neue EU Data Act – Auswirkungen auf Telematikdaten, TranspR 3, 2023, 117.
[268] *Specht-Riemenschneider,* Der Entwurf des Data Act, MMR 2022, 810.
[269] Vgl: *Hoeren*, Der neue EU Data Act – Auswirkungen auf Telematikdaten, TranspR 3, 2023, 117.
[270] Vgl: *Hoeren*, Der neue EU Data Act – Auswirkungen auf Telematikdaten, TranspR 3, 2023, 117.
[271] Vgl: *Richter*, Vereinbarkeit des Entwurfs zum Data Act und der DS-GVO, MMR 2023, 166.

Act, wenn er den Datenzugang mit Verweis auf das Datenschutzrecht zu eng fasst; gewährt er zu umfassend Zugang zu personenbezogenen Daten, verstößt er gegen die DSGVO."[272]

Es ist aber fraglich, ob ein PAYD-Versicherer überhaupt als Dateninhaber im Sinne des Data Act einzustufen ist. Wird zur Erhebung der Fahrzeug- und Telematikdaten eine eigene OBU verwendet, so ist der PAYD-Versicherer mE zweifellos als Dateninhaber einzustufen. Die Daten können aber auch durch die Technik des vernetzten Fahrzeuges generiert und dem Versicherer vom Fahrzeughersteller zur Verfügung gestellt werden. Der Begriff des Dateninhabers wird in Art 2 Abs 6 Data Act legaldefiniert und demnach gilt jene Person als Dateninhaber, welche durch den Data Act zur Bereitstellung der Daten verpflichtet ist. Diese Definition ist nicht nur sehr weit, sondern auch zirkulär[273] und damit wenig hilfreich. Aus den Erwägungsgründen ergibt sich, dass Dateninhaber jene natürliche oder juristische Person ist, die die faktisch-technische Kontrolle über das Produkt und die Daten hat. Werden personenbezogene Daten generiert, dann kommt es auch darauf an, wer nach der DSGVO zu deren Verarbeitung berechtigt ist[274].

In aller Regel hat der Hersteller des Produktes die Kontrolle über die generierten Daten. Bei einem Fahrzeug ist das primär der Fahrzeughersteller und nicht der PAYD-Versicherer, der ja gar kein physisches Produkt im Sinne des Data Acts herstellt. Er bietet mE auch keine mit dem Produkt verbundene Dienstleistung gemäß Art 2 Abs 3 Data Act an. Darunter versteht man nämlich einen Dienst, der so sehr mit dem Produkt verbunden ist, dass das Produkt ohne ihn nicht funktionsgemäß verwendet werden kann[275]. Ein Fahrzeug kann jedoch auch ohne Kfz-Versicherung problemlos verwendet werden[276]. Eine PAYD-Versicherung ist somit kein verbundener Dienst im Sinne des Data Act.

Allerdings ist der PAYD-Versicherer derjenige, der die erzeugten personenbezogenen Fahrzeugdaten nach der DSGVO rechtmäßig verwendet (er ist Verantwortlicher). Außerdem hat er sehr wohl eine gewisse Kontrolle über die Daten, insbesondere dann,

[272] *Heinzke*, Data Act: Auf dem Weg zur europäischen Datenwirtschaft, BB 2023, 201 (205).
[273] *Heinzke*, Data Act: Auf dem Weg zur europäischen Datenwirtschaft, BB 2023, 201 (205).
[274] *Hartmann/McGuire/Schulte-Nölke*, Datenzugang bei smarten Produkten nach dem Entwurf für ein Datengesetz (Data Act) (RDi 2023, 49) 54, 55.
[275] *Specht-Riemenschneider,* Data Act – Auf dem (Holz-)Weg zu mehr Dateninnovation? (ZRP 2022, 137) 138.
[276] Der Abschluss einer Kfz-Haftpflichtversicherung ist aus rechtlicher Sicht zwar erforderlich, spielt für die technisch-praktische Verwendbarkeit eines Fahrzeuges jedoch keine Rolle.

wenn er sie in seiner eigenen technisch-faktischen Herrschaftssphäre speichert[277]. Demnach ist der PAYD-Versicherer mE auch dann als Dateninhaber im Sinne des Data Act zu qualifizieren, wenn die Daten von der Fahrzeugtechnik des vernetzten Automobils erzeugt werden.

Für den PAYD-Versicherer sind das keine guten Nachrichten. Die Rechtsunsicherheit, die das BVwG-Urteil vom März 2023[278] geschaffen hat, wird durch den Data Act wesentlich verschärft. Der in Punkt 6.8 gemachte Vorschlag, der PAYD-Versicherer solle sicherheitshalber weder Auskunft über Telematikdaten erteilen noch einen Datentransfer ermöglichen, wäre nach dem Data Act fatal für den Versicherer.

Um sowohl dem Data Act als auch der DSGVO zu entsprechen, muss der PAYD-Versicherer sicherstellen, dass ausschließlich die betroffene Person einen Zugang zu den sie betreffenden personenbezogenen Daten erhält. Wird das vernetzte Produkt, dh das Fahrzeug, auch von anderen Personen als dem Versicherungsnehmer/der Versicherungsnehmerin gefahren, müsste der PAYD-Versicherer entweder die Zustimmung der betroffenen Person einholen oder deren Daten aussondern. Das ist praktisch unmöglich und scheitert einfach schon daran, dass dem PAYD-Versicherer die Identität der betroffenen dritten Person nicht bekannt ist.

6.9 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Art 22 DSGVO)

Datenverarbeitungen findet meist „im Verborgenen" statt[279] und sind für Laien kaum begreifbar. Komplexe Algorithmen, künstliche Intelligenz und Automatisation werden in vielen verschiedenen Unternehmensbereichen eingesetzt. Auch in der Banken- und Versicherungsbranche[280] verspricht man sich von diesen Technologien eine Steigerung von Effizienz und Ertrag. Wird eine Entscheidung vollautomatisiert, ohne menschliches Zutun getroffen, löst das aber mitunter Unbehagen[281] und die Befürchtung aus, zu einem

[277] *Specht-Riemenschneider*, Der Entwurf des Data Act (MMR 2022, 809) 813.
[278] BVwG 03.03.2023, W274 2248601-1. Zum Zeitpunkt 11.05.2023 nicht rechtskräftig.
[279] *Hötzendorfer*, Privacy by Design and by Default, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (137).
[280] *Determann*, Entscheidungsfindung auf Knopfdruck: Richtlinien für automatisierte Entscheidungen und Profiling (Teil I), Dako 2018/22 (31).
[281] *Schulte-Nölke*, Algorithmen und Verbraucherrecht in *Leupold* (Hrsg), Forum Verbraucherrecht 2019 (118).

„*Objekt eines Entscheidungsmechanismus*“[282] gemacht zu werden[283]. Die Art 29-Datenschutzgruppe teilt diese Bedenken und geht davon aus, dass Technologien zur automatischen Entscheidungsfindung beträchtliche Auswirkungen auf die Rechte und Freiheiten von betroffenen Personen entfalten können[284]. Zum Schutz davor sieht Art 22 DSGVO vor, dass die betroffene Person das Recht hat, nicht einer ausschließlich automatisierten Entscheidung unterworfen zu sein, wenn diese ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Unter automatisierten Entscheidungen versteht man Entscheidungen, die ausschließlich auf Basis einer automatisierten Verarbeitung getroffen werden. Der Begriff der Entscheidung ist weit auszulegen. Rein interne Berechnungen oder Bewertungen ohne Außenwirkung, fallen nicht darunter. Nach allgemeinem Sprachverständnis versteht man unter einer Entscheidung einen Akt, der eine gewisse Abschlusswirkung hat und bei dem eine Auswahl aus mindestens zwei Alternativen getroffen wird[285]. Eine Entscheidung beruht dann ausschließlich auf einer automatisierten Verarbeitung, wenn am Entscheidungsprozess keine natürliche Person beteiligt ist. Wenn natürliche Personen in den Entscheidungsprozess involviert werden, aber keinen wirklichen Einfluss auf die Entscheidung nehmen können, liegt ebenfalls eine automatisierte Entscheidung im Sinne des Art 22 DSGVO vor[286].

Bei PAYD-Tarifen wird in regelmäßigen Abständen, meist monatlich, die Höhe der Prämie entsprechend dem individuellem Fahrverhalten der Versicherungsnehmer*innen berechnet. Das wird in aller Regel automatisiert, algorithmenbasiert und ohne menschliche Beteiligung geschehen. Der Begriff der Entscheidung ist weit zu verstehen[287] und auch wenn der Versicherer bei der Festlegung der Prämienhöhe keine Ja/Nein-Entscheidung trifft, so trifft er letztlich eine Entscheidung über die Höhe der Prämie und setzt mit der Prämienvorschreibung einen Akt mit gewisser Abschluss– und Außenwirkung.

[282] *Haidinger* in *Knyrim,* DatKomm Art 22 DSGVO, RZ 1 (Stand 1.12.2022, rdb.at).
[283] Vgl auch: *Taeger/Gabel/Taeger*, 4. Aufl 2022, DS-GVO Art 22 RN 9.
[284] *Determann*, Entscheidungsfindung auf Knopfdruck: Richtlinien für automatisierte Entscheidungen und Profiling (Teil I), Dako 2018/22 (31).
[285] *Arning* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap 6, RZ 621 (Stand 1.4.2021, rdb.at).
[286] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 22 DSGVO, RZ 6, 7 (Stand 1.12.2020, rdb.at).
[287] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 22 DSGVO, RZ 6 (Stand 1.12.2020, rdb.at).

Eine weitere Voraussetzung für die Anwendbarkeit des Art 22 DSGVO ist, dass die automatisierte Entscheidung entweder rechtliche Folgen für die betroffene Person hat oder sie in einer ähnlichen Weise erheblich beeinträchtigt. Eine Entscheidung hat dann eine rechtliche Wirkung, wenn sie die Rechte einer Person betrifft, beispielsweise wenn ein Vertrag aufgelöst wird, Sozialleistungen genehmigt werden oder eine Einreisegenehmigung versagt wird[288] [289]. Eine erhebliche Beeinträchtigung ist dann gegeben, wenn die Entscheidung "*einen wesentlichen Einfluss auf die Lebensverhältnisse, das Verhalten oder die Entscheidungen der betroffenen Person"*[290] hat. Die Art 29-Datenschtutzgruppe räumt ein, dass es schwierig ist, zu definieren, wann eine Beeinträchtigung erheblich ist und wann nicht. Als Beispiele für eine erhebliche Beeinträchtigung nennt sie ua:

a) *Entscheidungen, die sich auf die finanzielle Lage einer Person auswirken, beispielsweise ihre Kreditwürdigkeit;*
b) *Entscheidungen, die den Zugang zu Gesundheitsdienstleistungen betreffen; Entscheidungen, die den Zugang zu Arbeitsplätzen verwehren oder Personen ernsthaft benachteiligen;*
c) *Entscheidungen, die sich auf den Zugang zu Bildung auswirken, beispielsweise Hochschulzulassungen*[291].

Aus diesen Beispielen ergibt sich, dass eine erhebliche Beeinträchtigung insbesondere dann gegeben ist, wenn sie die Verweigerung eines Vertragsabschluss, den Ausschluss oder die Diskriminierung der betroffenen Person zur Folge hat[292]. In der Literatur wird vertreten, dass eine erhebliche Beeinträchtigung nur dann vorliegt, wenn die Entscheidung nachteilige Konsequenzen für die betroffene Person hat[293] [294]. Zum Teil wird sogar vertreten, dass eine erhebliche Beeinträchtigung erst dann vorliegt, „*wenn die betroffene Person durch die Entscheidung in ihrer wirtschaftlichen oder persönlichen Entfaltung nachhaltig gestört wird*"[295].

[288] *Artikel-29-Datenschutzgruppe,* Automatisierte Entscheidungen im Einzelfall (WP251 rev.01) 23.
[289] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 22 DSGVO, RZ 11 (Stand 1.12.2020, rdb.at).
[290] *Haidinger* in *Knyrim,* DatKomm Art 22 DSGVO, RZ 26/2 (Stand 1.12.2022, rdb.at).
[291] *Artikel-29-Datenschutzgruppe,* Automatisierte Entscheidungen im Einzelfall (WP251 rev.01) 23, 24.
[292] *Haidinger* in *Knyrim,* DatKomm Art 22 DSGVO, RZ 26/2 (Stand 1.12.2022, rdb.at).
[293] *Scholz* in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 22, RN 35.
[294] *Feiler/Fina*, Datenschutzrechtliche Schranken für Big Data, MR 2013, 303 (306).
[295] *Arning* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle^2 Kap 6, RZ 631 (Stand 1.4.2021, rdb.at).

Es ist fraglich, ob die automatisierte Prämienfestsetzung bei einem PAYD-Tarif die betroffene Person erheblich beeinträchtigt oder nicht. Wie schon mehrfach ausgeführt, können PAYD-Tarife unterschiedlich ausgestaltet sein. Bei einem Tarifmodell, bei dem sich die Prämie durch risikoarmes Fahrverhalten lediglich reduzieren kann[296], sehe ich keine erhebliche Beeinträchtigung der betroffenen Person. Aus meiner Sicht ist Art 22 DSGVO auf diese Fälle nicht anwendbar.

Ich bin der Ansicht, dass aber selbst von PAYD-Tarifen mit gänzlich variabler Prämie keine erhebliche Beeinträchtigung ausgeht. Die individuelle Festsetzung der Prämie ist das wesentliches Element eines PAYD-Tarifes und stellt daher keine Beeinträchtigung dar, sondern ist vertragsimmanent. Sieht man sich die in der Literatur genannten Beispiele an, so liegt eine erhebliche Beeinträchtigung zum Beispiel dann vor, wenn ein Kredit verweigert, eine Stellenbewerbung abgelehnt oder der Universitätszugang verwehrt wird[297] [298]. In all diesen Fällen wirkt sich die Entscheidung mE gravierend auf die Lebensverhältnisse der betroffenen Person aus und kann sogar existentielle Auswirkungen auf die Finanzlage oder den weiteren Lebensweg einer betroffenen Person haben. Das Festlegen der Höhe einer Kfz-Versicherungsprämie im Rahmen eines PAYD-Tarifes ist mit den oben genannten Beispielen nicht vergleichbar. Diese Meinung steht auch mit der Ansicht der Art 29-Datenschutzgruppe im Einklang, wonach personenbezogene Preisdifferenzierungen nur dann erheblich beeinträchtigend sind, wenn bestimmte Personen dadurch von bestimmten Waren oder Dienstleistungen ausgeschlossen werden[299]. Eine nutzen- und risikobasierte Prämiengestaltung führt aber nicht zum Ausschluss bestimmter Personen von Kfz-Versicherungsprodukten. Das ist im Bereich der Haftpflichtversicherung durch § 25 KHVG sogar gesetzlich ausgeschlossen. Nach dieser Bestimmung hat eine Person, deren Antrag auf Abschluss einer Kfz-Haftpflichtversicherung von drei verschiedenen Versicherungen abgelehnt wurde, das Recht auf Zuweisung an einen Versicherer[300]. Den Versicherungsnehmer*innen steht es außerdem immer frei, sich für einen herkömmlichen Versicherungstarif zu entscheiden.

[296]Zu den unterschiedlichen Tarifmodellen siehe Punkt 2.4.
[297]*Feiler/Fina*, Datenschutzrechtliche Schranken für Big Data, MR 2013, 303 (306).
[298]Zur Ablehnung einer Stellenbewerbung vertritt *Taeger* eine andere (mE zu restriktive) Ansicht und sieht darin keine erhebliche Beeinträchtigung. Siehe dazu: *Taeger/Gabel/Taeger,* 4. Aufl 2022, DS-GVO Art 22 RN 47.
[299]*Artikel-29-Datenschutzgruppe,* Automatisierte Entscheidungen im Einzelfall (WP251 rev.01) 24.
[300]Vgl: https://www.vvo.at/vvo/vvo.nsf/sysPages/Kfz-Haftpflicht.html (abgerufen am 05.04.2023).

Mangels erheblicher Beeinträchtigung ist der Art 22 DSGVO mE daher nicht auf PAYD-Tarife anwendbar und zwar auch dann nicht, wenn die Prämie gänzlich variabel ist. Die Art 29-Datenschutzgruppe dürfte aber eine andere Ansicht vertreten. In ihren Leitlinien wird erklärt, auf welche Weise der betroffenen Person eine aussagekräftige Auskunft über die potenziellen Auswirkungen einer automatisierten Entscheidungsfindung erteilt werden könnte. In diesem Beispiel geht die Art 29-Datenschutzgruppe ganz selbstverständlich davon aus, dass die Festsetzung von Kfz-Versicherungsprämien im Rahmen eines PAYD-Tarifes eine automatisierte Einzelfallentscheidung im Sinne des Art 22 DSGVO ist[301]. Für die Zwecke dieser Master Thesis folge ich der Ansicht der Art 29-Datenschutzgruppe, allerdings mit Skepsis und auch nur hinsichtlich jener PAYD-Tarife mit gänzlich variabler Prämie.

Dieser Ansicht folgend, ist die automatisierte Festlegung der Prämienhöhe nur dann zulässig, wenn sich der Versicherer auf einen Ausnahmetatbestand des Art 22 Abs 2 DSVGO stützen kann:

lit a: Die Entscheidung ist für den Abschluss oder die Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen erforderlich.

lit b: Die Entscheidung ist aufgrund von Rechtsvorschriften zulässig.

lit c: Die Entscheidung ist mit ausdrücklicher Einwilligung der betroffenen Person erfolgt[302].

Zu lit a: Eine automatisierte Einzelfallentscheidung ist dann zulässig, wenn sie für den Abschluss oder die Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist. Das Kriterium der Erforderlichkeit ist eng auszulegen. Bei der Beurteilung ist zu fragen, ob auch eine andere, weniger eingreifende Form der Verarbeitung angewandt werden könnte[303]. Nach Ansicht der Art 29-Datenschutzgruppe ist die Erforderlichkeit von automatisierten Einzelfallentscheidungen dann zu bejahen, wenn eine nicht-automatisierte Entscheidungsfindung aufgrund der zu verarbeiteten Datenmenge nicht praxistauglich oder faktisch unmöglich wäre[304]. Konkret geht es um Massengeschäfte oder besonders zeitkritische Geschäfte, wie die Prüfung der

[301] *Artikel-29-Datenschutzgruppe,* Automatisierte Entscheidungen im Einzelfall (WP251 rev.01) 28, 29.
[302] *Arning* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap 6, RZ 637, 638 (Stand 1.4.2021, rdb.at).
[303] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 22 DSGVO, RZ 21 (Stand 1.12.2020, rdb.at).
[304] *Artikel-29-Datenschutzgruppe,* Automatisierte Entscheidungen im Einzelfall (WP251 rev.01) 25.

Kontodeckung bei einer Abhebung am Bankomaten[305], der Abschluss von Mobilfunkverträgen[306] oder die Bearbeitung von tausenden von Stellenbewerbungen[307]. Auch Versicherungsverträge sind ein typisches Massengeschäft und deren manuelle Abwicklung wäre in der Praxis nicht möglich. Es wäre wirtschaftlich völlig unvertretbar und praktisch nicht machbar, jede einzelne Kfz-Versicherungsprämie einmal monatlich durch eine Fachkraft berechnen zu lassen. Der Einsatz von automatisierten Entscheidungsprozessen ist daher erforderlich und der Ausnahmetatbestand des Art 22 Abs 2 lit a DSGVO ist erfüllt.

Zu lit b: Eine automatisierte Einzelfallentscheidung ist auch dann zulässig, wenn sie auf Grundlage einer entsprechenden gesetzlichen Bestimmung durchgeführt wird. Aus ErwGr 71 ergibt sich, dass hier va gesetzliche Bestimmungen zur Bekämpfung von Betrug und Steuerhinterziehung gemeint sind[308].

Zu lit c: Eine automatisierte Einzelfallentscheidung kann außerdem auf Basis einer Einwilligungserklärung der betroffenen Person erfolgen. Die Einwilligung muss ausdrücklich erklärt werden und sich explizit auf die automatisierte Einzellfallentscheidung beziehen[309] [310].

Setzt der Versicherer automatisierte Entscheidungen ein, hat er angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person zu treffen. Er hat sicherzustellen, dass die betroffene Person zumindest die folgenden Rechte ausüben kann:

- Erwirkung des Eingreifens einer natürlichen Person seitens des Verantwortlichen,
- Darlegung des eigenen Standpunkts und
- Anfechtung der Entscheidung[311] [312].

[305]Es ist strittig, ob derart einfache „Wenn-Dann-Entscheidungen" überhaupt in den Anwendungsbereich des Art 22 Abs 1 DSGVO fallen, wird aber überwiegend bejaht. Siehe dazu: *Paal/Pauly/Martini*, 3. Aufl 2021, DS-GVO Art 22 RN 15b.
[306]*Haidinger* in *Knyrim,* DatKomm Art 22 DSGVO, RZ 32 (Stand 1.12.2022, rdb.at).
[307]*Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 22 DSGVO, RZ 22 (Stand 1.12.2020, rdb.at).
[308]Vgl: ErwGr 71 DSGVO.
[309]*Arning* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap 6, RZ 646 (Stand 1.4.2021, rdb.at).
[310]*Taeger/Gabel/Taeger*, 4. Aufl 2022, DS-GVO Art 22 RN 63.
[311]*Ehmann/Selmayr/Hladjk*, 2. Aufl 2018, DS-GVO Art 22 RN 15.
[312]*Arning* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap 6, RZ 648 (Stand 1.4.2021, rdb.at).

Das bedeutet im Wesentlichen, dass die betroffene Person das Recht hat, eine Überprüfung der automatisiert getroffenen Entscheidung durch eine natürliche Person zu verlangen. Diese muss sich mit den Standpunkten der betroffenen Person auseinander setzen und muss die Befugnis haben eine Änderung der Entscheidung herbeizuführen[313] [314].

Profiling fällt dann in den Anwendungsbereich des Art 22 DSGVO, „*wenn im Rahmen von Profiling-Maßnahmen rein automatisierte Einzelfallentscheidungen ohne Beteiligung eines Menschen ergehen*[315]“. Anders gesagt: Profiling stellt einen besonders relevanten Anwendungsfall der automatisierten Entscheidungsfindung dar. Eine automatisierte Einzelfallentscheidung kann, muss aber nicht, auf Grundlage von Profiling ergehen[316]. Der Begriff „Profiling“ wird in Art 4 Z 4 DSGVO definiert und umfasst grob gesagt jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, persönliche Aspekte einer natürlichen Person zu analysieren oder vorherzusagen[317]. Bei der PAYD-Versicherung wird die Höhe der Prämie von persönlichen Aspekten abhängig gemacht. Der Versicherer analysiert das individuelle Fahrverhalten und stuft bestimmte Verhaltensmuster als riskant ein (zB schnelles Fahren). Es werden Aspekte wie Bremsverhalten, Fahrgeschwindigkeit oder Anzahl der gefahrenen Kilometer bewertet und der automatisierten Entscheidung über die Prämienhöhe zugrunde gelegt. Die Entscheidung über die Prämienhöhe bei einem PAYD-Tarif wird daher auf Basis eines vom Versicherer durchgeführten Profilings getroffen.

Ob die automatisierte Einzelfallentscheidung auf Grundlage von Profiling oder konventionell erhobenen Daten erfolgt, spielt für die rechtliche Beurteilung jedoch keine Rolle. Entscheidend für die Anwendbarkeit des Art 22 DSGVO ist vielmehr, ob die Festlegung der Prämienhöhe rechtliche Wirkungen gegenüber der betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (siehe dazu weiter oben).

---

[313] *Taeger/Gabel/Taeger,* 4. Aufl 2022, DS-GVO Art 22 RN 69.
[314] *Artikel-29-Datenschutzgruppe,* Automatisierte Entscheidungen im Einzelfall (WP251 rev.01) 30.
[315] *Arning* in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap 6, RZ 626 (Stand 1.4.2021, rdb.at).
[316] *Haidinger* in *Knyrim,* DatKomm Art 22 DSGVO, RZ 22 (Stand 1.12.2022, rdb.at).
[317] *Determann*, Entscheidungsfindung auf Knopfdruck: Richtlinien für automatisierte Entscheidungen und Profiling (Teil I), Dako 2018/22 (31).

6.9.1 Informationspflichten bei automatisierten Einzelfallentscheidungen

Kommen automatisierte Einzelfallentscheidungen zum Einsatz, hat der Verantwortliche zusätzliche Informations- und Auskunftspflichten zu beachten. Nach Art 13 Abs 2 lit f DSGVO, Art 14 Abs 2 lit g DSGVO und Art 15 Abs 1 lit h DSGVO ist die betroffene Person über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling zu informieren. Der betroffenen Person sind außerdem aussagekräftige Informationen über die involvierte Logik, die Tragweite und angestrebten Auswirkungen der automatisierten Entscheidungsfindung zur Verfügung zu stellen. Die DSGVO verpflichtet den Verantwortlichen aber nicht zur Offenlegung und Erläuterung von Algorithmen und Formeln. Wenn Gefahr besteht, dass durch Informationen zur involvierten Logik Geschäftsgeheimnisse offengelegt werden, kann die Auskunft eingeschränkt bzw allgemein gehalten werden[318]. Die Offenlegung der Berechnungsformel wäre in vielen Fällen ohnehin kontraproduktiv, weil diese für Laien idR nicht verständlich wäre. Der Verantwortlich muss daher einfache Wege finden um die involvierte Logik so zu beschreiben, dass die betroffene Person sie verstehen kann[319]. Die Art 29-Datenschutzgruppe empfiehlt mit „*echten, greifbaren Beispielen*“ zu arbeiten sowie Grafiken und Visualisierungen zu verwenden[320].

Die Art 29-Datenschutzgruppe gibt in ihren Leitlinien zu automatisierten Entscheidungen im Einzelfall ein Beispiel dafür, wie ein PAYD-Versicherer eine Auskunft nach Art 15 Abs 1 lit h DSGVO gestalten könnte: „*Ein Versicherungsunternehmen verwendet automatisierte Entscheidungen für die Festsetzung von Versicherungsprämien für Kraftfahrzeuge, die auf der Überwachung des Fahrverhaltens der Kunden basieren. Zur Veranschaulichung der Tragweite und der angestrebten Auswirkungen der Verarbeitung erläutert es, dass gefährliches Fahrverhalten zu höheren Versicherungsgebühren führen kann, und stellt seinen Kunden eine App zur Verfügung, bei der fiktive Fahrer miteinander verglichen werden, z. B. ein Fahrer mit gefährlichem Verhalten wie schnellem Beschleunigen und Bremsen in letzter Sekunde. Anhand von Grafiken werden Tipps gegeben, wie dieses Verhalten verbessert und folglich die Versicherungsprämie reduziert werden kann.*“[321]

[318] *Illibauer* in *Knyrim,* DatKomm Art 13 DSGVO, RZ 55 (Stand 1.12.2021, rdb.at).
[319] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 13 DSGVO, RZ 36 (Stand 1.12.2020, rdb.at).
[320] *Artikel-29-Datenschutzgruppe,* Automatisierte Entscheidungen im Einzelfall (WP251 rev.01) 27-29.
[321] *Artikel-29-Datenschutzgruppe,* Automatisierte Entscheidungen im Einzelfall (WP251 rev.01) 29.

7) Zusammenfassung

Im Zusammenhang mit PAYD-Versicherungsverträgen stellen sich zahlreiche datenschutzrechtliche Fragestellungen.

Versicherer, die PAYD-Verträge anbieten möchten, sollten sich im Klaren darüber sein, dass sie sich zwangsläufig in den einen oder anderen datenschutzrechtlichen Graubereich begeben werden. Das betrifft vor allem auf das Recht auf Auskunft, Berichtigung und Datenübertragbarkeit. Derzeit ist nicht klar, wie einerseits den Betroffenenrechten entsprochen und und andererseits die Verletzung von Rechten Dritter verhindert werden kann.

Versicherungsnehmer*innen sollte bewusst sein, dass ihr vernetztes Fahrzeug und ihr Smartphone riesige Mengen an Telematikdaten erzeugen, die vom Versicherer potentiell zu Zwecken genutzt werden, die weit über die Berechnung der Prämie hinausgehen. Sie sollten sich vor Abschluss eines PAYD-Versicherungsvertrages daher genügend Zeit nehmen, sich mit dem Informationsmaterial zum Datenschutz im Detail auseinander zu setzen und sich gut überlegen, zu welchen Verarbeitungszwecken sie eine Einwilligung abgeben möchten und zu welchen nicht. Andernfalls werden die Versicherungsnehmer*innen überrascht sein, wenn der Versicherer ihre Telematikdaten im Falle eines Unfalls gegen sie einsetzt. Die meisten Versicherungsnehmer*innen werden außerdem davon überrascht sein, dass die Ausübung einiger Betroffenenrechte durch strenge Nachweispflichten faktisch stark eingeschränkt ist.

Abschließend kann festgehalten werden, dass auch die verpflichtende Einführung des eCalls im Jahr 2018 zu keinem “Boom“ der Telematiktarife geführt hat und für die nächste Zeit ein solcher auch nicht zu erwarten ist. Das führe ich vor allem auf die bestehenden Rechtsunsicherheiten zurück, die sich zukünftig durch den Data Act noch verstärken werden.

8) Abstract

There are numerous legal questions in relation to PAYD insurance contracts, in particular concerning data protection. Insurance companies wanting to offer PAYD contracts, should be aware that they may find themselves in legally diffused areas. This is particular true concerning the right of access, rectification and data portability regarding telematics data. At present it is not clear, how an insurance company can meet the rights of the data subject without affecting the rights and freedoms of others.

Insurance holders should be aware of the fact, that their connected cars and smartphones produce enormous amounts of telematics data which might be used by an insurance company for various matters exceeding the matter of premium calculation. That is why insurance holders should take their time when concluding a PAYD insurance contract and should study the data protection information provided to them thoroughly. Insurance holders should consider carefully – and for each specific purpose - if they want to consent to the processing of their telematics data. Otherwise they might be surprised if the insurance company holds their telematics data against them in the event of damage. Most insurance holders will also be surprised that their right of access, rectification and data portability depends on them providing evidence for beeing the sole user of their car.

However, there was no increase in PAYD insurance contracts after the introduction of the eCall in 2018 and no increase is expected for the near future. In my opinion this is due to legal uncertainties, that will grow even further with the new Data Act.

9) Literatur

9.1 Kommentare und Fachzeitschriften

Albrecht in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Einführung zu Artikel 6, RN 4.

Arb. 9349, 10.486; SZ 53/101; ZAS 1987/12 uva.

Arning in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle^{2} Kap 6, RZ 76, 78, 352 - 355a, 462, 621, 626, 631, 637, 638 , 646 , 648 (Stand 1.4.2021, rdb.at).

Arning;Rohwedder in *Moos/Schefzig/Arning,* Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle^{2} Kap 5, RZ 69, 154, 159, 270, 291, 292 (Stand 1.4.2021, rdb.at).

Bäcker in BeckOK DatenschutzR, 43. Ed 1.11.2021, DS-GVO Art 2 RN 2.

Barth/Dokalik/Potyka, ABGB (MTK)^{27} § 1054 ABGB (Stand 1.7.2022, rdb.at).

Bergauer, Personenbezogene Daten, Begriff und Kategorien, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 52-53, 56, 60.

Blocher, Dein Handy, aber nicht deine Daten?, ZIIR 2022, 7-8.

Bönninger/Schüppel, Vertrauen erhalten – Datenschutz und Datensicherheit bei modernen Fahrzeugen, ZVR 2015, 474.

Brand, Zulässigkeit und Ausgestaltung von Telematiktarifen, VersR 2019, 725.

Brandl/Pfaffeneder, Datenschutzrechtliche Aspekte der Pay-As-You-Drive Versicherung, Aufsatzteil, Jahrbuch Datenschutzrecht 2014, 192-199.

Braun/Hasenauer, Die Rechtmäßigkeit der Verarbeitung gemäß Art 6 DSGVO (FN 1), Jahrbuch Datenschutzrecht 2018, 9 (18, 23).

Determann, Entscheidungsfindung auf Knopfdruck: Richtlinien für automatisierte Entscheidungen und Profiling (Teil I), Dako 2018/22 (31).

Deusch/*Eggendorfer*, Durchsetzung und Vollstreckung der Datenübertragbarkeit, KuR 2020, 105 (107).

Dix in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht Art 20, RN 7, 8.

Dix in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 15 RN 13.

Ehmann/Selmayr/Heberlein, 2. Aufl 2018, DS-GVO Art 5 RN 5, 13, 24, 31.

Ehmann/Selmayr/Heckmann/Paschke, 2. Aufl 2018, DS-GVO Art 7 RN 92.

Ehmann/Selmayr/Hladjk, 2. Aufl 2018, DS-GVO Art 22 RN 15.

Ehmann/Selmayr/Kamann/Braun, 2. Aufl 2018, DS-GVO Art 17 RN 64.

Ehmann/Selmayr/Schiff, 2. Aufl 2018, DS-GVO Art 9 RN 13, 27.

Ehmann/Selmayr/Zerdick, 2. Aufl 2018, DS-GVO Art 1 RN 3.

Ensthaler/Üge, Wem gehören die durch die Nutzung von Maschinen generierten Daten?, BB 2022, 2051.

Feiler/Fina, Datenschutzrechtliche Schranken für Big Data, MR 2013, 303 (306).

Fellner, Betroffenenrechte nach der DSGVO, VbR 2018/47 (88).

Fritz, Das Auskunftsrecht nach Art 15 DSGVO in der Entscheidungspraxis und Rechtsprechung, Jahrbuch Datenschutzrecht 2021, 65 (84).

Fritz, Jahrbuch Datenschutzrecht 2020, 156-158, 161, 162, 164, 167.

Gerpott/Berg, Pay-As-You-Drive Angebote von Erstversicherern für Privatkunden, Eine betriebswirtschaftliche Analyse, online publiziert am 7. Mai 2011 im Springer Verlag.

Gola/Heckmann/Franck, 3. Aufl 2022, DS-GVO Art 12 RN 26.

Gola/Heckmann/Pötters, 3. Aufl 2022, DS-GVO Art 5 RN 15, 35.

Gola/Heckmann/Schulz, 3. Aufl 2022, DS-GVO Art 6 RN 21, 24, 39, 59, 136, 139.

Gola/Heckmann/Schulz, 3. Aufl 2022, DS-GVO Art 9 RN 13.

Goricnik/Grünanger in *Grünanger/Goricnik*, Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] Kap 7, RZ 7.66, 7.70 (Stand 1.11.2018, rdb.at).

Grubmann, KHVG[5] § 40a KFG 1967, E 3 (Stand 1.2.2021, rdb.at).

Grubmann, VersVG[9] § 1, E 7 (Stand 1.7.2022, rdb.at).

Grubmann, VersVG[9] § 12, E 19, E 43, E 135, E 142, E 207 (Stand 1.7.2022, rdb.at).

Haidinger in Knyrim, Datenschutzrecht[4] Kap 5, RZ 5.17 (Stand 1.4.2020, rdb.at).

Haidinger in *Knyrim,* DatKomm Art 17 DSGVO, RZ 22 (Stand 1.12.2021, rdb.at).

Haidinger in *Knyrim,* DatKomm Art 18 DSGVO, RZ 1 (Stand 1.12.2021, rdb.at).

Haidinger in *Knyrim,* DatKomm Art 20 DSGVO, RZ 3, 20 (Stand 1.12.2022, rdb.at).

Haidinger in *Knyrim,* DatKomm Art 22 DSGVO, RZ 1, 22, 26/2, 32 (Stand 1.12.2022, rdb.at).

Haidinger, Die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (134).

Haidinger/*Löffler*, BVwG 15.12.2021, W176 2247780-1, Dako 3/2022, 65.

Hansen, Das Netz im Auto & das Auto im Netz, DuD 6/2015, 368, 369.

Hartmann/McGuire/Schulte-Nölke, Datenzugang bei smarten Produkten nach dem Entwurf für ein Datengesetz (Data Act) (RDi 2023, 49) 54, 55.

Heinzke, Data Act: Auf dem Weg zur europäischen Datenwirtschaft, BB 2023, 201 (203, 205).

Hoch, EvBl-LS 2016/168, ÖJZ 22/2016, 1035-136; OGH 15.6.2016, 7 Ob 86/16x.

Hödl in Knyrim, DatKomm Art 4 DSGVO, RZ 11 (Stand 1.12.2018, rdb.at).

Hoeren, Der neue EU Data Act – Auswirkungen auf Telematikdaten, TranspR 3, 2023, 117.

Hötzendorfer, Privacy by Design and by Default, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (137).

Hötzendorfer/Tschohl/Kastelitz in *Knyrim,* DatKomm Art 5 DSGVO, RZ 1, 3, 36, 44, 46, 57-59 (Stand 7.5.2020, rdb.at).

Hübelbauer, DSGVO: Das Recht auf Datenübertragbarkeit (Teil XIII), Dako 2017/64 (106, 107).

Illibauer in *Knyrim,* DatKomm Art 12 DSGVO, RZ 37 (Stand 1.12.2021,rdb.at).

Illibauer in *Knyrim,* DatKomm Art 13 DSGVO, RZ 20, 21, 35, 55 (Stand 1.12.2021, rdb.at).

Illibauer, Informationsrecht und Modalitäten für die Ausübung der Betroffenenrechte, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 116, 117.

Jahnel, Kommentar zur Datenschutz-Grundverordnung (Stand 1.12.2020, rdb.at).
JusGuide 2021/38/19745 (OGH).

Karg in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 4 Nr 1 RN 57.

Karsten/Wienroeder, Der Entwurf des Data Act - Auswirkungen auf die Automobilindustrie, RAW 2/2022, 99, 100.

Kastelitz in *Knyrim,* DatKomm Art 7 DSGVO, RZ 21, 22, 24, 32 (Stand 7.5.2020, rdb.at).

Kastelitz, Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 102, 104.

Kastelitz/Hötzendorfer/Tschohl in *Knyrim,* DatKomm Art 6 DSGVO, RZ 2, 39 (Stand 7.5.2020, rdb.at).

Kastelitz/Hötzendorfer/Tschohl in *Knyrim,* DatKomm Art 9 DSGVO, RZ 3, 19 (Stand 7.5.2020, rdb.at).

Klement in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 7 RN 10, 56, 57.

Krauß/Waidner, IT-Sicherheit und Datenschutz im vernetzten Fahrzeug, DuD 6/2015, 383.

Kühling/Buchner/Buchner/Petri, 3. Aufl 2020, DS-GVO Art 6 RN 40a, 153.

Kunnert, „Autonomes Fahren“ aus datenschutzrechtlicher Sicht, Autonomes Fahren und Recht in *Eisenberger, Lachmayer, Eisenberger* (Hrsg), 188-189, 191.

Lachmayer in *Knyrim*, DatKomm § 37 DSG, RZ 8 (Stand 7.5.2020, rdb.at).

Meyerdierks in Moos/Schefzig/Arning, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle^{2} Kap 3, RZ 13 (Stand 1.4.2021, rdb.at).

Moos in *Moos/Schefzig/Arning*, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle^{2} Kap 4, RZ 21 (Stand 1.4.2021, rdb.at).

Paal/Pauly/Frenzel, 3. Aufl 2021, DS-GVO Art 5 RN 1.

Paal/Pauly/Martini, 3. Aufl 2021, DS-GVO Art 22 RN 15b.

Paal/Pauly/Paal, 3. Aufl 2021, DS-GVO Art 15 RN 14, 15, 41.

Perner/Spitzer/Kodek, Bürgerliches Recht^{2}, 198.

Pletzer in *Kletečka/Schauer*, ABGB-ON$^{1.03}$ § 869, RZ 25 (Stand 1.8.2019, rdb.at).

Pollirer, Checkliste Erfüllung der Informationspflichten gem Art 13 und 14 DSGVO, Dako 2018/48 (87).

Pollirer, Checkliste für die Einwilligungserklärungen der Art 7 und 8 DSGVO, Dako 2017/56 (91).

Pollirer, Checkliste Löschkonzept, Dako 2017/23 (42).

Pscheidl, Was erwartet die Versicherungswirtschaft? EU-Legislaturperiode 2014-2019, VR 2015, H1-2, 44.

Quaas in BeckOK DatenschutzR, 43. Ed 1.2.2023, DS-GVO Art 12 RN 40.

Richter, Vereinbarkeit des Entwurfs zum Data Act und der DS-GVO, MMR 2023, 166.

Ritzer in *Ruhmannseder/Lehner/Beukelmann*, Compliance aktuell 15010, RZ 20 (Stand 1.5.2022, rdb.at).

Roßnagel in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 5 RN 50, 116, 154.

Roßnagel in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 6 Abs 4 RN 46.

Roßnagel, Fahrzeugdaten – wer darf über sie entscheiden?, SVR 8/2014, 281.

Schilchegger, Zur Erfüllung datenschutzrechtlicher Informationspflichten, ÖBA 2018, 319 (319).

Schmidt-Wudy in BeckOK DatenschutzR, 43. Ed 1.2.2023, DS-GVO Art 13 RN 42.

Scholz in *Simitis/Hornung/Spiecker gen. Döhmann*, 1. Aufl 2019, Datenschutzrecht, Art 22, RN 35.

Schröder, Datenschutzrecht für die Praxis[4], 14, 15, 17-18, 48-50, 166.

Schulte-Nölke, Algorithmen und Verbraucherrecht in *Leupold* (Hrsg), Forum Verbraucherrecht 2019 (118).

Schwichtenberg, „Pay as you drive" – neue und altbekannte Probleme, DuD 6/2015, 378.

Specht-Riemenschneider, Data Act – Auf dem (Holz-)Weg zu mehr Dateninnovation? (ZRP 2022, 137) 138.

Specht-Riemenschneider, Der Entwurf des Data Act (MMR 2022, 809) 809, 810, 813.

Stemmer in BeckOK DatenschutzR, 43. Ed 1.5.2022, DS-GVO Art 7 RN 64, 69.

Stingl, Smart Cars und der Datenschutz“ Datenschleuder oder sinnvolle Datenverwendung?, Jahrbuch Datenschutzrecht 2016, 166, 170-171, *Jahnel* (Hrsg).

Sydow/Marsch, DS-GVO/BDSG/*Ingold*, 3. Aufl 2022, DS GVO Art 13 RN 8.

Taeger/Gabel/Arning/Rothkegel, 4. Aufl 2022, DS-GVO Art 4 RN 14.

Taeger/Gabel/Taeger, 4. Aufl 2022, DS-GVO Art 22 RN 9, 47, 63, 69.

Verschraegen in *Kletečka/Schauer*, ABGB-ON$^{1.08}$ § 1054, RZ 25 (Stand 1.5.2020, rdb.at).

Warter, Rechtliche Vorgaben für ein Löschkonzept, Dako 2018/26 (29, 42).

Weichert, Datenschutz im Auto - Teil 1, Das Kfz als großes Smartphone auf Rädern, SVR 6/2014, 204.

Wybitul, EU-Datenschutz-Grundverordnung im Unternehmen Kap III, RZ 77 (Stand 11.8.2016, rdb.at).

Wybitul, EU-Datenschutz-Grundverordnung im Unternehmen Kap VI, RZ 362 (Stand 11.8.2016, rdb.at).

Zoppel, Digitale Anreizmodelle in der privaten Krankenversicherung und ihre Grenzen, ALJ 2022, 1-4.

9.2 Leitlinien uä

Artikel-29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit (WP 242 rev.01) 12-13.

Artikel-29-Datenschutzgruppe, Automatisierte Entscheidungen im Einzelfall (WP251 rev.01) 29.

Kurzpapier Nr 17 der dt Datenschutzkonferenz, Besondere Kategorien personenbezogener Daten, Stand: 27.03.2018, Seite 1, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_17.pdf (abgerufen am 07.02.2023).

Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, V2.0.

9.3 Online Quellen

(chronologisch geordnet nach Datum des Abrufs)

Müller, Data, data everywhere: Richtungsweisende Neuigkeiten zum Data Act; https://www.haufe.de/recht/weitere-rechtsgebiete/wirtschaftsrecht/eu-data-act_210_590968.html (abgerufen am 21.04.2023).

https://verbraucherrecht.at/rechtmaessige-einwilligung-datenverarbeitung/5289 (abgerufen am 07.04.2023).

https://www.vvo.at/vvo/vvo.nsf/sysPages/Kfz-Haftpflicht.html (abgerufen am 05.04.2023).

„Handy nicht persönlich genug für DSGVO-Schutz?!“; https://noyb.eu/de/handy-nicht-persoenlich-genug-fuer-dsgvo-schutz (abgerufen am 05.04.2023).

https://www.ionos.at/digitalguide/server/knowhow/was-ist-mac-spoofing/ (abgerufen am 12.01.2023).

Versicherungsverband Österreich (VVO), Jahresbericht 2021, Datenteil; https://www.vvo.at/vvo/vvo.nsf/sysPages/x52885E94068B6B49C125883600331E8D/$file/VVO_Jahresbericht_2021_Datenteil_August.pdf (abgerufen am 17.10.2022).

Presseaussendung der Allianz Gruppe in Österreich vom 17.12.2009; https://www.ots.at/presseaussendung/OTS_20091217_OTS0020/kfz-haftpflichtversicherung-feiert-ihren-80-geburtstag (abgerufen am 17.10.2022).

10) Judikatur

BVwG 16.10.2019, W256 2222862-1

BVwG 30.10.2019, W258 2216873-1

BVwG 13.11.2020, W274 2234946-1

BVwG 15.12.2021, W176 2247780-1

BVwG 12.05.2022, W252 2237237-1

BVwG 03.03.2023, W274 2248601-1

DSB 27.08.2018, DSB-D123.085/0003-DSB/2018

DSB 27.08.2018, DSB-D123.085/0003-DSB/2018

DSB 05.12.2018, DSB-D123.270/0009-DSB/2018

DSB 14.01.2019, DSB-D123.224/0004-DSB/2018

DSB 05.02.2019, DSB-D123.495/0007-DSB/2018

DSB 23.07.2019, DSB-D123.822/0005-DSB/2019

DSB 26.07.2019, DSB-D123.921/0005-DSB/2019

DSB 22.08.2019, DSB-D130.206/0006-DSB/2019

EuGH 19. 12. 2013, Rs C-209/12, *Endress*

EuGH 19.10.2016, C-582/14

EuGH 19. 12. 2019, verb Rs C-355/18 bis C-357/18 und C-479/18, *Rust-Hackner*

OGH 17.01.1990, 9 ObA365/89

OGH 19.03.2003, 7 Ob 31/03i

OGH 15.04.2010, 6 Ob 41/10p

OGH 31.08.2018, 6 Ob 140/18h

VfGH 12. 12. 2017, GZ E3249/2016 (VfSlg 20.227/2017)

OLG Stuttgart Urt. v. 31.3.2021 – 9 U 43/21, ZD 2021, 375

11) Abkürzungen

ABGB:	(österreichisches) Allgemein Bürgerliches Gesetzbuch
ABl:	Amtsblatt
AGB:	Allgemeine Geschäftsbedingungen
ALJ:	Zeitschrift “Austrian Law Journal“
Anm:	Anmerkung
Arb:	Sammlung arbeitsrechtlicher Entscheidungen
Art:	Artikel
Aufl:	Auflage
AVB:	Allgemeine Versicherungsbedingungen
BB:	Zeitschrift “Betriebs-Berater“
BDSG:	(bundesdeutsches) Bundesdatenschutzgesetz
BeckOK:	Beck'scher Online-Kommentar
BVwG:	(österreichisches) Bundesverwaltungsgericht
bzw:	beziehungsweise
CSV:	comma-separated values (ein Dateiformat)
Dako:	Zeitschrift “Datenschutz konkret“
DatenschutzR:	Datenschutzrecht
DatKomm:	Kommentar zum Datenschutzrecht
dh:	das heißt
DS-GVO:	Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2)
DS-RL:	Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
DSB:	(österreichische) Datenschutzbehörde
DSG:	(österreichisches) Datenschutzgesetz (Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten)
DSGVO:	Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2)
dt:	deutsch
DuD:	Zeitschrift “Datenschutz und Datensicherheit“

E:	Entscheidung
eCall:	Emergency call (Notruf)
Ed:	Edition
EDSA:	Europäischer Datenschutzausschuss
EMRK:	Europäische Menschenrechtskonvention
ErwGr:	Erwägungsgrund
etc:	et cetera (und so weiter)
EU:	Europäische Union
EuGH:	Gerichtshof der Europäischen Union (Europäischer Gerichtshof)
EvBl-LS:	Evidenzblatt der Rechtsmittelentscheidungen
ff:	fortfolgend
FN:	Fußnote
gem:	gemäß
gen:	genannt
GlBG:	(österreichisches) Gleichbehandlungsgesetz
GPS:	Global Positioning System (Globales Positionsbestimmungssystem)
GRC:	Charta der Grundrechte der Europäischen Union (ABl C 2012/326, 391)
GZ:	Geschäftszahl
hL:	herrschende Lehre
Hrsg:	Herausgeber
idR:	in der Regel
IP:	Internet Protocol
IT:	Informationstechnologie
iVm:	in Verbindung mit
Kap:	Kapitel
Kat:	Kategorie
KFG:	(österreichisches) Kraftfahrzeuggesetz
Kfz:	Kraftfahrzeug
KHVG:	(österreichisches) Kraftfahrzeug-Haftpflichtversicherungsgesetz
KSchG:	(österreichisches) Konsumentenschutzgesetz
KuR:	Zeitschrift “Kommunikation und Recht“
leg cit:	die zitierte Gesetzesstelle
lit:	littera (Buchstabe)
MAC:	Media Access Control (Medienzugriffssteuerung)

max:	maximal
mE:	meines Erachtens
mMn:	meiner Meinung nach
MMR:	Zeitschrift „Multimedia und Recht“
MR:	Zeitschrift „Medien und Recht“
MTK:	Manz Taschenkommentar
mwN:	mit weiteren Nachweisen
Nr:	Nummer
OBU:	On-Board-Unit
OGH:	(österreichischer) Oberster Gerichtshof
OLG:	Oberlandesgericht
ÖJZ:	Österreichische Jurist:innen-Zeitung
ON:	online
PAYD:	pay as you drive (“zahle wie du fährst“)
PIN:	Personal Identification Number (Persönliche Identifikationsnummer)
PKW:	Personenkraftwagen
PS:	Pferdestärke
RAW:	Zeitschrift “Recht Automobil Wirtschaft“
rdb:	Rechtsdatenbank
RDi:	Zeitschrift “Recht Digital“
RFID:	Radio-Frequency Identification (Identifizierung mit Hilfe elektromagnetischer Wellen)
RN:	Randnote
RS:	Rechtssatz
RZ:	Randziffer
SIM:	Subscriber Identity Module (Teilnehmer-Identifikationsmodul)
SVR:	Zeitschrift “Straßenverkehrsrecht“
SZ:	Entscheidungen des OGH in Zivilsachen
TKG:	(österreichisches) Telekommunikationsgesetz
TranspR:	Zeitschrift “Transportrecht“
ua:	unter anderem
uU:	unter Umständen
uva:	und viele andere
uvm:	und viele mehr

VAG:	(österreichisches) Versicherungsaufsichtsgesetz
VbR:	Zeitschrift für Verbraucherrecht
verb:	verbunden
VersR:	Zeitschrift für Versicherungsrecht, Haftungs- und Schadensrecht
VersVG:	(österreichisches) Versicherungsvertragsgesetz
VfGH:	(österreichischer) Verfassungsgerichtshof
VfSlg:	Sammlung der Erkenntnisse des Verfassungsgerichtshofes
VIN:	Vehicle Identification Number (Fahrzeug- Identifizierungsnummer)
VR:	Zeitschrift “Die Versicherungsrundschau“
VVO:	Versicherungsverband Österreich
WLAN:	Wireless Local Area Network (drahtloses Lokal-Netzwerk)
XML:	Extensible Markup Language (ein Dateiformat)
ZAS:	Zeitschrift für Arbeits- und Sozialrecht
zB:	zum Beispiel
ZIIR:	Zeitschrift für Informationsrecht
ZRP:	Zeitschrift für Rechtspolitik
ZVR:	Zeitschrift für Verkehrsrecht